The Universal Algebra of First Order Logic

Paul Ossientis

June 18, 2017

Contents

Chapter 1

Universal Algebra

1.1 Existence of Free Universal Algebra

1.1.1 Preliminaries

In the following, $\mathbf{N} = \{0, 1, 2, \ldots\}$ denotes the set of non-negative integers, while $\mathbf{N}^* = \{1, 2, \ldots\}$ is the set of positive integers. The integer 0 is also the empty set $\emptyset$, and for all $n \in \mathbf{N}^*$:

$$n = \{0, 1, \ldots, n-1\}$$

Recall that a *map* or *function* is a (possibly empty) set of ordered pairs f such that $y = y'$ whenever $(x, y) \in f$ and $(x, y') \in f$. The *domain* of f is the set:

$$\mathrm{dom}(f) = \{x : \exists y, (x, y) \in f\}$$

while the *range* of f is the set:

$$\mathrm{rng}(f) = \{y : \exists x, (x, y) \in f\}$$

The notation $f : A \to B$ indicates that f is a map with domain A and whose range is a subset of B. In particular, f is a subset of the cartesian product:

$$A \times B = \{(x, y) : x \in A, y \in B\}$$

The set of all maps $f : A \to B$ is denoted B^A. Note that $B^\emptyset = \{\emptyset\}$ as the empty set $\emptyset$ is the only map $f : \emptyset \to B$. The formula $B^\emptyset = \{\emptyset\}$ can equally be written $B^0 = 1$ which makes it easy to remember, and holds even if $B = 0$. If $A \neq \emptyset$ then $\emptyset^A = \emptyset$ as there is no map $f : A \to \emptyset$. The formula $\emptyset^A = \emptyset$ can equally be written $0^A = 0$ which is also easy to remember, but does not hold if $A = 0$. There is nothing deep or interesting about the empty map $\emptyset : \emptyset \to B$, $B^\emptyset$ or $\emptyset^A$. But they are often confusing and we should confront them at an early stage.

Regarding the cartesian product $A \times B$, it is very common to refer to it as A^2 whenever $A = B$. This may seem confusing at first since A^2 is the set of maps

$f : \{0, 1\} \to A$, which is not the same thing as the set of ordered pairs (x, y) with $x, y \in A$. However, it is natural to represent a map $f : \{0, 1\} \to A$ by the ordered pair $(f(0), f(1))$. If $x = f(0)$ and $y = f(1)$, then we are effectively representing $f = \{(0, x), (1, y)\}$ by the ordered pair (x, y). It makes communication easier. In summary, when we refer to (x, y) as the element of $A \times A$, things are exactly as they are. But if we are referring to (x, y) as an element of A^2, what we really mean is the map $f = \{(0, x), (1, y)\}$, i.e the maps $f : \{0, 1\} \to A$ such that $f(0) = x$ and $f(1) = y$. Note that the sets A and A^1 are also different.

1.1.2 Type of Universal Algebra

Definition 1 *A* Type of Universal Algebra *is a map* α *with* $\mathrm{rng}(\alpha) \subseteq \mathbf{N}$.

Since the empty set is a map with empty range, it is also is a type of universal algebra. When α is an element of $\mathbf{N}^n$, it is a map $\alpha : n \to \mathbf{N}$ which can be represented as the n-uple $(\alpha(0), \ldots, \alpha(n-1))$. If α is a type of universal algebra, its cardinal number represents the number of operators defined on any universal algebra of type α (which can be finite, infinite, countable or uncountable) while for all $i \in \mathrm{dom}(\alpha)$, $\alpha(i) \in \mathbf{N}$ represents the *arity* of the i-th operator so to speak, i.e. the number of arguments it has. If X is a universal algebra of type α, then an *operator* of arity $\alpha(i)$ is a map $f : X^{\alpha(i)} \to X$. Hence an operator of arity 1 is a map $f : X^1 \to X$ while an operator of arity 2 is a map $f : X^2 \to X$. What may be more unusual is an operator or arity 0, namely a map $f : X^0 \to X$. Since $X^0 = \{0\}$, an operator of arity 0 is therefore a map $f : \{0\} \to X$, which is a set $f = \{(0, f(0))\}$ containing the single ordered pair $(0, f(0))$. Fundamentally, there is not much difference between specifying an operator of arity 0 on X, and the constant element $f(0)$ of X. It is however convenient to allow the arity of an operator to be 0, so we do not have to treat constants and operators separately.

Universal algebras may have constants, like an identity element in a group. If G is a group with identity element e and product $\otimes$, it is possible to regard G as a universal algebra with 3 operators. The identity operator $f : \{0\} \to G$ is defined by $f(0) = e$, the product operator $f : G^2 \to G$ by $f(x) = x(0) \otimes x(1)$ and the inverse operator $f : G^1 \to G$ by $f(x) = x(0)^{-1}$. The type of this universal algebra could be $\alpha : 3 \to \mathbf{N}$ defined by $\alpha(0) = 0$, $\alpha(1) = 2$ and $\alpha(2) = 1$, that is $\alpha = \{(0, 0), (1, 2), (2, 1)\}$. Of course a group G has more properties than a universal algebra of type α because the operators need to satisfy certain conditions. Hence a group is arguably a universal algebra of type α, but the converse is not true in general.

There is something slightly unsatisfactory about definition (1), namely the fact that the arity of the operators are ordered. After all, a group is also a universal algebra of type $\alpha' = \{(0, 0), (1, 1), (2, 2)\}$ or even $\alpha'' = \{(*, 0), (+, 1), (@, 2)\}$ provided $*$, $+$ and $@$ denote distinct sets.

Let α be a type of universal algebra and $f \in \alpha$. Then f is an ordered pair $(i, \alpha(i))$ for some $i \in \mathrm{dom}(\alpha)$. From now on, we shall write $\alpha(f)$ rather than $\alpha(i)$. This notational convention is very convenient as we no longer need to

refer to $\text{dom}(\alpha)$, or $i \in \text{dom}(\alpha)$. If X is a universal algebra of type α, we simply require the existence of an operator $T(f) : X^{\alpha(f)} \to X$ for all $f \in \alpha$.

1.1.3 Definition of Universal Algebra

Definition 2 *Let α be a type of universal algebra. A* Universal Algebra *of type α is an ordered pair (X, T) where X is a set and T is a map with domain α, such that for $f \in \alpha$ we have $T(f) : X^{\alpha(f)} \to X$.*

In fact there is no need to keep writing $T(f)$ or (X, T) when everything is clear from the context. If X is a universal algebra of type α, then for all $f \in \alpha$ we have the operator $f : X^{\alpha(f)} \to X$, also denoted 'f'. Of course, if X and Y are two universal algebras of type α, then $f : X^{\alpha(f)} \to X$ and $f : Y^{\alpha(f)} \to Y$ are different sets in general. One is $T(f)$ where (X, T) is the first universal algebra referred to as 'X', while the other is $S(f)$ where (Y, S) is the second universal algebra referred to as 'Y'.

If α is the empty set, then T is a map with empty domain, i.e. the empty set itself. So $(X, \emptyset)$ is a universal algebra of empty type for any set X, which is not very different from the set X itself. A universal algebra of empty type is therefore a set with no structure. If α is not an empty type of universal algebra, then T has a non-empty domain and therefore cannot be empty. So there is at least one operator $T(f) : X^{\alpha(f)} \to X$. If X is the empty set then we must have $\alpha(f) \geq 1$, as there is no map $T(f) : \{0\} \to \emptyset$. In other words, there cannot be any constant in an empty universal algebra, as we should expect. Furthermore, any $T(f) : X^{\alpha(f)} \to X$ is in fact the empty map $\emptyset : \emptyset \to \emptyset$. In summary, if α is a type of universal algebra with constants (i.e. $\alpha(f) = 0$ for some $f \in \alpha$), then no universal algebra of type α can be empty, while if α has no constant (i.e. $\alpha(f) \geq 1$ for all $f \in \alpha$), then the only empty universal algebra of type α is $(\emptyset, T)$ where $T(f) = \emptyset$ for all $f \in \alpha$. So much for confronting the fear of the empty set.

1.1.4 Homomorphism of Universal Algebra

Recall that if f and g are both maps then $g \circ f$ is the set of ordered pairs:

$$g \circ f = \{(x, z) : \exists y, (x, y) \in f \text{ and } (y, z) \in g\}$$

It is easy to check that $g \circ f$ is also a map, namely that $z = z'$ whenever both (x, z) and (x, z') are elements of $g \circ f$.

Let $g : A \to B$ be a map. Then for all $x \in A$, it is a well established convention to denote $g(x)$ the unique element of B such that $(x, g(x)) \in g$. Now if $n \in \mathbf{N}$, we can define a map $g^n : A^n \to B^n$ by setting:

$$g^n(x_0, \ldots, x_{n-1}) = (g(x_0), \ldots, g(x_{n-1}))$$

or more rigorously:

$$\forall x \in A^n \ , \ \forall i \in n \ , \ g^n(x)(i) = g(x(i))$$

Note that if $n = 0$, then $g^0 : A^0 \to B^0$ is the map $g^0 : \{0\} \to \{0\}$. There is only one such map, defined by $g^0(0) = 0$ or $g^0 = \{(0,0)\}$. If $n = 1$, then $g^1 : A^1 \to B^1$ is the map defined by $g^1(\{(0,x)\}) = \{(0,g(x))\}$ for all $x \in A$. Anyone being confused by this last statement should remember that $\{(0,x)\}$ is simply the map $f : \{0\} \to A$ defined by $f(0) = x$ which is an element of A^1 not fundamentally different from the constant $x \in A$. Likewise $\{(0,g(x))\}$ is simply the map $f : \{0\} \to B$ defined by $f(0) = g(x)$ which is an element of B^1 not fundamentally different from $g(x) \in B$. From now, whenever it is clear from the context that $x \in A^n$ rather than $x \in A$, we shall write $g(x)$ rather than $g^n(x)$.

Definition 3 *Let X and Y be universal algebras of type α. We say that a map $g : X \to Y$ is a* morphism *or* homomorphism*, if and only if:*

$$\forall f \in \alpha \ , \ \forall x \in X^{\alpha(f)} \ , \ g \circ f(x) = f \circ g(x)$$

With stricter notations, given two universal algebras (X,T) and (Y,S) of type α, a map $g : X \to Y$ is a morphism, if and only if:

$$\forall f \in \alpha \ , \ \forall x \in X^{\alpha(f)} \ , \ g \circ T(f)(x) = S(f) \circ g^{\alpha(f)}(x)$$

Suppose $\alpha = \{(0,0),(1,2),(1,1)\}$ and let X, Y be universal algebras of type α. For example, let us assume that X and Y are groups. We have three operators[1] $T(0,0) : \{0\} \to X$, $T(1,2) : X^2 \to X$ and $T(1,1) : X^1 \to X$. To simplify notations, for all $x, y \in X$, let us define $e \in X$, $x \otimes y$ and x^{-1} as:[2]

$$e = T(0,0)(0) \ , \ x \otimes y = T(1,2)(x,y) \ , \ x^{-1} = T(2,1)(x)$$

Adopting similar conventions for the universal algebra Y, the first condition required for a map $g : X \to Y$ to be a morphism can be expressed as:

$$g(e) = g \circ T(0,0)(0) = T(0,0) \circ g^0(0) = T(0,0)(0) = e$$

While the second is, for all $x, y \in X$:

$$g(x \otimes y) = g \circ T(1,2)(x,y) = T(1,2) \circ g^2(x,y) = T(1,2) \circ (g(x), g(y)) = g(x) \otimes g(y)$$

Finally the last condition is, for all $x \in X$:

$$g(x^{-1}) = g \circ T(2,1)(x) = T(2,1) \circ g^1(x) = T(2,1) \circ g(x) = g(x)^{-1}$$

It follows that $g : X \to Y$ is a morphism, if and only if for all $x, y \in X$:

$$g(e) = e \ , \ g(x \otimes y) = g(x) \otimes g(y) \ , \ g(x^{-1}) = g(x)^{-1}$$

In particular, we see that a morphism (of universal algebra of type α) is no different from *group morphism* whenever X and Y are groups.

[1] T is a map with domain α. The notation $T(0,0)$ is a shortcut for $T((0,0))$.

[2] Here is an example when '(x,y)' does not really mean (x,y) in $x \otimes y = T(1,2)(x,y)$. Instead, (x,y) is a notational shortcut for the element $f \in X^2$ defined by $f = \{(0,x),(1,y)\}$. Equivalently, f is the map $f : 2 \to X$ defined by $f(0) = x$ and $f(1) = y$. Similarly 'x' does not really mean x in $T(2,1)(x)$, but is rather a notational shortcut for the element $f \in X^1$ defined by $f = \{(0,x)\}$. Equivalently, f is the map $f : 1 \to X$ defined by $f(0) = x$.

Proposition 1 *Let X, Y and Z be universal algebras of type α. If $g : X \to Y$ and $g' : Y \to Z$ are morphisms, then $g' \circ g : X \to Z$ is also a morphism.*

Proof
For all $f \in \alpha$ and $x \in X^{\alpha(f)}$ we have $g' \circ g \circ f(x) = g' \circ f \circ g(x) = f \circ g' \circ g(x)$.
.

1.1.5 Isomorphism of Universal Algebra

Recall that a map f is said to be *injective* or *one-to-one* if and only if $x = x'$ whenever $(x, y) \in f$ and $(x', y) \in f$. When this is the case, the set:

$$f^{-1} = \{(y, x) : (x, y) \in f\}$$

is also a map. If $f : A \to B$ then saying that f is injective can be expressed as:

$$\forall x, x' \in A \ , \ f(x) = f(x') \ \Rightarrow \ x = x'$$

However the domain of f^{-1} is the range of f or $\mathrm{rng}(f)$, which may not be the whole set B. We say that $f : A \to B$ is *surjective* or *onto* if and only if $\mathrm{rng}(f) = B$, or equivalently:

$$\forall y \in B \ , \ \exists x \in A \ , \ y = f(x)$$

Note that a map $f : A \to B$ is simply a set of ordered pairs with no *knowledge* of the set B. In other words, being given the set f will not give you the set B, which can be any set with $\mathrm{rng}(f) \subseteq B$. Saying that f is surjective is therefore not meaningful on its own, unless the set B is clear from the context.

We say that $f : A \to B$ is *bijective*, or that it is a *bijection* or *one-to-one correspondence* if and only if it is both injective and surjective. When this is the case we have $f^{-1} : B \to A$, and it is also a bijective map.

Definition 4 *Let X and Y be universal algebras of type α. We say that a map $g : X \to Y$ is an* isomorphism *if and only if g is a bijective morphism. If there exists an isomorphism $g : X \to Y$, we say that X and Y are* isomorphic*.*

Proposition 2 *Let X and Y be universal algebras of type α. If $g : X \to Y$ is an isomorphism, then $g^{-1} : Y \to X$ is also an isomorphism.*

Proof
Suppose $g : X \to Y$ is a morphism which is bijective. Then $g^{-1} : Y \to X$ is also bijective and we only need to check that it is a morphism. Let $f \in \alpha$ and $y \in Y^{\alpha(f)}$. We need to check that $g^{-1} \circ f(y) = f \circ g^{-1}(y)$, and since g is an injective map, this is equivalent to:

$$g \circ g^{-1} \circ f(y) = g \circ f \circ g^{-1}(y) \tag{1.1}$$

The l.h.s of (1.1) is clearly $f(y)$ and since $g : X \to Y$ is a morphism, the r.h.s is $f \circ g \circ g^{-1}(y)$. So it remains to check that $g \circ g^{-1}(y) = y$ for all $y \in Y^{\alpha(f)}$. This follows immediately from:

$$g \circ g^{-1}(y)(i) = g(g^{-1}(y)(i)) = g(g^{-1}(y(i))) = y(i)$$

which is true for all $i \in \alpha(f)$. .

1.1.6 Free Generator of Universal Algebra

Recall that if f is a map and A is a set, the *restriction* of f to A is the set:

$$f_{|A} = \{(x, y) : x \in A \text{ and } (x, y) \in f\}$$

This is also a set of ordered pairs such that $y = y'$ whenever $(x, y) \in f_{|A}$ and $(x, y') \in f_{|A}$. Hence the restriction $f_{|A}$ is also a map. Furthermore if $f : A' \to B$ and $A \subseteq A'$, then $f_{|A} : A \to B$.

Definition 5 *Let X be a universal algebra of type α. We call* free generator *of X any subset $X_0 \subseteq X$ with the following property: for any universal algebra Y of type α, and for any map $g_0 : X_0 \to Y$, there exists a unique morphism $g : X \to Y$ such that $g_{|X_0} = g_0$.*

Consider the set $X = \mathbf{N}$ together with the successor operator $s : \mathbf{N} \to \mathbf{N}$ defined by $s(n) = n + 1$. Then X can be viewed as a universal algebra of type $\alpha = \{(0, 1)\}$ where $T(0, 1) : X^1 \to X$ is defined as $T(0, 1)(n) = n(0) + 1$. Furthermore the set $X_0 = \{0\}$ is a free generator of X. To check this, let Y be another universal algebra of type α and assume that $g_0 : X_0 \to Y$ is an arbitrary map. We have to prove that g_0 can be uniquely extended into a morphism $g : X \to Y$. This is another way of saying that there exists a morphism $g : X \to Y$ such that $g_{|X_0} = g_0$, and that such morphism is unique. Since $X_0 = \{0\}$, we have $g_0 : \{0\} \to Y$. We define $e = g_0(0) \in Y$. Consider the map $g : X \to Y$ defined by the recursion $g(0) = e$ and $g(n+1) = s \circ g(n)$, where $s : Y^1 \to Y$ is the successor operator on Y. To check that g is a morphism, we need to check the single condition for all $n \in X$:

$$g \circ s(n) = s \circ g(n)$$

which is true from the very definition of g. Hence we have proved the existence of a morphism $g : X \to Y$, and since $g(0) = e = g_0(0)$ we have $g_{|X_0} = g_0$. It remains to check that g is unique. Suppose that $g' : X \to Y$ is another morphism such that $g'_{|X_0} = g_0$, i.e. $g'(0) = e$. In particular $g'(0) = g(0)$. Furthermore, since g' is a morphism, if $g'(n) = g(n)$ for some $n \in X$, then:

$$g'(n + 1) = s \circ g'(n) = s \circ g(n) = g(n + 1)$$

This proves by induction that $g'(n) = g(n)$ for all $n \in X$, i.e. that $g' = g$.

We have proved that $\{0\}$ is a free generator of $\mathbf{N}$ viewed as a universal algebra with a single successor operator. Note that the empty set alone would be too small to be a free generator of $\mathbf{N}$. If $g_0 : \emptyset \to Y$ is a map then g_0 has to be the empty set, and it is not difficult to extend g_0 into a full morphism $g : X \to Y$ whenever Y is not empty. Indeed pick an arbitrary $e \in Y$ and define g by the same recursion as before, $g(0) = e$ and $g(n+1) = s \circ g(n)$. We obtain a morphism such that $g_{|X_0} = \emptyset = g_0$. However, such morphism will not be unique as there are in general many ways to choose the element $e \in Y$. This shows that the empty set is not a free generator of $\mathbf{N}$ viewed as a universal algebra with

a single successor operator. In fact, we could have made the argument simpler: consider $Y = \emptyset$ which is a universal algebra of type α by setting $T(f) = \emptyset$ for all $f \in \alpha$[3]. Consider the map $g_0 : \emptyset \to Y$ which is just the empty map. Then it is impossible to extend g_0 to a full morphism $g : X \to Y$, for the simple reason that there cannot exist any map $g : X \to \emptyset$ since X is not empty.

We now claim that $X_0 = \{0, 1\}$ is too large to be a free generator of $\mathbf{N}$. In the case of $X_0 = \emptyset$, we failed to obtain uniqueness when Y had more than one element, and we failed to obtain existence for $Y = \emptyset$. In the case of $X_0 = \{0, 1\}$, we will fail to obtain existence. Indeed consider $Y = \mathbf{N}$ and $g_0 : X_0 \to Y$ defined by $g_0(0) = 2$ and $g_0(1) = 4$. Then no morphism $g : X \to Y$ can extend g_0, as otherwise:

$$4 = g_0(1) = g(1) = g(0 + 1) = g(0) + 1 = g_0(0) + 1 = 3$$

So we have seen that $X_0 = \emptyset$ is too small, while $X_0 = \{0, 1\}$ is too large to be a free generator of $\mathbf{N}$. This last statement is in fact misleading as size is not everything. Consider $X_0 = \{1\}$ with $Y = \mathbf{N}$ and $g_0 : X_0 \to Y$ defined by $g_0(1) = 0$. Then no morphism $g : X \to Y$ can extend g_0 as otherwise:

$$0 = g_0(1) = g(1) = g(0 + 1) = g(0) + 1$$

contradicting the fact that $g(0) \in \mathbf{N}$. So $X_0 = \{1\}$ is not a free generator of $\mathbf{N}$ viewed as a universal algebra with successor operator.

Suppose we now regard $\mathbf{N}$ as a universal algebra of type $\alpha = \{(0, 1), (1, 0)\}$ by adding to the successor operator the operator $T(1, 0) : \{0\} \to \mathbf{N}$ defined by $T(1, 0)(0) = 0$. In effect, we are giving $\mathbf{N}$ additional structure by singling out the element 0. We now claim that the empty set $X_0 = \emptyset$ is a free generator of $\mathbf{N}$. So let Y be a universal algebra of type α and consider a map $g_0 : X_0 \to Y$. Since $X_0 = \emptyset$, g_0 is necessarily the empty map $g_0 = \emptyset$. We need to show that g_0 can be uniquely extended into a morphism $g : X \to Y$. Since Y is a universal algebra of type α, we have an operator $T(1, 0) : \{0\} \to Y$. Define $e = T(1, 0)(0) \in Y$ and consider $g : X \to Y$ defined by the recursion $g(0) = e$ and $g(n + 1) = s \circ g(n)$. Then g is a morphism as it satisfies the two conditions:

$$g \circ T(1, 0)(0) = g(0) = e = T(1, 0)(0) = T(1, 0) \circ g^0(0)$$

and:

$$g \circ T(0, 1)(n) = g \circ s(n) = g(n + 1) = s \circ g(n) = T(0, 1) \circ g^1(n)$$

Furthermore, $g_{|X_0} = \emptyset = g_0$, and since any other morphism $g' : X \to Y$ would need to satisfy $g'(0) = e$ and $g'(n + 1) = s \circ g'(n)$, a simple induction argument shows that g is in fact unique. So we have proved that $X_0 = \emptyset$ is a free generator of $\mathbf{N}$ viewed as a universal algebra of type α.

Before we end this section, let us confront our fear of the empty set once more. We have just seen that it is possible for $X_0 = \emptyset$ to be a free generator of a

[3]We have $T(f) : Y^{\alpha(f)} \to Y$ since $\alpha(f) \geq 1$ for all $f \in \alpha$. The empty set $Y = \emptyset$ is a universal algebra of type α only when α has no constant, i.e. no operator with arity 0.

universal algebra which is not empty. But such universal algebra had a constant 0. Suppose now that α is a type of universal algebra without constant, i.e. such that $\alpha(f) \geq 1$ for all $f \in \alpha$. Then the empty set $X = \emptyset$ is a universal algebra of type α, provided the map T of domain α is defined as $T(f) = \emptyset$ for all $f \in \alpha$. Then $T(f)$ is indeed a map $T(f) : X^{\alpha(f)} \to X$, and it is the only possible choice. We claim that X is the only universal algebra of type α which can have $X_0 = \emptyset$ as a free generator. So first we show that $X_0 = \emptyset$ is indeed a free generator of X. Suppose Y is a universal algebra of type α and let $g_0 : X_0 \to Y$ be a map. Then g_0 is necessarily the empty map. Define $g = g_0 = \emptyset$. Then $g : X \to Y$ and in fact g is a morphism since the conditions required $\forall f \in \alpha$, $\forall x \in X^{\alpha(f)} \ldots$ are vacuously satisfied, as $X^{\alpha(f)} = \emptyset$ whenever $X = \emptyset$ and $\alpha(f) \geq 1$. We clearly have $g_{|X_0} = \emptyset = g_0$. Furthermore, the morphism $g = \emptyset$ is unique, since it is the only possible map $g : X \to Y$. So we have proved that $X_0 = \emptyset$ is a free generator of $X = \emptyset$ viewed as a universal algebra of type α. We now show that $X = \emptyset$ is the only universal algebra of type α which can have $X_0 = \emptyset$ as a free generator. So suppose $X_0 = \emptyset$ is a free generator of some universal algebra X of type α. Let $Y = \emptyset$ be viewed as a universal algebra of type α with the obvious structure T. Consider the empty map $g_0 : X_0 \to Y$. Since X_0 is a free generator, g_0 can be extended into a morphism $g : X \to Y$. But since Y is empty, there exists no map $g : X \to Y$, unless X is also empty. So we have proved that $X = \emptyset$.

1.1.7 Free Universal Algebra

Definition 6 *A Universal Algebra is said to be* free *if it has a free generator.*

We have already seen a few examples of free universal algebras. The set $\mathbf{N}$ with the successor operator $s : \mathbf{N}^1 \to \mathbf{N}$, or the set $\mathbf{N}$ with both the successor operator and the constant 0. We have seen that $\emptyset$ is also a free universal algebra of type α, whenever α has no constant. Along the same lines, any set X is a free universal algebra of empty type. Indeed take $X_0 = X$ and suppose Y is any set while $g_0 : X_0 \to Y$ is a map. There exists a unique map $g : X \to Y$ such that $g_{|X_0} = g_0$, namely g_0 itself. Furthermore, the conditions required for $g : X \to Y$ to be a morphism are vacuously satisfied when $\alpha = \emptyset$. Hence we see that $X_0 = X$ is a free generator of X, as a universal algebra of empty type.

It would be wrong to think that most universal algebras are free. Before we proceed, let us find a simple example of universal algebra which is not free. The empty set $\emptyset$ is not a universal algebra of type α unless α has no constant. When this is the case the empty set is free. So let us try a slightly bigger set, namely $X = \{0\}$. If α is the empty type, then X is free, with itself as a free generator. Suppose $\alpha = \{(0, 0)\}$. Then the only possible structure on X is given by $T(0, 0) : \{0\} \to X$ defined by $T(0, 0)(0) = 0$. In other words, there is only one possible choice of constant within X. Unfortunately X is still free, with the empty set as a free generator. For if Y is another universal algebra of type $\alpha = \{(0, 0)\}$ and $g_0 : \emptyset \to Y$ is a map, there exists a unique morphism $g : X \to Y$ which extends g_0, namely the map g defined by $g(0) = 0$, where the r.h.s '0' refer to the constant of Y. So we need to choose a slightly more

complex structure on X. Consider $\alpha = \{(0,1)\}$. Since $X = \{0\}$, there is only one possible choice of operator $T(0,1) : X^1 \to X$, namely $T(0,1)(0) = 0$. With this particular structure, X becomes a universal algebra of the same type as $\mathbf{N}$ with a single successor operator $s : \mathbf{N}^1 \to \mathbf{N}$. We claim that X is not free. If it was free, there would exist $X_0 \subseteq X$ which is a free generator of X. The only possible values for X_0 are $X_0 = \emptyset$ and $X_0 = \{0\}$. Now $X_0 = \emptyset$ cannot be a free generator of X. As we have already seen, since α has no constant, the empty set is the only universal algebra of type α which can have an empty free generator. Suppose now that $X_0 = \{0\}$ is a free generator of X. We shall arrive at a contradiction. Consider the map $g_0 : X_0 \to \mathbf{N}$ defined by $g_0(0) = 0$. Since X_0 is a free generator of X, there exists a unique morphism $g : X \to \mathbf{N}$ such that $g_{|X_0} = g_0$. In fact, we must have $g = g_0$ since $X_0 = X$. But $g = g_0$ is not a morphism. Indeed, If g was a morphism, we would have:

$$0 = g(0) = g \circ T(0,1)(0) = s \circ g(0) = 0 + 1 = 1$$

So we have found a simple example of universal algebra which is not free, namely $X = \{0\}$ of type $\alpha = \{(0,1)\}$ with the only possible operator $T(0,1) : X^1 \to X$.

Of course, having one single example of universal algebra which fails to be free is little evidence so far. The following proposition shows that free universal algebras are in fact pretty rare. There is *essentially* at most *one* free universal algebra of type α, for a given cardinality of free generator.

Proposition 3 *Suppose X and Y are two free universal algebras of type α with free generators X_0 and Y_0 respectively. If there exists a bijection $j : X_0 \to Y_0$, then X and Y are isomorphic.*

Proof
Since $Y_0 \subseteq Y$ we also have $j : X_0 \to Y$. Since X_0 is a free generator of X, there exists a unique morphism $g : X \to Y$ such that $g_{|X_0} = j$. We claim that g is in fact an isomorphism. To show this, we only need to prove that $g : X \to Y$ is bijective. We shall do so by finding a map $g' : Y \to X$ such that $g' \circ g = id_X$ and $g \circ g' = id_Y$ where $id_X : X \to X$ and $id_Y : Y \to Y$ are the identity mappings. Since $j : X_0 \to Y_0$ is a bijection, we have $j^{-1} : Y_0 \to X_0$. In particular, $j^{-1} : Y_0 \to X$ and since Y_0 is a free generator of Y there exists a unique morphism $g' : Y \to X$ such that $g'_{|Y_0} = j^{-1}$. We will complete the proof by showing that $g' \circ g = id_X$ and $g \circ g' = id_Y$. Since both $g : X \to Y$ and $g' : Y \to X$ are morphisms, $g' \circ g : X \to X$ is also a morphism. Furthermore:

$$(g' \circ g)_{|X_0} = g' \circ (g_{|X_0}) = g' \circ j = g'_{|Y_0} \circ j = j^{-1} \circ j = id_{X_0}$$

It follows that $g' \circ g : X \to X$ is a morphism which extends $id_{X_0} : X_0 \to X$. Since X_0 is a free generator of X, such morphism is unique. As $id_X : X \to X$ is also a morphism such that $(id_X)_{|X_0} = id_{X_0}$ we conclude that $g' \circ g = id_X$. We prove similarly that $g \circ g' = id_Y$. **.**

1.1.8 Construction of Free Universal Algebra

In this section, we explicitly construct a free universal algebra of type α whose free generator is a *copy* of a given set X_0. In a later section, we shall prove the existence of a free universal algebra whose generator is the set X_0 itself. Recall that if A and B are sets, the *difference* $A \setminus B$ is defined as:

$$A \setminus B = \{x : x \in A \text{ and } x \notin B\}$$

This notion will be used while proving the following proposition:

Proposition 4 *Let α be a type of universal algebra and X_0 be a set. Define:*

$$Y_0 = \{(0, x) : x \in X_0\} \ , \ Y_{n+1} = Y_n \cup \bar{Y}_n \ , \ n \in \mathbf{N}$$

with:

$$\bar{Y}_n = \left\{(1, (f, x)) : \ f \in \alpha \ , \ x \in Y_n^{\alpha(f)}\right\}$$

Let:

$$Y = \bigcup_{n=0}^{+\infty} Y_n$$

and T be the map with domain α defined by setting $T(f) : Y^{\alpha(f)} \to Y$ as:

$$T(f)(x) = (1, (f, x))$$

Then (Y, T) is a free universal algebra of type α with free generator Y_0.

Proof
First we need to check that we indeed have $T(f) : Y^{\alpha(f)} \to Y$ for all $f \in \alpha$. It is clear that $T(f)$ is a well defined map with domain $Y^{\alpha(f)}$. However given $x \in Y^{\alpha(f)}$, we need to check that $T(f)(x) \in Y$. In order to do so, it is sufficient to show the existence of $n \in \mathbf{N}$ such that $x \in Y_n^{\alpha(f)}$ as this will imply that:

$$T(f)(x) = (1, (f, x)) \in \bar{Y}_n \subseteq Y_{n+1} \subseteq Y$$

If $\alpha(f) = 0$ then $Y_n^{\alpha(f)} = Y^{\alpha(f)} = 1$ for all $n \in \mathbf{N}$ and in particular $x \in Y_n^{\alpha(f)}$. So we assume that $\alpha(f) \geq 1$. Since $x : \alpha(f) \to Y$, given $i \in \alpha(f)$ we have $x(i) \in Y$. So there exists $n_i \in \mathbf{N}$ such that $x(i) \in Y_{n_i}$. If we define:

$$n = \max(n_0, \ldots, n_{\alpha(f)-1})$$

since $Y_{n_i} \subseteq Y_n$ for all $i \in \alpha(f)$, we see that $x(i) \in Y_n$ for all $i \in \alpha(f)$. It follows that $x : \alpha(f) \to Y_n$, i.e. $x \in Y_n^{\alpha(f)}$ and we have proved that $T(f) : Y^{\alpha(f)} \to Y$ for all $f \in \alpha$ as required. It follows that Y is a set and T is a map with domain α such that $T(f) : Y^{\alpha(f)} \to Y$ for all $f \in \alpha$. So (Y, T) is a universal algebra of type α. It remains to show that (Y, T) is free with Y_0 as a free generator. So let (Z, S) be a universal algebra of type α and $g_0 : Y_0 \to Z$ be a map. We need to show that g_0 can be uniquely extended into a morphism $g : Y \to Z$.

We define g by setting $g_{|Y_0} = g_0$ and $g_{|(Y_{n+1})} = g_{n+1}$ where each g_n is a map $g_n : Y_n \to Z$ and the sequence $(g_n)_{n\in\mathbf{N}}$ is defined by recursion with the property that $(g_{n+1})_{|Y_n} = g_n$ for all $n \in \mathbf{N}$. Specifically, we define $g_{n+1}(y) = g_n(y)$ for all $y \in Y_n$, and given $y \in Y_{n+1} \setminus Y_n \subseteq \bar{Y}_n$, we consider $f \in \alpha$ and $x \in Y_n^{\alpha(f)}$ such that $y = (1, (f, x))$. Note that such representation of y exists and is clearly unique. We then define $g_{n+1}(y)$ by setting:

$$g_{n+1}(y) = S(f)(g_n^{\alpha(f)}(x)) \tag{1.2}$$

Recall that $g_n^{\alpha(f)} : Y_n^{\alpha(f)} \to Z^{\alpha(f)}$ is the map defined by $g_n^{\alpha(f)}(x)(i) = g_n(x(i))$ for all $i \in \alpha(f)$. Since $S(f) : Z^{\alpha(f)} \to Z$ it follows that $g_{n+1}(y)$ as given by equation (1.2) is a well-defined element of Z. This completes our recursion and we have a sequence of maps $g_n : Y_n \to Z$ such that $(g_{n+1})_{|Y_n} = g_n$ for all $n \in \mathbf{N}$. From this last property, it follows that $g : Y \to Z$ is itself well-defined by setting $g_{|Y_n} = g_n$ for all $n \in \mathbf{N}$. So we have map $g : Y \to Z$ such that $g_{|Y_0} = g_0$. We shall now check that g is a morphism. So let $f \in \alpha$ and $x \in Y^{\alpha(f)}$. We need to check that $g \circ T(f)(x) = S(f) \circ g^{\alpha(f)}(x)$. Since $x \in Y^{\alpha(f)}$ we have already shown the existence of $n \in \mathbf{N}$ such that $x \in Y_n^{\alpha(f)}$. In fact, let us pick n to be the smallest of such integers. By definition we have $T(f)(x) = (1, (f, x))$. From this equality and $x \in Y_n^{\alpha(f)}$, it follows that $T(f)(x)$ is an element of $\bar{Y}_n \subseteq Y_{n+1}$. We claim that $T(f)(x)$ is in fact an element of $Y_{n+1} \setminus Y_n$. So we need to show that $T(f)(x) \notin Y_n$. Suppose to the contrary that $T(f)(x) \in Y_n$. Let $k \in \mathbf{N}$ denote the smallest integer such that $T(f)(x) \in Y_k$. Note that $k \leq n$. If $k = 0$ we obtain $(1, (f, x)) = (0, x')$ for some $x' \in X_0$ which is a contradiction. So $k \geq 1$ and $Y_k = Y_{k-1} \cup \bar{Y}_{k-1}$. From the minimality of k we have $T(f)(x) \notin Y_{k-1}$. It follows that $T(f)(x) \in \bar{Y}_{k-1}$. So there exist $f' \in \alpha$ and $x' \in Y_{k-1}^{\alpha(f)}$ such that:

$$(1, (f, x)) = T(f)(x) = (1, (f', x'))$$

From this we see that $x = x' \in Y_{k-1}^{\alpha(f)}$. Since $k \leq n$, we have $k - 1 < n$ and $x \in Y_{k-1}^{\alpha(f)}$ contradicts the minimality of n. So we have shown that $T(f)(x) \in Y_n$ leads to a contradiction, and it follows that $T(f)(x) \in Y_{n+1} \setminus Y_n$. Thus:

$$g \circ T(f)(x) = g_{n+1}(T(f)(x)) = S(f)(g_n^{\alpha(f)}(x)) = S(f) \circ g^{\alpha(f)}(x)$$

where the last equality follows from $g_n = g_{|Y_n}$ and $x \in Y_n^{\alpha(f)}$. This completes our proof of the fact that $g : Y \to Z$ is a morphism. It remains to check that g is unique. So let $g' : Y \to Z$ be another morphism such that $g'_{|Y_0} = g_0$. We shall prove by induction that $g_{|Y_n} = g'_{|Y_n}$ for all $n \in \mathbf{N}$. Since $g_{|Y_0} = g_0 = g'_{|Y_0}$, this is clearly true for $n = 0$. So we assume that $n \in \mathbf{N}$ and $y \in Y_{n+1}$. We need to show that $g(y) = g'(y)$. From the induction hypothesis, the equality is true for $y \in Y_n$. So we may assume that $y \in Y_{n+1} \setminus Y_n \subseteq \bar{Y}_n$. In particular, there exist $f \in \alpha$ and $x \in Y_n^{\alpha(f)}$ such that $y = (1, (f, x))$. It follows that $y = T(f)(x)$ and finally:

$$g(y) = g \circ T(f)(x) = S(f) \circ g^{\alpha(f)}(x) = S(f) \circ g'^{\alpha(f)}(x) = g' \circ T(f)(x) = g'(y)$$

where the third equality follows from the induction hypothesis and $x \in Y_n^{\alpha(f)}$.
.

1.1.9 Cantor's Theorem

Given an arbitrary set X_0, we were able to construct a free universal algebra of type α whose free generator Y_0 is a copy of X_0, i.e. a set for which there exists a bijection $j : X_0 \to Y_0$. Our aim is to go slightly beyond that and find a free universal algebra of type α with free generator the set X_0 itself. For this, we shall need a couple of set theoretic results which we include in this section and the following for the sake of completeness. In particular we shall need to prove that any set A has a disjoint copy of itself, i.e. that there exist a set B with $A \cap B = \emptyset$ and a bijection $j : A \to B$. To prove this result, we shall make use of Cantor's Theorem which is the focus of the present section.

Given a set A, recall that $\mathcal{P}(A)$ denotes the *power set* of A, i.e. the set of all subsets of A, that is:

$$\mathcal{P}(A) = \{B : B \subseteq A\}$$

Note that there is an obvious bijection $j : 2^A \to \mathcal{P}(A)$, which is defined by $j(x) = \{a \in A : x(a) = 1\}$. Cantor's Theorem asserts that $\mathcal{P}(A)$ has higher cardinality than the set A, i.e. that there exists no injective map $j : \mathcal{P}(A) \to A$. Most of us will be familiar with this result, and indeed other similar results such as the fact that $\mathbf{R}$ has higher cardinality than $\mathbf{N}$. Some of us may remember a version of *Cantor's diagonal argument*. We restrict our attention to the interval $]0, 1[$ and consider every $x \in]0, 1[$ as a sequence $x = 0.11010111001\ldots$ This sequence is not unique but after some ironing out, we may be convinced that $]0, 1[$ has the same cardinality as $2^{\mathbf{N}}$ which in turn has the same cardinality as $\mathcal{P}(\mathbf{N})$. Hence Cantor's diagonal argument essentially proves that $\mathcal{P}(\mathbf{N})$ is a bigger set than $\mathbf{N}$, and $\mathbf{R}$ having a higher cardinality than $\mathbf{N}$ is essentially a particular case of Cantor's Theorem.

There is an easy way to remember the proof of Cantor's Theorem, which is to think of Russell's paradox. Bertrand Russell discovered that $\{x : x \notin x\}$ cannot be a set, or more precisely that the statement:

$$\exists y \forall x [x \in y \leftrightarrow x \notin x]$$

leads to a contradiction. If $a = \{x : x \notin x\}$ is a set, then $a \in a$ implies that $a \notin a$, while $a \notin a$ implies that $a \in a$. Now suppose we have a bijection $j : \mathcal{P}(A) \to A$ (we assume this is a bijection rather than an injection to make this discussion simpler). Then every element of A can be *viewed* as a subset of A. It is tempting to consider the set of those elements of A which *do not belong to themselves*, but rather than considering the meaning of '$\in$' literally as in $a = \{x \in A : x \notin x\}$, we need to adjust slightly with $a = j(\{x \in A : x \notin j^{-1}(x)\}) \in A$. Following Russell's argument, we then ask whether $a \in A$ *belongs to itself*, or specifically if $a \in j^{-1}(a)$. But assuming $a \in j^{-1}(a)$ leads to $a \notin j^{-1}(a)$, while assuming $a \notin j^{-1}(a)$ leads to $a \in j^{-1}(a)$. So we have proved that there cannot exist a bijection $j : \mathcal{P}(A) \to A$. The following lemma deals with an injection rather

than a bijection. We need to be slightly more careful, but the idea underlying the proof is the same.

Lemma 1 (Cantor's Theorem) *Let A be an arbitrary set. There exists no injective map $j : \mathcal{P}(A) \to A$.*

Proof
Suppose $j : \mathcal{P}(A) \to A$ is an injective map and define $b^* = j(B^*)$ where:

$$B^* = \{b \in A : \ \exists B \in \mathcal{P}(A) \ , \ b = j(B) \text{ and } b \notin B\}$$

We shall complete the proof by showing that both $b^* \in B^*$ and $b^* \notin B^*$ lead to a contradiction. So suppose first that $b^* \in B^*$. There exists $B \in \mathcal{P}(A)$ such that $b^* = j(B)$ and $b^* \notin B$. Hence in particular we have $j(B^*) = b^* = j(B)$ and since j is an injective map, it follows that $B^* = B$. So we see that $b^* \notin B^*$ which contradicts the initial assumption of $b^* \in B^*$. We now assume that $b^* \notin B^*$. Since $b^* = j(B^*)$, taking $B = B^*$ we see that there exists $B \in \mathcal{P}(A)$ such that $b^* = j(B)$ and $b^* \notin B$. Hence it follows that $b^* \in B^*$ which contradicts the initial assumption of $b^* \notin B^*$. **.**

1.1.10 Disjoint Copy of a Set

In this section we prove that any set A has a disjoint copy of itself, namely that there exists a set B with $A \cap B = \emptyset$ and a bijection $j : A \to B$. We shall prove this result using Cantor's Theorem (lemma (1)) as well as the Axiom of Choice. There are probably many other ways to prove it, some of which not involving the Axiom of Choice. It is in fact unknown to me whether this can be proved within **ZF** rather than **ZFC**.[4]

Given a set A, recall that the Axiom of Choice states the existence of a *choice function* on A, i.e. the existence of a map $k : \mathcal{P}(A) \setminus \{\emptyset\} \to A$ such that $k(x) \in x$ for all $x \in \mathcal{P}(A) \setminus \{\emptyset\}$. A choice function on A is simply a map which *chooses* an arbitrary element from every non-empty subset of A.

Lemma 2 *Let A be an arbitrary set. There exists a set B with $A \cap B = \emptyset$ and a bijective map $j : A \to B$.*

Proof
For all $x \in \mathcal{P}(A)$ define $A_x = \{(x, y) : y \in A\}$. There is a clear bijection between A and A_x, namely $j_x : A \to A_x$ defined by $j_x(y) = (x, y)$. We shall complete the proof by taking $B = A_x$ for some $x \in \mathcal{P}(A)$ for which $A \cap A_x = \emptyset$. Of course we need to check that it is always possible to do so. Suppose to the contrary that $A \cap A_x \neq \emptyset$ for all $x \in \mathcal{P}(A)$. Using the Axiom of Choice, there exists a choice function $k : \mathcal{P}(A) \setminus \{\emptyset\} \to A$. We define $j : \mathcal{P}(A) \to A$ by setting $j(x) = k(A \cap A_x)$. Note that $j(x)$ is well defined since $A \cap A_x \neq \emptyset$. We obtain a

[4]For those interested, there is a thread on `sci.math` entitled "[Set Theory] A set has a disjoint copy of itself" (which may have the answer to the **ZF** question). I am grateful to those who contributed to this thread. The proof of lemma (2) is due to Robin Chapman.

map $j : \mathcal{P}(A) \to A$ such that $j(x) \in A \cap A_x$ for all $x \in \mathcal{P}(A)$. It is now sufficient to show that j is injective, as this will contradict Cantor's Theorem. So suppose $x, x' \in \mathcal{P}(A)$ are such that $j(x) = j(x')$. Since $j(x) \in A_x$ there exists $y \in A$ such that $j(x) = (x, y)$. Similarly, there exists $y' \in A$ such that $j(x') = (x', y')$. From $j(x) = j(x')$ we obtain $(x, y) = (x', y')$ and it follows in particular that $x = x'$. So we have proved that $j : \mathcal{P}(A) \to A$ is indeed an injective map. .

Given a set X_0, our goal is to obtain a free universal algebra of type α with free generator the set X_0 itself. Defining $Y_0 = \{(0, x) : x \in X_0\}$, we were able to construct a free universal algebra Y with free generator Y_0, as described in proposition (4). So we have an injection $j : X_0 \to Y$, where Y is a free universal algebra of type α. In fact, this injection is a bijection between X_0 and Y_0, the free generator of Y. In order for us to construct a free universal algebra with free generator X_0, all we need is a copy of Y containing X_0. In other words we need a set X with $X_0 \subseteq X$ and a bijection $g : X \to Y$. Once we have this set X and the bijection $g : X \to Y$, we can easily *carry over* the structure of universal algebra from Y onto X, by choosing the structure on X which turns the bijection $g : X \to Y$ into an isomorphism. However, we want X_0 to be a free generator of X. One way to ensure this is to request that the bijection $g : X \to Y$ carries X_0 onto Y_0. In other words, we want the restriction $g_{|X_0}$ to coincide with the bijection $j : X_0 \to Y_0$. The following lemma shows the existence of the set X with the bijection $g : X \to Y$ satisfying the required property $g_{|X_0} = j$.

Note that the idea of starting from an injection $X_0 \to Y$ and obtaining a copy of Y containing X_0 while *preserving* this injection can be used in many other cases. Most of us are familiar with the way the ring of integers $\mathbf{Z}$ is created as a quotient set $(\mathbf{N} \times \mathbf{N})/\sim$ with the appropriate equivalence relation. We obtain an embedding $j_1 : \mathbf{N} \to \mathbf{Z}$. We then construct the field $\mathbf{Q}$ of rational numbers and we obtain another embedding $j_2 : \mathbf{Z} \to \mathbf{Q}$. We go on by constructing the field $\mathbf{R}$ of real numbers and the field $\mathbf{C}$ of complex numbers with their associated embedding $j_3 : \mathbf{Q} \to \mathbf{R}$ and $j_4 : \mathbf{R} \to \mathbf{C}$. Strictly speaking, the set theoretic inclusions $\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$ are false and most living mathematicians do not care. The inclusion $\mathbf{N} \subseteq \mathbf{Z}$ has to be true. If it is not, it needs to be re-interpreted in a way which makes it true. In computing terms, mathematicians are effectively *overloading* the operators $\in$ and $\subseteq$. This is all very nice and fine in practice. But assuming we wanted to *code* or *compile* a *high level* mathematical statement into a *low level* expression of first order predicate logic, it may be that defining $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{C}$ in a way which avoids the overloading of primitive symbols, will make our life a lot easier. We believe the aim of creating a formal high level mathematical language whose statements could be compiled as formulas of first order logic is a worthy objective. Such high level language would most likely need to allow the overloading of symbols. So it may be that whether $\mathbf{N} \subseteq \mathbf{Z}$ is literally true or not will not matter. There is a fascinating website [45] on `http://www.metamath.org/` created by Norman Megill where these questions are likely to have been answered. It is certainly our intention to use this reference more and more as this document progresses.

Recall that if $f : A \to B$ is a map and $A' \subseteq A$, then $f(A')$ is the set:

$$f(A') = \{y : \exists x \ , \ x \in A' \text{ and } \ (x, y) \in f\}$$

which coincides with $\text{rng}(f_{|A'})$. In particular, $f(A) = \text{rng}(f)$. The notation $f(A')$ is a case of overloading. The meaning of $f(x)$ must be derived from the context, and depends on whether x is viewed as an element of A or a subset of A. It can easily be both, as 0 is both an element and a subset of 1. Some authors will use the notation $f[A']$ rather than $f(A')$.

Lemma 3 *Let X_0 and Y be sets and $j : X_0 \to Y$ be an injective map. There exist a set X and a bijection $g : X \to Y$ such that $X_0 \subseteq X$ and $g_{|X_0} = j$.*

Proof
Consider the set $A = X_0 \cup Y$. Using lemma (2) there exists a set B with $A \cap B = \emptyset$ and a bijective map $i : A \to B$. Define:

$$X = X_0 \cup i(Y \setminus j(X_0))$$

and $g : X \to Y$ by setting $g(x) = j(x)$ for all $x \in X_0$ and $g(x) = i^{-1}(x)$ for all $x \in i(Y \setminus j(X_0))$. Note first that $g(x)$ is well defined since $x \in X_0$ and $x \in i(Y \setminus j(X_0))$ cannot occur at the same time, as $X_0 \subseteq A$, $i(Y \setminus j(X_0)) \subseteq B$ and $A \cap B = \emptyset$. Note also that $g(x)$ is defined for all $x \in X$. To show that we have $g : X \to Y$ we need to check that $g(x) \in Y$ for all $x \in X$. If $x \in X_0$ then this is clear since $j : X_0 \to Y$ and $g(x) = j(x)$. If $x \in i(Y \setminus j(X_0))$, then x can be written as $x = i(y)$ for some $y \in Y \setminus j(X_0)$. It follows that $g(x) = i^{-1}(x) = y \in Y$. So we have proved that $g : X \to Y$. We obviously have $X_0 \subseteq X$ and $g_{|X_0} = j$. So we shall complete the proof by showing that $g : X \to Y$ is a bijection. First we show that it is surjective. So let $y \in Y$. We need to show that $y = g(x)$ for some $x \in X$. If $y \in j(X_0)$ then $y = j(x)$ for some $x \in X_0$ and in particular $y = g(x)$. Otherwise $y \in Y \setminus j(X_0)$ and taking $x = i(y) \in i(Y \setminus j(X_0))$ we see that $y = i^{-1}(x)$ and in particular $y = g(x)$. So we have proved that g is surjective. To show that it is injective, let $x, x' \in X$ and assume that $g(x) = g(x')$. We need to show that $x = x'$. Note first that we cannot have $x \in X_0$ while $x' \in i(Y \setminus j(X_0))$. If this was the case, we would have $g(x) = j(x) \in j(X_0)$ while $g(x') = i^{-1}(x') \in Y \setminus j(X_0)$ contradicting the fact that $g(x) = g(x')$ as one lies in $j(X_0)$ while the other does not. Similarly, we cannot have $x \in i(Y \setminus j(X_0))$ while $x' \in X_0$. It follows that either both x and x' lie in X_0 or they both lie in $i(Y \setminus j(X_0))$. In the first case we obtain $j(x) = g(x) = g(x') = j(x')$ and since $j : X_0 \to Y$ is injective we see that $x = x'$. In the second case, we obtain $i^{-1}(x) = g(x) = g(x') = i^{-1}(x')$ and since $i^{-1} : B \to A$ is injective we see that $x = x'$. So we have proved that g is injective, and finally $g : X \to Y$ is a bijection. .

1.1.11 Main Existence Theorem

Given a set X_0, we are now in a position to prove the existence of a free universal algebra of type α with X_0 as free generator. As already hinted in the previous

section, the proof essentially runs in three stages. We start using proposition (4) to construct a free universal algebra Y with free generator $Y_0 = \{(0, x) : x \in X_0\}$. We then use lemma (3) to obtain a copy X of Y and a bijection $g : X \to Y$ which preserves the bijection $j : X_0 \to Y_0$. We finally define on X the unique structure of universal algebra of type α turning $g : X \to Y$ into an isomorphism.

Theorem 1 *Let α be a type of universal algebra and X_0 be an arbitrary set. There exists a free universal algebra of type α with free generator X_0. Such universal algebra is unique up to isomorphism.*

Proof
Uniqueness up to isomorphism is a direct consequence of proposition (3). So we only need to prove the existence. If we define $Y_0 = \{(0, x) : x \in X_0\}$, from proposition (4) we have a free universal algebra Y with free generator Y_0. Furthermore, the map $j : X_0 \to Y$ defined by $j(x) = (0, x)$ for all $x \in X_0$ is an injective map. Using lemma (3) there exist a set X and a bijection $g : X \to Y$ such that $X_0 \subseteq X$ and $g_{|X_0} = j$. At this stage, the set X is only a set, not a universal algebra of type α. However, using the bijection $g : X \to Y$ we can easily carry over the structure from Y onto X. Specifically, we define a map T with domain α by setting $T(f) : X^{\alpha(f)} \to X$ to be defined by:

$$\forall x \in X^{\alpha(f)} \ , \ T(f)(x) = g^{-1} \circ f \circ g(x) \tag{1.3}$$

where it is understood that 'f' on the r.h.s. of this equation is a shortcut for the operator $f : Y^{\alpha(f)} \to Y$ and 'g' refers to $g^{\alpha(f)} : X^{\alpha(f)} \to Y^{\alpha(f)}$, while g^{-1} is simply the inverse $g^{-1} : Y \to X$. So $T(f)$ as defined by equation (1.3) is indeed a map $T(f) : X^{\alpha(f)} \to X$. It follows that (X, T) is now a universal algebra of type α and $X_0 \subseteq X$. We shall complete the proof of this theorem by showing that X_0 is a free generator of X. Note that this is hardly surprising since $j : X_0 \to Y_0$ is a bijection which coincide with the bijection $g : X \to Y$ on X_0, and we know that Y_0 is a free generator of Y. In order to prove this formally, let Z be a universal algebra of type α and $h_0 : X_0 \to Z$ be a map. We need to show that h_0 can be uniquely extended into a morphism $h : X \to Z$. Before we do so, note that from equation (1.3) we have for all $x \in X^{\alpha(f)}$:

$$g \circ T(f)(x) = f \circ g(x)$$

which shows that $g : X \to Y$ is not only a bijection, but also a morphism, i.e. g is an isomorphism. Now from $h_0 : X_0 \to Z$ we obtain a map $h_0 \circ j^{-1} : Y_0 \to Z$. Since Y_0 is a free generator of Y, there exists a morphism $h' : Y \to Z$ such that $h'_{|Y_0} = h_0 \circ j^{-1}$. It follows that $h : X \to Z$ defined by $h = h' \circ g$ is a morphism, and furthermore, we have:

$$h_{|X_0} = h' \circ g_{|X_0} = h' \circ j = h'_{|Y_0} \circ j = h_0 \circ j^{-1} \circ j = h_0$$

So we have proved the existence of a morphism $h : X \to Z$ such that $h_{|X_0} = h_0$. It remains to check that $h : X \to Z$ is in fact unique. So suppose h' now refers

to a morphism $h' : X \to Z$ such that $h'_{|X_0} = h_0$. Then $h \circ g^{-1} : Y \to Z$ and $h' \circ g^{-1} : Y \to Z$ are two morphisms which coincide on Y_0, since:

$$(h \circ g^{-1})_{|Y_0} = h_{|X_0} \circ j^{-1} = h_0 \circ j^{-1} = h'_{|X_0} \circ j^{-1} = (h' \circ g^{-1})_{|Y_0}$$

It follows that $h \circ g^{-1} = h' \circ g^{-1}$, from the uniqueness property of Y_0 being a free generator of Y. We conclude that $h = h'$. .

1.2 Structural Induction, Structural Recursion

1.2.1 Unique Representation in Free Universal Algebra

In an earlier section, we claimed that most universal algebras were not free. The following theorem arguably provides the most convincing evidence of this fact. Let X be a group viewed as a universal algebra of type $\alpha = \{(0,0),(1,1),(2,2)\}$, where the product $T(2,2) : X^2 \to X$ is denoted $\otimes$. Then the following theorem shows that X cannot be a free universal algebra of type α unless:

$$x_1 \otimes y_1 = x_2 \otimes y_2 \;\Rightarrow\; x_1 = x_2 \text{ and } y_1 = y_2$$

for all x_1, x_2, y_1 and $y_2 \in X$. This is a pretty strong condition. In fact, we can easily show that X can never be a free universal algebra of type α. Indeed, let $e = T(0,0)(0)$ be the identity element of X. Then $e = e \otimes e$, or equivalently:

$$T(0,0)(0) = T(2,2)(e,e)$$

The following theorem shows this cannot be true in a free universal algebra.

Theorem 2 *Let X be a free universal algebra of type α with free generator $X_0 \subseteq X$. Then for all $y \in X$, one and only one of the following is the case:*

$$\begin{array}{ll} (i) & y \in X_0 \\ (ii) & y = f(x) \quad , \; f \in \alpha \; , \; x \in X^{\alpha(f)} \end{array}$$

Furthermore, the representation (ii) is unique, that is:

$$f(x) = f'(x') \;\Rightarrow\; f = f' \text{ and } x = x'$$

for all $f, f' \in \alpha$, $x \in X^{\alpha(f)}$ and $x' \in X^{\alpha(f')}$.

Proof
We shall first prove the theorem for a particular case of free universal algebra of type α. Instead of looking at X itself, we shall first consider the free universal algebra Y with free generator $Y_0 = \{(0,x) : x \in X_0\}$ as described in proposition (4). So let $y \in Y$ and suppose that $y \notin Y_0$. There exists $n \in \mathbf{N}$ such that $y \in Y_{n+1}$. Let n denote the smallest of such integers. Then $y \in Y_{n+1} \setminus Y_n \subseteq \bar{Y}_n$. Hence, there exist $f \in \alpha$ and $x \in Y_n^{\alpha(f)}$ such that $y = (1,(f,x))$. However by definition, we have $f(x) = (1,(f,x))$. Since $Y_n^{\alpha(f)} \subseteq Y^{\alpha(f)}$, we have found $f \in \alpha$

and $x \in Y^{\alpha(f)}$ such that $y = f(x)$. This shows that (ii) is satisfied whenever (i) is not. We shall now prove that (i) and (ii) cannot occur simultaneously. Indeed if $y = f(x)$ for some $f \in \alpha$ and $x \in Y^{\alpha(f)}$, then $y = (1, (f, x))$. If y is also an element of Y_0 then $y = (0, x')$ for some $x' \in X_0$, which is a contradiction as $0 \neq 1$. So we have proved that one and one only of (i) and (ii) must occur. It remains to show that the representation (ii) is unique. So suppose $f(x) = f'(x')$ for some $f, f' \in \alpha$, $x \in Y^{\alpha(f)}$ and $x' \in Y^{\alpha(f')}$. Then we have $(1, (f, x)) = (1, (f', x'))$ and it follows immediately that $f = f'$ and $x = x'$. So we have proved the theorem in the case of the free universal algebra Y. We shall now prove the theorem for X. Consider the bijection $j : X_0 \to Y_0$ defined by $j(x) = (0, x)$. Then we also have $j : X_0 \to Y$ and since X_0 is a free generator of X, the map j can be uniquely extended into a morphism $g : X \to Y$. Similarly, the map $j^{-1} : Y_0 \to X$ can be uniquely extended into a morphism $g' : Y \to X$. Furthermore, since $g' \circ g : X \to X$ is a morphism such that:

$$(g' \circ g)_{|X_0} = g' \circ j = g'_{|Y_0} \circ j = j^{-1} \circ j = (id_X)_{|X_0}$$

we conclude by uniqueness that $g' \circ g = id_X$ and similarly $g \circ g' = id_Y$. This shows that $g : X \to Y$ and $g' : Y \to X$ are in fact isomorphisms which are inverse of each other. Of course we already knew that X and Y were isomorphic from the existence of the bijection $j : X_0 \to Y_0$. But we now have a particular isomorphism $g : X \to Y$ which is such that $g_{|X_0} = j$. This should allow us to complete the proof of the theorem. So suppose $y \in X$ and $y \notin X_0$. Let $y' = g(y) \in Y$. Since the theorem is true for Y, either (i) or (ii) is true for y'. We claim that $y' \in Y_0$ is impossible, as otherwise:

$$y = g' \circ g(y) = g'(y') = g'_{|Y_0}(y') = j^{-1}(y') \in X_0$$

which contradicts the assumption $y \notin X_0$. It follows that (ii) is true for y', i.e. $y' = f(x')$ for some $f \in \alpha$ and $x' \in Y^{\alpha(f)}$. Taking $x = g'(x') \in X^{\alpha(f)}$, since $g' : Y \to X$ is a morphism we obtain:

$$y = g'(y') = g' \circ f(x') = f \circ g'(x') = f(x)$$

which shows that (ii) is true for y. We now prove that (i) and (ii) cannot occur simultaneously. Suppose that $y \in X_0$ and $y = f(x)$ for some $f \in \alpha$ and $x \in X^{\alpha(f)}$. Taking $y' = g(y) \in Y$ and $x' = g(x) \in Y^{\alpha(f)}$, we obtain:

$$y' = g(y) = g_{|X_0}(y) = j(y) \in Y_0$$

and furthermore:

$$y' = g(y) = g \circ f(x) = f \circ g(x) = f(x')$$

which shows that (i) and (ii) are simultaneously true for $y' \in Y$, which is a contradiction. To complete the proof of the theorem, it remains to show that the representation (ii) is unique. So suppose $f(x) = f'(x')$ for some $f, f' \in \alpha$, $x \in X^{\alpha(f)}$ and $x' \in X^{\alpha(f')}$. We obtain:

$$f(g(x)) = f \circ g(x) = g \circ f(x) = g \circ f'(x') = f'(g(x'))$$

From the uniqueness of the representation (ii) in Y, it follows that $f = f'$ and $g(x) = g(x') \in Y^{\alpha(f)}$. Hence, for all $i \in \alpha(f)$:

$$g(x(i)) = g(x)(i) = g(x')(i) = g(x'(i))$$

and since $g : X \to Y$ is injective, we conclude that $x(i) = x'(i)$. This being true for all $i \in \alpha(f)$, we have proved that $x = x'$. **.**

Proposition 5 *A free universal algebra of type α has a unique free generator.*

Proof
Let X be a free universal algebra of type α. Suppose $X_0 \subseteq X$ and $Y_0 \subseteq X$ are both free generators of X. We need to show that $X_0 = Y_0$. First we show that $X_0 \subseteq Y_0$. So let $y \in X_0$. Applying theorem (2) of page 21 to X with free generator Y_0 we see that if $y \notin Y_0$ there exists $f \in \alpha$ and $x \in X^{\alpha(f)}$ such that $y = f(x)$. But this contradicts theorem (2) applied to X with free generator X_0 since $y \in X_0$, and (i) and (ii) cannot occur simultaneously. it follows that $y \in Y_0$ and we have proved that $X_0 \subseteq Y_0$. The reverse inclusion is proved in a similar fashion. **.**

1.2.2 Order in Free Universal Algebra

In this section, we define the notion of *order* on a free universal algebra. This notion will prove useful on several occasions, and specifically when proving in proposition (14) that a free generator is also a *generator*. Loosely speaking, given a universal algebra X of type α, the *order on* X is a map $\omega : X \to \mathbf{N}$ representing the degree of complexity of the elements of X, viewed as expressions in a formal language. For instance suppose X is of type $\alpha = \{(0, 2)\}$ with one single binary operator $\oplus : X^2 \to X$ and free generator $X_0 = \{0\}$. We have $\omega(0) = 0$ while $\omega(0 \oplus 0) = 1$ and $\omega(0 \oplus (0 \oplus 0)) = 2$. The complexity of a formula is sometimes a useful tool to carry out induction arguments over $\mathbf{N}$. For those already familiar with the subject, we do not define the order $\omega : X \to \mathbf{N}$ by structural recursion, e.g. $\omega(0) = 0$ and $\omega(x \oplus y) = 1 + \max(\omega(x), \omega(y))$. Instead, we shall embed $\mathbf{N}$ with the appropriate structure of universal algebra of type α, and consider $\omega : X \to \mathbf{N}$ as the unique morphism such that $\omega_{|X_0} = 0$. In effect, we are limiting ourselves to definitions by recursions over $\mathbf{N}$, which is a standard mathematical argument already used in proposition (4). We shall not make use of definitions by structural recursion on free universal algebras, until the principle has been justified in a later section.

Definition 7 *Let α be a type of universal algebra. We call* default structure of type α *on* $\mathbf{N}$ *the map T with domain α such that $T(f) : \mathbf{N}^{\alpha(f)} \to \mathbf{N}$ is:*

$$\forall n \in \mathbf{N}^{\alpha(f)} \ , \ T(f)(n) = 1 + \max\{n(i) : i \in \alpha(f)\}$$

for all $f \in \alpha$, where it is understood that $\max(\emptyset) = 0$.

Definition 8 *Let X be a free universal algebra of type α with free generator $X_0 \subseteq X$. We call* order *on X the unique morphism $\omega : X \to \mathbf{N}$ such that $\omega_{|X_0} = 0$, where $\mathbf{N}$ is embedded with its default structure of type α. Given $x \in X$, we call* order of x *the integer $\omega(x) \in \mathbf{N}$ where ω is the order on X.*

Proposition 6 *Let X be a free universal algebra of type α with free generator $X_0 \subseteq X$ and $\omega : X \to \mathbf{N}$ be the order on X. Then for all $x \in X$ we have:*

$$\omega(x) = 0 \;\Leftrightarrow\; x \in X_0$$

Furthermore, for all $f \in \alpha$ and $x \in X^{\alpha(f)}$ we have:

$$\omega(f(x)) = 1 + \max\{\omega(x(i)) : i \in \alpha(f)\}$$

Proof
First we show the equality. Suppose $f \in \alpha$ and $x \in X^{\alpha(f)}$. Let T denote the default structure of type α on $\mathbf{N}$ as per definition (7). Since $\omega : X \to \mathbf{N}$ is a morphism, we have:

$$\begin{aligned} \omega(f(x)) &= T(f)(\omega(x)) \\ &= 1 + \max\{\omega(x)(i) : i \in \alpha(f)\} \\ &= 1 + \max\{\omega(x(i)) : i \in \alpha(f)\} \end{aligned}$$

We now show the equivalence. Since $\omega_{|X_0} = 0$ from definition (8), it is clear that $y \in X_0$ implies $\omega(y) = 0$. Suppose conversely that $y \in X$ and $\omega(y) = 0$. We need to show that $y \in X_0$. Suppose to the contrary that $y \notin X_0$. From theorem (2) of page 21 there exist $f \in \alpha$ and $x \in X^{\alpha(f)}$ such that $y = f(x)$. So:

$$\omega(y) = \omega(f(x)) = 1 + \max\{\omega(x(i)) : i \in \alpha(f)\} \geq 1$$

which contradicts the initial assumption of $\omega(y) = 0$. **.**

Suppose $X = \mathbf{N}$ is the free universal algebra of type $\alpha = \{(0,1)\}$ with the single successor operator $s : X^1 \to X$ and free generator $X_0 = \{0\}$. Then $\omega(0) = 0$ while $\omega(1) = \omega(s(0)) = 1 + \omega(0) = 1$. If we now regard $X = \mathbf{N}$ as the free universal algebra of type $\alpha = \{(0,1),(1,0)\}$ by adding the constant 0, then X now has $X_0 = \emptyset$ as free generator. Furthermore:

$$\omega(0) = \omega(T(1,0)(0)) = 1 + max(\emptyset) = 1$$

More generally, the order of constants in a free universal algebra is 1 and not 0. Only the elements of the free generator have order 0.

We shall now complete this section with a small proposition on the structure of a free universal algebra in relation to its order mapping. Note that the definition of X_0 below is consistent with the existing notation X_0 referring to the free generator of X, since we have $\omega(x) = 0 \;\Leftrightarrow\; x \in X_0$.

Proposition 7 *Let X be a free universal algebra of type α with free generator $X_0 \subseteq X$. Let $\omega : X \to \mathbf{N}$ be the order on X and define:*

$$X_n = \{x \in X \;:\; \omega(x) \leq n\}\;,\; n \in \mathbf{N}$$

Then for all $n \in \mathbf{N}$ we have:

$$X_{n+1} = X_n \cup \{f(x) \ : \ f \in \alpha \ , \ x \in (X_n)^{\alpha(f)}\}$$

Proof
First we show the inclusion $\supseteq$. It is clear that $X_n \subseteq X_{n+1}$. So let $f \in \alpha$ and $x \in (X_n)^{\alpha(f)}$. We need to show that $f(x) \in X_{n+1}$ that is $\omega(f(x)) \leq n+1$ which follows from proposition (6) and:

$$\omega(f(x)) = 1 + \max\{\omega(x(i)) : i \in \alpha(f)\} \leq 1 + n$$

where the inequality stems from $\omega(x(i)) \leq n$ for all $i \in \alpha(f)$. We now prove the inclusion $\subseteq$. So suppose $y \in X_{n+1} \setminus X_n$. Then we must have $\omega(y) = n+1$ and in particular $\omega(y) \neq 0$. From proposition (6) it follows that $y \notin X_0$ and consequently using theorem (2) of page 21 we see that y can be uniquely represented as $y = f(x)$ for some $f \in \alpha$ and $x \in X^{\alpha(f)}$. It remains to show that x is actually an element of $(X_n)^{\alpha(f)}$, i.e. that $x(i) \in X_n$ for all $i \in \alpha(f)$ which is vacuously true in the case when $\alpha(f) = 0$. So let $i \in \alpha(f)$. We have:

$$1 + \omega(x(i)) \leq 1 + \max\{\omega(x(i)) : i \in \alpha(f)\} = \omega(f(x)) = \omega(y) = n+1$$

from which we conclude that $\omega(x(i)) \leq n$ as requested. **.**

1.2.3 Universal Sub-Algebra of Universal Algebra

In this section we introduce the notion of universal sub-algebras. The main motivation for this will appear later when we investigate equivalence relations and congruences on universal algebras. An equivalence relation on a universal algebra X is a subset of $X \times X$ with certain closure properties, and can therefore be regarded as a universal sub-algebra of $X \times X$, provided the latter has been embedded with the appropriate structure of universal algebra. Rather, than focussing on the specifics of $X \times X$, we will study universal sub-algebras in a general setting.

Definition 9 *Let X be a universal algebra of type α. We say that $Y \subseteq X$ is a* Universal Sub-Algebra *of X if and only if it is closed under every operator i.e.*

$$\forall f \in \alpha \ , \ \forall x \in X^{\alpha(f)} \ , \ [\ x \in Y^{\alpha(f)} \ \Rightarrow \ f(x) \in Y \ ]$$

If Y is a universal sub-algebra of X, we call induced structure on Y *the map T with domain α such that for all $f \in \alpha$, the operator $T(f) : Y^{\alpha(f)} \to Y$ is:*

$$\forall x \in Y^{\alpha(f)} \ , \ T(f)(x) = f(x) \in Y$$

Let X be a universal algebra of type α and Y be a universal sub-algebra of X. Given $f \in \alpha$, when using loose notations we have two operators $f : X^{\alpha(f)} \to X$ and $f : Y^{\alpha(f)} \to Y$. However, the latter is simply the restriction of the former to the smaller domain $Y^{\alpha(f)} \subseteq X^{\alpha(f)}$, and the notation '$f(x)$' is therefore unambiguous whenever x is an element of $Y^{\alpha(f)}$. The best example of universal sub-algebras are possibly homomorphic images of universal algebras. We have:

Proposition 8 *Let $h : X \to Y$ be a homomorphism between two universal algebras X and Y of type α. Then the image $h(X)$ is a sub-algebra of Y.*

Proof
Let $f \in \alpha$ and $y \in h(X)^{\alpha(f)}$. We need to show that $f(y) \in h(X)$. However, for all $i \in \alpha(f)$ we have $y(i) \in h(X)$. Hence there exists $x_i \in X$ such that $y(i) = h(x_i)$. Let $x \in X^{\alpha(f)}$ be defined by $x(i) = x_i$ for all $i \in \alpha(f)$. Then we have $y(i) = h(x_i) = h(x(i)) = h(x)(i)$ for all $i \in \alpha(f)$ and consequently $y = h(x)$. Since $h : X \to Y$ is a homomorphism, it follows that $f(y) = f \circ h(x) = h \circ f(x) = h(x^*)$ with $x^* = f(x)$. So we have found $x^* \in X$ such that $f(y) = h(x^*)$ and we conclude that $f(y) \in h(X)$. .

The restrictions of homomorphisms to universal sub-algebras are themselves homomorphisms. We had to say this once to avoid future logical flaws in forthcoming arguments. For example, if $h : X \to Y$ is a morphism and X_0 is a sub-algebra of X, we would like to use proposition (8) to argue that $h(X_0)$ is a sub-algebra of Y. This is indeed the case, but we need to argue that $h_{|X_0} : X_0 \to Y$ is a morphism.

Proposition 9 *Let $h : X \to Y$ be a morphism between two universal algebras of type α. Given a sub-algebra $X_0 \subseteq X$, the restriction $h_{|X_0}$ is a morphism.*

Proof
Given $f \in \alpha$ and $x \in X_0^{\alpha(f)}$ we need to check the equality $h \circ f(x) = f \circ h(x)$. This follows from the fact that every operator $f : X_0^{\alpha(f)} \to X_0$ is the restriction of $f : X^{\alpha(f)} \to X$ and $h : X_0 \to Y$ is the restriction of $h : X \to Y$. .

Let $\mathcal{A}$ be a non-empty set. Recall that $\cap\mathcal{A}$ is the set defined by:

$$\cap\mathcal{A} = \{x : \forall Z \in \mathcal{A}\ ,\ x \in Z\}$$

When $\mathcal{A} = \emptyset$, the set $\cap\mathcal{A}$ is normally not defined, as there is no such things as *the set of all sets*. Suppose now that $\mathcal{A}$ is a non-empty set of subsets of a given set X. Since $\mathcal{A}$ is non-empty, it has an element $Z \in \mathcal{A}$ which by assumption is a subset of X. So every element $x \in Z$ is also an element of X and it follows that $\cap\mathcal{A}$ could equally have been defined as:

$$\cap\mathcal{A} = \{x \in X : \forall Z \in \mathcal{A}\ ,\ x \in Z\}$$

This last expression is now meaningful when $\mathcal{A} = \emptyset$, and yields $\cap\emptyset = X$. Hence we shall adopt the convention that $\cap\mathcal{A} = X$ whenever $\mathcal{A} = \emptyset$ is viewed as a set of subsets of X, and X is clearly given from the context.

Proposition 10 *Let X be a universal algebra of type α and $\mathcal{A}$ be a set of universal sub-algebras of X. Then $\cap\mathcal{A}$ is a universal sub-algebra of X.*

Proof
Let $Y = \cap\mathcal{A}$. We need to show that Y is a universal sub-algebra of X. So let $f \in \alpha$ and $x \in Y^{\alpha(f)}$. We need to show that $f(x) \in Y$. So let $Z \in \mathcal{A}$. We need to show that $f(x) \in Z$. But $Y \subseteq Z$ and $x \in Y^{\alpha(f)}$. So $x \in Z^{\alpha(f)}$. Since Z is a universal sub-algebra of X, we conclude that $f(x) \in Z$. .

Definition 10 *Let X be a universal algebra of type α and $X_0 \subseteq X$. Let $\mathcal{A}$ be the set of universal sub-algebras of X defined by:*

$$\mathcal{A} = \{Y : X_0 \subseteq Y \text{ and } Y \text{ universal sub-algebra of } X\}$$

We call Universal Sub-Algebra of X generated by X_0 *the universal sub-algebra of X denoted $\langle X_0 \rangle$ and defined by $\langle X_0 \rangle = \cap \mathcal{A}$.*

Proposition 11 *Let X be a universal algebra of type α and $X_0 \subseteq X$. Then, the universal sub-algebra $\langle X_0 \rangle$ generated by X_0 is the smallest universal sub-algebra of X* containing X_0*, i.e. such that $X_0 \subseteq \langle X_0 \rangle$.*

Proof
Define $\mathcal{A} = \{Y : X_0 \subseteq Y$ and Y universal sub-algebra of $X\}$. From definition (10), we have $\langle X_0 \rangle = \cap \mathcal{A}$. We need to show that $\langle X_0 \rangle$ is a universal sub-algebra of X which contains X_0, and that it is the smallest universal sub-algebra of X with such property. Since every element of $\mathcal{A}$ is a universal sub-algebra of X, from proposition (10), $\langle X_0 \rangle = \cap \mathcal{A}$ is also a universal sub-algebra of X. To show that $X_0 \subseteq \langle X_0 \rangle$ assume that $x \in X_0$. We need to show that $x \in \cap \mathcal{A}$. So let $Y \in \mathcal{A}$. We need to show that $x \in Y$. But this is clear since $X_0 \subseteq Y$. So we have proved that $\langle X_0 \rangle$ is a universal sub-algebra of X containing X_0. Suppose that Y is another universal sub-algebra of X such that $X_0 \subseteq Y$. We need to show that $\langle X_0 \rangle$ is *smaller* than Y, that is $\langle X_0 \rangle \subseteq Y$. But Y is clearly an element of $\mathcal{A}$. Hence if $x \in \langle X_0 \rangle = \cap \mathcal{A}$, it follows immediately that $x \in Y$. This shows that $\langle X_0 \rangle \subseteq Y$. **.**

Suppose X and Y are universal algebras of type α and $g : X \to Y$ is a morphism. Given $X_0 \subseteq X$, the following proposition asserts that the direct image $g(\langle X_0 \rangle)$ of the universal sub-algebra of X generated by X_0 is also the universal sub-algebra $\langle g(X_0) \rangle$ of Y generated by the direct image $g(X_0)$.

Proposition 12 *Let X, Y be universal algebras of type α and $g : X \to Y$ be a morphism. For every subset $X_0 \subseteq X$ we have the following equality:*

$$g(\langle X_0 \rangle) = \langle g(X_0) \rangle$$

Proof
First we show $\supseteq$: by virtue of proposition (11), $\langle g(X_0) \rangle$ is the smallest sub-algebra of Y containing the direct image $g(X_0)$. In order to prove $\supseteq$, it is therefore sufficient to show that $g(\langle X_0 \rangle)$ is a sub-algebra of Y with $g(\langle X_0 \rangle) \supseteq g(X_0)$. This last inclusion follows immediately from $\langle X_0 \rangle \supseteq X_0$. Being a homomorphic image of the sub-algebra $\langle X_0 \rangle$, the fact that $g(\langle X_0 \rangle)$ is a sub-algebra of Y follows from proposition (8). So we now prove $\subseteq$. Consider the subset X_1 defined by:

$$X_1 = \{\, x \in \langle X_0 \rangle \;:\; g(x) \in \langle g(X_0) \rangle \,\}$$

In order to prove $\subseteq$, it is sufficient to prove that $\langle X_0 \rangle \subseteq X_1$. Thus we need to show that X_1 is a sub-algebra of X with $X_0 \subseteq X_1$. The fact that $X_0 \subseteq X_1$ follows from the inclusions $X_0 \subseteq \langle X_0 \rangle$ and $g(X_0) \subseteq \langle g(X_0) \rangle$. So it remains to

show that X_1 is a sub-algebra of X. Consider $f \in \alpha$ and $x \in X_1^{\alpha(f)}$. We need to show that $f(x) \in X_1$. However, from $X_1 \subseteq \langle X_0 \rangle$ we obtain $x \in \langle X_0 \rangle^{\alpha(f)}$ and it follows that $f(x) \in \langle X_0 \rangle$ since $\langle X_0 \rangle$ is a sub-algebra of X. In order to show that $f(x) \in X_1$, it remains to prove that $g \circ f(x) \in \langle g(X_0) \rangle$. Having assumed that $g : X \to Y$ is a morphism, this amounts to showing that $f \circ g(x) \in \langle g(X_0) \rangle$. However, since $\langle g(X_0) \rangle$ is a sub-algebra of Y, in order to show that $f \circ g(x) \in \langle g(X_0) \rangle$ we simply need to prove that $g(x) \in \langle g(X_0) \rangle^{\alpha(f)}$. Thus given $i \in \alpha(f)$, we need to show that $g(x)(i) = g(x(i)) \in \langle g(X_0) \rangle$. It is therefore sufficient to prove that $x(i) \in X_1$ which follows from $x \in X_1^{\alpha(f)}$. .

Let X be a universal algebra of type α and $X_0 \subseteq X$. The universal sub-algebra $\langle X_0 \rangle$ generated by X_0 was defined in terms of an intersection $\cap \mathcal{A}$. This may be viewed as a *definition from above*: we start from universal sub-algebras which are larger than $\langle X_0 \rangle$, including X itself, and we *reduce* these universal sub-algebras by taking the intersection between them, until we arrive at $\langle X_0 \rangle$. The following proposition may be viewed as a *definition from below*. We start from the smallest possible set, which is the generator X_0, and we gradually *add* all the elements which should belong to $\langle X_0 \rangle$ in view of its closure properties. Note that the *definition from below* makes use of a recursion principle, whereas the *definition from above* does not.

Proposition 13 *Let X be a universal algebra of type α and $X_0 \subseteq X$. Define:*

$$X_{n+1} = X_n \cup \bar{X}_n \ , \ n \in \mathbf{N}$$

with:

$$\bar{X}_n = \left\{ f(x) : \ f \in \alpha \ , \ x \in X_n^{\alpha(f)} \right\}$$

Then:

$$\langle X_0 \rangle = \bigcup_{n=0}^{+\infty} X_n$$

Proof
Let $Y = \cup_{n \in \mathbf{N}} X_n$. We need to show that $Y = \langle X_0 \rangle$. First we show that $Y \subseteq \langle X_0 \rangle$. It is sufficient to prove by induction that $X_n \subseteq \langle X_0 \rangle$ for all $n \in \mathbf{N}$. Since $X_0 \subseteq \langle X_0 \rangle$, this is obviously true for $n = 0$. Suppose we have $X_n \subseteq \langle X_0 \rangle$. We claim that $X_{n+1} \subseteq \langle X_0 \rangle$. It is sufficient to prove that $\bar{X}_n \subseteq \langle X_0 \rangle$. So let $f \in \alpha$ and $x \in X_n^{\alpha(f)}$. We have to show that $f(x) \in \langle X_0 \rangle$. But since $X_n \subseteq \langle X_0 \rangle$, we have $X_n^{\alpha(f)} \subseteq \langle X_0 \rangle^{\alpha(f)}$. It follows that $x \in \langle X_0 \rangle^{\alpha(f)}$. But $\langle X_0 \rangle$ is a universal sub-algebra of X, and we conclude that $f(x) \in \langle X_0 \rangle$. This completes our induction argument, and we have proved that $Y \subseteq \langle X_0 \rangle$. We now show that $\langle X_0 \rangle \subseteq Y$. Since $X_0 \subseteq Y$, from proposition (11), $\langle X_0 \rangle$ being the smallest universal sub-algebra containing X_0, it is sufficient to show that Y is also a universal sub-algebra of X. So let $f \in \alpha$ and $x \in Y^{\alpha(f)}$. We need to show that $f(x) \in Y$. It is sufficient to show that $x \in X_n^{\alpha(f)}$ for some $n \in \mathbf{N}$, as this will imply $f(x) \in \bar{X}_n \subseteq X_{n+1} \subseteq Y$. If $\alpha(f) = 0$ then $X_n^{\alpha(f)} = 1 = Y^{\alpha(f)}$ for all $n \in \mathbf{N}$ and $x \in X_n^{\alpha(f)}$ for all $n \in \mathbf{N}$. Suppose $\alpha(f) \geq 1$. Given $i \in \alpha(f)$,

since $x \in Y^{\alpha(f)}$ we have $x(i) \in Y$. So there exists $n_i \in \mathbf{N}$ such that $x(i) \in X_{n_i}$. Define $n \in \mathbf{N}$ by:

$$n = \max(n_0, \ldots, n_{\alpha(f)-1})$$

Since $X_{n_i} \subseteq X_n$, we have $x(i) \in X_n$ for all $i \in \alpha(f)$. So $x \in X_n^{\alpha(f)}$. .

1.2.4 Generator of Universal Algebra

In this section, we prove that a free generator is also a generator. This is one case where considering the order $\omega : X \to \mathbf{N}$ on a free universal algebra X can be seen to be very useful.

Definition 11 *Let X be a universal algebra of type α and $X_0 \subseteq X$. We say that X_0 is a* generator *of X, if and only if $\langle X_0 \rangle = X$.*

Proposition 14 *Let X be a universal algebra of type α and $X_0 \subseteq X$. If X_0 is a free generator of X, then it is also a generator of X.*

Proof
Suppose X_0 is a free generator of X. We want to show that X_0 is a generator of X, i.e. that $\langle X_0 \rangle = X$. Suppose to the contrary that there exists $y \in X$ such that $y \notin \langle X_0 \rangle$. Let $\omega : X \to \mathbf{N}$ be the order on the free universal algebra X and consider the set:

$$A = \{\omega(y) : y \in X \ , \ y \notin \langle X_0 \rangle\}$$

Then A is a non-empty subset of $\mathbf{N}$ which therefore has a smallest element. So assume that $y \notin \langle X_0 \rangle$ corresponds to the smallest element of A. Since $X_0 \subseteq \langle X_0 \rangle$, it is clear that $y \notin X_0$. Since X is a free universal algebra, from theorem (2) of page 21 there exist $f \in \alpha$ and $x \in X^{\alpha(f)}$ such that $y = f(x)$. It follows from proposition (6) that:

$$\omega(y) = \omega(f(x)) = 1 + \max\{\omega(x(i)) : i \in \alpha(f)\}$$

In particular, we see that $\omega(x(i)) < \omega(y)$ for all $i \in \alpha(f)$. From the minimality of $\omega(y)$ it follows that $x(i) \in \langle X_0 \rangle$ for all $i \in \alpha(f)$. So $x \in \langle X_0 \rangle^{\alpha(f)}$. Note that this conclusion holds even if $\alpha(f) = 0$, and the argument presented is perfectly valid in that case. Now since $\langle X_0 \rangle$ is a universal sub-algebra of X, we conclude from $x \in \langle X_0 \rangle^{\alpha(f)}$ that $f(x) \in \langle X_0 \rangle$. So we have proved that $y \in \langle X_0 \rangle$ which contradicts the initial assumption. .

1.2.5 Proof by Structural Induction

We are all familiar with the notion of *proof by induction over* $\mathbf{N}$. Let ϕ be a formula of first order logic and u be a variable. In order to prove that $\phi[n/u]$ is true for all $n \in \mathbf{N}$, a *proof by induction over* $\mathbf{N}$ consists in proving first that $\phi[0/u]$ is true, and then proving the implication $\phi[n/u] \to \phi[n+1/u]$ for all $n \in \mathbf{N}$. A *proof by induction over* $\mathbf{N}$ is legitimate as the following is a theorem:

$$[\,\phi[0/u] \wedge (\forall n \in \mathbf{N} \ , \ \phi[n/u] \to \phi[n+1/u])\,] \to (\forall n \in \mathbf{N} \ , \ \phi[n/u]) \qquad (1.4)$$

Hence for every formula ϕ of first order logic and every variable u, we have a corresponding theorem (1.4). This correspondence may be called a *theorem schema*, in the same way that **ZFC** has a few *axiom schema*. If we denote $\texttt{Th}[\phi, u]$ the theorem obtained in (1.4) from the formula ϕ and the variable u, then the statement $\forall\phi\forall u\texttt{Th}[\phi, u]$ cannot be represented as a formula of first order logic, and is therefore not a *theorem*. It may be called a *meta-theorem*, which is a part of *meta-mathematics*. It is said that a meta-theorem can also become a theorem, but only as part of a wider formal system. There is something fundamentally disturbing about meta-theorems: most of us do not understand them. There is always a high level of discomfort when referring to *formulas of first order logic* and *variables* without having defined any of those terms. It is also problematic to use notations such as '$\phi[n/u]$' (ϕ with n in place of u) which is most likely not always meaningful: some form of restriction should probably be imposed on the variables u and n, unless maybe ϕ is viewed as an equivalence class rather than a string. The truth is we do not really know.

At the same time, there is something fascinating and magical about meta-mathematics: one of our favorite meta-theorems states that given a property $\phi[u]$, if there exists an ordinal β such that $\phi[\beta]$, then there exists a smallest ordinal with such property. This is powerful. This is not something we want to give up. And yet we hardly understand it, and it is not something we can prove. Suppose we had a compiler which would transform a high level mathematical statement into a formula of first order logic; suppose we had defined the notion of *mathematical proof* as a finite sequence of low level formulas satisfying certain properties. Then a meta-theorem would not be compiled and would not be proved. But we could use its *meta-proof* to *teach* our compiler to automatically generate the appropriate fragment of code needed to construct a proof of $\texttt{Th}[\phi, u]$ from the formula ϕ. There is light at the end of the tunnel.

In this section, we shall make little mention of the ordinals so as to keep as wide an audience as possible. As it turns out, every $n \in \mathbf{N}$ is an ordinal and the set $\mathbf{N}$ itself is an ordinal (also denoted ω), but what really matters is the fact already used before that every non-empty subset of $\mathbf{N}$ has a smallest element. Now suppose we want to prove theorem (1.4) given a formula ϕ and a variable u: we assume the left-hand-side of (1.4) is true. We then consider the set:

$$A = \{n \in \mathbf{N} : \neg\phi[n/u]\}$$

and we need to show that $A = \emptyset$. Note that the existence of the set A is a direct consequence of the Axiom Schema of Comprehension which makes the formula:

$$\forall\mathbf{N}\exists A[\forall n(n \in A \leftrightarrow (n \in \mathbf{N}) \wedge (\neg\phi[n/u]))]$$

an axiom of **ZFC**. Now suppose $A \neq \emptyset$. Then A is a non-empty subset of $\mathbf{N}$ which therefore has a smallest element, say $n \in \mathbf{N}$. Since $\phi[0/u]$ is true, we must have $n \neq 0$. So $n \geq 1$ and $n - 1 \in \mathbf{N}$. From the minimality of n, it follows that $\phi[n-1/u]$ is true. From the implication $\phi[n-1/u] \rightarrow \phi[n/u]$ we conclude that $\phi[n/u]$ is also true, contradicting the fact that $n \in A$. So we have shown that $A = \emptyset$, which completes the proof of theorem (1.4).

Because our proof was somehow parameterized with the formula ϕ, we could call it a *meta-proof*. So we have just produced a piece of meta-mathematics. However, this could have been avoided: when dealing with mathematical induction over $\mathbf{N}$, there is no need to consider a formula ϕ of first order predicate logic. Attempting to prove that a property is true for all $n \in \mathbf{N}$ is not fundamentally different from proving that a particular subset of $\mathbf{N}$, namely the subset on which the property is true coincide with the whole of $\mathbf{N}$. So let $Y \subseteq \mathbf{N}$ be a subset of $\mathbf{N}$. In order to prove that $Y = \mathbf{N}$, it is sufficient to show that $0 \in Y$ and furthermore that $(n \in Y) \to (n+1 \in Y)$ for all $n \in \mathbf{N}$. Indeed, the following is a theorem:

$$\forall Y \subseteq \mathbf{N} \ , \ [\,(0 \in Y) \wedge \forall n((n \in Y) \to (n+1 \in Y))\,] \to (Y = \mathbf{N}) \tag{1.5}$$

No more meta-mathematics, no more guilt. We are back to the solid grounds of standard mathematical arguments. We may be wrong and deluded in our beliefs, but we certainly lose the awareness of it. The proof of theorem (1.5) is essentially the same but without the disturbing reference to the formula ϕ: suppose the complement of Y in $\mathbf{N}$ is a non empty-set. It has a smallest element n which cannot be 0. From $n-1 \in Y$ we obtain $n \in Y$ which is a contradiction.

We can now resume our study of universal algebras and deal with the topic of *proof by structural induction*. Let X be a universal algebra of type α and suppose $X_0 \subseteq X$ is a generator of X. In order to prove that a property holds for all $y \in X$, it is sufficient to prove that the property is true for all $y \in X_0$ and furthermore given $f \in \alpha$ and $x \in X^{\alpha(f)}$, that the property is also true for $f(x)$ whenever it is true for all $x(i)$'s with $i \in \alpha(f)$. Just like in the case of induction over $\mathbf{N}$, it would be possible to consider a formula ϕ of first order predicate logic, and indulge in meta-mathematics. Instead, we shall safely quote:

Theorem 3 *Let X be a universal algebra of type α. Let $X_0 \subseteq X$ be a generator of X. Suppose $Y \subseteq X$ is a subset of X with the following properties:*

$$\begin{array}{ll} (i) & x \in X_0 \ \Rightarrow \ x \in Y \\ (ii) & (\forall i \in \alpha(f) \ , \ x(i) \in Y) \ \Rightarrow \ f(x) \in Y \end{array}$$

where (ii) holds for all $f \in \alpha$ and $x \in X^{\alpha(f)}$. Then $Y = X$.

Proof
We need to show that $Y = X$. From (i) we see immediately that $X_0 \subseteq Y$. Since X_0 is a generator of X, we have $\langle X_0 \rangle = X$. Consequently, it is sufficient to prove that Y is a universal sub-algebra of X, as this would imply that $\langle X_0 \rangle \subseteq Y$, and finally $X \subseteq Y$. In order to show that Y is a universal sub-algebra of X, consider $f \in \alpha$ and $x \in Y^{\alpha(f)}$. We need to prove that $f(x) \in Y$. From (ii), it is sufficient to show that $x(i) \in Y$ for all $i \in \alpha(f)$. This follows from $x \in Y^{\alpha(f)}$. **.**

Note that theorem (3) does not require X to be a free universal algebra, but simply that it should have a generator $X_0 \subseteq X$. Furthermore, if $f \in \alpha$ is such that $\alpha(f) = 0$, then (ii) reduces to $f(0) \in Y$. In other words, in order to prove that a property holds for every element of a universal algebra with constants, the least we can do is check that every constant has the required property.

1.2.6 Definition by Recursion over N

Our aim is to introduce the idea of *definition by structural recursion* on a free universal algebra of type α. We shall deal with the subject in a later section. In this section, we shall concentrate on a simpler notion, that of *definition by recursion over* $\mathbf{N}$, also known as *definition by simple recursion*. Consider the function $g : \mathbf{N} \to \mathbf{N}$ defined by $g(0) = 0$ and:

$$g(n+1) = (n+1).\, g(n)\ ,\ \forall n \in \mathbf{N}$$

The existence of the function g is often taken for granted. Most of us needed many years as mathematical students before it finally occurred that the truth of the following statement was far from obvious:

$$\exists g[\,(g : \mathbf{N} \to \mathbf{N}) \wedge (g(0) = 1) \wedge (\forall n \in \mathbf{N}\ ,\ g(n+1) = (n+1).\, g(n))\,]$$

Loosely speaking, defining a map g by recursion consists in first defining $g(0)$, and having defined $g(0)$, $g(1)$,$\ldots g(n-1)$, to then specify what $g(n)$ is *as a function of* all the preceding values $g(0)$, $g(1)$,$\ldots$, $g(n-1)$. More formally, suppose A is a set and we wish to define a map $g : \mathbf{N} \to A$ by recursion over $\mathbf{N}$. We first define $g(0) \in A$, and then define $g(n)$ as a function of $g_{|n}$. In other words, we set $g(n) = h(g_{|n})$ for some function h. Incidentally, the function h is called an *oracle function*, as it enables us to predict what the next value of g is, given all the preceding values. Of course, we want everything to make sense: so $h(g_{|n})$ should always be meaningful, and since our objective is to obtain $g : \mathbf{N} \to A$ in which case $g_{|n} \in A^n$ for all $n \in \mathbf{N}$, we should probably request that the oracle function be a map $h : \cup_{n\in\mathbf{N}} A^n \to A$. We could imagine an oracle function with a wider domain and a wider range (as long as $h(g_{|n})$ is a well defined element of A), but this is not likely to add much to the generality of the present discussion. So we shall stick to $h : \cup_{n\in\mathbf{N}} A^n \to A$. One thing to note is that the expression $g(n) = h(g_{|n})$ is also meaningful in the case of $n = 0$. It is therefore unnecessary to define $g(0)$ separately: just set $h(\emptyset)$ appropriately and request that $g(n) = h(g_{|n})$ for all $n \in \mathbf{N}$ rather than just $n \in \mathbf{N}^*$. In the above example of $g(n) = n!$ and $A = \mathbf{N}$, the oracle function $h : \cup_{n\in\mathbf{N}} \mathbf{N}^n \to \mathbf{N}$ should be defined by setting $h(\emptyset) = 1$ and for all $n \in \mathbf{N}^*$ and $g : n \to \mathbf{N}$:

$$h(g) = n.g(n-1)$$

Note that this definition is legitimate since $\mathbf{N}^n \cap \mathbf{N}^{n'} = \emptyset$ for $n \neq n'$.

We are now faced with a crucial question, namely that of the truth of the following statement, given a set A and an oracle function $h : \cup_{n\in\mathbf{N}} A^n \to A$.

$$\exists g[\,(g : \mathbf{N} \to A) \wedge (\forall n \in \mathbf{N}\ ,\ g(n) = h(g_{|n})\,]$$

This will be proved in the next lemma, together with the uniqueness of the function $g : \mathbf{N} \to A$. However before we proceed, a few comments are in order. The proof of lemma (4) below may appear daunting and tedious, as we systematically check a variety of small technical details. However, there is not

much to it. The key to remember is that a *recursion over* $\mathbf{N}$ is nothing but an *induction over* $\mathbf{N}$. Specifically, for all $n \in \mathbf{N}$, there must exist a map $g : n \to \mathbf{N}$ with the right property, for if there exists an $n \in \mathbf{N}$ for which this is not the case, choosing n to be the smallest of such integer, we can extend the map $g : (n-1) \to A$ using $g(n) = h(g_{|n})$ and obtain a map $g' : n \to A$ with the right property, thereby reaching a contradiction. Once the induction argument is complete, proving the existence of a map $g : \mathbf{N} \to A$ is easily done by gathering together all the ordered pairs contained in the various maps $g' : n \to A$ for $n \in \mathbf{N}$, which incidentally are extensions of one another.

Lemma 4 *Let A be a set and $h : \cup_{n \in \mathbf{N}} A^n \to A$ be a map. There exists a unique map $g : \mathbf{N} \to A$ such that $g(n) = h(g_{|n})$ for all $n \in \mathbf{N}$.*

Proof
First we prove the uniqueness property. Suppose $g, g' : \mathbf{N} \to A$ are maps such that $g(n) = h(g_{|n})$ and $g'(n) = h(g'_{|n})$ for all $n \in \mathbf{N}$. We need to show that $g = g'$, i.e. that $g(n) = g'(n)$ for all $n \in \mathbf{N}$. One way to achieve this is to prove that $g_{|n} = g'_{|n}$ for all $n \in \mathbf{N}$, for which we shall use an induction argument. Since $g_{|0} = \emptyset = g'_{|0}$ the property is true for $n = 0$. Suppose it is true for $n \in \mathbf{N}$. Then $g_{|n} = g'_{|n}$ and consequently $g(n) = h(g_{|n}) = h(g'_{|n}) = g'(n)$. Hence:

$$g_{|(n+1)} = g_{|n} \cup \{(n, g(n))\} = g'_{|n} \cup \{(n, g'(n))\} = g'_{|(n+1)}$$

and we see that the property is true for $n + 1$. This completes the proof of the uniqueness property. In order to prove the existence of $g : \mathbf{N} \to A$ with $g(n) = h(g_{|n})$ for all $n \in \mathbf{N}$, we shall first restrict our attention to finite domains and prove by induction the existence for all $n \in \mathbf{N}$ of a map $g : n \to A$ such that $g(k) = h(g_{|k})$ for all $k \in n$. This is clearly true for $n = 0$, since the empty set is a map $g : 0 \to A$ for which the condition $g(k) = h(g_{|k})$ for all $k \in 0$ is vacuously satisfied. So we assume $n \in \mathbf{N}$, and the existence of a map $g : n \to A$ such that $g(k) = h(g_{|k})$ for all $k \in n$. We need to show the existence of a map $g' : (n + 1) \to A$ such that $g'(k) = h(g'_{|k})$ for all $k \in n + 1$. Consider the map $g' : (n + 1) \to A$ defined by $g'_{|n} = g$ and $g'(n) = h(g)$, and suppose $k \in n + 1$. We need to check that $g'(k) = h(g'_{|k})$. If $k = n$, we need to check that $g'(n) = h(g'_{|n}) = h(g)$ which is true by definition of g'. If $k \in n$, then:

$$g'(k) = g'_{|n}(k) = g(k) = h(g_{|k}) = h(g'_{|k})$$

This completes our induction argument and for all $n \in \mathbf{N}$ we have proved the existence of a map $g : n \to A$ such that $g(k) = h(g_{|k})$ for all $k \in n$. In fact we claim that such a map is unique. For if $g' : n \to A$ is another such map, an identical induction argument to the one already used shows that $g(k) = g'(k)$ for all $k \in n$. Hence, for all $n \in \mathbf{N}$, we have proved the existence of a *unique* map $g_n : n \to A$ such that $g_n(k) = h((g_n)_{|k})$ for all $k \in n$. Note that from the uniqueness property we must have $(g_{n+1})_{|n} = g_n$ for all $n \in \mathbf{N}$. So every g_{n+1} is an extension of g_n. We are now in a position to prove the existence of a map

$g : \mathbf{N} \to A$ such that $g(n) = h(g_{|n})$ for all $n \in \mathbf{N}$, by considering $g = \cup_{n\in\mathbf{N}} g_n$. First we show that g is indeed a map. It is clearly a set of ordered pairs. Suppose $(x, y) \in g$ and $(x, y') \in g$. We need to show that $y = y'$. However, there exist $n, n' \in \mathbf{N}$ such that $(x, y) \in g_n$ and $(x, y') \in g_{n'}$. Without loss of generality, we may assume that $n \leq n'$. From the above uniqueness property, we must have $(g_{n'})_{|n} = g_n$. From $(x, y) \in g_n$ we obtain $x \in n$ and consequently:

$$y' = g_{n'}(x) = (g_{n'})_{|n}(x) = g_n(x) = y$$

So we have proved that g is indeed a map. It is clear that $\mathrm{dom}(g) = \mathbf{N}$ and $\mathrm{rng}(g) \subseteq A$. So g is a map $g : \mathbf{N} \to A$. It remains to check that $g(n) = h(g_{|n})$ for all $n \in \mathbf{N}$. So suppose $n \in \mathbf{N}$. Let $k \in n + 1$. Since $(k, g_{n+1}(k)) \in g_{n+1} \subseteq g$, we obtain $g_{n+1}(k) = g(k)$. It follows in particular that $(g_{n+1})_{|n} = g_{|n}$ and $g_{n+1}(n) = g(n)$. Since $g_{n+1}(k) = h((g_{n+1})_{|k})$ for all $k \in n + 1$ we conclude that:

$$g(n) = g_{n+1}(n) = h((g_{n+1})_{|n}) = h(g_{|n})$$

.

There is however one thing to note: the proof of lemma (4) tacitly makes use of the Axiom Schema of Replacement without any explicit mention of the fact. This is one other thing we usually take for granted. We have avoided any mention of the Axiom Schema of Replacement to keep the proof leaner, thereby following standard mathematical practice. However, considering the low level nature of the result being proved, we feel it is probably beneficial to say a few words about it, or else the whole proof could be construed as a cheat. At some point, we considered the set $g = \cup_{n\in\mathbf{N}} g_n$ which is really a notational shortcut for $g = \cup B$ where $B = \{g' : \exists n \in \mathbf{N}\ ,\ g' = g_n\}$. Recall that given a set z, the set $\cup z$ is defined as:

$$\cup z = \{x : \exists y\ ,\ (x \in y) \wedge (y \in z)\}$$

The existence of this set is guaranteed by the Axiom of Union. So it would seem that defining $g = \cup_{n\in\mathbf{N}} g_n$ is a simple application of the Axiom of Union and of course it is. But there is more to the story: we need to justify the fact that B is indeed a set and we have not done so. If we knew that $G : \mathbf{N} \to \cup_{n\in\mathbf{N}} A^n$ defined by $G(n) = g_n$ was a map, then B would simply be the range of G, i.e. $B = \mathrm{rng}(G)$. Showing that B is a set would still require the Axiom Schema of Replacement (as far as we can tell), but it would not be controversial to remain silent about it. But why is G not a map? Why can't we define $G : \mathbf{N} \to \cup_{n\in\mathbf{N}} A^n$ by setting $G(n) = g_n$ for all $n \in \mathbf{N}$? This is something we do all the time.

Consider $n \in \mathbf{N}$. We proved the existence and uniqueness of a map $g : n \to A$ such that $g(k) = h(g_{|k})$ for all $k \in n$. We then *labeled* this unique map as 'g_n'. In fact, we proved that the following formula of first order predicate logic:

$$G[n, g] = (n \in \mathbf{N}) \wedge [\,(g : n \to A) \wedge (\forall k \in n\ ,\ g(k) = h(g_{|k}))\,]$$

is a functional class with domain $\mathbf{N}$. We have not formally defined what a *functional class* is and we are not able to do so at this stage. Informally, G

is a functional class as a formula of first order predicate logic where two free variables n and g (in that order) have been singled out, and which satisfies:

$$\forall n \forall g \forall g' [\, G[n,g] \wedge G[n,g'] \rightarrow (g = g') \,]$$

where $G[n,g']$ has the *obvious* meaning. Note that G has other variables such as A and h, while $\mathbf{N}$ is a constant. The functional class G has a domain:

$$\mathrm{dom}(G)[n] = \exists g \, G[n,g]$$

which is itself a formula of first order predicate logic with the free variable n singled out, something which we should call a *class*. As it turns out, we have:

$$\forall n [\, \mathrm{dom}(G)[n] \leftrightarrow (n \in \mathbf{N}) \,]$$

which allows us to say that the functional class G has domain $\mathbf{N}$. In general, the domain of a functional class need not be a set. The functional class $G[n,g]$ also has a range, which is defined as the class:

$$\mathrm{rng}(G)[g] = \exists n \, G[n,g]$$

The Axiom Schema of Replacement asserts that if the domain of a functional class is a set, then its range is also a set. More formally:

$$\exists B \forall g [\, (g \in B) \leftrightarrow \mathrm{rng}(G)[g] \,]$$

which shows as requested, that $B = \{g' : \exists n \in \mathbf{N} \ , \ g' = g_n\}$ is indeed a set, since '$g' = g_n$' is simply a notational shortcut for '$G[n,g']$'. So much for proving that B is a set. We did not need to define a map $G : \mathbf{N} \rightarrow \cup_{n \in \mathbf{N}} A^n$ by setting $G(n) = g_n$ for all $n \in \mathbf{N}$. We considered a functional class instead. But the question still stands: the practice of casually defining a map $G : \mathbf{N} \rightarrow \cup_{n \in \mathbf{N}} A^n$ by setting $G(n) = g_n$ is very common. Surely, it is a legitimate practice. To avoid a confusing conflict of notation let us keep 'G' as referring to our functional class, and consider the map $G^* : \mathbf{N} \rightarrow \cup_{n \in \mathbf{N}} A^n$ defined by $G^*(n) = g_n$ for all $n \in \mathbf{N}$. What we are really saying is that G^* is the set of ordered pairs defined by $G^* = \{(n, g_n) : n \in \mathbf{N}\}$ or equivalently $G^* = \{(n,g) : G[n,g]\}$. This definition is legitimate provided G^* is really a set. More formally, we need to prove:

$$\exists G^* \forall z [\, (z \in G^*) \leftrightarrow \exists n \exists g [(z = (n,g)) \wedge G[n,g]] \,] \tag{1.6}$$

However, G is a functional class whose domain is the set $\mathbf{N}$, while its range is the set B. Hence, we have the implication $G[n,g] \rightarrow ((n,g) \in \mathbf{N} \times B)$, and it follows that (1.6) can equivalently be expressed as:

$$\exists G^* \forall z [\, (z \in G^*) \leftrightarrow (z \in \mathbf{N} \times B) \wedge \phi[z] \,] \tag{1.7}$$

where $\phi[z]$ stands for $\exists n \exists g [(z = (n,g)) \wedge G[n,g]]$. Since (1.7) is a direct consequence of the Axiom Schema of Comprehension, this completes our proof that G^* is indeed a set. So much for lemma (4).

Unfortunately, we are not in a position to close our discussion on the subject of *recursion over* $\mathbf{N}$. Yes we have lemma (4), of which we gave a rather detailed proof, including final meta-mathematical remarks which hopefully were as convincing as one could have made them. The truth is, lemma (4) is rather useless, as it does not do what we need: suppose we want to define the map g with domain $\mathbf{N}$, by setting $g(0) = \{0\}$ and $g(n+1) = \mathcal{P}(g(n))$ for all $n \in \mathbf{N}$. In order to apply lemma (4) we need to produce a set A. Yet we have no idea what the set A should be. So we are back to the very beginning of this section, asking the very same question as initially: does there exists a map g with domain $\mathbf{N}$ such that $g(0) = \{0\}$ and $g(n+1) = \mathcal{P}(g(n))$ for all $n \in \mathbf{N}$? Of course once we know that g exists, it is possible for us to produce a set A, namely $A = \text{rng}(g)$ or anything larger. We can define an oracle function $h : \cup_{n\in\mathbf{N}} A^n \to A$ by setting $h(\emptyset) = \{0\}$ and $h(g) = \mathcal{P}(g(n-1))$ for all $n \in \mathbf{N}^*$ and $g : n \to A$. At this stage, lemma (4) works like a dream. But it is clearly too late, as we needed to know the existence of g in the first place.

One may argue that defining $g(0) = \{0\}$ and $g(n+1) = \mathcal{P}(g(n))$ is not terribly useful, and it may be that lemma (4) is pretty much all we need in practice. But remember proposition (4) in which we claim to have constructed a free universal algebra of type α. We crucially defined the sequence $(Y_n)_{n\in\mathbf{N}}$ with a recursion over $\mathbf{N}$, by setting $Y_0 = \{(0, x) : x \in X_0\}$, $Y_{n+1} = Y_n \cup \bar{Y}_n$ and:

$$\bar{Y}_n = \left\{(1, (f, x)) : \ f \in \alpha \ , \ x \in Y_n^{\alpha(f)}\right\} \ , \ \forall n \in \mathbf{N}$$

Just as in the case of $g(n+1) = \mathcal{P}(g(n))$, it is not clear what set A should be used in order to apply lemma (4). We need something more powerful.

Let us go back to the initial problem: we would like to define a map g with domain $\mathbf{N}$ by first specifying $g(0)$, and having defined $g(0)$, $g(1)$, ..., $g(n-1)$, by specifying what $g(n)$ is *as a function of* $g(0)$, $g(1)$,..., $g(n-1)$. So we need an oracle function $h : \cup_{n\in\mathbf{N}} A^n \to A$ so as to be able to set $g(n) = h(g_{|n})$. Finding such an oracle function will not be an easy task without a set A. But why should A be a set? The only reason we insisted on A being a set was to keep clear of the flakiness of meta-mathematics. We wanted a theorem proper, namely lemma (4), with a solid proof based on a standard mathematical argument. In the case of induction, it was possible for us to stay within the realm of standard mathematics. When it comes to recursion, it would seem that we have no choice but to step outside of it.

So let us assume that A is a class, namely a formula of first order predicate logic with a variable x singled out. We could denote this class $A[x]$ to emphasize the fact that A is viewed as a *predicate* over the variable x. Of course, the formula A may have many other variables, and in fact x itself need not be a free variable of A. We could have $A[x] = \neg\bot$, also denoted $A[x] = \top$ or indeed:

$$A[x] = (\forall x(x \in x)) \vee \neg(\forall x(x \in x))$$

The class A is simply such that $\forall x A[x]$ is a true statement. This class is the *largest* possible, since $A[x]$ is true for all x. We could call $A[x]$ the *category of*

all sets also denoted **Set**, but we have no need to do so. Note that it is possible for this class to have x as a free variable, as in:

$$A[x] = (y \in x) \vee \neg(y \in x)$$

The good thing about having A as a class is that it no longer requires us to know what it is: if we have no idea as to which class to pick, we can simply decide that A is the class of all sets. Now we need an oracle function $h : \cup_{n\in\mathbf{N}} A^n \to A$. Since A is not a set but a class, we should be looking for a functional class $H : \cup_{n\in\mathbf{N}} A^n \to A$, rather than a function. But we hardly know what this means, and a few clarifications are in order: first of all, given a functional class $H[x, y]$, given two classes $A[x]$ and $B[x]$, we need to give meaning to the statement $H : B \to A$. Informally, this statement should indicate that H is a functional class with domain B and range *inside* A. The fact that $H[x, y]$ is a functional class is formally translated as:

$$\forall x \forall y \forall y' [\, H[x, y] \wedge H[x, y'] \to (y = y') \,]$$

The fact that H has domain B can be written as:

$$\forall x [\, B[x] \leftrightarrow \exists y (H[x, y]) \,]$$

and finally expressing that the range of H is *inside* A can be written as:

$$\forall y [\, \exists x (H[x, y]) \to A[y] \,]$$

So we now know what the statement $H : B \to A$ formally represents. If we intend to give meaning to $H : \cup_{n\in\mathbf{N}} A^n \to A$, we still need to spell out what the class $\cup_{n\in\mathbf{N}} A^n$ is. First we define the class $A^n[x]$ for $n \in \mathbf{N}$. Informally, $A^n[x]$ should indicate that x is a map with domain n and range *inside* A, i.e.:

$$A^n[x] = (x \text{ is a map}) \wedge (\mathrm{dom}(x) = n) \wedge \forall y [\, (y \in \mathrm{rng}(x) \to A[y]) \,]$$

Finally, the class $\cup_{n\in\mathbf{N}} A^n$ should be defined as:

$$\left(\cup_{n\in\mathbf{N}} A^n\right)[x] = \exists n [\, (n \in \mathbf{N}) \wedge A^n[x] \,]$$

So the statement $H : \cup_{n\in\mathbf{N}} A^n \to A$ is now meaningful. So suppose it is true. We are looking for a map $g : \mathbf{N} \to A$ such that $g(n) = H(g_{|n})$ for all $n \in \mathbf{N}$. Things are starting to be clearer. The statement $g : \mathbf{N} \to A$ is clearly represented by:

$$(g \text{ is a map}) \wedge (\mathrm{dom}(g) = \mathbf{N}) \wedge \forall y [\, (y \in \mathrm{rng}(g) \to A[g]) \,]$$

while the statement $g(n) = H(g_{|n})$ is an intuitive way of saying $H[g_{|n}, g(n)]$. Furthermore, if we have $H : \cup_{n\in\mathbf{N}} A^n \to A$ and $g : \mathbf{N} \to A$, then for all $n \in A$ it is easy to check that $g_{|n} : n \to A$, by which we mean that $A^n[g_{|n}]$ is true. It follows that $\mathrm{dom}(H)[g_{|n}]$ is true, and consequently since H is functional, there exists a unique y_n such that $H[g_{|n}, y_n]$, which furthermore is such that $A[y_n]$ is

true. We would like $g : \mathbf{N} \to A$ to be such that $g(n)$ is precisely that unique y_n, for all $n \in \mathbf{N}$. So it all makes sense.

As an example, let us go back to the case when $g(n+1) = \mathcal{P}(g(n))$ for all $n \in \mathbf{N}$ with $g(0) = \{0\}$. Because we have no idea what the class A should be, let us pick A to be the class of all sets. We need to find an oracle functional class $H : \cup_{n\in\mathbf{N}} A^n \to A$ which correctly sets up our recursion objective. Informally speaking, we want $H(\emptyset) = \{0\}$ and $H(g) = \mathcal{P}(g(n-1))$ for all $n \in \mathbf{N}^*$ and $g : n \to A$. If we want to formally code up the functional class $H[g, y]$ as a formula of first order predicate logic, since $A^0[g] = (g = \emptyset)$, this can be done as:

$$H[g, y] = [A^0[g] \wedge (y = \{0\})] \vee \exists n[(n \in \mathbf{N}^*) \wedge A^n[g] \wedge (y = \mathcal{P}(g(n-1)))]$$

The fundamental question is this: does there exist a map g with domain $\mathbf{N}$ such that $g(n) = H(g_{|n})$ for all $n \in \mathbf{N}$? This is the object of meta-theorem (1) below.

Before, we proceed with the proof of meta-theorem (1), a few remarks may be in order: we were compelled by the nature of the problem to indulge in a fair amount of meta-mathematical discussions, i.e. discussions involving formulas of first order logic, variables, classes and functional classes, terms which have not been defined anywhere. This of course falls very short of the usually accepted standards of mathematical proof. It is however better than nothing at all. We do not have the conceptual tools to do much more at this stage. It is hoped that the study of universal algebras and the introduction of formal languages as algebraic structures will eventually allow us to handle meta-mathematics without the hand waving. For now, we did everything we could and were as careful as possible in attempting to give legitimacy to the principle of recursion over $\mathbf{N}$. So we shall accept the existence of a sequence $(Y_n)_{n\in\mathbf{N}}$ such that $Y_{n+1} = Y_n \cup \bar{Y}_n$ for all $n \in \mathbf{N}$, where:

$$\bar{Y}_n = \left\{(1, (f, x)) : \ f \in \alpha \ , \ x \in Y_n^{\alpha(f)}\right\} \ , \ \forall n \in \mathbf{N}$$

with the belief the existence of $(Y_n)_{n\in\mathbf{N}}$ could be formally proven within **ZFC**, if we precisely knew what that means. If it so happens that one of our conclusions is wrong, it is very likely that the error will be caught at some point, once we have clarified the ideas of formal languages and formal proofs.

Metatheorem 1 *Let A be a class and $H : \cup_{n\in\mathbf{N}} A^n \to A$ be a functional class. There exists a unique map $g : \mathbf{N} \to A$ such that $g(n) = H(g_{|n})$ for all $n \in \mathbf{N}$.*

Proof
First we prove the uniqueness property. Suppose $g, g' : \mathbf{N} \to A$ are maps such that $g(n) = H(g_{|n})$ and $g'(n) = H(g'_{|n})$ for all $n \in \mathbf{N}$. We need to show that $g = g'$, i.e. that $g(n) = g'(n)$ for all $n \in \mathbf{N}$. One way to achieve this is to prove that $g_{|n} = g'_{|n}$ for all $n \in \mathbf{N}$, for which we shall use an induction argument. Since $g_{|0} = \emptyset = g'_{|0}$ the property is true for $n = 0$. Suppose it is true for $n \in \mathbf{N}$. Then $g_{|n} = g'_{|n}$ and consequently $g(n) = H(g_{|n}) = H(g'_{|n}) = g'(n)$. Hence:

$$g_{|(n+1)} = g_{|n} \cup \{(n, g(n))\} = g'_{|n} \cup \{(n, g'(n))\} = g'_{|(n+1)}$$

and we see that the property is true for $n+1$. This completes the proof of the uniqueness property. In order to prove the existence of $g : \mathbf{N} \to A$ with $g(n) = H(g_{|n})$ for all $n \in \mathbf{N}$, we shall first restrict our attention to finite domains and prove by induction the existence for all $n \in \mathbf{N}$ of a map $g : n \to A$ such that $g(k) = H(g_{|k})$ for all $k \in n$. This is clearly true for $n = 0$, since the empty set is a map $g : 0 \to A$ for which the condition $g(k) = H(g_{|k})$ for all $k \in 0$ is vacuously satisfied. So we assume $n \in \mathbf{N}$, and the existence of a map $g : n \to A$ such that $g(k) = H(g_{|k})$ for all $k \in n$. We need to show the existence of a map $g' : (n+1) \to A$ such that $g'(k) = H(g'_{|k})$ for all $k \in n+1$. Consider the map $g' : (n+1) \to A$ defined by $g'_{|n} = g$ and $g'(n) = H(g)$, and suppose $k \in n+1$. We need to check that $g'(k) = H(g'_{|k})$. If $k = n$, we need to check that $g'(n) = H(g'_{|n}) = H(g)$ which is true by definition of g'. If $k \in n$, then:

$$g'(k) = g'_{|n}(k) = g(k) = H(g_{|k}) = H(g'_{|k})$$

This completes our induction argument and for all $n \in \mathbf{N}$ we have proved the existence of a map $g : n \to A$ such that $g(k) = H(g_{|k})$ for all $k \in n$. In fact we claim that such a map is unique. For if $g' : n \to A$ is another such map, an identical induction argument to the one already used shows that $g(k) = g'(k)$ for all $k \in n$. Hence, for all $n \in \mathbf{N}$, we have proved the existence of a *unique* map $g : n \to A$ such that $g(k) = H(g_{|k})$ for all $k \in n$. It follows that:

$$G[n, g] = (n \in \mathbf{N}) \wedge [\, (g : n \to A) \wedge (\forall k \in n \ ,\ g(k) = H(g_{|k}))\,]$$

is a functional class with domain $\mathbf{N}$. From the Axiom Schema of Replacement:

$$\mathrm{rng}(G) = \{g : \exists n \in \mathbf{N} \ ,\ G[n, g]\}$$

is therefore a set. We define $g = \cup \mathrm{rng}(G)$ and we shall complete our proof by showing that $g : \mathbf{N} \to A$ is a map such that $g(n) = H(g_{|n})$ for all $n \in \mathbf{N}$. First we show that g is a set of ordered pairs. Let $z \in g$. There exists $g' \in \mathrm{rng}(G)$ such that $z \in g'$. Since $g' \in \ rng(G)$, we have $G[n, g']$ for some $n \in \mathbf{N}$. It follows that $g' : n \to A$ and in particular g' is a set of ordered pairs. From $z \in g'$ we see that z is an ordered pair. We then show that g is functional. So we assume that $(x, y) \in g$ and $(x, y') \in g$. We need to show that $y = y'$. Since $g = \cup \mathrm{rng}(G)$, there exist $g_1, g_2 \in \mathrm{rng}(G)$ such that $(x, y) \in g_1$ and $(x, y') \in g_2$. Furthermore, there exist $n_1, n_2 \in \mathbf{N}$ such that $G[n_1, g_1]$ and $G[n_2, g_2]$. Without loss of generality we may assume that $n_1 \leq n_2$. From $G[n_2, g_2]$ it is not difficult to show that $G[n_1, (g_2)_{|n_1}]$ is also true. Since G is functional, it follows that $g_1 = (g_2)_{|n_1}$. From $(x, y) \in g_1$ and $g_1 : n_1 \to A$ we obtain $x \in n_1$. Hence:

$$y' = g_2(x) = (g_2)_{|n_1}(x) = g_1(x) = y$$

We now show that $\mathrm{dom}(g) = \mathbf{N}$. First we show that $\mathbf{N} \subseteq \mathrm{dom}(g)$. So let $n \in \mathbf{N}$. We need to show that $n \in \mathrm{dom}(g)$. However, the functional class G has domain $\mathbf{N}$. In particular, there exists g' such that $G[n+1, g']$ is true. From $g' : (n+1) \to A$ we see that $(n, g'(n)) \in g'$. Furthermore, from $G[n+1, g']$ we see

that $g' \in \text{rng}(G)$. Since $g = \cup \text{rng}(G)$, we conclude that $(n, g'(n)) \in g$, and in particular $n \in \text{dom}(g)$. We now prove that $\text{dom}(g) \subseteq \mathbf{N}$. So let $x \in \text{dom}(g)$. We need to show that $x \in \mathbf{N}$. However, there exists y such that $(x, y) \in g$. Hence, there exists $g' \in \text{rng}(G)$ such that $(x, y) \in g'$. Furthermore, there exists $n \in \mathbf{N}$ such that $G[n, g']$ is true. In particular, we have $g' : n \to A$ and we conclude from $(x, y) \in g'$ that $x \in n \subseteq \mathbf{N}$. So $x \in \mathbf{N}$. In order to show that $g : \mathbf{N} \to A$, it remains to check that $A[g(n)]$ is true for all $n \in \mathbf{N}$. So let $n \in \mathbf{N}$. We need to show that $A[g(n)]$ is true. However $n \in n+1$ and since G has domain $\mathbf{N}$, there exists g' such that $G[n+1, g']$. From $g' : (n+1) \to A$ we obtain $(n, g'(n)) \in g'$. Furthermore, $A[g'(n)]$ is true. From $G[n+1, g']$ we obtain $g' \in \text{rng}(G)$, and it follows that $(n, g'(n)) \in g$. Hence we see that $g'(n) = g(n)$ and since $A[g'(n)]$ is true we conclude that $A[g(n)]$ is also true. So we have proved that $g : \mathbf{N} \to A$ is a map. It remains to check that $g(n) = H(g_{|n})$ for all $n \in \mathbf{N}$. So let $n \in \mathbf{N}$. We need to show that $g(n) = H(g_{|n})$. Consider once more the map $g' \in \text{rng}(G)$ such that $G[n+1, g']$ is true. Since $g' : (n+1) \to A$, for all $k \in n+1$ we have $(k, g'(k)) \in g'$ and consequently $(k, g'(k)) \in g$. It follows that $g'(k) = g(k)$ for all $k \in n+1$, and we see that $g'_{|n} = g_{|n}$ as well as $g'(n) = g(n)$. From $G[n+1, g']$ we also have $g'(k) = H(g'_{|k})$ for all $k \in n+1$. In particular, we have:

$$g(n) = g'(n) = H(g'_{|n}) = H(g_{|n})$$

.

1.2.7 Definition by Structural Recursion

Let $\alpha = \{(0,1), (1,2)\}$ and X_0 be a set. We know from theorem (1) of page 20 that there exists a free universal algebra X of type α whose free generator is X_0. Let us denote $\neg : X^1 \to X$ and $\wedge : X^2 \to X$ the two operators on X. This particular choice of notations should invite us to view X as a free universal algebra of *propositional logic*. We know from theorem (2) of page 21 that any *proposition* ϕ of X is either an *atomic proposition* $\phi = p$ for some $p \in X_0$, or the *negation* of a proposition $\phi = \neg\phi_1$ or the *conjunction* of two propositions $\phi = \phi_1 \wedge \phi_2$. These three cases are exclusive, and these representations are unique. In effect, the free universal algebra X is partitioned into three parts $X = X_0 \uplus X_\neg \uplus X_\wedge$. If A is a set, then any map $g : X \to A$ could be defined by specifying the three restrictions $g_{|X_0}$, $g_{|X_\neg}$ and $g_{|X_\wedge}$ separately. We saw from proposition (6) that the order $\omega : X \to \mathbf{N}$ had this sort of three-fold structure:

$$\forall \phi \in X \ , \ \omega(\phi) = \begin{cases} 0 & \text{if} \quad \phi = p \in X_0 \\ 1 + \omega(\phi_1) & \text{if} \quad \phi = \neg\phi_1 \\ 1 + \max(\omega(\phi_1), \omega(\phi_2)) & \text{if} \quad \phi = \phi_1 \wedge \phi_2 \end{cases} \tag{1.8}$$

However, we did not invoke equation (1.8) as a definition of the order $\omega : X \to \mathbf{N}$ as this would not guarantee the existence of ω. This is very similar to the simple recursion problem: defining a map $g : \mathbf{N} \to \mathbf{N}$ by setting $g(0) = 1$ and $g(n+1) = (n+1).g(n)$ does not in itself guarantee the existence of g. We now know that g exists, but we needed to justify the principle of *definition by*

recursion over $\mathbf{N}$ in the form of lemma (4) and meta-theorem (1) of page 38. Equation (1.8) is clearly recursive as it links $\omega(\phi)$ on the left-hand-side to other values $\omega(\phi_1)$ and $\omega(\phi_2)$ assigned by the map ω to other points. It is not obvious that ω exists so we had to find some other way to define it. And yet we may feel there is nothing wrong with equation (1.8). From a computing point of view, it seems pretty obvious that any computation of $\omega(\phi)$ would terminate. For instance taking $\phi = \neg(p_1 \wedge ((\neg p_2) \wedge p_3))$, equation (1.8) would lead to:

$$\begin{aligned}
\omega(\phi) &= \omega(\neg(p_1 \wedge ((\neg p_2) \wedge p_3))) \\
&= 1 + \omega(p_1 \wedge ((\neg p_2) \wedge p_3)) \\
&= 2 + \max(\omega(p_1), \omega((\neg p_2) \wedge p_3)) \\
&= 2 + \omega((\neg p_2) \wedge p_3) \\
&= 3 + \max(\omega(\neg p_2), \omega(p_3)) \\
&= 3 + \omega(\neg p_2) \\
&= 4 + \omega(p_2) \\
&= 4
\end{aligned}$$

Equation (1.8) is a case of *definition by structural recursion*. There are many natural mappings on X which could be defined in a similar way. For instance, suppose we needed a map $g : X \to \mathcal{P}(X_0)$ returning the set of all atomic propositions involved in a formula $\phi \in X$. In the case of $\phi = \neg(p_1 \wedge ((\neg p_2) \wedge p_3))$, we would have $g(\phi) = \{p_1, p_2, p_3\}$. A natural way to define the map g is:

$$\forall \phi \in X \ , \ g(\phi) = \begin{cases} \{p\} & \text{if} \quad \phi = p \in X_0 \\ g(\phi_1) & \text{if} \quad \phi = \neg\phi_1 \\ g(\phi_1) \cup g(\phi_2) & \text{if} \quad \phi = \phi_1 \wedge \phi_2 \end{cases} \tag{1.9}$$

As another example, suppose we had a truth table $v : X_0 \to \{0, 1\}$ indicating whether an atomic proposition p is true ($v(p) = 1$) or false ($v(p) = 0$) for all $p \in X_0$. We would like to define a map $g : X \to \{0, 1\}$ indicating whether a proposition ϕ is true ($g(\phi) = 1$) or false ($g(\phi) = 0$). Once again, it is natural to define the map g using structural recursion:

$$\forall \phi \in X \ , \ g(\phi) = \begin{cases} v(p) & \text{if} \quad \phi = p \in X_0 \\ 1 - g(\phi_1) & \text{if} \quad \phi = \neg\phi_1 \\ g(\phi_1).g(\phi_2) & \text{if} \quad \phi = \phi_1 \wedge \phi_2 \end{cases} \tag{1.10}$$

We know that equations (1.9) and (1.10) are fine: we just need to prove it.

So let us go back to a more general setting and consider a free universal algebra X of type α with free generator $X_0 \subseteq X$. Let A be a set. We would like to define a map $g : X \to A$ by structural recursion. We know from theorem (2) of page 21 that any element of X is either an element of X_0, or an element of the form $f(x)$ for some unique $f \in \alpha$ and $x \in X^{\alpha(f)}$. Defining $g : X \to A$ by structural recursion consists first in specifying $g(x)$ for all $x \in X_0$. So we need a map $g_0 : X_0 \to A$ with the understanding that $g(x) = g_0(x)$ for all $x \in X_0$. For all $f \in \alpha$ and $x \in X^{\alpha(f)}$, we then want to specify $g(f(x))$ as a function of

all the individual $g(x(i))$'s for all $i \in \alpha(f)$. So we need a map $h(f) : A^{\alpha(f)} \to A$ with the understanding that $g(f(x)) = h(f)(g(x))$. Note that if $\alpha(f) = 0$, this amounts to having a map $h(f) : \{0\} \to A$ and requesting that $g(f(0)) = h(f)(0)$. In other words, it amounts to specifying the value $h(f)(0)$ assigned by the map g to the constant $f(0)$. We are now in a position to ask the key question: given a map $g_0 : X_0 \to A$ and given a map $h(f) : A^{\alpha(f)} \to A$ for all $f \in \alpha$, does there exist a map $g : X \to A$ such that $g_{|X_0} = g_0$ and $g(f(x)) = h(f)(g(x))$ for all $f \in \alpha$ and $x \in X^{\alpha(f)}$? This question is dealt with in the following theorem.

To prove theorem (4), we are effectively resorting to the same trick as the one used to define the order $\omega : X \to \mathbf{N}$ in definition (8): once we give ourselves a map $h(f) : A^{\alpha(f)} \to A$ for all $f \in \alpha$, we are effectively specifying a structure of universal algebra of type α on A, and requesting that $g(f(x)) = h(f)(g(x))$ is simply asking that $g : X \to A$ be a morphism. The existence of g such that $g_{|X_0} = g_0$ is guaranteed by the fact that X_0 is a free generator of X.

Theorem 4 *Let X be a free universal algebra of type α with free generator $X_0 \subseteq X$. Let A be a set and $g_0 : X_0 \to A$ be a map. Let h be a map with domain α such that $h(f)$ is a map $h(f) : A^{\alpha(f)} \to A$ for all $f \in \alpha$. Then, there exists a unique map $g : X \to A$ such that:*

$$\begin{array}{ll} (i) & x \in X_0 \ \Rightarrow g(x) = g_0(x) \\ (ii) & x \in X^{\alpha(f)} \ \Rightarrow g(f(x)) = h(f)(g(x)) \end{array}$$

where (ii) holds for all $f \in \alpha$.

Proof
Since h is a map with domain α and we have $h(f) : A^{\alpha(f)} \to A$ for all $f \in \alpha$, the ordered pair (A, h) is in fact a universal algebra of type α. Since $g_0 : X \to A$ is a map and X is a free universal algebra of type α with free generator X_0, there exists a unique morphism $g : X \to A$ such that $g_{|X_0} = g_0$. From this last equality, we see that (i) is satisfied. Since g is a morphism, for all $f \in \alpha$ and $x \in X^{\alpha(f)}$ we have:

$$g(f(x)) = g \circ f(x) = h(f) \circ g(x) = h(f)(g(x))$$

where it is understood that '$g(x)$' on the right-hand-side of this equation refers to the element of $A^{\alpha(f)}$ defined by $g(x)(i) = g(x(i))$ for all $i \in \alpha(f)$. Hence we see that (ii) is satisfied by $g : X \to A$ for all $f \in \alpha$. So we have proved the existence of $g : X \to A$ such that (i) and (ii) holds for all $f \in \alpha$. Suppose $g' : X \to A$ is another map with such property. Then g' is clearly a morphism with $g'_{|X_0} = g_0$ and it follows from the uniqueness of g that $g' = g$. **.**

This was disappointingly simple. One would have expected the principle of *definition by structural recursion* to be a lot more complicated than that of recursion over $\mathbf{N}$. And it can be. We effectively restricted ourselves to the simple case of $g : X \to A$ where A is a set rather than a class, and $g(f(x))$ is simply a function of the $g(x(i))$'s. This would be similar to considering $g : \mathbf{N} \to A$ given a set A, and requesting that $g(n) = h \circ g(n-1)$ rather than

$g(n) = h(g_{|n})$. Anticipating on future events, suppose X is a free algebra of first order logic, generated by atomic propositions $(x \in y)$ (with x, y belonging to a set of *variables* V), with the constant $\bot$, the binary operator $\to$ and a unary quantification operator $\forall x$ for every variable $x \in V$. Given a set M with a binary relation $r \subseteq M \times M$ and a map $a : V \to M$ (a *variables assignment*), a natural thing to ask is which of the formulas $\phi \in X$ are *true* with respect to the model (M, r) under the assignment $a : V \to M$. In other words, it is very tempting to define a truth function $g_a : X \to 2 = \{0, 1\}$ with the formula:

$$g_a(\phi) = \begin{cases} 1_r(\, a(x), a(y)\,) & \text{if} \quad \phi = (x \in y) \\ 0 & \text{if} \quad \phi = \bot \\ g_a(\phi_1) \to g_a(\phi_2) & \text{if} \quad \phi = \phi_1 \to \phi_2 \\ \min\{\, g_b(\phi_1) \;:\; b = a \text{ on } V \setminus \{x\}\,\} & \text{if} \quad \phi = \forall x \phi_1 \end{cases}$$

being understood that $g_a(\phi_1) \to g_a(\phi_2)$ is the usual $\neg g_a(\phi_1) \vee g_a(\phi_2)$ in $\{0, 1\}$. This definition of the concept of *truth* will be seen to be flawed: it is clear enough at this stage that theorem (4) will not be directly applicable to this case, since we are attempting to define $g_a : X \to 2$ in terms of other functions $g_b : X \to 2$. We will need to find some other way to prove the existence of g_a. Going back to propositional logic, another possible example is the following:

$$\forall \phi \in X \;,\; g(\phi) = \begin{cases} \{0\} & \text{if} \quad \phi = p \in X_0 \\ \mathcal{P}(g(\phi_1)) & \text{if} \quad \phi = \neg \phi_1 \\ g(\phi_1) \times g(\phi_2) & \text{if} \quad \phi = \phi_1 \wedge \phi_2 \end{cases} \tag{1.11}$$

This would constitute a case when theorem (4) fails to be applicable, as there is no obvious set A for $g : X \to A$. We shall not provide a meta-theorem for this.

We shall however now provide a stronger version of theorem (4) which will be required at a later stage of this document. For example, when studying the Hilbert deductive system on the free algebra of first order predicate logic $\mathbf{P}(V)$, we shall define the notion of *proofs* as elements of another free algebra $\mathbf{\Pi}(V)$, which in turn will lead to the following recursion:

$$\forall \pi \in \mathbf{\Pi}(V) \;,\; \mathrm{Val}(\pi) = \begin{cases} \phi & \text{if} \quad \pi = \phi \in \mathbf{P}(V) \\ \phi & \text{if} \quad \pi = \partial\phi,\ \phi \in \mathbf{A}(V) \\ \bot \to \bot & \text{if} \quad \pi = \partial\phi,\ \phi \notin \mathbf{A}(V) \\ M(\mathrm{Val}(\pi_1), \mathrm{Val}(\pi_2)) & \text{if} \quad \pi = \pi_1 \oplus \pi_2 \\ \forall x \mathrm{Val}(\pi_1) & \text{if} \quad \pi = \nabla x \pi_1,\ x \notin \mathrm{Sp}(\pi_1) \\ \bot \to \bot & \text{if} \quad \pi = \nabla x \pi_1,\ x \in \mathrm{Sp}(\pi_1) \end{cases}$$

when attempting to define $\mathrm{Val}(\pi)$ as representing the conclusion being proved by the proof π. The details of this definition are not important at this stage, but we should simply notice that given a variable x and the associated unary operator $\nabla x : \mathbf{\Pi}(V) \to \mathbf{\Pi}(V)$, we were unable to define $\mathrm{Val}(\nabla x \pi_1)$ simply in terms of $\mathrm{Val}(\pi_1)$ as an application of theorem (4) would require. The definition of $\mathrm{Val}(\nabla x \pi_1)$ is also based on whether $x \in \mathrm{Sp}(\pi_1)$, i.e. on whether x is a free variable of the premises involved in the proof π_1. Going back to the general

setting of an arbitrary free algebra X of type α, this is therefore a case when given $f \in \alpha$ and $x \in X^{\alpha(f)}$, $g(f(x))$ is not simply defined in terms of $g(x)$, but is also based on x itself. So we would like to set $g(f(x)) = h(f)(g(x), x)$ rather than the more restrictive $g(f(x)) = h(f)(g(x))$ of theorem (4).

The proof of the following theorem is identical in spirit to that of Lemma (4). The only new idea is the introduction of the subsets $X_n \subseteq X$ of proposition (7):

$$X_n = \{x \in X \ : \ \omega(x) \leq n\} \ , \ n \in \mathbf{N}$$

where $\omega : X \to \mathbf{N}$ is the order mapping of definition (8) which allows to reduce our problem to that of induction over $\mathbf{N}$. Once we have shown the existence of maps $g_n : X_n \to A$ with the right property, and which are extensions of one another, we prove the existence of the larger map $g : X \to A$ simply by collecting the appropriate ordered pairs in one single set $g = \cup_{n \in \mathbf{N}} g_n$. Note that it is probably possible to prove theorem (5) using lemma (4) rather than duplicating what is essentially the same argument.

Theorem 5 *Let X be a free universal algebra of type α with free generator $X_0 \subseteq X$. Let A be a set and $g_0 : X_0 \to A$ be a map. Let h be a map with domain α such that $h(f)$ is a map $h(f) : A^{\alpha(f)} \times X^{\alpha(f)} \to A$ for all $f \in \alpha$. Then, there exists a unique map $g : X \to A$ such that:*

$$\begin{array}{ll} (i) & x \in X_0 \ \Rightarrow g(x) = g_0(x) \\ (ii) & x \in X^{\alpha(f)} \ \Rightarrow g(f(x)) = h(f)(g(x), x) \end{array}$$

where (ii) holds for all $f \in \alpha$.

Proof
We shall first prove the uniqueness property. So suppose $g, g' : X \to A$ are two maps satisfying (i) and (ii) above. We need to show that $g = g'$ or equivalently that $g(x) = g'(x)$ for all $x \in X$. We shall do so using a structural induction argument based on theorem (3) of page 31. Since X_0 is a generator of X, we shall first check this is the case when $x \in X_0$. This follows immediately from (i) and $g(x) = g_0(x) = g'(x)$. We proceed with our induction argument by considering an arbitrary $f \in \alpha$ and assuming $x \in X^{\alpha(f)}$ is such that $g(x(i)) = g'(x(i))$ for all $i \in \alpha(f)$. We need to show that $g(f(x)) = g'(f(x))$. Recall that the notation $g(x)$ in (ii) above refers to the element of $A^{\alpha(f)}$ defined by $g(x)(i) = g(x(i))$ for all $i \in \alpha(f)$. In the case when $\alpha(f) = 0$ we have $g(x) = 0$. So with this in mind and a similar notational convention for $g'(x)$, our hypothesis leads to $g(x) = g'(x)$, and using (ii) above we obtain:

$$g(f(x)) = h(f)(g(x), x) = h(f)(g'(x), x) = g'(f(x))$$

This completes our induction argument and the proof of uniqueness. We shall now prove the existence of the map $g : X \to A$. We define:

$$X_n = \{x \in X \ : \ \omega(x) \leq n\} \ , \ n \in \mathbf{N}$$

where $\omega : X \to \mathbf{N}$ is the order on X as per definition (8). Note that from proposition (6) we have $x \in X_0 \;\Leftrightarrow\; \omega(x) = 0$ so this new definition does not conflict with the notation X_0 used for the free generator on X. We now consider the subset $Y \subseteq \mathbf{N}$ of all $n \in \mathbf{N}$ which satisfy the property that there exists a unique map $g_n : X_n \to A$ such that:

$$\begin{aligned} &(iii) \qquad x \in X_0 \;\Rightarrow g_n(x) = g_0(x) \\ &(iv) \qquad f(x) \in X_n \;\Rightarrow g_n(f(x)) = h(f)(g_n(x), x) \end{aligned}$$

where (iv) holds for all $f \in \alpha$ and $x \in X^{\alpha(f)}$. In order to prove the existence of the map $g : X \to A$, it is sufficient to prove that $Y = N$. We shall first prove this is the case. So suppose $Y = \mathbf{N}$. We need to show the existence of the map $g : X \to A$. Define $g = \cup_{n \in N} g_n$. Each g_n being a map is a set of ordered pairs. So g is also a set of ordered pairs. In fact, it is a functional set of ordered pairs:

$$\forall x, y, y' \;,\; ((x, y) \in g) \wedge ((x, y') \in g) \;\Rightarrow\; (y = y')$$

Suppose this is true for the time being. Then g is a map. Furthermore, since $g_n : X_n \to A$ and $X_n \subseteq X$ for all $n \in \mathbf{N}$ we have:

$$(x, y) \in g \;\Rightarrow\; \exists n \in \mathbf{N}[(x, y) \in g_n] \;\Rightarrow\; (x \in X) \wedge (y \in A)$$

So it is clear that $\mathrm{dom}(g) \subseteq X$ and $\mathrm{rng}(g) \subseteq A$. In fact, since every $x \in X$ is an element of X_n for any $n \geq \omega(x)$, we have $\mathrm{dom}(g) = X$ and we conlude that $g : X \to A$. In order to prove the existence of $g : X \to A$ it remains to show that (i) and (ii) above are satisfied. So let $x \in X_0$. From $(x, g_0(x)) \in g_0 \subseteq g$ it follows immediately that $g(x) = g_0(x)$ which shows that (i) is indeed true. Let $f \in \alpha$ and $x \in X^{\alpha(f)}$. Picking $n \in \mathbf{N}$ large enough so that $f(x) \in X_n$ we obtain $(f(x), g_n(f(x))) \in g_n \subseteq g$ from which we conclude that $g(f(x)) = g_n(f(x))$. Furthermore, for all $i \in \alpha(f)$ from proposition (6) we have $\omega(f(x)) \geq \omega(x(i))$ which shows that $x(i) \in X_n$ and consequently $(x_i, g_n(x(i))) \in g_n \subseteq g$ i.e. $g(x(i)) = g_n(x(i))$. This being true for all $i \in \alpha(f)$, we obtain $g(x) = g_n(x)$, an equality which is still true when $\alpha(f) = 0$. Hence, using (iv) above we have:

$$g(f(x)) = g_n(f(x)) = h(f)(g_n(x), x) = h(f)(g(x), x)$$

which shows that (ii) is indeed true. This completes the proof of the existence of $g : X \to A$ having admitted that g is a functional relation. We shall now go back to this particular point and show that g is indeed functional. So let x, y, y' be sets and assume that $(x, y) \in g$ and $(x, y') \in g$. We need to show that $y = y'$. Let $n \in \mathbf{N}$ be the smallest integer such that $(x, y) \in g_n$ and likewise let $n' \in \mathbf{N}$ be the smallest integer such that $(x, y') \in g_{n'}$. Without loss of generality, we may assume that $n \leq n'$ and consequently $X_n \subseteq X_{n'}$. Consider the restriction $(g_{n'})_{|X_n} : X_n \to A$. Since $g_{n'} : X_{n'} \to A$ satisfies (iii) and (iv) above for n', for all $z \in X_0$ we have $(g_{n'})_{|X_n}(z) = g_{n'}(z) = g_0(z)$ and furthermore given $f \in \alpha$ and $z \in X^{\alpha(f)}$ such that $f(z) \in X_n$ we have:

$$(g_{n'})_{|X_n}(f(z)) = g_{n'}(f(z)) = h(f)(g_{n'}(z), z) = h(f)((g_{n'})_{|X_n}(z), z)$$

where the last equality follows from the fact that $z(i) \in X_n$ for all $i \in \alpha(f)$. Hence we see that the map $(g_{n'})_{|X_n} : X_n \to A$ also satisfies (iii) and (iv) above and from the uniqueness property of g_n we conclude that $(g_{n'})_{|X_n} = g_n$. We are now in a position to prove that $y = y'$. From $(x, y) \in g_n$ we obtain $x \in X_n$ and $y = g_n(x)$ while from $(x, y') \in g_{n'}$ we obtain $y' = g_{n'}(x) = (g_{n'})_{|X_n}(x)$. From $(g_{n'})_{|X_n} = g_n$ we therefore conclude that $y = y'$. This completes our proof of the existence of the map $g : X \to A$ having assumed the equality $Y = \mathbf{N}$. We shall complete the proof of this theorem by showing the equality $Y = \mathbf{N}$ is indeed true. So given $n \in \mathbf{N}$ we need to show the existence and uniqueness of a map $g_n : X_n \to A$ which satisfies (iii) and (iv) above. First we prove the uniqueness. So we assume that $g, g' : X_n \to A$ are two maps satisfying (iii) and (iv) above and we need to show that $g(x) = g'(x)$ for all $x \in X_n$. We shall do so by proving the implication $x \in X_n \ \Rightarrow \ g(x) = g'(x)$ by structural induction on X, using theorem (3) of page 31. First we check that this is true for $x \in X_0$. In this case from (iii) above we obtain immediately $g(x) = g_0(x) = g'(x)$. Next we consider $f \in \alpha$ and $x \in X^{\alpha(f)}$ such that the implication $x(i) \in X_n \ \Rightarrow \ g(x(i)) = g'(x(i))$ is true for all $i \in \alpha(f)$, i.e. $g(x) = g'(x)$, an equality which is still true in the case when $\alpha(f) = 0$. We need to check the implication $f(x) \in X_n \ \Rightarrow \ g(f(x)) = g'(f(x))$, which in fact follows immediately from (iv) and:

$$g(f(x)) = h(f)(g(x), x) = h(f)(g'(x), x) = g'(f(x))$$

This completes our structural induction argument and $g_n : X_n \to A$ is indeed unique. We shall now prove the existence $g_n : X_n \to A$ using an induction argument on $\mathbf{N}$. For $n = 0$, we already have a map $g_0 : X_0 \to A$ which clearly satisfies (iii) above. It also vacuously satifies (iv) as theorem (2) of page 21 shows no element of X_0 can be of the form $f(x)$ for $f \in \alpha$ and $x \in X^{\alpha(f)}$. So we assume that $g_n : X_n \to A$ exists for a given $n \in \mathbf{N}$ and we need to show the existence of $g_{n+1} : X_{n+1} \to A$. Recall the equality from proposition (7):

$$X_{n+1} = X_n \cup \{f(x) \ : \ f \in \alpha \ , \ x \in (X_n)^{\alpha(f)}\}$$

So we shall define $g_{n+1} : X_{n+1} \to A$ by setting $(g_{n+1})_{|X_n} = g_n$ and:

$$g_{n+1}(y) = h(f)(g_n(x), x)$$

for all $y \in X_{n+1} \setminus X_n$, where $y = f(x)$ is the unique representation of y with $f \in \alpha$ and $x \in (X_n)^{\alpha(f)}$. Such representation is indeed unique, as follows from theorem (2) of page 21. We have thus defined a map $g_{n+1} : X_{n+1} \to A$ and it remains to check that g_{n+1} satisfies (iii) and (iv) above. So let $x \in X_0$. Since g_n satisfies (iii) we have $g_{n+1}(x) = (g_{n+1})_{|X_n}(x) = g_n(x) = g_0(x)$ and g_{n+1} also satisfies (iii). So let $f \in \alpha$ and $x \in X^{\alpha(f)}$ be such that $y = f(x) \in X_{n+1}$. We need to show that $g_{n+1}(f(x)) = h(f)(g_{n+1}(x), x)$. We shall distinguish two cases: first we assume that $f(x) \in X_n$. Then, since (iv) is true for g_n:

$$g_{n+1}(f(x)) \quad = \quad (g_{n+1})_{|X_n}(f(x))$$

$$
\begin{array}{rcl}
 & = & g_n(f(x)) \\
(iv) \text{ true } g_n \ \rightarrow & = & h(f)(g_n(x), x) \\
 & = & h(f)((g_{n+1})_{|X_n}(x), x) \\
 & = & h(f)(g_{n+1}(x), x)
\end{array}
$$

We now assume that $f(x) \in X_{n+1} \setminus X_n$. From $x \in (X_n)^{\alpha(f)}$ we obtain:

$$
\begin{array}{rcl}
g_{n+1}(f(x)) & = & h(f)(g_n(x), x) \\
 & = & h(f)((g_{n+1})_{|X_n}(x), x) \\
 & = & h(f)(g_{n+1}(x), x)
\end{array}
$$

So we have proved that g_{n+1} satisfies (iv) above as requested. **.**

1.2.8 Generating Functions

Definition 12 *We call* generating function *any map $F : \mathcal{P}(U) \rightarrow \mathcal{P}(U)$ with:*

$$X \subseteq Y \ \Rightarrow F(X) \subseteq F(Y)$$

for all $X, Y \in \mathcal{P}(U)$, where U is an arbitrary set, called a universe.

Definition 13 *Let $F : \mathcal{P}(U) \rightarrow \mathcal{P}(U)$ be a generating function and $X \subseteq U$.*

- (i) *We say that X is F-*closed *if and only if $F(X) \subseteq X$*
- (ii) *We say that X is F-*consistent *if and only if $X \subseteq F(X)$*
- (iii) *We say that X is a* fixed point of F *if and only if $F(X) = X$*

Proposition 15 *Let $F : \mathcal{P}(U) \rightarrow \mathcal{P}(U)$ be a generating function and $X \subseteq U$. if X is F-closed, then so is $F(X)$. If X is F-consistent, then so is $F(X)$.*

Proof
Suppose $X \subseteq U$ is F-closed. Then we have $F(X) \subseteq X$. Since F is a generating function we obtain $F(F(X)) \subseteq F(X)$. Hence we see that $F(X)$ is F-closed. Likewise, if X is F-consistent then $X \subseteq F(X)$ and consequently $F(X) \subseteq F(F(X))$ and $F(X)$ is therefore F-consistent. **.**

Proposition 16 *Let $F : \mathcal{P}(U) \rightarrow \mathcal{P}(U)$ be a generating function and $\mathcal{A} \subseteq \mathcal{P}(U)$ be a set of F-closed subsets of U. Then $\cap A$ is itself F-closed.*

Proof
Recall that $\cap\mathcal{A}$ is the subset of U defined by $\cap\mathcal{A} = \{x \in U \ , \ \forall X \in \mathcal{A} \ , \ x \in X\}$. This set is well-defined even when $\mathcal{A} = \emptyset$. So we assume that X is F-closed for all $X \in \mathcal{A}$ and we need to show that $F(\cap\mathcal{A}) \subseteq \cap\mathcal{A}$. In other words, given $x \in F(\cap\mathcal{A})$ and $X \in \mathcal{A}$, we need to show that $x \in X$. Hence it is sufficient to prove the inclusion $F(\cap\mathcal{A}) \subseteq X$ for all $X \in \mathcal{A}$. So let $X \in \mathcal{A}$. We have $\cap\mathcal{A} \subseteq X$ and since F is a generating function we obtain $F(\cap\mathcal{A}) \subseteq F(X)$. However since X is F-closed, we also have $F(X) \subseteq X$. We conclude that $F(\cap\mathcal{A}) \subseteq X$. **.**

Proposition 17 *Let $F : \mathcal{P}(U) \to \mathcal{P}(U)$ be a generating function and $\mathcal{A} \subseteq \mathcal{P}(U)$ be a set of F-consistent subsets of U. Then $\cup A$ is itself F-consistent.*

Proof
Recall that $\cup\mathcal{A}$ is the subset of U defined by $\cup\mathcal{A} = \{x | \exists X \in \mathcal{A} \ , \ x \in X\}$. So we assume that X is F-consistent for all $X \in \mathcal{A}$ and we need to show that $\cup\mathcal{A} \subseteq F(\cup\mathcal{A})$. In other words, given $X \in \mathcal{A}$ and $x \in X$, we need to show that $x \in F(\cup\mathcal{A})$. Hence it is sufficient to prove the inclusion $X \subseteq F(\cup\mathcal{A})$ for all $X \in \mathcal{A}$. So let $X \in \mathcal{A}$. We have $X \subseteq \cup\mathcal{A}$ and since F is a generating function we obtain $F(X) \subseteq F(\cup\mathcal{A})$. However since X is F-consistent, we also have $X \subseteq F(X)$. We conclude that $X \subseteq F(\cup\mathcal{A})$ as requested. .

Definition 14 *Let $F : \mathcal{P}(U) \to \mathcal{P}(U)$ be a generating function and $\mathcal{A}$ be the set of all F-closed subsets of U. We define $\mu F = \cap\mathcal{A}$.*

Definition 15 *Let $F : \mathcal{P}(U) \to \mathcal{P}(U)$ be a generating function and $\mathcal{A}$ be the set of all F-consistent subsets of U. We define $\nu F = \cup\mathcal{A}$.*

1.3 Relation on Universal Algebra

1.3.1 Relation and Congruence on Universal Algebra

A relation is a set of ordered pairs. If X is a set then a *relation on* X is a set of ordered pairs which is also a subset of $X \times X$. A map $g : A \to B$ between two sets A and B is a particular type of relation which is a subset of $A \times B$. It is a *functional relation* as it satisfies the property:

$$\forall x \forall y \forall y' [\, ((x, y) \in g) \wedge ((x, y') \in g) \to (y = y') \,]$$

A map $g : X \to X$ is a functional relation on X. In this section we shall introduce other types of relations on X, which are of particular interest. Most of us will be familiar with *equivalent relations* on X. An *equivalence relation on* X is a relation on X which is *reflexive*, *symmetric* and *transitive*. A relation $\sim$ is said to be *reflexive* if and only if it satisfies:

$$\forall x [\, (x \in X) \to (x \sim x) \,]$$

Note that it is very common to write $x \sim x$ and $x \sim y$ rather than $(x, x) \in\sim$ or $(x, y) \in\sim$. A relation $\sim$ on X is said to be *symmetric* if and only if it satisfies:

$$\forall x \forall y [\, (x \sim y) \to (y \sim x) \,]$$

Finally, a relation $\sim$ on X is said to be *transitive* if and only if:

$$\forall x \forall y \forall z [\, (x \sim y) \wedge (y \sim z) \to (x \sim z) \,]$$

We shall now introduce a new type of relation on X, in the case when X is a universal algebra of type α. Note that given $f \in \alpha$ and $x, y \in X^{\alpha(f)}$, we

shall write $x \sim y$ as a notational shortcut for the statement $x(i) \sim y(i)$ for all $i \in \alpha(f)$. Note that if $\alpha(f) = 0$ then $x \sim y$ is vacuously true. Beware that the symbol $\sim$ thus becomes overloaded. In effect, we are defining new relations $\sim$ on X^n for $n \in \mathbf{N}$. So $0 \sim 0$ may be vacuously true when referring to the relation on X^0, but may not be true (if $0 \in X$) with respect to the relation on X.

Definition 16 *Let X be a universal algebra of type α. Let $\sim$ be a relation on X. We say that $\sim$ is a* congruent relation *on X, if and only if:*

$$\forall f \in \alpha \ , \ \forall x, y \in X^{\alpha(f)} \ , \quad x \sim y \ \Rightarrow f(x) \sim f(y)$$

It follows that if X is a universal algebra of type α with constants, and $\sim$ is a congruent relation on X, then $f(0) \sim f(0)$ for all $f \in \alpha$ such that $\alpha(f) = 0$.

Definition 17 *Let X be a universal algebra of type α. We call* congruence *on X any equivalence relation on X which is a congruent relation on X.*

The notion of *congruence* on a universal algebra is very important. This is particularly the case when dealing with free universal algebras. As already seen following theorem (2) of page 21, most interesting algebraic structures are not free (a notable exception being formal languages encountered in logic textbooks). A congruence $\sim$ on a universal algebra X of type α will allow us to define a new universal algebra $[X]$ of type α, called the *quotient universal algebra of X*. We shall see that quotients of free universal algebras are in fact everywhere. This is probably one of the reasons free universal algebras are key. A good example of congruence is the kernel of a morphism:

Definition 18 *Let $h : X \to Y$ be a homomorphism between two universal algebras X and Y of type α. We call* kernel *of h the relation* $\ker(h)$ *on X:*

$$\ker(h) = \{ (x, y) \in X \times X \ : \ h(x) = h(y) \}$$

Proposition 18 *Let $h : X \to Y$ be a homomorphism between two universal algebras X and Y of type α. Then* $\ker(h)$ *is a congruence on X.*

Proof
The relation $\ker(h)$ is clearly reflexive, symmetric and transitive. So it is an equivalence relation on X. It remains to show it is also a congruent relation. For an easier formalism, denote $\ker(h) = \sim$. Let $f \in \alpha$ and $x, y \in X^{\alpha(f)}$ such that $x \sim y$. We need to show that $f(x) \sim f(y)$ which is $h \circ f(x) = h \circ f(y)$:

$$h \circ f(x) = f \circ h(x) = f \circ h(y) = h \circ f(y)$$

The first and third equality are just expressing the fact that h is a morphism, while the second equality follows from $h(x) = h(y)$, itself a consequence of the fact that for all $i \in \alpha(f)$ we have $h(x)(i) = h(x(i)) = h(y(i)) = h(y)(i)$. .

1.3.2 Congruence Generated by a Set

Let X be a universal algebra of type α and $R_0 \subseteq X \times X$. Then R_0 is a relation on X. However, R_0 may not have the right properties and in particular may not be a congruence on X. In this section, we prove the existence of the *congruence generated by* R_0, namely the smallest congruence on X containing R_0 in the sense of inclusion. The notion of *congruence generated* by a subset of $X \times X$ is a very handy way of creating interesting congruences on X. As we shall see, it is possible to view a congruence on X as a universal sub-algebra of $X \times X$, provided the latter has been embedded with the right structure of universal algebra. The congruence generated by R_0 will be seen to be the universal sub-algebra of $X \times X$ generated by R_0, as per definition (10).

Before we proceed, we shall review a few simple lemmas which show that common properties of a relation such as reflexivity, symmetry, transitivity and being a congruent relation, are in fact akin to closure properties.

Lemma 5 *Let X be a set and $T_x : (X \times X)^0 \to X \times X$ be defined by:*

$$T_x(0) = (x, x) \ , \ (\forall x \in X)$$

A relation $\sim$ is reflexive on X if and only if it is closed under T_x for all $x \in X$.

Proof
Suppose $\sim$ is closed under T_x for all $x \in X$. We need to show that $\sim$ is a reflexive relation on X. So let $x \in X$. We need to show that $x \sim x$. Since $0 \in (\sim)^0$, we obtain $T_x(0) \in \sim$. Hence we see that $(x, x) \in \sim$ or equivalently $x \sim x$. Conversely, suppose $\sim$ is a reflexive relation on X. We need to show that $\sim$ is closed under T_x for all $x \in X$. So let $x \in X$. We need to show that $\sim$ is closed under T_x. So let $u \in (\sim)^0$. We need to show that $T_x(u) \in \sim$. But $u = 0$ and $T_x(0) = (x, x)$. So we need to show that $(x, x) \in \sim$ or equivalently $x \sim x$ which follows immediately from the reflexivity of $\sim$. **.**

If X is a set and $z \in (X \times X)^1$ then z is a map $z : \{0\} \to X \times X$. So $z(0)$ is an ordered pair (x, y). Recall that the notation '(x, y)' may be used as a notational shortcut to refer to the map $z : \{0\} \to X \times X$ defined by $z(0) = (x, y)$.

Lemma 6 *Let X be a set and $\sigma : (X \times X)^1 \to X \times X$ be defined by:*

$$\forall (x, y) \in (X \times X)^1 \ , \ \sigma(x, y) = (y, x)$$

A relation $\sim$ is symmetric on X if and only if it is closed under σ.

Proof
Suppose $\sim$ is closed under σ. We need to show that $\sim$ is a symmetric relation on X. So let $x, \ y \in X$ such that $x \sim y$. We need to show that $y \sim x$. Since $(x, y) \in (\sim)^1$, we obtain $\sigma(x, y) \in \sim$. Hence we see that $(y, x) \in \sim$ or equivalently $y \sim x$. Conversely, suppose $\sim$ is a symmetric relation on X. We need to show that $\sim$ is closed under σ. So let $(x, y) \in (\sim)^1$. We need to show that $\sigma(x, y) \in \sim$. So we need to show that $(y, x) \in \sim$ or equivalently $y \sim x$ which follows immediately from the symmetry of $\sim$ and $x \sim y$ **.**

If X is a set and $z \in (X \times X)^2$ then z is a map $z : \{0,1\} \to X \times X$. So $z(0)$ is an ordered pair (x,y) and $z(1)$ is an ordered pair (y',z). Recall that the notation '$[(x,y),(y',z)]$' may be used as a notational shortcut to refer to the map $z : \{0,1\} \to X \times X$ defined by $z(0) = (x,y)$ and $z(1) = (y',z)$.

Lemma 7 *Let X be a set and $\tau : (X \times X)^2 \to X \times X$ be defined by:*

$$\tau[(x,y),(y',z)] = \begin{cases} (x,y) & \text{if} \quad y \neq y' \\ (x,z) & \text{if} \quad y = y' \end{cases}$$

A relation $\sim$ is transitive on X if and only if it is closed under τ.

Proof
Suppose $\sim$ is closed under τ. We need to show that $\sim$ is a transitive relation on X. So let x, y, $z \in X$ such that $x \sim y$ and $y \sim z$. We need to show that $x \sim z$. Since $[(x,y),(y,z)] \in (\sim)^2$ we obtain $\tau[(x,y),(y,z)] \in \sim$. Hence we see that $(x,z) \in \sim$ or equivalently $x \sim z$. Conversely, suppose $\sim$ is a transitive relation on X. We need to show that $\sim$ is closed under τ. So let $[(x,y),(y',z)] \in (\sim)^2$. Then $x \sim y$ and $y' \sim z$ and we need to show that $\tau[(x,y),(y',z)] \in \sim$. If $y \neq y'$ then we need to show that $(x,y) \in \sim$ which is true by assumption. If $y = y'$ then $y \sim z$ and we need to show that $(x,z) \in \sim$ or equivalently $x \sim z$ which follows immediately from the transitivity of $\sim$ and $x \sim y$ and $y \sim z$. **.**

Let X be a set and $\pi_0, \pi_1 : X \times X \to X$ be the projection mappings, namely the maps defined by $\pi_0(x,y) = x$ and $\pi_1(x,y) = y$ for all $x, y \in X$. Following our well established convention, for all $n \in \mathbf{N}$ recall that 'π_0' may be used as a notational shortcut for $\pi_0^n : (X \times X)^n \to X^n$ defined by $\pi_0^n(z)(i) = \pi_0(z(i))$ for all $i \in n$. A similar comment obviously applies to π_1.

Lemma 8 *Let X be a universal algebra of type α. Consider the structure of universal algebra of type α on $X \times X$ defined by:*

$$T(f)(z) = (f \circ \pi_0(z), f \circ \pi_1(z)) \ , \ \forall z \in (X \times X)^{\alpha(f)} \ , \ \forall f \in \alpha$$

where $\pi_0, \pi_1 : X \times X \to X$ are the projection mappings. Then, a relation $\sim$ is a congruent relation on X, if and only if it is closed under $T(f)$ for all $f \in \alpha$.

Proof
Note from definition (9) that $\sim$ being closed under $T(f)$ for all $f \in \alpha$ could equally have been phrased as $\sim$ being a universal sub-algebra of $X \times X$ viewed as a universal algebra of type α. Note also that given $z \in (X \times X)^{\alpha(f)}$ for $f \in \alpha$, $\pi_0(z)$ and $\pi_1(z)$ are well-defined elements of $X^{\alpha(f)}$ (specifically we have $\pi_0(z)(i) = \pi_0(z(i))$ for all $i \in \alpha(f)$ with similar equalities for $\pi_1(z)$). It follows that $f \circ \pi_0(z)$ and $f \circ \pi_1(z)$ are well-defined elements of X and we see that $T(f)$ is indeed a well-defined operator $T(f) : (X \times X)^{\alpha(f)} \to X \times X$. We now proceed with the proof: suppose $\sim$ is closed under $T(f)$ for all $f \in \alpha$. We need to show that $\sim$ is a congruent relation on X. So let $f \in \alpha$ and $x, y \in X^{\alpha(f)}$ and suppose that $x \sim y$. We need to show that $f(x) \sim f(y)$. Define $z \in (X \times X)^{\alpha(f)}$ by $z(i) = (x(i), y(i))$ for all $i \in \alpha(f)$, being understood that $z = 0$ is $\alpha(f) = 0$.

From $x \sim y$, we have $x(i) \sim y(i)$ for all $i \in \alpha(f)$. It follows that $z(i) \in \sim$ for all $i \in \alpha(f)$ and consequently $z \in (\sim)^{\alpha(f)}$. Since $\sim$ is closed under $T(f)$ we obtain $T(f)(z) \in \sim$. However, for all $i \in \alpha(f)$ we have $\pi_0(z)(i) = \pi_0(z(i)) = x(i)$ and therefore $\pi_0(z) = x$. Similarly we have $\pi_1(z) = y$. It follows that:

$$T(f)(z) = (f \circ \pi_0(z), f \circ \pi_1(z)) = (f(x), f(y))$$

From $T(f)(z) \in \sim$ we conclude that $f(x) \sim f(y)$. Conversely, suppose $\sim$ is a congruent relation on X. We need to show that $\sim$ is closed under $T(f)$ for all $f \in \alpha$. So let $f \in \alpha$ and $z \in (\sim)^{\alpha(f)}$. We need to show that $T(f)(z) \in \sim$. Define $x, y \in X^{\alpha(f)}$ by setting $x = \pi_0(z)$ and $y = \pi_1(z)$. Then $T(f)(z) = (f(x), f(y))$ and it remains to show that $f(x) \sim f(y)$. Since $\sim$ is a congruent relation on X, this will be achieved by showing that $x \sim y$, or equivalently that $x(i) \sim y(i)$ for all $i \in \alpha(f)$. However, for all $i \in \alpha(f)$ we have $x(i) = \pi_0(z)(i) = \pi_0(z(i))$ and similarly $y(i) = \pi_1(z(i))$. It follows that $z(i) = (x(i), y(i))$. Consequently, we only need to show that $z(i) \in \sim$ for all $i \in \alpha(f)$. But this is an immediate consequence of $z \in (\sim)^{\alpha(f)}$. **.**

Theorem 6 *Let X be a universal algebra of type α and $R_0 \subseteq X \times X$. Then, there exists a unique smallest congruence $\sim$ on X such that $R_0 \subseteq \sim$.*

Proof
First we show the uniqueness. Suppose $\sim$ and $\simeq$ are two congruence on X which are both the smallest congruence on X containing R_0. Since $\simeq$ is a congruence on X containing R_0, from the minimality of $\sim$ we obtain $\sim \subseteq \simeq$. Likewise, since $\sim$ is a congruence on X containing R_0, from the minimality of $\simeq$ we obtain $\simeq \subseteq \sim$. We now show the existence. For all $x \in X$, let $T_x : (X \times X)^0 \to X \times X$ be defined as in lemma (5). Let $\sigma : (X \times X)^1 \to X \times X$ be defined as in lemma (6) and $\tau : (X \times X)^2 \to X \times X$ be defined as in lemma (7). For all $\alpha \in f$, let $T(f) : (X \times X)^{\alpha(f)} \to X \times X$ be defined as in lemma (8). Consider the sets $\alpha_0 = \{((0, x), 0) : x \in X\}$, $\alpha_1 = \{((1, 0), 1)\}$, $\alpha_2 = \{((2, 0), 2)\}$ and $\alpha_3 = \{((3, f), \alpha(f)) : f \in \alpha\}$. Note that these sets are all maps with range inside $\mathbf{N}$. Furthermore, their domains are pairwise disjoint. It follows that $\alpha^* = \alpha_0 \cup \alpha_1 \cup \alpha_2 \cup \alpha_3$ is a map with range inside $\mathbf{N}$, i.e. $\mathrm{rng}(\alpha^*) \subseteq \mathbf{N}$. In other words, α^* is a type of universal algebra. Let T^* be the map with domain α^*, such that $T^*(f) : (X \times X)^{\alpha^*(f)} \to X \times X$ for all $f \in \alpha^*$ and $T^*(f)$ is defined as:

$$T^*(f) = \begin{cases} T_x & \text{if} \quad f \in \alpha_0 \ , \ f = ((0, x), 0) \ , \ x \in X \\ \sigma & \text{if} \quad f \in \alpha_1 \ , \ f = ((1, 0), 1) \\ \tau & \text{if} \quad f \in \alpha_2 \ , \ f = ((2, 0), 2) \\ T(f') & \text{if} \quad f \in \alpha_3 \ , \ f = ((3, f'), \alpha(f')) \ , \ f' \in \alpha \end{cases} \tag{1.12}$$

Note that equation (1.12) is indeed such that $T^*(f) : (X \times X)^{\alpha^*(f)} \to X \times X$ for all $f \in \alpha^*$. It follows that the ordered pair $(X \times X, T^*)$ is a universal algebra of type α^*. Using definition (10), let $\sim = \langle R_0 \rangle$ be the universal sub-algebra of $X \times X$ generated by $R_0 \subseteq X \times X$. We shall complete the proof of the theorem

by showing that the relation $\sim$ has all the requested properties. First we show that $\sim$ is a congruence on X. Since $\sim$ is a universal sub-algebra of $X \times X$, it is closed under every operator $T^*(f)$ for all $f \in \alpha^*$. In particular, it is closed under T_x for all $x \in X$. It follows from lemma (5) that $\sim$ is a reflexive relation on X. Similarly $\sim$ is closed under σ and τ, and we see from lemma (6) and lemma (7) that $\sim$ is a symmetric and transitive relation on X. Furthermore, $\sim$ is closed under every operator $T(f')$ for all $f' \in \alpha$ and it follows from lemma (8) that $\sim$ is a congruent relation on X. So we have proved that $\sim$ is an equivalence relation on X which is a congruent relation, i.e. that $\sim$ is a congruence on X. From $\sim = \langle R_0 \rangle$ we obtain immediately $R_0 \subseteq \sim$. It remains to show that $\sim$ is the smallest congruence on X with $R_0 \subseteq \sim$. So we assume that R is a congruence on X such that $R_0 \subseteq R$. We need to show that $\sim \subseteq R$. Since $\sim = \langle R_0 \rangle$ and $R_0 \subseteq R$ it is sufficient to show that R is a universal sub-algebra of $X \times X$, as this will imply $\langle R_0 \rangle \subseteq R$ by virtue of proposition (11), and finally $\sim \subseteq R$. So suppose $f \in \alpha^*$. We need to show that R is closed under $T^*(f)$. If $f \in \alpha_0$ then $f = ((0, x), 0)$ for some $x \in X$ and we need to show that R is closed under T_x which follows immediately from lemma (5) and the reflexivity of R. If $f \in \alpha_1$ then we need to show that R is closed under σ which follows immediately from lemma (6) and the symmetry of R. If $f \in \alpha_2$ then we need to show that R is closed under τ which follows immediately from lemma (7) and the transitivity of R. Finally, if $f \in \alpha_3$ then $f = ((3, f'), \alpha(f'))$ for some $f' \in \alpha$ and we need to show that R is closed under $T(f')$, which follows immediately from lemma (8) and the fact that R is a congruent relation on X. In all four possible cases, we have proved that R is closed under $T^*(f)$. .

Definition 19 *Let X be a universal algebra of type α and $R_0 \subseteq X \times X$. We call* congruence on X generated by R_0 *the smallest congruence on X containing R_0.*

1.3.3 Quotient of Universal Algebra

In this section we define the *quotient universal algebra* $[X]$ *of type* α derived from a universal algebra X of type α and a congruence $\sim$ on X. Given $x \in X$, we shall denote $[x]$ the *equivalent class of x modulo* $\sim$, namely:

$$[x] = \{y \in X : x \sim y\}$$

Note that $[x] = [y]$ is equivalent to $x \sim y$ for all $x, y \in X$. Given $f \in \alpha$ and $x \in X^{\alpha(f)}$, $[x]$ to denote the element of $[X]^{\alpha(f)}$ defined by $[x](i) = [x(i)]$.

Theorem 7 *Let X be a universal algebra of type α and $\sim$ be a congruence on X. Given $x \in X$, let $[x]$ denote the equivalence class of x modulo $\sim$ and $[X]$ be the quotient set $[X] = \{[x] : x \in X\}$. Let $\pi : X \to [X]$ be defined by $\pi(x) = [x]$ for all $x \in X$. Then, there exists a unique structure of universal algebra of type α on $[X]$ such that π is a surjective morphism. Furthermore:*

$$\forall x \in X^{\alpha(f)} \ , \ f([x]) = [f(x)] \tag{1.13}$$

for all $f \in \alpha$. This structure is called the quotient structure on $[X]$.

Proof
Note that given $f \in \alpha$ and $x \in X^{\alpha(f)}$, $[x]$ refers to the element of $[X]^{\alpha(f)}$ defined by $[x](i) = [x(i)]$ for all $i \in \alpha(f)$, being understood that $[x] = 0$ is $\alpha(f) = 0$. It follows that equation (1.13) is meaningful. Note also that $\pi : X \to [X]$ is a surjective map, regardless of any structure on $[X]$. We shall first prove the existence of a structure of universal algebra of type α on $[X]$ which makes $\pi : X \to [X]$ into a morphism. We need to show the existence of a map T with domain α such that $T(f) : [X]^{\alpha(f)} \to [X]$ for all $f \in \alpha$ and:

$$\forall x \in X^{\alpha(f)} \ , \ \pi \circ f(x) = T(f) \circ \pi(x) \tag{1.14}$$

So let $f \in \alpha$. We need to define some $T(f) : [X]^{\alpha(f)} \to [X]$. Let $x^* \in [X]^{\alpha(f)}$. We need to define $T(f)(x*)$. First we shall show that there exists $x \in X^{\alpha(f)}$ such that $x^* = [x]$. Indeed, for all $i \in \alpha(f)$, $x^*(i)$ is an element of $[X]$. So there exists $x_i \in X$ such that $x^*(i) = [x_i]$. Define $x \in X^{\alpha(f)}$ by setting $x(i) = x_i$ for all $i \in \alpha(f)$, being understood that $x = 0$ if $\alpha(f) = 0$. Then, for all $i \in \alpha(f)$ we have $[x](i) = [x(i)] = [x_i] = x^*(i)$ and it follows that $[x] = x^*$. We now define $T(f)(x^*) = [f(x)]$. We need to check that this definition is valid, namely that $[f(x)]$ is independent of the particular $x \in X^{\alpha(f)}$ such that $x^* = [x]$. So suppose that $x, y \in X^{\alpha(f)}$ such that $[x] = [y]$. We need to show that $[f(x)] = [f(y)]$ or equivalently that $f(x) \sim f(y)$. Since $\sim$ is a congruence, this will be achieved by showing that $x \sim y$ or equivalently that $x(i) \sim y(i)$ for all $i \in \alpha(f)$. However, $[x] = [y]$ and it follows that $[x(i)] = [x](i) = [y](i) = [y(i)]$ for all $i \in \alpha(f)$ from which we obtain $x(i) \sim y(i)$. So we have proved that $T(f)(x^*)$ is well defined. Furthermore since $T(f)(x^*) = [f(x)]$, we have $T(f)(x^*) \in [X]$. Hence we have successfully defined $T(f) : [X]^{\alpha(f)} \to [X]$ for all $f \in \alpha$. It follows that the ordered pair $([X], T)$ is a universal algebra of type α. it remains to check that $\pi : X \to [X]$ is a morphism under this particular structure, i.e. that equation (1.14) is satisfied for all $f \in \alpha$. So let $x \in X^{\alpha(f)}$ and $x^* = [x]$. We have:

$$\pi \circ f(x) = [f(x)] = T(f)(x^*) = T(f)([x]) = T(f) \circ \pi(x)$$

This completes our proof of the existence of a structure of universal algebra of type α on $[X]$ such that $\pi : X \to [X]$ is a surjective morphism. We shall now prove the uniqueness. So suppose S is another map with domain α such that $S(f) : [X]^{\alpha(f)} \to [X]$ for all $f \in \alpha$ with respect to which π is a morphism. We need to show that $S = T$. So let $f \in \alpha$. We need to show that $S(f) = T(f)$. So let $x^* \in [X]^{\alpha(f)}$. We need to show that $S(f)(x^*) = T(f)(x^*)$. Let $x \in X^{\alpha(f)}$ be such that $x^* = [x]$. Since π is a morphism under S we obtain:

$$S(f)(x^*) = S(f)([x]) = S(f) \circ \pi(x) = \pi \circ f(x) = [f(x)] = T(f)(x^*)$$

We shall complete the proof of the theorem by showing that equation (1.13) holds for all $f \in \alpha$. So let $x \in X^{\alpha(f)}$. We need to show that $f([x]) = [f(x)]$. But this follows immediately from $T(f)([x]) = [f(x)]$ and the fact that '$f([x])$' is a notational shortcut for '$T(f)([x])$'. .

1.3.4 First Isomorphism Theorem

Let $h : X \to Y$ be a homomorphism between two universal algebras X and Y of type α. We know from proposition (18) that $\ker(h)$ is a congruence on X. From theorem (7) we obtain the quotient universal algebra $[X]$ of type α derived from X and $\ker(h)$. Furthermore from proposition (8) the homomorphic image $h(X)$ is a sub-algebra of Y and in particular, it is also a universal algebra of type α. As it turns out, the algebras $[X]$ and $h(X)$ are isomorphic. This is of course hardly surprising for anyone who has done a little bit of algebra before.

Theorem 8 *Let $h : X \to Y$ be a homomorphism between two universal algebras X and Y of type α. Let $[X]$ be the quotient universal algebra of type α derived from X and the congruence $\ker(h)$. Let $h^* : [X] \to h(X)$ be defined as:*

$$\forall x \in X \ , \ h^*([x]) = h(x)$$

Then h^* is an isomorphism between $[X]$ and $h(X)$.

Proof
Before we start, we should point out that the map $h^* : [X] \to h(X)$ is well defined by the formula $h^*([x]) = h(x)$ since $h(x)$ is independent of the particular choice of $x \in [x]$. Indeed, if $x' \in [x]$, then $x' \sim x$ which is $(x', x) \in \ker(h)$ and consequently $h(x') = h(x)$. Now we need to show that h^* is a bijective morphism. First we show that it is bijective. It is clearly surjective, so we shall prove that h^* is injective. Let $x, x' \in X$ such that $h^*([x]) = h^*([x'])$. We need to show that $[x] = [x']$. However, our assumption can equally be written as $h(x) = h(x')$ which is the same as $(x, x') \in \ker(h)$ or $x \sim x'$. Hence we obtain $[x] = [x']$ as requested. It remains to show that h^* is a morphism. So let $f \in \alpha$ and $x^* \in [X]^{\alpha(f)}$. We need to show that $h^* \circ f(x^*) = f \circ h^*(x^*)$. However, for all $i \in \alpha(f)$ we have $x^*(i) \in [X]$. So there exists $x_i \in X$ such that $x^*(i) = [x_i]$. Let $x \in X^{\alpha(f)}$ be defined by $x(i) = x_i$ for all $i \in \alpha(f)$. Then we have $x^*(i) = [x_i] = [x(i)] = [x](i)$ and consequently $x^* = [x]$. Hence:

$$\begin{aligned}
h^* \circ f(x^*) &= h^* \circ f([x]) \\
\text{theorem (7)} \ \to \ &= h^*([f(x)]) \\
&= h(f(x)) \\
h \text{ is a morphism} \ \to \ &= f \circ h(x) \\
\text{A: to be proved} \ \to \ &= f \circ h^*([x]) \\
&= f \circ h^*(x^*)
\end{aligned}$$

So it remains to show that $h(x) = h^*([x])$. For all $i \in \alpha(f)$, we have:

$$h(x)(i) = h(x(i)) = h^*([x(i)]) = h^*([x](i)) = h^*([x])(i)$$

Note that this proof works very well when $\alpha(f) = 0$. ∎

As an application of the first isomorphism theorem (8), we now present a result which we are unlikely to use again but which may be viewed as a vindication of the effort we have put into the analysis of free universal algebras.

In theorem (1) of page 20, given an arbitrary set X_0 we showed the existence of a free universal algebra X of type α with free generator X_0. In theorem (7) of page 53, given a congruence $\sim$ on X we showed how to construct the *quotient* universal algebra $[X]$ of type α. The following theorem shows that the construction mechanism $X_0 \to X \to [X]$ is as general as it gets: *every* universal algebra of type α is in fact some quotient universal algebra $[X]$ derived from a free universal algebra X and a congruence $\sim$ on X. Consequently, if we ever wish to *construct* a universal algebra of a certain type and with certain properties, there is absolutely no loss in generality in first considering a free universal algebra, and subsequently finding the appropriate congruence on it so as to fit the required properties.

For instance, suppose we have a free universal algebra X with a binary operator $\otimes$. We would like this operator to be commutative. We should only make sure our congruence $\sim$ on X contains the set:

$$A = \{(x \otimes y, y \otimes x) : x, y \in X\}$$

If this is the case, the corresponding operator $\otimes$ on the quotient universal algebra $[X]$ will indeed be commutative. For if $x^*, y^* \in [X]$ and $x, y \in X$ are such that $x^* = [x]$ and $y^* = [y]$, then from theorem (7) of page 53 we have:

$$x^* \otimes y^* = [x] \otimes [y] = [x \otimes y] = [y \otimes x] = [y] \otimes [x] = y^* \otimes x^*$$

Theorem 9 *Any universal algebra of type α is isomorphic to the quotient $[X]$ of some free universal algebra X of type α, relative to some congruence on X.*

Proof
Let Y be a universal algebra of type α and $X_0 = Y$. From theorem (1) of page 20 there exists a free universal algebra X of type α with free generator X_0. In particular $X_0 \subseteq X$. Consider the identity mapping $j : X_0 \to Y$. Since X_0 is a free generator of X, there exists a unique morphism $g : X \to Y$ such that $g_{|X_0} = j$. Let $\sim = \ker(g)$ be the kernel of g. From proposition (18) we know that $\sim$ is a congruence on X. We shall complete the proof of this theorem by showing the corresponding quotient universal algebra $[X]$ is isomorphic to Y. From the first isomorphism theorem (8) we know that the map $g^* : [X] \to g(X)$ defined by $g^*([x]) = g(x)$ is an isomorphism. So it is sufficient to show that $g(X) = Y$, i.e. that g is a surjective morphism. So let $y \in Y$. We need to show the existence of $x \in X$ such that $g(x) = y$. But $Y = X_0 \subseteq X$ and:

$$g(y) = g_{|X_0}(y) = j(y) = y$$

.

1.4 Sub-Formula in Free Universal Algebra

1.4.1 Sub-Formula of Formula in Free Universal Algebra

In this section we formalize the notion of sub-formula in a free universal algebra. Specifically, given a free universal algebra X of type α, we define a relation $\preceq$

on X such that $\phi \preceq \psi$ expresses the fact that *the formula ϕ is a sub-formula of the formula ψ*. For example, when studying our *free universal algebra of first order logic* in a later part of this document, we shall want to say that the formula $\phi = \forall x(x \in y)$ is a sub-formula of the formula $\psi = \forall y \forall x(x \in y)$. This notion will prove important when defining substitutions of variables which are *valid* for a given formula ϕ. Loosely speaking, a substitution is valid for ϕ if no free variable gets caught under the *scope of a quantifier*. Making this idea precise requires the notion of sub-formula. In order to add further motivation to this topic, we shall point out that *valid substitutions* are themselves a key notion when defining *specialization axioms*, which are axioms of the form $\forall x \phi \rightarrow \phi[y/x]$ where the substitution $[y/x]$ of the variable y in place of x is valid for ϕ. It is very important for us to properly define the idea of *valid substitutions*: if we allow too much freedom in which a variable y can be substituted for x, our axioms may prove too much including statements which are not true. On the other hand, if we are too restrictive our axioms may prove too little and Gödel's completeness theorem may fail to be true.

The notion of sub-formula can easily be defined on any free universal algebra and not just in the context of first order logic. So we shall write $x \preceq y$ rather than $\phi \preceq \psi$ and carry out the analysis in its general setting. Given a free universal algebra X of type α with free generator $X_0 \subseteq X$, for all $y \in X$ we shall define the set $\mathrm{Sub}(y)$ of all sub-formulas of y, and simply define $x \preceq y$ as equivalent to $x \in \mathrm{Sub}(y)$. The key idea to remember is that given $f \in \alpha$ and $x \in X^{\alpha(f)}$, the sub-formulas of $f(x)$ are $f(x)$ itself, as well as the sub-formulas of every $x(i)$, for all $i \in \alpha(f)$. As shall see, the relation $\preceq$ is a partial order on X, i.e. a relation which is reflexive, anti-symmetric and transitive on X. Recall that $\preceq$ is said to be anti-symmetric if and only if for all $x, y \in X$ we have:

$$(x \preceq y) \wedge (y \preceq x) \;\Rightarrow\; (x = y)$$

Definition 20 *Let X be a free universal algebra of type α with free generator $X_0 \subseteq X$. We call* sub-formula mapping *the map $\mathrm{Sub} : X \rightarrow \mathcal{P}(X)$ defined by:*

$$\begin{array}{lll} (i) & x \in X_0 \;\Rightarrow\; \mathrm{Sub}(x) = \{x\} \\ (ii) & x \in X^{\alpha(f)} \;\Rightarrow\; \mathrm{Sub}(f(x)) = \{f(x)\} \cup \bigcup\limits_{i \in \alpha(f)} \mathrm{Sub}(x(i)) \end{array}$$

where (ii) holds for all $f \in \alpha$. Given $x, y \in X$, we say that x is a sub-formula of y*, denoted $x \preceq y$, if and only if $x \in \mathrm{Sub}(y)$.*

Proposition 19 *The structural recursion of definition (19) is legitimate.*

Proof
We need to show the existence of a unique map $\mathrm{Sub} : X \rightarrow \mathcal{P}(X)$ such that (i) and (ii) of definition (19) hold. We do so by applying theorem (5) of page 44

with $A = \mathcal{P}(X)$ and $g_0 : X \to A$ defined by $g_0(x) = \{x\}$ for all $x \in X_0$. Given $f \in \alpha$ we take $h(f) : A^{\alpha(f)} \times X^{\alpha(f)} \to A$ defined by:

$$h(f)(a, x) = \{f(x)\} \cup \bigcup_{i \in \alpha(f)} a(i)$$

From theorem (5) of page 44 we obtain the existence and uniqueness of a map $g : X \to A$ which satisfies $g(x) = \{x\}$ for all $x \in X_0$, and for $f \in \alpha$, $x \in X^{\alpha(f)}$:

$$g(f(x)) = h(f)(g(x), x) = \{f(x)\} \cup \bigcup_{i \in \alpha(f)} g(x)(i) = \{f(x)\} \cup \bigcup_{i \in \alpha(f)} g(x(i))$$

which is exactly (ii) of definition (19) with $g = \text{Sub}$. .

1.4.2 The Sub-Formula Partial Order

The objective of this section is to show that $\preceq$ is a partial order.

Proposition 20 *Let X be a free universal algebra of type α with free generator $X_0 \subseteq X$. The relation $\preceq$ on X is reflexive.*

Proof
We need to show that $x \in \text{Sub}(x)$ for all $x \in X$. We shall prove this result by structural induction using theorem (3) of page 31. If $x \in X_0$ then $\text{Sub}(x) = \{x\}$ and the property $x \in \text{Sub}(x)$ is clear. Suppose $f \in \alpha$ and $x \in X^{\alpha(f)}$ are such that $x(i) \in \text{Sub}(x(i))$ for all $i \in \alpha(f)$. We need to show the property is also true for $f(x)$, i.e that $f(x) \in \text{Sub}(f(x))$. This follows immediately from:

$$\text{Sub}(f(x)) = \{f(x)\} \cup \bigcup_{i \in \alpha(f)} \text{Sub}(x(i))$$

.

Proposition 21 *Let X be a free universal algebra of type α with free generator $X_0 \subseteq X$. For all $x, y \in X$ we have the equivalence:*

$$x \preceq y \;\Leftrightarrow\; \text{Sub}(x) \subseteq \text{Sub}(y)$$

In particular, the relation $\preceq$ on X is transitive.

Proof
First we show the implication $\Leftarrow$. Let $x, y \in X$ such that $\text{Sub}(x) \subseteq \text{Sub}(y)$. From proposition (20) we have $x \in \text{Sub}(x)$ and consequently $x \in \text{Sub}(y)$ which shows that $x \preceq y$. We now show the reverse implication $\Rightarrow$. We shall do so by considering the property $P(y)$ defined for $y \in X$ as:

$$\forall x \in X \ , \ [\ x \in \text{Sub}(y) \ \Rightarrow \ \text{Sub}(x) \subseteq \text{Sub}(y)\ ]$$

We shall prove $P(y)$ for all $y \in X$ by structural induction using theorem (3) of page 31. First we assume that $y \in X_0$. Then $\text{Sub}(y) = \{y\}$ and the condition

$x \in \mathrm{Sub}(y)$ implies that $x = y$. In particular $x \in X_0$ and $\mathrm{Sub}(x) = \{x\}$ which shows that the inclusion $\mathrm{Sub}(x) \subseteq \mathrm{Sub}(y)$ is indeed true. So the property $P(y)$ holds for $y \in X_0$. Let $f \in \alpha$ and $y \in X^{\alpha(f)}$ be such that $P(y(i))$ holds for all $i \in \alpha(f)$. We need to show that the property $P(f(y))$ is also true. So let $x \in X$ be such that $x \in \mathrm{Sub}(f(y))$. We need to show that $\mathrm{Sub}(x) \subseteq \mathrm{Sub}(f(y))$. However, from definition (19) we have:

$$\mathrm{Sub}(f(y)) = \{f(y)\} \cup \bigcup_{i \in \alpha(f)} \mathrm{Sub}(y(i)) \tag{1.15}$$

Hence the condition $x \in \mathrm{Sub}(f(y))$ implies that $x = f(y)$ or $x \in \mathrm{Sub}(y(i))$ for some $i \in \alpha(f)$. Suppose first that $x = f(y)$. Then $\mathrm{Sub}(x) \subseteq \mathrm{Sub}(f(y))$ follows immediately. Suppose now that $x \in \mathrm{Sub}(y(i))$ for some $i \in \alpha(f)$. Having assumed the property $P(y(i))$ is true, it follows that $\mathrm{Sub}(x) \subseteq \mathrm{Sub}(y(i))$ and finally from equation (1.15) we conclude that $\mathrm{Sub}(x) \subseteq \mathrm{Sub}(f(y))$. This completes our induction argument and the proof that $P(y)$ holds for all $y \in X$.

.

Proving the relation $\preceq$ is reflexive and transitive worked pretty well with structural induction arguments. The proof that $\preceq$ is anti-symmetric will also rely on induction but will be seen to be more difficult. Given $f \in \alpha$ and $x \in X^{\alpha(f)}$ a key step in the argument will be to claim that $f(x)$ cannot be a sub-formula of any $x(i)$ for all $i \in \alpha(f)$. This seems pretty obvious but requires some care. We shall achieve this by using the order mapping $\omega : X \to \mathbf{N}$ as per definition (8) of page 24. Recall that given $x \in X$ the order $\omega(x)$ offers some measure of complexity for the formula x. The next proposition shows that if x is a sub-formula of y, then it has no greater complexity than y. Since we already know from proposition (6) that $f(x)$ has greater complexity than every $x(i)$, we shall easily conclude that $f(x)$ cannot be a sub-formula of $x(i)$.

Proposition 22 *Let X be a universal algebra of type α with free generator $X_0 \subseteq X$. Then for all $x, y \in X$ we have:*

$$x \preceq y \;\Rightarrow\; \omega(x) \leq \omega(y)$$

where $\omega : X \to \mathbf{N}$ is the order mapping of definition (8).

Proof
Given $y \in X$ consider the property $P(y)$ defined by:

$$\forall x \in X \;,\; [\; x \in \mathrm{Sub}(y) \;\Rightarrow\; \omega(x) \leq \omega(y) \;]$$

We shall complete the proof of this proposition by showing $P(y)$ is true for all $y \in X$, which we shall do by a structural induction argument using theorem (3) of page 31. First we assume that $y \in X_0$. Then $\mathrm{Sub}(y) = \{y\}$ and the condition $x \in \mathrm{Sub}(y)$ implies that $x = y$ and in particular $\omega(x) \leq \omega(y)$. So the property $P(y)$ is true whenever $y \in X_0$. Next we assume that $f \in \alpha$ and $y \in X^{\alpha(f)}$ are such that $P(y(i))$ is true for all $i \in \alpha(f)$. We need to show the property $P(f(y))$

is also true. So let $x \in X$ be such that $x \in \mathrm{Sub}(f(y))$. We need to show that $\omega(x) \leq \omega(f(y))$. From definition (19) we have:

$$\mathrm{Sub}(f(y)) = \{f(y)\} \cup \bigcup_{i \in \alpha(f)} \mathrm{Sub}(y(i))$$

Hence the condition $x \in \mathrm{Sub}(f(y))$ implies that $x = f(y)$ or $x \in \mathrm{Sub}(y(i))$ for some $i \in \alpha(f)$. Suppose first that $x = f(y)$. Then $\omega(x) \leq \omega(f(y))$ follows immediately. Suppose now that $x \in \mathrm{Sub}(y(i))$ for some $i \in \alpha(f)$. Having assumed the property $P(y(i))$ is true, it follows that $\omega(x) \leq \omega(y(i))$. Using proposition (8) we obtain:

$$\omega(x) \leq \omega(y(i)) < 1 + \max\{\omega(y(i)) : i \in \alpha(f)\} = \omega(f(y))$$

So we have proved that $\omega(x) < \omega(f(y))$ and in particular $\omega(x) \leq \omega(f(y))$. This completes our induction argument and the proof that $P(y)$ holds for all $y \in X$.
.

Proposition 23 *Let X be a free universal algebra of type α with free generator $X_0 \subseteq X$. The relation $\preceq$ on X is anti-symmetric.*

Proof
Given $x, y \in X$ we have to show that if $x \preceq y$ and $y \preceq x$ then $x = y$. Given $y \in X$ consider the property $P(y)$ defined by:

$$\forall x \in X \ , \ [(x \preceq y) \wedge (y \preceq x) \ \Rightarrow \ (x = y) \ ]$$

We shall complete the proof of this proposition by showing $P(y)$ is true for all $y \in X$, which we shall do by a structural induction argument using theorem (3) of page 31. First we assume that $y \in X_0$. We need to show that $P(y)$ is true. So let $x \in X$ be such that $x \preceq y$ and $y \preceq x$. In particular we have $x \preceq y$, i.e. $x \in \mathrm{Sub}(y)$. From $y \in X_0$ we obtain $\mathrm{Sub}(y) = \{y\}$ and we conclude that $x = y$ as requested. So $P(y)$ is indeed true for all $y \in X_0$. Next we assume that $f \in \alpha$ and $y \in X^{\alpha(f)}$ are such that $P(y(i))$ is true for all $i \in \alpha(f)$. We need to show that $P(f(y))$ is also true. So let $x \in X$ be such that $x \preceq f(y)$ and $f(y) \preceq x$. We need to show that $x = f(y)$. Suppose to the contrary that $x \neq f(y)$. We shall arrive at a contradiction. From $x \preceq f(y)$ we obtain $x \in \mathrm{Sub}(f(y))$ and from definition (19) we have:

$$\mathrm{Sub}(f(y)) = \{f(y)\} \cup \bigcup_{i \in \alpha(f)} \mathrm{Sub}(y(i)) \tag{1.16}$$

Having assumed that $x \neq f(y)$ it follows that $x \in \mathrm{Sub}(y(i))$ for some $i \in \alpha(f)$. Hence we have proved that $x \preceq y(i)$ for some $i \in \alpha(f)$. However, it is clear from equation (1.16) that $\mathrm{Sub}(y(i)) \subseteq \mathrm{Sub}(f(y))$ and it follows from proposition (21) that $y(i) \preceq f(y)$. From the assumption $f(y) \preceq x$, we obtain $y(i) \preceq x$ by transitivity. Hence we see that $x \in X$ is an element such that $x \preceq y(i)$ and $y(i) \preceq x$. From our induction hypothesis, we know that $P(y(i))$ is true. From

$x \preceq y(i)$ and $y(i) \preceq x$ we therefore obtain $x = y(i)$. In particular, using proposition (6) of page 24 we have:

$$\omega(x) = \omega(y(i)) < 1 + \max\{\omega(y(i)) : i \in \alpha(f)\} = \omega(f(y))$$

So we have proved that $\omega(x) < \omega(f(y))$. However, from $f(y) \preceq x$ and proposition (22) we obtain $\omega(f(y)) \leq \omega(x)$. This is our desired contradiction. .

Proposition 24 *Let X be a free universal algebra of type α with free generator $X_0 \subseteq X$. The relation $\preceq$ on X is a partial order.*

Proof
The relation $\preceq$ is reflexive, anti-symmetric and transitive as can be seen from propositions (20), (23) and (21) respectively. It is therefore a partial order. .

1.4.3 Increasing Map on Free Universal Algebra

Recall that a pre-ordered set is an ordered pair $(A, \leq)$ where A is a set and $\leq$ is a preorder on A, namely a binary relation on A which is reflexive and transitive. In the following chapters, we shall encounter many cases of maps $v : X \to A$ where X is a free universal algebra and A is pre-ordered set. For example, if $X = \mathbf{P}(V)$ is the free universal algebra of first order logic of definition (23) and $A = \mathcal{P}(V)$ is the power set of V (the set of variables), we shall encounter the maps $\text{Var} : X \to A$ and $\text{Bnd} : X \to A$ which respectively return the set of variables and bound variables of a formula $\phi \in X$. Another example is $X = \mathbf{\Pi}(V)$ of definition (65), i.e. the free universal algebra of proofs on $\mathbf{P}(V)$ for which we shall have a map $\text{Hyp} : X \to A$ where $A = \mathcal{P}(\mathbf{P}(V))$ returning the set of all hypothesis of a proof $\pi \in X$. We shall also have a map $\text{Var} : \mathbf{\Pi}(V) \to A$ where $A = \mathcal{P}(V)$ returning the set of variables being used in a proof $\pi \in X$. All these cases are examples of maps $v : X \to A$ which are *increasing* in the sense that $v(x) \leq v(y)$ whenever x is a sub-formula of y i.e. $x \preceq y$. For example if ψ is a sub-formula of ϕ then $\text{Var}(\psi) \subseteq \text{Var}(\phi)$, or if ρ is a sub-proof of π then $\text{Hyp}(\rho) \subseteq \text{Hyp}(\pi)$. The following proposition allows us to establish this type of result once and for all with the right level of abstraction.

Proposition 25 *Let X be a free universal algebra of type α with free generator $X_0 \subseteq X$. Let $(A, \leq)$ be a pre-ordered set and $v : X \to A$ be a map such that:*

$$\forall i \in \alpha(f)\ ,\ v(x(i)) \leq v(f(x))$$

for all $f \in \alpha$ and $x \in X^{\alpha(f)}$. Then for all $x, y \in X$ we have the implication:

$$x \preceq y \ \Rightarrow\ v(x) \leq v(y)$$

Proof
Given $y \in X$ we need to show the property: $\forall x \in X\ \ [\, x \preceq y \ \Rightarrow\ v(x) \leq v(y)\,]$. We shall do so by structural induction using theorem (3) of page 31. First we

assume that $y \in X_0$. We need to show the property is true for y. So let $x \preceq y$ be a sub-formula of y. We need to show that $v(x) \leq v(y)$. However, since $y \in X_0$ we have $\mathrm{Sub}(y) = \{y\}$. So from $x \preceq y$ we obtain $x \in \mathrm{Sub}(y)$ and consequently $x = y$. So $v(x) \leq v(y)$ follows from the reflexivity of the preorder $\leq$. Next we assume that $f \in \alpha$ and $y \in X^{\alpha(f)}$ is such that $y(i)$ satisfies our property for all $i \in \alpha(f)$. We need to show that same is true of $f(y)$. So let $x \preceq f(y)$ be a sub-formula of $f(y)$. We need to show that $v(x) \leq v(f(y))$. However we have:

$$x \in \mathrm{Sub}(f(y)) = \{f(y)\} \cup \bigcup_{i \in \alpha(f)} \mathrm{Sub}(y(i))$$

So we shall distinguish two cases: first we assume that $x = f(y)$. Then the inequality $v(x) \leq v(f(y))$ follows from the reflexivity of $\leq$. Next we assume that $x \in \mathrm{Sub}(y(i))$ for some $i \in \alpha(f)$. Then we have $x \preceq y(i)$ and having assumed $y(i)$ satisfies our induction property, we obtain $v(x) \leq v(y(i))$. However, by assumption we have $v(y(i)) \leq v(f(y))$ and $v(x) \leq v(f(y))$ follows from the transitivity of the preorder $\leq$ on A. This completes our induction argument. .

1.4.4 Structural Substitution between Free Algebras

If V and W are sets and $\sigma : V \to W$ is a map, we shall see from definition (24) and definition (74) that it is possible to define corresponding $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ or $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ which are substitutions of variable inside formulas or inside proofs. These maps are not morphisms of free universal algebras, if only because $\mathbf{P}(V)$ and $\mathbf{P}(W)$ do not have the same type. However, these maps are pretty close to being morphism, and we shall now study some of their common properties under the possible abstraction of *structural substitution*. Recall that given a type of universal algebra α and $f \in \alpha$, the arity of f is denoted $\alpha(f)$.

Definition 21 *Let α and β be two types of universal algebra. We say that a map $q : \alpha \to \beta$ is* arity preserving*, if and only if for all $f \in \alpha$ we have:*

$$\beta \circ q(f) = \alpha(f)$$

In other words the arity of the operator $q(f) \in \beta$ is the same as that of $f \in \alpha$.

Recall that the 'σ' which appears on the right-hand-side of (ii) in definition (21) below refers to the map $\sigma : X^{\alpha(f)} \to Y^{\alpha(f)}$ defined by $\sigma(x)(i) = \sigma(x(i))$ for all $i \in \alpha(f)$. It follows that the expression $q(f)(\sigma(x))$ is always meaningful since $q : \alpha \to \beta$ is arity preserving and $\alpha(f)$ is precisely the arity of $q(f)$.

Definition 22 *Let X, Y be free universal algebras of type α, β and with free generators X_0, Y_0 respectively. A map $\sigma : X \to Y$ is a* structural substitution *if and only if there exists an arity preserving map $q : \alpha \to \beta$ such that:*

$$\begin{array}{ll} (i) & x \in X_0 \ \Rightarrow \ \sigma(x) \in Y_0 \\ (ii) & x \in X^{\alpha(f)} \ \Rightarrow \ \sigma(f(x)) = q(f)(\sigma(x)) \end{array}$$

where (ii) holds for all $f \in \alpha$.

One of the motivations to consider structural substitutions is to prove the following proposition in a general setting. If $\sigma : X \to Y$ is a structural substitution between two free universal algebras, then given $x, y \in X$ we have:

$$y \preceq x \;\Rightarrow\; \sigma(y) \preceq \sigma(x)$$

In other words, if y is a sub-formula of x then $\sigma(y)$ is also a sub-formula of $\sigma(x)$. This property can be summarized with the inclusion $\sigma(\mathrm{Sub}(x)) \subseteq \mathrm{Sub}(\sigma(x))$ for all $x \in X$. As it turns out, the reverse inclusion is also true:

Proposition 26 *Let X, Y be free universal algebras and $\sigma : X \to Y$ be a structural substitution. Then for all $x \in X$ we have the equality:*

$$\mathrm{Sub}(\sigma(x)) = \sigma(\mathrm{Sub}(x))$$

i.e. the sub-formulas of $\sigma(x)$ are the images of the sub-formulas of x by σ.

Proof
Given $x \in X$ we need to show that $\mathrm{Sub}(\sigma(x)) = \sigma(\mathrm{Sub}(x))$. We shall do so with a structural induction argument, using theorem (3) of page 31. First we assume that $x \in X_0$. Since $\sigma : X \to Y$ is structural we have $\sigma(x) \in Y_0$ and so:

$$\mathrm{Sub}(\sigma(x)) = \{\sigma(x)\} = \sigma(\{x\}) = \sigma(\mathrm{Sub}(x))$$

So let $f \in \alpha$ and $x \in X^{\alpha(f)}$ be such that the equality is true for all $x(i)$ with $i \in \alpha(f)$. We need to show the equality is also true for $f(x)$. Since $\sigma : X \to Y$ is a structural substitution, let $q : \alpha \to \beta$ be an arity preserving map for which (ii) of definition (21) holds. Then we have the equalities:

$$\begin{aligned}
\mathrm{Sub}(\sigma(f(x))) &= \mathrm{Sub}(\, q(f)(\sigma(x))\,) \\
\text{def. (19)} \;\to\; &= \{\, q(f)(\sigma(x))\,\} \cup \bigcup_{i \in \beta(q(f))} \mathrm{Sub}(\,\sigma(x)(i)\,) \\
q \text{ arity preserving} \;\to\; &= \{\sigma(f(x))\} \cup \bigcup_{i \in \alpha(f)} \mathrm{Sub}(\,\sigma(x(i))\,) \\
\text{induction} \;\to\; &= \{\sigma(f(x))\} \cup \bigcup_{i \in \alpha(f)} \sigma(\,\mathrm{Sub}(x(i))\,) \\
&= \sigma(\,\{f(x)\} \cup \bigcup_{i \in \alpha(f)} \mathrm{Sub}(x(i))\,) \\
\text{def. (19)} \;\to\; &= \sigma(\,\mathrm{Sub}(f(x))\,)
\end{aligned}$$

.

Chapter 2

The Free Universal Algebra of First Order Logic

2.1 Formula of First Order Logic

2.1.1 Preliminaries

This work is an attempt to provide an *algebraization of first order logic with terms and without equality*. Due to personal ignorance, we are not in a position to say much of the history of this problem, or the existing literature. We shall nonetheless endeavor to give here an honest account of our little understanding. Any specialist who believes this account can be improved in any way is welcome to contact the author. The idea of turning first order logic into algebra is not new. Following wikipedia, it appears Alfred Tarski initially worked on the algebraization of first order logic without terms and with equality, which led to the emergence of cylindric algebras. At a later stage, Paul Halmos developed a version without equality, which led to polyadic algebras. There is also a categorical approach initially due to William Lawvere, leading to functorial semantics. The most recent treatment of algebraization of first order logic without terms seems to be the work of Ildikó Sain in [52]. There is also the categorical work of George Voutsadakis, for example in [64] following a recent trend of *abstract algebraic logic* which seems to have been initiated by W.J. Blok and D. Pigozzi [6]. A new book [1] from Hajnal Andréka, István Németi and Ildikó Sain on algebraic logic is about to be released. There are a few older monographs on cylindric algebras such as [2] and Paul Halmos [28] on polyadic algebras. It is our understanding that most of the work done so far has focussed on first order logic *without terms*, an exception being the paper from Janis Cirulis [11], of which we are hoping to get a copy soon. The algebraization of first order logic *with terms* seems to have received far less attention than its counterpart *without terms*, as it fails to fall under the scope of currently known techniques of abstract algebraic logic. Before we complete our history tour, we would like to mention the books of

Donald W. Barnes and John M. Mack [4] and P.T. Johnstone [32] which are the initial motivation for the present work. For a mathematician not trained in formal logic, these books have something magical. It is hard for us to say if they succeeded in presenting their subject. Many of the proofs are very short and require a fair amount of maturity. This document is an attempt to follow their trail while making the material accessible to less sophisticated readers. We shall now explain our purpose in more details.

Our aim is to study mathematical statements as mathematical objects of their own. We believe universal algebras are likely to be the right tool for this study. We would like to represent the set of all possible mathematical statements as a universal algebra of some type. Without knowing much of the details at this stage, we shall call this universal algebra *the universal algebra of first order logic*. The elements of this universal algebra will be called *formulas of first order logic*. It may appear as somewhat naive to refer to *the* universal algebra of first order logic as if we had some form of uniqueness property. There are after all many logical systems which may be classified as *first order*, and many more algebras arising from these systems. However, we are looking for an algebra which is minimal in some sense, and encompasses *the language of* **ZF** on which most of modern mathematics can be built. When looking at a given mathematical statement, we are often casually told that it could be (at least in principle) coded into the language of **ZF**. Oh really? We would love to see that. There are so many issues surrounding this question, it does not seem obvious at all. One cannot simply define predicates of ever increasing complexity and hope to blindly substitutes these definitions within formulas. Most mathematical objects are not uniquely defined as sets, but are complex structures which are known up to isomorphism. The list of difficulties is endless. And there is of course category theory. Granted category theory will never fit into the language of **ZF**, so we shall need another algebra for that. But who knows? it may be that *the universal algebra of first order logic* will be applicable to category theory: once we can formally define a predicate of a single variable, we can formally define a class as a proper mathematical object and dwell into the wonders of meta-mathematics without the intuition and the hand waving.

So much for finding the names. The real challenge is to determine the appropriate definitions. We saw in theorem (9) of page 56, that there was no loss of generality in viewing our universal algebra as a quotient of a free universal algebra, modulo the right congruence. One possible way to define the universal algebra of first order logic is therefore to provide specific answers to the following questions: First, a free generator X_0 needs to be chosen. We then need to agree on a specific type of universal algebra α in order to derive a free universal algebra X of type α with free generator X_0. Finally, a decision needs to be made on what the *appropriate* congruence $\sim$ on X should be.

These we believe are the right questions. For those already familiar with elements of formal logic, we may outline now a possible answer. Having chosen a formal language with a deductive system on it, we can consider the relation $\sim$ defined by $\phi \sim \psi$ if and only if the formulas $\phi \to \psi$ and $\psi \to \phi$ are both provable with respect to this deductive system. This choice of particular congruence gives

rise to a Lindenbaum-Tarski algebra. So it is possible our universal algebra of first order logic is just a particular case of Lindenbaum-Tarski (and it would probably have been sensible to call it that way). However at this point of the document, we do not know whether the provability of $\phi \to \psi$ is decidable. We may have heard a few things about the undecidability of first order logic and suspect that $\vdash (\phi \to \psi)$ is in fact undecidable. If this was the case, a computer would not be able to tell in general whether the equivalence $\phi \sim \psi$ holds. This would be highly unsatisfactory. Whatever congruence we eventually choose, surely we should want it to be decidable. The universal algebra of first order logic is about mathematical statements, not theorems. Those statements which happen to have the same *meaning* should be regarded as identical, and a computer program should be able to establish this identity. Those mathematical statements which happen to be mathematically equivalent should be dealt with by proof theory, model theory and set theory.

2.1.2 The Free Universal Algebra of First Order Logic

In this section, we shall limit our investigation to the free generator X_0 and type of universal algebra α, postponing the issue of congruence to later parts of this document. So we are looking to define the *free universal algebra of first order logic*. First we shall deal with the free generator X_0. The elements of X_0 should represent the most elementary mathematical statements. Things like $(x \in y)$ or $(x = y)$ are possible candidates for membership to X_0. We could also have constant symbols and regard $(0 \in y)$ or $(x = \pi)$ as elementary statements. More generally, statements such as $R[x, y]$ or even $S[s, 0, u, \pi, w]$ could be viewed as elementary statements, where R and S are so-called *predicate symbols*. We may even consider $R[f(1, y), z]$ where f is a so-called *function symbol*. As far as we are concerned, the universal algebra of first order logic should be the mathematical language of the lowest possible level. In computing terms, it should be akin to assembly language. There should be no *constant*, no *function symbol* and no *predicate symbol* beyond the customary '$\in$'. Even the equality '$=$' should be banned. The universal algebra of first order logic should contain the bare minimum required to express every standard mathematical statement. This bare minimum we believe can be based simply on elementary propositions of the form $(x \in y)$ where x and y belong to a set of variable V. So our free generator X_0 should therefore be reduced to:

$$X_0 = \{(x \in y) \ : \ x, y \in V\}$$

Turning now to the type of universal algebra α, we believe the minimal set of operations (also known as *connectives*) required to express every standard mathematical statement consists in the *contradiction constant* $\bot$, which is an operator of arity 0, the *implication operator* $\to$ which is a binary operator, and for all $x \in V$, the *quantification operator* $\forall x$ which is a unary operator. So the free universal algebra of first order logic should consist in elements of the form:

$$\bot \ , \ (x \in y) \ , \ \forall x \forall y \, (x \in y) \ , \ \forall z[(z \in x) \to (z \in y)] \ , \ \text{etc.}$$

At this point in time, we have very little to justify this choice, beyond its simplicity. Clearly, there would be no point in defining and studying a *free universal algebra of first order logic* which does not fulfill its role. At some stage, we will need to consider higher level formal languages which are actually usable by human beings to express interesting mathematics, and show that high level statements can effectively be compiled into the low level. This we believe is the only way to vindicate our choice. For now, we hope simply to reassure the reader that our conception of *bare minimum* is sensible: for example, the negation operator could be compiled as $\neg\phi = (\phi \to \bot)$, the disjunction and conjunction operators as $\phi \vee \psi = \neg\phi \to \psi$ and $\phi \wedge \psi = \neg(\neg\phi \vee \neg\psi)$ respectively, the equivalence operator as $(\phi \leftrightarrow \psi) = [(\phi \to \psi) \wedge (\psi \to \phi)]$ and finally the equality predicate as:

$$(x = y) = \forall z[(z \in x) \leftrightarrow (z \in y)] \wedge \forall z[(x \in z) \leftrightarrow (y \in z)]$$

This does not tell us how to introduce constant symbols and function symbols, and we are still a very long way to ever compile a statement such as:

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} e^{-x^2/2} dx = 1$$

We hope to address some of these questions in later parts of this document. For now, we shall rest on the belief that our *free universal algebra of first order logic* is the right tool to consider and study.

But assuming our faith is justified, assuming that interesting mathematical statements can effectively be compiled as *formulas of first order logic*, one important question still remains: why should we care about a *low level* algebra whose *mathematical statements* are so remote from day to day mathematics? Why not consider a high level language directly? The answer is twofold: From a purely mathematical point of view it is a lot easier to deal with a simple algebra. For instance, if we are looking to prove anything by structural induction, we only need to consider $(x \in y)$, $\bot$, $\to$ and $\forall x$ for all $x \in V$ which would not be the case with a more complex algebra. Furthermore from a computing perspective, we are unlikely to write sensible software unless we start from the very simple and move on to the high level. A computer chip typically understands a very limited set of instructions. High level languages are typically compiled into a sequence of these elementary tasks. Without thinking very hard on this, it is a natural thing to believe that a similar approach should be used for meta-mathematics. At the end of the day, if it is indeed the case that deep mathematical statements can be compiled as formulas of first order logic, focussing on these formulas will surely prove very useful.

Definition 23 *Let V be a set. We call* First Order Logic Type associated with V*, the type of universal algebra α defined by:*

$$\alpha = \{\bot, \to\} \cup \{\forall x \ : \ x \in V\}$$

where $\bot = ((0,0),0)$, $\to = ((1,0),2)$ and $\forall x = ((2,x),1)$ given $x \in V$.

There is no particular conditions imposed on the set V, which could be empty, finite, infinite, countable or uncountable. The set α of definition (22) is a set of ordered pairs which is functional. It is therefore a map with domain $\mathrm{dom}(\alpha) = \{(0,0),(1,0)\} \cup \{(2,x) : x \in V\}$ and range $\mathrm{rng}(\alpha) = \{0,1,2\}$. Since $\mathrm{rng}(\alpha) \subseteq \mathbf{N}$, by virtue of definition (1) α is indeed a type of universal algebra. With our customary abuse of notation described in page 6, we have $\alpha(\perp) = 0$, $\alpha(\rightarrow) = 2$ and $\alpha(\forall x) = 1$ for all $x \in V$. It follows that $\perp$ is understood to be an operator of arity 0, while $\rightarrow$ is binary and $\forall x$ is unary.

Definition 24 *Let V be a set with first order logic type α. We call* Free Universal Algebra of First Order Logic associated with V*, the free universal algebra $\mathbf{P}(V)$ of type α with free generator $\mathbf{P}_0(V) = V \times V$.*

The free universal algebra $\mathbf{P}(V)$ exists by virtue of theorem (1) of page 20. It is also unique up to isomorphism and we have $\mathbf{P}_0(V) \subseteq \mathbf{P}(V)$. For all $x, y \in V$ the ordered pair (x, y) will be denoted $(x \in y)$. It follows that the free generator $\mathbf{P}_0(V)$ of $\mathbf{P}(V)$ is exactly what we had promised:

$$\mathbf{P}_0(V) = \{(x \in y) \ : \ x, y \in V\}$$

Furthermore, we have the operators $\perp : \mathbf{P}(V)^0 \rightarrow \mathbf{P}(V)$, $\rightarrow : \mathbf{P}(V)^2 \rightarrow \mathbf{P}(V)$ and $\forall x : \mathbf{P}(V)^1 \rightarrow \mathbf{P}(V)$. We shall refer to the constant $\perp(0)$ simply as $\perp$. Given $\phi, \psi \in \mathbf{P}(V)$, we shall write $\phi \rightarrow \psi$ instead of $\rightarrow (\phi, \psi)$. Given $x \in V$ and $\phi \in \mathbf{P}(V)$, we shall write $\forall x \phi$ instead of $\forall x(\phi)$.

2.1.3 Variable Substitution in Formula

Let V be a set and $x, y, z \in V$. Then $\phi = \forall x(x \in z)$ and $\psi = \forall y(y \in z)$ are elements of $\mathbf{P}(V)$. In the case when $x \neq z$ and $y \neq z$ most of us would regard ϕ and ψ as being the same *mathematical statement*. Yet from theorem (2) of page 21, ϕ and ψ are distinct elements of $\mathbf{P}(V)$ when $x \neq y$. We are still a long way to have a clear opinion on what an appropriate congruence on $\mathbf{P}(V)$ should be. Yet we feel that whatever our choice of congruence $\sim$, we should have $\phi \sim \psi$. So we need to formalize the idea that *replacing the variable x in $\phi = \forall x(x \in z)$ by the variable y* does not change the *meaning* of the formula ϕ. The first step is for us to formally define the notion of variable substitution.

Variable substitutions is a key idea in every textbook of mathematical logic. However, the usual treatment attempts to define substitutions where variables are replaced by *terms*. Since quantification can only occur with respect to a variable, only free occurrences of variables are substituted with terms, leaving bound occurrences unchanged. This creates a major drawback: if $\sigma : V \rightarrow W$ is a map and $\phi \in \mathbf{P}(V)$, we certainly want the substituted formula $\sigma(\phi)$ to be an element of $\mathbf{P}(W)$, which would be impossible to achieve if we were to leave bound occurrences of variables unchanged. So contrary to standard practice, we shall define a notion of variable substitution where every variable is *carried over* by $\sigma : V \rightarrow W$. Defining $\sigma : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$ from the map $\sigma : V \rightarrow W$ we believe is very fruitful. This type of substitution will not be capture-avoiding in general,

but this is no different from the general treatment where we often require a term t to be *substitutable* for a variable x in ϕ, or to be *free for* x in ϕ. Note that our formal language $\mathbf{P}(V)$ has no term beyond the variables themselves. So focussing on variables only for substitutions is no restriction of generality. In our view, terms or constants should not exist in a low level mathematical statement. The constant $\pi = 3.14159\ldots$ should be a low level predicate $\pi(x)$, and given a predicate $Q(x)$ the statement $Q(\pi)$ obtained by substituting the variable x by the ground term π, should in fact be the statement $\forall x[\pi(x) \to Q(x)]$ which is syntactically a very different operation from a substitution of variable.

Definition 25 *Let V and W be two sets and $\sigma : V \to W$ be a map. We call* substitution mapping between $\mathbf{P}(V)$ and $\mathbf{P}(W)$ associated with $\sigma : V \to W$ *the map $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ defined by the structural recursion:*

$$\forall \phi \in \mathbf{P}(V)\ ,\ \sigma^*(\phi) = \begin{cases} (\sigma(x) \in \sigma(y)) & \text{if} \quad \phi = (x \in y) \\ \bot & \text{if} \quad \phi = \bot \\ \sigma^*(\phi_1) \to \sigma^*(\phi_2) & \text{if} \quad \phi = \phi_1 \to \phi_2 \\ \forall \sigma(x)\, \sigma^*(\phi_1) & \text{if} \quad \phi = \forall x \phi_1 \end{cases} \tag{2.1}$$

This is one of our first definition by *structural recursion*. The principle of such definition on a free universal algebra is justified by virtue of theorem (4) of page 42. As this is one of our first use of this theorem, we shall make sure its application is done appropriately by checking all the relevant details.

Proposition 27 *The structural recursion of* definition (24) *is legitimate.*

Proof
We need to show the existence and uniqueness of the map $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ satisfying equation (2.1). We shall do so by applying theorem (4) of page 42 to the free universal algebra $\mathbf{P}(V)$ with free generator $X_0 = \mathbf{P}_0(V)$ and the set $A = \mathbf{P}(W)$. First we define $g_0 : X_0 \to A$ by $g_0(x \in y) = (\sigma(x) \in \sigma(y))$ for all $x, y \in V$. Next, given $f \in \alpha$ we need to define an operator $h(f) : A^{\alpha(f)} \to A$. For all $\phi_1, \phi_2 \in A$ and for all $x \in V$, we set:

$$\begin{aligned} &(i) \qquad h(\bot)(0) = \bot \\ &(ii) \qquad h(\to)(\phi_1, \phi_2) = \phi_1 \to \phi_2 \\ &(iii) \qquad h(\forall x)(\phi_1) = \forall \sigma(x) \phi_1 \end{aligned}$$

Applying theorem (4) of page 42, there exists a unique map $\sigma^* : \mathbf{P}(V) \to A$ such that $\sigma^*_{|X_0} = g_0$ and for all $f \in \alpha$ and $y \in \mathbf{P}(V)^{\alpha(f)}$:

$$\sigma^*(f(y)) = h(f)(\sigma^*(y)) \tag{2.2}$$

In other words, there exists a unique map $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ such that for all $x, y \in V$ we have $\sigma^*(x \in y) = (\sigma(x) \in \sigma(y))$ and which satisfies equation (2.2). Taking $f = \bot$ and $y = 0$ in equation (2.2) we obtain:

$$\sigma^*(\bot) = \sigma^*(\bot(0)) = h(\bot)(0) = \bot \tag{2.3}$$

Taking $f = \rightarrow$ and $y = (\phi_1, \phi_2) \in \mathbf{P}(V)^2$ we obtain:

$$\sigma^*(\phi_1 \rightarrow \phi_2) = h(\rightarrow)(\sigma^*(\phi_1), \sigma^*(\phi_2)) = \sigma^*(\phi_1) \rightarrow \sigma^*(\phi_2) \tag{2.4}$$

Finally, taking $f = \forall x$ and $y = \phi_1 \in \mathbf{P}(V)^1$ given $x \in V$:

$$\sigma^*(\forall x \phi_1) = h(\forall x)(\sigma^*(\phi_1)) = \forall \sigma(x)\, \sigma^*(\phi_1) \tag{2.5}$$

Since equations (2.3), (2.4) and (2.5) are exactly as equation (2.1), we conclude there is a unique map $\sigma^* : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$ satisfying equation (2.1). **.**

Let U, V, W be sets while $\tau : U \rightarrow V$ and $\sigma : V \rightarrow W$ are maps. From definition (24) we obtain the substitution mappings $\tau^* : \mathbf{P}(U) \rightarrow \mathbf{P}(V)$ and $\sigma^* : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$. However, $\sigma \circ \tau : U \rightarrow W$ is also a map and we therefore have a substitution mapping $(\sigma \circ \tau)^* : \mathbf{P}(U) \rightarrow \mathbf{P}(W)$. One natural question to ask is whether $(\sigma \circ \tau)^*$ coincide with the composition $\sigma^* \circ \tau^*$. The following proposition shows that it is indeed the case. As a consequence, we shall be able to simplify our notations by referring to the substitution mappings τ^*, σ^* and $(\sigma \circ \tau)^*$ simply as τ, σ and $\sigma \circ \tau$, i.e. we shall *drop* the '$*$' when referring to a substitution mapping. Whether the notation '$\sigma \circ \tau$' is understood to mean $\sigma^* \circ \tau^*$ or $(\sigma \circ \tau)^*$ no longer matters since the two mappings coincide anyway.

Proposition 28 *Let U, V and W be sets. Let $\tau : U \rightarrow V$ and $\sigma : V \rightarrow W$ be maps. Let $\tau^* : \mathbf{P}(U) \rightarrow \mathbf{P}(V)$ and $\sigma^* : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$ be the substitution mappings associated with τ and σ respectively. Then:*

$$(\sigma \circ \tau)^* = \sigma^* \circ \tau^*$$

where $(\sigma \circ \tau)^* : \mathbf{P}(U) \rightarrow \mathbf{P}(W)$ is the substitution mapping associated with $\sigma \circ \tau$.

Proof
We need to show that $(\sigma \circ \tau)^*(\phi) = \sigma^* \circ \tau^*(\phi)$ for all $\phi \in \mathbf{P}(U)$. We shall do so by structural induction, using theorem (3) of page 31. Since $\mathbf{P}_0(U)$ is a generator of $\mathbf{P}(U)$, we show first that the property is true on $\mathbf{P}_0(U)$. So let $\phi = (x \in y) \in \mathbf{P}_0(U)$, where $x, y \in U$. We have:

$$(\sigma \circ \tau)^*(\phi) = (\, \sigma(\tau(x)) \in \sigma(\tau(y))\,) = \sigma^*(\, \tau(x) \in \tau(y)\,) = \sigma^* \circ \tau^*(\phi)$$

Next we check that the property is true for $\bot \in \mathbf{P}(U)$:

$$(\sigma \circ \tau)^*(\bot) = \bot = \sigma^*(\bot) = \sigma^* \circ \tau^*(\bot)$$

Next we check that the property is true for $\phi = \phi_1 \rightarrow \phi_2$, if it is true for ϕ_1, ϕ_2:

$$\begin{aligned}
(\sigma \circ \tau)^*(\phi) &= (\sigma \circ \tau)^*(\phi_1) \rightarrow (\sigma \circ \tau)^*(\phi_2) \\
&= \sigma^*(\tau^*(\phi_1)) \rightarrow \sigma^*(\tau^*(\phi_2)) \\
&= \sigma^*(\, \tau^*(\phi_1) \rightarrow \tau^*(\phi_2)\,) \\
&= \sigma^*(\tau^*(\phi_1 \rightarrow \phi_2)) \\
&= \sigma^* \circ \tau^*(\phi)
\end{aligned}$$

Finally we check that the property is true for $\phi = \forall x \phi_1$, if it is true for ϕ_1:

$$\begin{aligned}(\sigma \circ \tau)^*(\phi) &= \forall \sigma(\tau(x))\,(\sigma \circ \tau)^*(\phi_1) \\ &= \forall \sigma(\tau(x))\,\sigma^*(\tau^*(\phi_1)) \\ &= \sigma^*(\forall \tau(x) \tau^*(\phi_1)) \\ &= \sigma^*(\tau^*(\forall x \phi_1)) \\ &= \sigma^* \circ \tau^*(\phi)\end{aligned}$$

.

In the case when $W = V$ and $\sigma : V \to W$ is the identity mapping defined by $\sigma(x) = x$ for all $x \in V$, equation (2.1) of definition (24) becomes:

$$\forall \phi \in \mathbf{P}(V)\ ,\ \sigma(\phi) = \begin{cases} (x \in y) & \text{if} \quad \phi = (x \in y) \\ \bot & \text{if} \quad \phi = \bot \\ \sigma(\phi_1) \to \sigma(\phi_2) & \text{if} \quad \phi = \phi_1 \to \phi_2 \\ \forall x\, \sigma(\phi_1) & \text{if} \quad \phi = \forall x \phi_1 \end{cases}$$

It seems pretty obvious that $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$ is also the identity mapping, i.e. that $\sigma(\phi) = \phi$ for all $\phi \in \mathbf{P}(V)$. Yet, formally speaking, there seems to be no other way but to prove this once and for all. So we shall do so now:

Proposition 29 *Let V be a set and $i : V \to V$ be the identity mapping. Then, the associated substitution mapping $i : \mathbf{P}(V) \to \mathbf{P}(V)$ is also the identity.*

Proof
We need to show that $i(\phi) = \phi$ for all $\phi \in \mathbf{P}(V)$. We shall do so by structural induction, using theorem (3) of page 31. Since $\mathbf{P}_0(V)$ is a generator of $\mathbf{P}(V)$, we show first that the property is true on $\mathbf{P}_0(V)$. So let $\phi = (x \in y) \in \mathbf{P}_0(V)$:

$$i(\phi) = (\, i(x) \ \in \ i(y)\,) = (x \in y) = \phi$$

The property is clearly true for $\bot \in \mathbf{P}(V)$ since $i(\bot) = \bot$. Next we check that the property is true for $\phi = \phi_1 \to \phi_2$, if it is true for $\phi_1, \phi_2 \in \mathbf{P}(V)$:

$$i(\phi) = i(\phi_1) \to i(\phi_2) = \phi_1 \to \phi_2 = \phi$$

Finally we check that the property is true for $\phi = \forall x \phi_1$, if it is true for ϕ_1:

$$i(\phi) = \forall i(x) i(\phi_1) = \forall x \phi_1 = \phi$$

.

Since $\mathbf{P}(V)$ is a free universal algebra, every formula $\phi \in \mathbf{P}(V)$ has a well defined set of sub-formulas $\mathrm{Sub}(\phi)$ as per definition (19) of page 57. If V and W are sets and $\sigma : V \to W$ is a map with associated substitution mapping $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$, then given $\phi \in \mathbf{P}(V)$ and a sub-formula $\psi \preceq \phi$ it seems pretty obvious that the image $\sigma(\psi)$ is also a sub-formula of $\sigma(\phi)$. In fact, the converse is also true and the sub-formulas of $\sigma(\phi)$ are simply the images $\sigma(\psi)$ by σ of the sub-formulas $\psi \preceq \phi$. This property stems from the fact that $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is a structural substitution, as per definition (21).

Proposition 30 *Let V, W be sets and $\sigma : V \to W$ be a map. The associated substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is a structural substitution and for all $\phi \in \mathbf{P}(V)$:*

$$\mathrm{Sub}(\sigma(\phi)) = \sigma(\mathrm{Sub}(\phi))$$

Proof
By virtue of proposition (26) it is sufficient to prove that $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is a structural substitution as per definition (21). Let $\alpha(V)$ and $\alpha(W)$ denote the first order logic types associated with V and W respectively as per definition (22). Let $q : \alpha(V) \to \alpha(W)$ be the map defined by:

$$\forall f \in \alpha(V)\ ,\ q(f) = \begin{cases} \bot & \text{if} \quad f = \bot \\ \to & \text{if} \quad f = \to \\ \forall\sigma(x) & \text{if} \quad f = \forall x \end{cases}$$

Then q is clearly arity preserving. In order to show that σ is a structural substitution, we simply need to check that properties (i) and (ii) of definition (21) are met. First we start with property (i): so let $\phi \in \mathbf{P}_0(V)$. Then $\phi = (x \in y)$ for some $x, y \in V$ and we need to show that $\sigma(\phi) \in \mathbf{P}_0(W)$ which follows immediately from $\sigma(\phi) = \sigma(x) \in \sigma(y)$. So we now show property (ii). Given $f \in \alpha(V)$, given $\phi \in \mathbf{P}(V)^{\alpha(f)}$ we need to show that $\sigma(f(\phi)) = q(f)(\sigma(\phi))$. First we assume that $f = \bot$. Then $\alpha(f) = 0$, $\phi = 0$ and consequently:

$$\begin{aligned} \sigma(f(\phi)) &= \sigma(\bot(0)) \\ \bot(0) \text{ denoted '}\bot\text{'} \ \to &= \sigma(\bot) \\ \text{def. (24)} \ \to &= \bot \\ \bot(0) \text{ denoted '}\bot\text{'} \ \to &= \bot(0) \\ \sigma : \{0\} \to \{0\} \ \to &= q(\bot)(\sigma(0)) \\ &= q(f)(\sigma(\phi)) \end{aligned}$$

Next we assume that $f = \to$. Then $\alpha(f) = 2$ and given $\phi = (\phi_0, \phi_1)$:

$$\begin{aligned} \sigma(f(\phi)) &= \sigma(\phi_0 \to \phi_1) \\ \text{def. (24)} \ \to &= \sigma(\phi_0) \to \sigma(\phi_1) \\ \sigma : \mathbf{P}(V)^2 \to \mathbf{P}(W)^2 \ \to &= q(\to)(\sigma(\phi_0, \phi_1)) \\ &= q(f)(\sigma(\phi)) \end{aligned}$$

Finally we assume that $f = \forall x$, $x \in V$. Then $\alpha(f) = 1$ and given $\phi = (\phi_0)$:

$$\begin{aligned} \sigma(f(\phi)) &= \sigma(\forall x \phi_0) \\ \text{def. (24)} \ \to &= \forall\sigma(x)\sigma(\phi_0) \\ \sigma : \mathbf{P}(V)^1 \to \mathbf{P}(W)^1 \ \to &= q(\forall x)(\sigma(\phi_0)) \\ &= q(f)(\sigma(\phi)) \end{aligned}$$

.

2.1.4 Variable Substitution and Congruence

Let V, W be sets and $\sigma : V \to W$ be a map. From definition (24) we have a substitution mapping $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ which we still denote 'σ' by virtue of proposition (28). Suppose we have a congruence on $\mathbf{P}(V)$ and a congruence on $\mathbf{P}(W)$, both denoted $\sim$ for the purpose of this discussion. Given $\phi, \psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$, it will often be useful for us to know whether the substitution mapping σ *preserves the equivalence* of ϕ and ψ, i.e. whether $\sigma(\phi) \sim \sigma(\psi)$. When this is the case, a very common strategy to go about the proof is to consider a relation $\equiv$ on $\mathbf{P}(V)$ defined by $\phi \equiv \psi$ if and only if $\sigma(\phi) \sim \sigma(\psi)$, and to argue that $\equiv$ is in fact a congruence on $\mathbf{P}(V)$. Once we know that $\equiv$ is a congruence on $\mathbf{P}(V)$, a proof of $\sigma(\phi) \sim \sigma(\psi)$ is simply achieved by showing an inclusion of the form $R_0 \subseteq \equiv$ where R_0 is a *generator* of the congruence $\sim$ on $\mathbf{P}(V)$, in the sense of definition (18). Indeed, such an inclusion implies that $\sim \subseteq \equiv$ from which we see that for all $\phi, \psi \in \mathbf{P}(V)$ we have:

$$\phi \sim \psi \;\Rightarrow\; \sigma(\phi) \sim \sigma(\psi)$$

The following proposition confirms that $\equiv$ is a congruence on $\mathbf{P}(V)$.

Proposition 31 *Let V and W be sets and $\sigma : V \to W$ be a map. Let $\sim$ be an arbitrary congruence on $\mathbf{P}(W)$ and let $\equiv$ be the relation on $\mathbf{P}(V)$ defined by:*

$$\phi \equiv \psi \;\Leftrightarrow\; \sigma(\phi) \sim \sigma(\psi)$$

for all $\phi, \psi \in \mathbf{P}(V)$. Then $\equiv$ is a congruence on $\mathbf{P}(V)$.

Proof
Since the congruence $\sim$ on $\mathbf{P}(W)$ is an equivalence relation, $\equiv$ is clearly reflexive, symmetric and transitive on $\mathbf{P}(V)$. So we simply need to show that $\equiv$ is a congruent relation on $\mathbf{P}(V)$. Since $\sim$ is reflexive, we have $\sigma(\bot) \sim \sigma(\bot)$ and so $\bot \equiv \bot$. Suppose ϕ_1, ϕ_2, ψ_1 and $\psi_2 \in \mathbf{P}(V)$ are such that $\phi_1 \equiv \psi_1$ and $\phi_2 \equiv \psi_2$. Define $\phi = \phi_1 \to \phi_2$ and $\psi = \psi_1 \to \psi_2$. We need to show that $\phi \equiv \psi$, or equivalently that $\sigma(\phi) \sim \sigma(\psi)$. This follows from the fact that $\sigma(\phi_1) \sim \sigma(\psi_1)$, $\sigma(\phi_2) \sim \sigma(\psi_2)$ and furthermore:

$$\begin{aligned}
\sigma(\phi) &= \sigma(\phi_1 \to \phi_2) \\
&= \sigma(\phi_1) \to \sigma(\phi_2) \\
&\sim \sigma(\psi_1) \to \sigma(\psi_2) \\
&= \sigma(\psi_1 \to \psi_2) \\
&= \sigma(\psi)
\end{aligned}$$

where the intermediate $\sim$ crucially depends on $\sim$ being a congruent relation on $\mathbf{P}(W)$. We now suppose that $\phi_1, \psi_1 \in \mathbf{P}(V)$ are such that $\phi_1 \equiv \psi_1$. Let $x \in V$ and define $\phi = \forall x \phi_1$ and $\psi = \forall x \psi_1$. We need to show that $\phi \equiv \psi$, or equivalently that $\sigma(\phi) \sim \sigma(\psi)$. This follows from $\sigma(\phi_1) \sim \sigma(\psi_1)$ and:

$$\sigma(\phi) \;=\; \sigma(\forall x \phi_1)$$

$$
\begin{aligned}
&= \forall\sigma(x)\,\sigma(\phi_1)\\
&\sim \forall\sigma(x)\sigma(\psi_1)\\
&= \sigma(\forall x\psi_1)\\
&= \sigma(\psi)
\end{aligned}
$$

where the intermediate $\sim$ crucially depends on $\sim$ being a congruent relation. .

2.1.5 Variable of a Formula

Let V be a set and $x, y \in V$. Then $\phi = \forall x(x \in y)$ is an element of $\mathbf{P}(V)$. In this section, we aim to formalize the idea that the *set of variables* of ϕ is $\{x, y\}$. Hence we want to define a map $\mathrm{Var} : \mathbf{P}(V) \to \mathcal{P}(V)$ such that $\mathrm{Var}(\phi) = \{x, y\}$.

Definition 26 *Let V be a set. The map* $\mathrm{Var} : \mathbf{P}(V) \to \mathcal{P}(V)$ *defined by the following structural recursion is called* variable mapping on $\mathbf{P}(V)$*:*

$$
\forall\phi \in \mathbf{P}(V)\ ,\ \mathrm{Var}(\phi) = \begin{cases} \{x, y\} & \text{if} \quad \phi = (x \in y) \\ \emptyset & \text{if} \quad \phi = \bot \\ \mathrm{Var}(\phi_1) \cup \mathrm{Var}(\phi_2) & \text{if} \quad \phi = \phi_1 \to \phi_2 \\ \{x\} \cup \mathrm{Var}(\phi_1) & \text{if} \quad \phi = \forall x\phi_1 \end{cases} \tag{2.6}
$$

We say that $x \in V$ is a variable *of $\phi \in \mathbf{P}(V)$ if and only if $x \in \mathrm{Var}(\phi)$.*

Proposition 32 *The structural recursion of* definition (25) *is legitimate.*

Proof
We need to show the existence and uniqueness of $\mathrm{Var} : \mathbf{P}(V) \to \mathcal{P}(V)$ satisfying equation (2.6). This follows from an immediate application of theorem (4) of page 42 to the free universal algebra $\mathbf{P}(V)$ and the set $A = \mathcal{P}(V)$, using $g_0 : \mathbf{P}_0(V) \to A$ defined by $g_0(x \in y) = \{x, y\}$ for all $x, y \in V$, and the operators $h(f) : A^{\alpha(f)} \to A$ $(f \in \alpha)$ defined for all $V_1, V_2 \in A$ and $x \in V$ as:

$$
\begin{aligned}
&(i) \qquad h(\bot)(0) = \emptyset\\
&(ii) \qquad h(\to)(V_1, V_2) = V_1 \cup V_2\\
&(iii) \qquad h(\forall x)(V_1) = \{x\} \cup V_1
\end{aligned}
$$

.

Recall that a set A is said to be finite if and only if there exists a bijection $j : n \to A$ for some $n \in \mathbf{N}$. The set A is said to be infinite if it is not finite. Note that if A and B are finite sets, then $A \cup B$ is also finite. We shall accept this fact without proof in this document. The following proposition shows that a formula of first order predicate logic always has a finite number of variables.

Proposition 33 *Let V be a set and $\phi \in \mathbf{P}(V)$. Then* $\mathrm{Var}(\phi)$ *is finite.*

Proof
Given $\phi \in \mathbf{P}(V)$, we need to show that $\mathrm{Var}(\phi)$ is a finite set. We shall do so by structural induction using theorem (3) of page 31. Since $\mathbf{P}_0(V)$ is a generator of $\mathbf{P}(V)$, we first check that the property is true for $\phi \in \mathbf{P}_0(V)$. So suppose $\phi = (x \in y)$ for some $x, y \in V$. Since $\mathrm{Var}(\phi) = \{x, y\}$, it is indeed a finite set. Next we check that the property is true for $\bot \in \mathbf{P}(V)$, which is clear since $\mathrm{Var}(\bot) = \emptyset$. Next we check that the property is true for $\phi = \phi_1 \to \phi_2$, if it is true for $\phi_1, \phi_2 \in \mathbf{P}(V)$. This follows immediately from $\mathrm{Var}(\phi) = \mathrm{Var}(\phi_1) \cup \mathrm{Var}(\phi_2)$ which is clearly a finite set if both $\mathrm{Var}(\phi_1)$ and $\mathrm{Var}(\phi_2)$ are finite. Finally we check that the property is true for $\phi = \forall x \phi_1$ if it is true for ϕ_1. This is also immediate from $\mathrm{Var}(\phi) = \{x\} \cup \mathrm{Var}(\phi_1)$ and the fact that $\mathrm{Var}(\phi_1)$ is finite. **.**

In the following proposition we show that if $\psi \preceq \phi$ is a sub-formula of ϕ, then the variables of ψ are also variables of ϕ as we should expect:

Proposition 34 *Let V be a set and $\phi, \psi \in \mathbf{P}(V)$. Then we have:*

$$\psi \preceq \phi \;\Rightarrow\; \mathrm{Var}(\psi) \subseteq \mathrm{Var}(\phi)$$

Proof
This is a simple application of proposition (25) to $\mathrm{Var} : X \to A$ where $X = \mathbf{P}(V)$ and $A = \mathcal{P}(V)$ where the preorder $\leq$ on A is the usual inclusion $\subseteq$. We simply need to check that given $\phi_1, \phi_2 \in \mathbf{P}(V)$ and $x \in V$ we have the inclusions $\mathrm{Var}(\phi_1) \subseteq \mathrm{Var}(\phi_1 \to \phi_2)$, $\mathrm{Var}(\phi_2) \subseteq \mathrm{Var}(\phi_1 \to \phi_2)$ and $\mathrm{Var}(\phi_1) \subseteq \mathrm{Var}(\forall x \phi_1)$ which follow immediately from the recursive definition (25). **.**

Let V, W be sets and $\sigma : V \to W$ be a map with associated substitution mapping $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$. Given $\phi \in \mathbf{P}(V)$, the variables of ϕ are the elements of the set $\mathrm{Var}(\phi)$. The following proposition allows us to determine which are the variables of $\sigma(\phi)$. Specifically:

$$\mathrm{Var}(\sigma(\phi)) = \{\sigma(x) \;:\; x \in \mathrm{Var}(\phi)\}$$

In other words the variables of $\sigma(\phi)$ coincide with the range of the restriction $\sigma_{|\mathrm{Var}(\phi)}$. As discussed in page 19, this range is denoted $\sigma(\mathrm{Var}(\phi))$.

Proposition 35 *Let V and W be sets and $\sigma : V \to W$ be a map. Then:*

$$\forall \phi \in \mathbf{P}(V)\ ,\ \mathrm{Var}(\sigma(\phi)) = \sigma(\mathrm{Var}(\phi))$$

where $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ also denotes the associated substitution mapping.

Proof
Given $\phi \in \mathbf{P}(V)$, we need to show that $\mathrm{Var}(\sigma(\phi)) = \{\sigma(x) : x \in \mathrm{Var}(\phi)\}$. We shall do so by structural induction using theorem (3) of page 31. Since $\mathbf{P}_0(V)$ is a generator of $\mathbf{P}(V)$, we first check that the property is true for $\phi \in \mathbf{P}_0(V)$. So suppose $\phi = (x \in y) \in \mathbf{P}_0(V)$ for some $x, y \in V$. Then we have:

$$\begin{aligned} \mathrm{Var}(\sigma(\phi)) &= \mathrm{Var}(\sigma(x \in y)) \\ &= \mathrm{Var}(\,\sigma(x) \in \sigma(y)\,) \end{aligned}$$

$$
\begin{aligned}
&= \{\sigma(x), \sigma(y)\} \\
&= \{\sigma(u) : u \in \{x, y\}\} \\
&= \{\sigma(u) : u \in \mathrm{Var}(x \in y)\} \\
&= \{\sigma(x) : x \in \mathrm{Var}(\phi)\}
\end{aligned}
$$

Next we check that the property is true for $\perp \in \mathbf{P}(V)$:

$$\mathrm{Var}(\sigma(\perp)) = \mathrm{Var}(\perp) = \emptyset = \{\sigma(x) : x \in \mathrm{Var}(\perp)\}$$

Next we check that the property is true for $\phi = \phi_1 \to \phi_2$ if it is true for ϕ_1, ϕ_2:

$$
\begin{aligned}
\mathrm{Var}(\sigma(\phi)) &= \mathrm{Var}(\sigma(\phi_1 \to \phi_2)) \\
&= \mathrm{Var}(\sigma(\phi_1) \to \sigma(\phi_2)) \\
&= \mathrm{Var}(\sigma(\phi_1)) \cup \mathrm{Var}(\sigma(\phi_2)) \\
&= \{\, \sigma(x) : x \in \mathrm{Var}(\phi_1) \,\} \cup \{\, \sigma(x) : x \in \mathrm{Var}(\phi_2) \,\} \\
&= \{\, \sigma(x) : x \in \mathrm{Var}(\phi_1) \cup \mathrm{Var}(\phi_2) \,\} \\
&= \{\, \sigma(x) : x \in \mathrm{Var}(\phi_1 \to \phi_2) \,\} \\
&= \{\, \sigma(x) : x \in \mathrm{Var}(\phi) \,\}
\end{aligned}
$$

Finally we check that the property is true for $\phi = \forall x \phi_1$ if it is true for ϕ_1:

$$
\begin{aligned}
\mathrm{Var}(\sigma(\phi)) &= \mathrm{Var}(\sigma(\forall x \phi_1)) \\
&= \mathrm{Var}(\forall \sigma(x)\, \sigma(\phi_1)) \\
&= \{\, \sigma(x) \,\} \cup \mathrm{Var}(\sigma(\phi_1)) \\
&= \{\, \sigma(x) \,\} \cup \{\, \sigma(u) : u \in \mathrm{Var}(\phi_1) \,\} \\
&= \{\, \sigma(u) : u \in \{x\} \cup \mathrm{Var}(\phi_1) \,\} \\
&= \{\, \sigma(u) : u \in \mathrm{Var}(\forall x \phi_1) \,\} \\
&= \{\, \sigma(x) : x \in \mathrm{Var}(\phi) \,\}
\end{aligned}
$$

.

Let V, W be sets and $\sigma : V \to W$ be a map with associated substitution mapping $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$. It will soon be apparent that whether or not $\sigma : V \to W$ is injective plays a crucial role. For example if $\phi = \forall x \forall y (x \in y)$ with $x \neq y$ and $\sigma(x) = u$ while $\sigma(y) = v$, we obtain $\sigma(\phi) = \forall u \forall v (u \in v)$. When σ is injective we have $u \neq v$ and it is possible to argue in some sense that the *meaning* of $\sigma(\phi)$ is the same as that of ϕ. If σ is not an injective map, then we no longer have the guarantee that $u \neq v$. In that case $\sigma(\phi)$ may be equal to $\forall u \forall u (u \in u)$, which is a different mathematical statement from that of ϕ. Substitution mappings which arise from an injective map are therefore important. However, there will be cases when we shall need to consider a map $\tau : V \to W$ which is not injective. One common example is the map $[y/x] : V \to V$ defined in definition (26) which replaces a variable x by a variable y, but leaves the variable y as it is, if already present in the formula. Since $[y/x](x) = y = [y/x](y)$, this map is not injective when $x \neq y$. This map is not

the same as the map $[y:x] : V \to V$ defined in definition (27) which permutes the two variables x and y. In contrast to $[y/x]$ the permutation $[y : x]$ is an injective map. However if a formula $\phi \in \mathbf{P}(V)$ does not contain the variable y, it is easy to believe that the associated substitution mappings $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ and $[y : x] : \mathbf{P}(V) \to \mathbf{P}(V)$ have an identical effect on the formula ϕ, or in other words that $[y/x](\phi) = [y : x](\phi)$. If this is the case, many things can be said about the formula $[y/x](\phi)$ despite the fact that $[y/x]$ is not an injective map, simply because of the equality $[y/x](\phi) = [y:x](\phi)$. More generally, many things can be said about a formula $\tau(\phi)$ whenever it coincides with a formula $\sigma(\phi)$, and σ is an injective map. To achieve the equality $\sigma(\phi) = \tau(\phi)$ we only need σ and τ to coincide on $\mathrm{Var}(\phi)$ as we shall now check in the following proposition.

Proposition 36 *Let V and W be sets and $\sigma, \tau : V \to W$ be two maps. Then:*

$$\sigma_{|\mathrm{Var}(\phi)} = \tau_{|\mathrm{Var}(\phi)} \quad \Leftrightarrow \quad \sigma(\phi) = \tau(\phi)$$

for all $\phi \in \mathbf{P}(V)$, where $\sigma, \tau : \mathbf{P}(V) \to \mathbf{P}(W)$ are also the substitution mappings.

Proof
Given $\phi \in \mathbf{P}(V)$, we need to show that if σ and τ coincide on $\mathrm{Var}(\phi) \subseteq V$, then $\sigma(\phi) = \tau(\phi)$, and conversely that if $\sigma(\phi) = \tau(\phi)$, then σ and τ coincide on $\mathrm{Var}(\phi)$. We shall do so by structural induction using theorem (3) of page 31. Since $\mathbf{P}_0(V)$ is a generator of $\mathbf{P}(V)$, we first check that the equivalence is true for $\phi \in \mathbf{P}_0(V)$. So suppose $\phi = (x \in y)$ for some $x, y \in V$, and suppose furthermore that $\sigma_{|\mathrm{Var}(\phi)} = \tau_{|\mathrm{Var}(\phi)}$. Since $\mathrm{Var}(\phi) = \{x, y\}$ it follows that $\sigma(x) = \tau(x)$ and $\sigma(y) = \tau(y)$. Hence, we have the following equalities:

$$\begin{aligned} \sigma(\phi) &= \sigma(x \in y) \\ &= (\,\sigma(x) \in \sigma(y)\,) \\ &= (\,\tau(x) \in \tau(y)\,) \\ &= \tau(x \in y) \\ &= \tau(\phi) \end{aligned}$$

Conversely, if $\sigma(\phi) = \tau(\phi)$ then $(\,\sigma(x) \in \sigma(y)\,) = (\,\tau(x) \in \tau(y)\,)$ and it follows that $\sigma(x) = \tau(x)$ and $\sigma(y) = \tau(y)$. So σ and τ coincide on $\mathrm{Var}(\phi)$. Next we check that the equivalence is true for $\bot \in \mathbf{P}(V)$. Since $\mathrm{Var}(\bot) = \emptyset$, we always have the equality $\sigma_{|\mathrm{Var}(\bot)} = \emptyset = \tau_{|\mathrm{Var}(\bot)}$. Furthermore $\sigma(\bot) = \bot = \tau(\bot)$ is also always true. So the equivalence does indeed hold. Next we check that the equivalence is true for $\phi = \phi_1 \to \phi_2$, if it is true for $\phi_1, \phi_2 \in \mathbf{P}(V)$. So we assume that σ and τ coincide on $\mathrm{Var}(\phi)$. We need to prove that $\sigma(\phi) = \tau(\phi)$. However, since $\mathrm{Var}(\phi) = \mathrm{Var}(\phi_1) \cup \mathrm{Var}(\phi_2)$, σ and τ coincide both on $\mathrm{Var}(\phi_1)$ and $\mathrm{Var}(\phi_2)$. Having assumed the property is true for ϕ_1 and ϕ_2 it follows that $\sigma(\phi_1) = \tau(\phi_1)$ and $\sigma(\phi_2) = \tau(\phi_2)$. Hence:

$$\begin{aligned} \sigma(\phi) &= \sigma(\phi_1 \to \phi_2) \\ &= \sigma(\phi_1) \to \sigma(\phi_2) \end{aligned}$$

$$
\begin{aligned}
&= \tau(\phi_1) \to \tau(\phi_2) \\
&= \tau(\phi_1 \to \phi_2) \\
&= \tau(\phi)
\end{aligned}
$$

Conversely if $\sigma(\phi) = \tau(\phi)$ then we obtain $\sigma(\phi_1) \to \sigma(\phi_2) = \tau(\phi_1) \to \tau(\phi_2)$. Using theorem (2) of page 21 it follows that $\sigma(\phi_1) = \tau(\phi_1)$ and $\sigma(\phi_2) = \tau(\phi_2)$. Having assumed the equivalence is true for ϕ_1 and ϕ_2 we conclude that σ and τ coincide on $\mathrm{Var}(\phi_1)$ and $\mathrm{Var}(\phi_2)$ and consequently they coincide on $\mathrm{Var}(\phi)$. Finally we check that the equivalence is true for $\phi = \forall x \phi_1$ if it is true for ϕ_1. So we assume that σ and τ coincide on $\mathrm{Var}(\phi)$. We need to show $\sigma(\phi) = \tau(\phi)$. However, since $\mathrm{Var}(\phi) = \{x\} \cup \mathrm{Var}(\phi_1)$, σ and τ coincide on $\mathrm{Var}(\phi_1)$ and we have $\sigma(x) = \tau(x)$. Having assumed the property is true for ϕ_1 it follows that $\sigma(\phi_1) = \tau(\phi_1)$, and consequently:

$$
\begin{aligned}
\sigma(\phi) &= \sigma(\forall x \phi_1) \\
&= \forall \sigma(x)\, \sigma(\phi_1) \\
&= \forall \tau(x)\, \tau(\phi_1) \\
&= \tau(\forall x \phi_1) \\
&= \tau(\phi)
\end{aligned}
$$

Conversely if $\sigma(\phi) = \tau(\phi)$ then we obtain $\forall \sigma(x)\, \sigma(\phi_1) = \forall \tau(x)\, \tau(\phi_1)$. Using theorem (2) of page 21 it follows that $\sigma(\phi_1) = \tau(\phi_1)$ and $\sigma(x) = \tau(x)$. Having assumed the equivalence is true for ϕ_1 we conclude that σ and τ coincide on $\mathrm{Var}(\phi_1)$ and consequently they coincide on $\mathrm{Var}(\phi) = \{x\} \cup \mathrm{Var}(\phi_1)$. .

2.1.6 Substitution of Single Variable

In definition (24) we introduced the notion of substitution mapping associated with a given map. Our motivation was to formalize the idea that $\forall x(x \in z)$ and $\forall y(y \in z)$ were identical mathematical statements when $z \notin \{x, y\}$, or equivalently that replacing the variable x by the variable y in $\forall x(x \in z)$ did not change the *meaning* of the formula. We are now in a position to formally define the *substitution* of a variable by another.

Definition 27 *Let V be a set and $x, y \in V$. We call* substitution of y in place of x, *the map $[y/x] : V \to V$ defined by:*

$$
\forall u \in V \ , \ [y/x](u) = \begin{cases} y & \text{if} \quad u = x \\ u & \text{if} \quad u \neq x \end{cases}
$$

If we denote $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ the associated substitution mapping, given $\phi \in \mathbf{P}(V)$ the image $[y/x](\phi)$ is called ϕ with y in place of x *and denoted $\phi[y/x]$.*

The *substitution of y in place of x* has a fundamental flaw: it is not an injective map. In most introductory texts on mathematical logic, this is hardly a problem as the set of variables V is always assumed to be infinite. So if we wish

to argue that $\forall x \forall y(x \in y)$ is the same mathematical statement as $\forall y \forall x(y \in x)$, we can always choose a variable $z \notin \{x, y\}$ and prove the equivalence as:

$$\begin{aligned} \forall x \forall y(x \in y) &\sim \forall z \forall y(z \in y) \\ &\sim \forall z \forall x(z \in x) \\ &\sim \forall y \forall x(y \in x) \end{aligned}$$

Unfortunately, this will not be possible in the case when $V = \{x, y\}$ and $x \neq y$, i.e. when V has only two elements. As we shall see in later parts of this document, a congruence defined on $\mathbf{P}(V)$ in terms of the substitution mapping $[y/x]$ will lead to the paradoxical situation of $\forall x \forall y(x \in y) \not\sim \forall y \forall x(y \in x)$ when $V = \{x, y\}$. To remedy this fact, we shall introduce the *permutation* mapping $[y : x]$ and use this as the basis of a new congruence which will turn out to be simpler, equivalent to the traditional notion based on $[y/x]$ for V infinite, and working equally well for V finite or infinite.

Definition 28 *Let V be a set and $x, y \in V$. We call* permutation of x and y, *the map $[y : x] : V \to V$ defined by:*

$$\forall u \in V \ , \ [y : x](u) = \begin{cases} y & \text{if} \quad u = x \\ x & \text{if} \quad u = y \\ u & \text{if} \quad u \notin \{x, y\} \end{cases}$$

If we denote $[y : x] : \mathbf{P}(V) \to \mathbf{P}(V)$ the associated substitution mapping, given $\phi \in \mathbf{P}(V)$ the image $[y : x](\phi)$ is denoted $\phi[y : x]$.

An immediate consequence of this definition is:

Proposition 37 *Let V, W be sets and $\sigma : V \to W$ be an injective map. Then for all $x, y \in V$ we have the following equality:*

$$\sigma \circ [y : x] = [\sigma(y) : \sigma(x)] \circ \sigma$$

Proof
Let $u \in V$. We shall distinguish three cases. First we assume $u \notin \{x, y\}$. Then:

$$\sigma \circ [y : x](u) = \sigma(u) = [\sigma(y) : \sigma(x)] \circ \sigma(u)$$

where the last equality crucially depends on $\sigma(u) \notin \{\sigma(x), \sigma(y)\}$ which itself follows from the injectivity of σ and $u \notin \{x, y\}$. We now assume that $u = x$:

$$\begin{aligned} \sigma \circ [y : x](u) &= \sigma(y) \\ &= [\sigma(y) : \sigma(x)] \circ \sigma(x) \\ &= [\sigma(y) : \sigma(x)] \circ \sigma(u) \end{aligned}$$

Finally, we assume that $u = y$ and obtain:

$$\begin{aligned} \sigma \circ [y : x](u) &= \sigma(x) \\ &= [\sigma(y) : \sigma(x)] \circ \sigma(y) \\ &= [\sigma(y) : \sigma(x)] \circ \sigma(u) \end{aligned}$$

In all cases we see that $\sigma \circ [y:x](u) = [\sigma(y):\sigma(x)] \circ \sigma(u)$ as requested. .

As already noted, the permutation $[y:x]$ is injective while the substitution $[y/x]$ is not. However, there will be cases when the formulas $\phi[y/x]$ and $\phi[y:x]$ coincide, given a formula ϕ. Knowing when the equality holds is important and one simple sufficient condition is $y \notin \mathrm{Var}(\phi)$, as will be seen from the following:

Proposition 38 *Let V be a set and $U \subseteq V$. Then for all $x, y \in V$ we have:*

$$y \notin U \;\Rightarrow\; [y/x]_{|U} = [y:x]_{|U}$$

Proof
We assume that $y \notin U$. Let $u \in U$. We need to show that $[y/x](u) = [y:x](u)$. We shall distinguish three cases: first we assume that $u \notin \{x, y\}$. Then the equality is clear. Next we assume that $u = x$. Then the equality is also clear. Finally we assume that $u = y$. In fact, this cannot occur since $y \notin U$ and $u \in U$.
.

Proposition 39 *Let V be a set and $x, y \in V$. Let $\phi \in \mathbf{P}(V)$. Then, we have:*

$$y \notin \mathrm{Var}(\phi) \;\Rightarrow\; \phi[y/x] = \phi[y:x]$$

Proof
We assume that $y \notin \mathrm{Var}(\phi)$. We need to show that $\phi[y/x] = \phi[y:x]$. From proposition (36) it is sufficient to show that $[y/x]$ and $[y:x]$ coincide on $\mathrm{Var}(\phi)$, which follows immediately from $y \notin \mathrm{Var}(\phi)$ and proposition (38). .

When replacing a variable x by a variable y in a formula ϕ, and subsequently replacing the variable y by a variable z, we would expect the outcome to be the same as replacing the variable x by the variable z directly. This is in fact the case, provided y is not already a variable of ϕ. Assuming x, y and z are distinct variables, a simple counterexample is $\phi = (x \in y)$.

Proposition 40 *Let V be a set and $x, y, z \in V$. Then for all $\phi \in \mathbf{P}(V)$:*

$$y \notin \mathrm{Var}(\phi) \;\Rightarrow\; \phi[y/x][z/y] = \phi[z/x]$$

Proof
Suppose $y \notin \mathrm{Var}(\phi)$. We need to show that $[z/y] \circ [y/x](\phi) = [z/x](\phi)$. From proposition (36) it is sufficient to prove that $[z/y] \circ [y/x]$ and $[z/x]$ coincide on $\mathrm{Var}(\phi)$. So let $u \in \mathrm{Var}(\phi)$. We need to show that $[z/y] \circ [y/x](u) = [z/x](u)$. Since $y \notin \mathrm{Var}(\phi)$ we have $u \neq y$. Suppose first that $u = x$. Then we have:

$$[z/y] \circ [y/x](u) = [z/y](y) = z = [z/x](u)$$

Suppose now that $u \neq x$. Then $u \notin \{x, y\}$ and furthermore:

$$[z/y] \circ [y/x](u) = [z/y](u) = u = [z/x](u)$$

In any case, we have proved that $[z/y] \circ [y/x](u) = [z/x](u)$. .

When replacing a variable x by a variable y in a formula ϕ, we would expect all occurrences of the variable x to have disappeared in $\phi[y/x]$. In other words, we would expect the variable x *not* to be a variable of the formula $\phi[y/x]$. This is indeed the case when $x \neq y$, a condition which may easily be forgotten.

Proposition 41 *Let V be a set, $x, y \in V$ with $x \neq y$. Then for all $\phi \in \mathbf{P}(V)$:*

$$x \notin \mathrm{Var}(\phi[y/x])$$

Proof
Suppose to the contrary that $x \in \mathrm{Var}(\phi[y/x])$. From proposition (35), we have $\mathrm{Var}(\phi[y/x]) = [y/x](\mathrm{Var}(\phi))$. So there exists $u \in \mathrm{Var}(\phi)$ such that $x = [y/x](u)$. If $x \neq u$ we obtain $[y/x](u) = u$ and consequently $x = u$. If $x = u$ we obtain $[y/x](u) = y$ and consequently $x = y$. In both cases we obtain a contradiction.
.

2.1.7 Free Variable of a Formula

When $\phi = \forall x(x \in y)$ the variables of ϕ are x and y i.e. $\mathrm{Var}(\phi) = \{x, y\}$. However, it is clear that a critical distinction exists between the role played by the variables x and y. The situation is very similar to that of an integral $\int f(x, y)\, dx$ where x is nothing but a dummy variable. A dummy variable can be replaced. In contrast, the variable y cannot be replaced without affecting much of what is *meant* by the integral, or the formula ϕ. The variable y is called a *free variable* of the formula ϕ. In this section, we formally define the notion of free variable and prove a few elementary properties which are related to it.

Definition 29 *Let V be a set. The map* $\mathrm{Fr} : \mathbf{P}(V) \to \mathcal{P}(V)$ *defined by the following structural recursion is called* free variable mapping on $\mathbf{P}(V)$*:*

$$\forall \phi \in \mathbf{P}(V)\ ,\ \mathrm{Fr}(\phi) = \begin{cases} \{x, y\} & \text{if} \quad \phi = (x \in y) \\ \emptyset & \text{if} \quad \phi = \bot \\ \mathrm{Fr}(\phi_1) \cup \mathrm{Fr}(\phi_2) & \text{if} \quad \phi = \phi_1 \to \phi_2 \\ \mathrm{Fr}(\phi_1) \setminus \{x\} & \text{if} \quad \phi = \forall x \phi_1 \end{cases} \tag{2.7}$$

We say that $x \in V$ is a free variable *of $\phi \in \mathbf{P}(V)$ if and only if $x \in \mathrm{Fr}(\phi)$.*

Proposition 42 *The structural recursion of* definition (28) *is legitimate.*

Proof
We need to show the existence and uniqueness of $\mathrm{Fr} : \mathbf{P}(V) \to \mathcal{P}(V)$ satisfying equation (2.7). This follows from an immediate application of theorem (4) of page 42 to the free universal algebra $\mathbf{P}(V)$ and the set $A = \mathcal{P}(V)$, using $g_0 : \mathbf{P}_0(V) \to A$ defined by $g_0(x \in y) = \{x, y\}$ for all $x, y \in V$, and the operators $h(f) : A^{\alpha(f)} \to A$ $(f \in \alpha)$ defined for all $V_1, V_2 \in A$ and $x \in V$ as:

$$\begin{aligned} &(i) && h(\bot)(0) = \emptyset \\ &(ii) && h(\to)(V_1, V_2) = V_1 \cup V_2 \\ &(iii) && h(\forall x)(V_1) = V_1 \setminus \{x\} \end{aligned}$$

.

In proposition (35), given a map $\sigma : V \to W$ with associated substitution mapping $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ and given a formula ϕ, we checked that the variables

of $\sigma(\phi)$ were simply the elements of the direct image of $\mathrm{Var}(\phi)$ by σ, that is $\mathrm{Var}(\sigma(\phi)) = \sigma(\mathrm{Var}(\phi))$. We now show two similar results for the free variables of $\sigma(\phi)$, namely $\mathrm{Fr}(\sigma(\phi)) \subseteq \sigma(\mathrm{Fr}(\phi))$ in the general case and $\mathrm{Fr}(\sigma(\phi)) = \sigma(\mathrm{Fr}(\phi))$ in the case when some restriction is imposed on the map σ, which we require to be injective on the domain $\mathrm{Var}(\phi)$. If $\phi = \forall x(x \in y)$ and σ is not injective on $\{x, y\}$, then it is possible to have $\sigma(\phi) = \forall x(x \in x)$ which would clearly contradict $\mathrm{Fr}(\sigma(\phi)) = \sigma(\mathrm{Fr}(\phi))$. However, the requirement that $\sigma_{|\mathrm{Var}(\phi)}$ be injective will be shown to be sufficient but is not necessary. If $\phi = (x \in y)$ and $\sigma = [y/x]$, we have $\sigma(\phi) = (y \in y)$ and the equality $\mathrm{Fr}(\sigma(\phi)) = \sigma(\mathrm{Fr}(\phi))$ still holds. We start with the general case leading to the weaker inclusion:

Proposition 43 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\phi \in \mathbf{P}(V)$:*

$$\mathrm{Fr}(\sigma(\phi)) \subseteq \sigma(\mathrm{Fr}(\phi))$$

where $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ also denotes the associated substitution mapping.

Proof
Given $\phi \in \mathbf{P}(V)$, we need to show the inclusion $\mathrm{Fr}(\sigma(\phi)) \subseteq \{\sigma(x) : x \in \mathrm{Fr}(\phi)\}$. We shall do so by structural induction using theorem (3) of page 31. Since $\mathbf{P}_0(V)$ is a generator of $\mathbf{P}(V)$, we first check that the property is true for $\phi \in \mathbf{P}_0(V)$. So suppose $\phi = (x \in y) \in \mathbf{P}_0(V)$ for some $x, y \in V$. Then, we have:

$$\begin{aligned}
\mathrm{Fr}(\sigma(\phi)) &= \mathrm{Fr}(\sigma(x \in y)) \\
&= \mathrm{Fr}(\,\sigma(x) \in \sigma(y)\,) \\
&= \{\sigma(x), \sigma(y)\} \\
&= \{\sigma(u) : u \in \{x, y\}\} \\
&= \{\sigma(u) : u \in \mathrm{Fr}(x \in y)\} \\
&= \{\sigma(x) : x \in \mathrm{Fr}(\phi)\}
\end{aligned}$$

Having proved the equality, it follows in particular that the inclusion $\subseteq$ is true. Next we check that the property is true for $\bot \in \mathbf{P}(V)$:

$$\mathrm{Fr}(\sigma(\bot)) = \mathrm{Fr}(\bot) = \emptyset \subseteq \{\sigma(x) : x \in \mathrm{Fr}(\bot)\}$$

Next we check that the property is true for $\phi = \phi_1 \to \phi_2$ if it is true for ϕ_1, ϕ_2:

$$\begin{aligned}
\mathrm{Fr}(\sigma(\phi)) &= \mathrm{Fr}(\sigma(\phi_1 \to \phi_2)) \\
&= \mathrm{Fr}(\sigma(\phi_1) \to \sigma(\phi_2)) \\
&= \mathrm{Fr}(\sigma(\phi_1)) \cup \mathrm{Fr}(\sigma(\phi_2)) \\
&\subseteq \{\,\sigma(x) : x \in \mathrm{Fr}(\phi_1)\,\} \cup \{\,\sigma(x) : x \in \mathrm{Fr}(\phi_2)\,\} \\
&= \{\,\sigma(x) : x \in \mathrm{Fr}(\phi_1) \cup \mathrm{Fr}(\phi_2)\,\} \\
&= \{\,\sigma(x) : x \in \mathrm{Fr}(\phi_1 \to \phi_2)\,\} \\
&= \{\,\sigma(x) : x \in \mathrm{Fr}(\phi)\,\}
\end{aligned}$$

Finally we check that the property is true for $\phi = \forall x \phi_1$ if it is true for ϕ_1:

$$\begin{array}{rcl} \mathrm{Fr}(\sigma(\phi)) & = & \mathrm{Fr}(\sigma(\forall x \phi_1)) \\ & = & \mathrm{Fr}(\forall \sigma(x)\, \sigma(\phi_1)) \\ & = & \mathrm{Fr}(\sigma(\phi_1)) \setminus \{\sigma(x)\} \\ & \subseteq & \{\, \sigma(u) : u \in \mathrm{Fr}(\phi_1)\,\} \setminus \{\sigma(x)\} \\ \text{see below} \rightarrow & \subseteq & \{\, \sigma(u) : u \in \mathrm{Fr}(\phi_1) \setminus \{x\}\,\} \\ & = & \{\, \sigma(u) : u \in \mathrm{Fr}(\forall x \phi_1)\,\} \\ & = & \{\, \sigma(x) : x \in \mathrm{Fr}(\phi)\,\} \end{array}$$

We shall complete the proof by justifying the used inclusion:

$$\{\, \sigma(u) : u \in \mathrm{Fr}(\phi_1)\,\} \setminus \{\sigma(x)\} \subseteq \{\, \sigma(u) : u \in \mathrm{Fr}(\phi_1) \setminus \{x\}\,\}$$

So suppose $y = \sigma(u)$ for some $u \in \mathrm{Fr}(\phi_1)$ and $y \neq \sigma(x)$. Then in particular $u \neq x$, and if follows that $y = \sigma(u)$ with $u \in \mathrm{Fr}(\phi_1) \setminus \{x\}$. .

We now prove a second version of proposition (43) which requires stronger assumptions but leads to an equality rather than mere inclusion:

Proposition 44 *Let V and W be sets and $\sigma : V \to W$ be a map. Let $\phi \in \mathbf{P}(V)$ be such that $\sigma_{|\mathrm{Var}(\phi)}$ is an injective map. Then, we have:*

$$\mathrm{Fr}(\sigma(\phi)) = \sigma(\mathrm{Fr}(\phi))$$

where $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ also denotes the associated substitution mapping.

Proof
Given $\phi \in \mathbf{P}(V)$ such that $\sigma_{|\mathrm{Var}(\phi)}$ is injective, we need to show the equality $\mathrm{Fr}(\sigma(\phi)) = \{\sigma(x) : x \in \mathrm{Fr}(\phi)\}$. We shall do so by structural induction using theorem (3) of page 31. Since $\mathbf{P}_0(V)$ is a generator of $\mathbf{P}(V)$, we first check that the property is true for $\phi \in \mathbf{P}_0(V)$. So suppose $\phi = (x \in y) \in \mathbf{P}_0(V)$ for some $x, y \in V$. Then, regardless of whether $\sigma(x) = \sigma(y)$ or not, we have:

$$\begin{array}{rcl} \mathrm{Fr}(\sigma(\phi)) & = & \mathrm{Fr}(\sigma(x \in y)) \\ & = & \mathrm{Fr}(\, \sigma(x) \in \sigma(y)\,) \\ & = & \{\sigma(x), \sigma(y)\} \\ & = & \{\sigma(u) : u \in \{x, y\}\} \\ & = & \{\sigma(u) : u \in \mathrm{Fr}(x \in y)\} \\ & = & \{\sigma(x) : x \in \mathrm{Fr}(\phi)\} \end{array}$$

Next we check that the property is true for $\perp \in \mathbf{P}(V)$:

$$\mathrm{Fr}(\sigma(\perp)) = \mathrm{Fr}(\perp) = \emptyset = \{\sigma(x) : x \in \mathrm{Fr}(\perp)\}$$

Next we check that the property is true for $\phi = \phi_1 \to \phi_2$ if it is true for ϕ_1, ϕ_2. Note that if $\sigma_{|\mathrm{Var}(\phi)}$ is injective, it follows from $\mathrm{Var}(\phi) = \mathrm{Var}(\phi_1) \cup \mathrm{Var}(\phi_2)$

that both $\sigma_{|\mathrm{Var}(\phi_1)}$ and $\sigma_{|\mathrm{Var}(\phi_2)}$ are injective, and consequently:

$$\begin{aligned}
\mathrm{Fr}(\sigma(\phi)) &= \mathrm{Fr}(\sigma(\phi_1 \to \phi_2)) \\
&= \mathrm{Fr}(\sigma(\phi_1) \to \sigma(\phi_2)) \\
&= \mathrm{Fr}(\sigma(\phi_1)) \cup \mathrm{Fr}(\sigma(\phi_2)) \\
&= \{\, \sigma(x) : x \in \mathrm{Fr}(\phi_1) \,\} \cup \{\, \sigma(x) : x \in \mathrm{Fr}(\phi_2) \,\} \\
&= \{\, \sigma(x) : x \in \mathrm{Fr}(\phi_1) \cup \mathrm{Fr}(\phi_2) \,\} \\
&= \{\, \sigma(x) : x \in \mathrm{Fr}(\phi_1 \to \phi_2) \,\} \\
&= \{\, \sigma(x) : x \in \mathrm{Fr}(\phi) \,\}
\end{aligned}$$

Finally we check that the property is true for $\phi = \forall x \phi_1$ if it is true for ϕ_1. Note that if $\sigma_{|\mathrm{Var}(\phi)}$ is injective, it follows from $\mathrm{Var}(\phi) = \{x\} \cup \mathrm{Var}(\phi_1)$ that $\sigma_{|\mathrm{Var}(\phi_1)}$ is also injective, and consequently:

$$\begin{aligned}
\mathrm{Fr}(\sigma(\phi)) &= \mathrm{Fr}(\sigma(\forall x \phi_1)) \\
&= \mathrm{Fr}(\forall \sigma(x)\, \sigma(\phi_1)) \\
&= \mathrm{Fr}(\sigma(\phi_1)) \setminus \{\sigma(x)\} \\
&= \{\, \sigma(u) : u \in \mathrm{Fr}(\phi_1) \,\} \setminus \{\sigma(x)\} \\
\text{see below} \to &= \{\, \sigma(u) : u \in \mathrm{Fr}(\phi_1) \setminus \{x\} \,\} \\
&= \{\, \sigma(u) : u \in \mathrm{Fr}(\forall x \phi_1) \,\} \\
&= \{\, \sigma(x) : x \in \mathrm{Fr}(\phi) \,\}
\end{aligned}$$

We shall complete the proof by justifying the used equality:

$$\{\, \sigma(u) : u \in \mathrm{Fr}(\phi_1) \,\} \setminus \{\sigma(x)\} = \{\, \sigma(u) : u \in \mathrm{Fr}(\phi_1) \setminus \{x\} \,\}$$

First we show the inclusion $\subseteq$. Suppose $y = \sigma(u)$ for some $u \in \mathrm{Fr}(\phi_1)$ and $y \neq \sigma(x)$. Then in particular $u \neq x$, and if follows that $y = \sigma(u)$ with $u \in \mathrm{Fr}(\phi_1) \setminus \{x\}$. We now show the reverse inclusion $\supseteq$. Suppose $y = \sigma(u)$ for some $u \in \mathrm{Fr}(\phi_1) \setminus \{x\}$. Then in particular $y = \sigma(u)$ for some $u \in \mathrm{Fr}(\phi_1)$ and we need to show that $y \neq \sigma(x)$. Suppose to the contrary that $y = \sigma(x)$. Then $\sigma(u) = \sigma(x)$ with $u \in \mathrm{Fr}(\phi_1) \subseteq \mathrm{Var}(\phi_1) \subseteq \mathrm{Var}(\phi)$ and $x \in \mathrm{Var}(\phi)$. Having assumed that $\sigma_{|\mathrm{Var}(\phi)}$ is injective, we obtain $u = x$, contradicting the fact that $u \in \mathrm{Fr}(\phi_1) \setminus \{x\}$. .

For an easy future reference, we now apply proposition (44) to the single variable substitution mapping $\sigma = [y/x]$. We require that $y \notin \mathrm{Var}(\phi)$ to guarantee the injectivity of the map $\sigma_{|\mathrm{Var}(\phi)}$.

Proposition 45 *Let V be a set, $\phi \in \mathbf{P}(V)$, $x, y \in V$ with $y \notin \mathrm{Var}(\phi)$. Then:*

$$\mathrm{Fr}(\phi[y/x]) = \begin{cases} \mathrm{Fr}(\phi) \setminus \{x\} \cup \{y\} & \text{if} \quad x \in \mathrm{Fr}(\phi) \\ \mathrm{Fr}(\phi) & \text{if} \quad x \notin \mathrm{Fr}(\phi) \end{cases}$$

Proof
Let $\phi \in \mathbf{P}(V)$ such that $y \notin \mathrm{Var}(\phi)$. Let $\sigma : V \to V$ be the single variable substitution map $\sigma = [y/x]$ defined by $\sigma(x) = y$ and $\sigma(u) = u$ for $u \neq x$. From the assumption $y \notin \mathrm{Var}(\phi)$ it follows that $\sigma_{|\mathrm{Var}(\phi)}$ is an injective map. Indeed, suppose $\sigma(u) = \sigma(v)$ for some $u, v \in \mathrm{Var}(\phi)$. We need to show that $u = v$, which is clearly the case when $u \neq x$ and $v \neq x$. So suppose $u = x$ and $v \neq x$. From $\sigma(u) = \sigma(v)$ we obtain $y = v$ contradicting the assumption $y \notin \mathrm{Var}(\phi)$. So $u = x$ and $v \neq x$ is impossible and likewise $u \neq x$ and $v = x$ is an impossible case. Of course the case $u = x$ and $v = x$ leads to $u = v$. So we have proved that $u = v$ in all possible cases and $\sigma_{|\mathrm{Var}(\phi)}$ is indeed an injective map. From proposition (44) it follows that $\mathrm{Fr}(\sigma(\phi)) = \sigma(\mathrm{Fr}(\phi))$, i.e. $\mathrm{Fr}(\phi[y/x]) = \sigma(\mathrm{Fr}(\phi))$. We shall complete the proof by showing that $\sigma(\mathrm{Fr}(\phi)) = \mathrm{Fr}(\phi) \setminus \{x\} \cup \{y\}$ when $x \in \mathrm{Fr}(\phi)$, while $\sigma(\mathrm{Fr}(\phi)) = \mathrm{Fr}(\phi)$ when $x \notin \mathrm{Fr}(\phi)$. First we assume that $x \notin \mathrm{Fr}(\phi)$. We need to show that $\sigma(\mathrm{Fr}(\phi)) = \mathrm{Fr}(\phi)$. First we show the inclusion $\subseteq$. So suppose $z = \sigma(u)$ for some $u \in \mathrm{Fr}(\phi)$. We need to show that $z \in \mathrm{Fr}(\phi)$. Since $u \in \mathrm{Fr}(\phi)$, it is sufficient to prove that $\sigma(u) = u$. Hence it is sufficient to show that $u \neq x$ which follows immediately from the assumption $x \notin \mathrm{Fr}(\phi)$. This completes our proof of $\subseteq$. We now show the reverse inclusion $\supseteq$. So suppose $z \in \mathrm{Fr}(\phi)$. We need to show that $z = \sigma(u)$ for some $u \in \mathrm{Fr}(\phi)$. It is sufficient to show that $z = \sigma(z)$ or $z \neq x$ which follows from $z \in \mathrm{Fr}(\phi)$ and $x \notin \mathrm{Fr}(\phi)$. This completes our proof in the case when $x \notin \mathrm{Fr}(\phi)$. We now assume that $x \in \mathrm{Fr}(\phi)$. We need to show that $\sigma(\mathrm{Fr}(\phi)) = \mathrm{Fr}(\phi) \setminus \{x\} \cup \{y\}$. First we prove the inclusion $\subseteq$. So suppose $z = \sigma(u)$ for some $u \in \mathrm{Fr}(\phi)$. We assume that $z \neq y$ and we need to show that $z \in \mathrm{Fr}(\phi)$ and $z \neq x$. First we show that $z \neq x$. So suppose to the contrary that $z = x$. Then $\sigma(u) = x$. If $u \neq x$ we obtain $\sigma(u) = u \neq x$. Hence it follows that $u = x$ and consequently $\sigma(u) = \sigma(x)$. So $z = y$ contradicting the initial assumption. So we need to show that $z \in \mathrm{Fr}(\phi)$. Once again, since $z = \sigma(u)$ and $u \in \mathrm{Fr}(\phi)$, it is sufficient to prove that $\sigma(u) = u$ or $u \neq x$. So suppose to the contrary that $u = x$. Then $z = \sigma(u) = \sigma(x) = y$ which contradicts the initial assumption $z \neq y$. This completes our proof of $\subseteq$. We now show the reverse inclusion $\supseteq$. Having assumed that $x \in \mathrm{Fr}(\phi)$, we have $y = \sigma(x) \in \sigma(\mathrm{Fr}(\phi))$. So it remains to show that $\sigma(\mathrm{Fr}(\phi)) \supseteq \mathrm{Fr}(\phi) \setminus \{x\}$. So suppose $z \in \mathrm{Fr}(\phi)$ and $z \neq x$. We need to show that $z = \sigma(u)$ for some $u \in \mathrm{Fr}(\phi)$ for which it is clearly sufficient to prove that $z = \sigma(z)$ or $z \neq x$, which is true by assumption. **.**

In proposition (31) we showed that the relation $\equiv$ defined by $\phi \equiv \psi$ if and only if $\sigma(\phi) \sim \sigma(\psi)$ was a congruence on $\mathbf{P}(V)$, given an arbitrary substitution $\sigma : V \to W$ and congruence $\sim$ on $\mathbf{P}(W)$. The objective was to obtain an easy way to prove an implication of the form $\phi \sim \psi \;\Rightarrow\; \sigma(\phi) \sim \sigma(\psi)$ where $\sim$ is another congruence on $\mathbf{P}(V)$ for which there is a known generator R_0. We are now interested in an implication of the form $\phi \sim \psi \;\Rightarrow\; \mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$. One natural step towards proving such an implication consists in showing that the relation $\equiv$ defined by $\phi \equiv \psi$ if and only if $\mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$, is itself a congruence on $\mathbf{P}(V)$. This is the purpose of the next proposition.

Proposition 46 *Let V be a set and $\equiv$ be the relation on $\mathbf{P}(V)$ defined by:*

$$\phi \equiv \psi \;\Leftrightarrow\; \mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$$

for all $\phi, \psi \in \mathbf{P}(V)$. Then $\equiv$ is a congruence on $\mathbf{P}(V)$.

Proof
The relation $\equiv$ is clearly reflexive, symmetric and transitive on $\mathbf{P}(V)$. So we simply need to show that $\equiv$ is a congruent relation on $\mathbf{P}(V)$. By reflexivity, we already have $\bot \equiv \bot$. Suppose ϕ_1, ϕ_2, ψ_1 and $\psi_2 \in \mathbf{P}(V)$ are such that $\phi_1 \equiv \psi_1$ and $\phi_2 \equiv \psi_2$. Define $\phi = \phi_1 \to \phi_2$ and $\psi = \psi_1 \to \psi_2$. We need to show that $\phi \equiv \psi$, or equivalently that $\mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$. This follows from the fact that $\mathrm{Fr}(\phi_1) = \mathrm{Fr}(\psi_1)$, $\mathrm{Fr}(\phi_2) = \mathrm{Fr}(\psi_2)$ and:

$$\begin{aligned}
\mathrm{Fr}(\phi) &= \mathrm{Fr}(\phi_1 \to \phi_2) \\
&= \mathrm{Fr}(\phi_1) \cup \mathrm{Fr}(\phi_2) \\
&= \mathrm{Fr}(\psi_1) \cup \mathrm{Fr}(\psi_2) \\
&= \mathrm{Fr}(\psi_1 \to \psi_2) \\
&= \mathrm{Fr}(\psi)
\end{aligned}$$

We now suppose that $\phi_1, \psi_1 \in \mathbf{P}(V)$ are such that $\phi_1 \equiv \psi_1$. Let $x \in V$ and define $\phi = \forall x \phi_1$ and $\psi = \forall x \psi_1$. We need to show that $\phi \equiv \psi$, or equivalently that $\mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$. This follows from the fact that $\mathrm{Fr}(\phi_1) = \mathrm{Fr}(\psi_1)$ and:

$$\mathrm{Fr}(\phi) = \mathrm{Fr}(\forall x \phi_1) = \mathrm{Fr}(\phi_1) \setminus \{x\} = \mathrm{Fr}(\psi_1) \setminus \{x\} = \mathrm{Fr}(\forall x \psi_1) = \mathrm{Fr}(\psi)$$

.

2.1.8 Bound Variable of a Formula

As already noted, the variable x in $\forall x(x \in y)$ or the integral $\int f(x,y)\,dx$ is a dummy variable. In mathematical logic, dummy variables are called *bound variables*. For the sake of completeness, we now formally define the set of bound variables of a formula ϕ, i.e. the set of all variables which appear in some quantifier $\forall x$ within the formula ϕ. It should be noted that a variable x can be both a bound variable and a free variable, as is the case for the formula:

$$\phi = \forall x(x \in y) \to (x \in y)$$

Definition 30 *Let V be a set. The map* $\mathrm{Bnd} : \mathbf{P}(V) \to \mathcal{P}(V)$ *defined by the following structural recursion is called* bound variable mapping *on $\mathbf{P}(V)$:*

$$\forall \phi \in \mathbf{P}(V)\ ,\ \mathrm{Bnd}(\phi) = \begin{cases} \emptyset & \textit{if} \quad \phi = (x \in y) \\ \emptyset & \textit{if} \quad \phi = \bot \\ \mathrm{Bnd}(\phi_1) \cup \mathrm{Bnd}(\phi_2) & \textit{if} \quad \phi = \phi_1 \to \phi_2 \\ \{x\} \cup \mathrm{Bnd}(\phi_1) & \textit{if} \quad \phi = \forall x \phi_1 \end{cases} \tag{2.8}$$

We say that $x \in V$ is a bound variable *of $\phi \in \mathbf{P}(V)$ if and only if $x \in \mathrm{Bnd}(\phi)$.*

Proposition 47 *The structural recursion of* definition (29) *is legitimate.*

Proof
We need to show the existence and uniqueness of $\mathrm{Bnd} : \mathbf{P}(V) \to \mathcal{P}(V)$ satisfying equation (2.8). This follows from an immediate application of theorem (4) of page 42 to the free universal algebra $\mathbf{P}(V)$ and the set $A = \mathcal{P}(V)$, using $g_0 : \mathbf{P}_0(V) \to A$ defined by $g_0(x \in y) = \emptyset$ for all $x, y \in V$, and the operators $h(f) : A^{\alpha(f)} \to A$ $(f \in \alpha)$ defined for all $V_1, V_2 \in A$ and $x \in V$ as:

$$\begin{array}{ll} (i) & h(\bot)(0) = \emptyset \\ (ii) & h(\to)(V_1, V_2) = V_1 \cup V_2 \\ (iii) & h(\forall x)(V_1) = \{x\} \cup V_1 \end{array}$$

.

Given a set V and $\phi \in \mathbf{P}(V)$, the intersection $\mathrm{Fr}(\phi) \cap \mathrm{Bnd}(\phi)$ is not empty in general. The formula $\phi = (x \in y) \to \forall x(x \in y)$ is an example where such intersection is not empty. However:

Proposition 48 *Let V be a set and $\phi \in \mathbf{P}(V)$. Then we have:*

$$\mathrm{Var}(\phi) = \mathrm{Fr}(\phi) \cup \mathrm{Bnd}(\phi) \tag{2.9}$$

Proof
We shall prove the inclusion (2.9) by structural induction using theorem (3) of page 31. Since $\mathbf{P}_0(V)$ is a generator of $\mathbf{P}(V)$, we first check that the inclusion is true for $\phi \in \mathbf{P}_0(V)$. So suppose $\phi = (x \in y) \in \mathbf{P}_0(V)$ for some $x, y \in V$. Then:

$$\begin{array}{rcl} \mathrm{Var}(\phi) & = & \mathrm{Var}(x \in y) \\ & = & \{x, y\} \\ & = & \{x, y\} \cup \emptyset \\ & = & \mathrm{Fr}(x \in y) \cup \mathrm{Bnd}(x \in y) \\ & = & \mathrm{Fr}(\phi) \cup \mathrm{Bnd}(\phi) \end{array}$$

Next we check that the property is true for $\bot \in \mathbf{P}(V)$:

$$\mathrm{Var}(\bot) = \emptyset = \mathrm{Fr}(\bot) \cup \mathrm{Bnd}(\bot)$$

Next we check that the property is true for $\phi = \phi_1 \to \phi_2$ if it is true for ϕ_1, ϕ_2:

$$\begin{array}{rcl} \mathrm{Var}(\phi) & = & \mathrm{Var}(\phi_1 \to \phi_2) \\ & = & \mathrm{Var}(\phi_1) \cup \mathrm{Var}(\phi_2) \\ & = & \mathrm{Fr}(\phi_1) \cup \mathrm{Bnd}(\phi_1) \cup \mathrm{Fr}(\phi_2) \cup \mathrm{Bnd}(\phi_2) \\ & = & \mathrm{Fr}(\phi_1 \to \phi_2) \cup \mathrm{Bnd}(\phi_1 \to \phi_2) \\ & = & \mathrm{Fr}(\phi) \cup \mathrm{Bnd}(\phi) \end{array}$$

Finally we check that the property is true for $\phi = \forall x \phi_1$ if it is true for ϕ_1:

$$\begin{aligned}
\mathrm{Var}(\phi) &= \mathrm{Var}(\forall x \phi_1) \\
&= \{x\} \cup \mathrm{Var}(\phi_1) \\
&= \{x\} \cup \mathrm{Fr}(\phi_1) \cup \mathrm{Bnd}(\phi_1) \\
&= \{x\} \cup (\,\mathrm{Fr}(\phi_1) \setminus \{x\}\,) \cup \mathrm{Bnd}(\phi_1) \\
&= \mathrm{Fr}(\forall x \phi_1) \cup \mathrm{Bnd}(\forall x \phi_1) \\
&= \mathrm{Fr}(\phi) \cup \mathrm{Bnd}(\phi)
\end{aligned}$$

.

In the following proposition we show that if $\psi \preceq \phi$ is a sub-formula of ϕ, then the bound variables of ψ are also bound variables of ϕ. Note that this property is not true of free variables since $\mathrm{Fr}(\phi_1) \not\subseteq \mathrm{Fr}(\forall x \phi_1))$ in general.

Proposition 49 *Let V be a set and $\phi, \psi \in \mathbf{P}(V)$. Then we have:*

$$\psi \preceq \phi \;\Rightarrow\; \mathrm{Bnd}(\psi) \subseteq \mathrm{Bnd}(\phi)$$

Proof
This is a simple application of proposition (25) to the map $\mathrm{Bnd} : X \to A$ where $X = \mathbf{P}(V)$ and $A = \mathcal{P}(V)$ where the preorder $\leq$ on A is the usual inclusion $\subseteq$. We simply need to check that given $\phi_1, \phi_2 \in \mathbf{P}(V)$ and $x \in V$ we have the inclusions $\mathrm{Bnd}(\phi_1) \subseteq \mathrm{Bnd}(\phi_1 \to \phi_2)$, $\mathrm{Bnd}(\phi_2) \subseteq \mathrm{Bnd}(\phi_1 \to \phi_2)$ and $\mathrm{Bnd}(\phi_1) \subseteq \mathrm{Bnd}(\forall x \phi_1)$ which follow immediately from definition (29). .

Let V, W be sets and $\sigma : V \to W$ be a map with associated substitution mapping $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$. Given $\phi \in \mathbf{P}(V)$, the bound variables of ϕ are the elements of the set $\mathrm{Bnd}(\phi)$. The following proposition allows us to determine which are the bound variables of $\sigma(\phi)$. Specifically:

$$\mathrm{Bnd}(\sigma(\phi)) = \{\sigma(x) \;:\; x \in \mathrm{Bnd}(\phi)\}$$

In other words the bound variables of $\sigma(\phi)$ coincide with the range of the restriction $\sigma_{|\mathrm{Bnd}(\phi)}$. As discussed in page 19, this range is denoted $\sigma(\mathrm{Bnd}(\phi))$.

Proposition 50 *Let V and W be sets and $\sigma : V \to W$ be a map. Then:*

$$\forall \phi \in \mathbf{P}(V)\;,\; \mathrm{Bnd}(\sigma(\phi)) = \sigma(\mathrm{Bnd}(\phi))$$

where $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ also denotes the associated substitution mapping.

Proof
Given $\phi \in \mathbf{P}(V)$, we need to show that $\mathrm{Bnd}(\sigma(\phi)) = \{\sigma(x) : x \in \mathrm{Bnd}(\phi)\}$. We shall do so by structural induction using theorem (3) of page 31. Since $\mathbf{P}_0(V)$ is a generator of $\mathbf{P}(V)$, we first check that the property is true for $\phi \in \mathbf{P}_0(V)$. So suppose $\phi = (x \in y) \in \mathbf{P}_0(V)$ for some $x, y \in V$. Then we have:

$$\mathrm{Bnd}(\sigma(\phi)) \quad = \quad \mathrm{Bnd}(\sigma(x \in y))$$

$$
\begin{aligned}
&= \mathrm{Bnd}(\,\sigma(x) \in \sigma(y)\,) \\
&= \emptyset \\
&= \{\sigma(u) : u \in \emptyset\} \\
&= \{\sigma(u) : u \in \mathrm{Bnd}(x \in y)\} \\
&= \{\sigma(x) : x \in \mathrm{Bnd}(\phi)\}
\end{aligned}
$$

Next we check that the property is true for $\perp \in \mathbf{P}(V)$:

$$\mathrm{Bnd}(\sigma(\perp)) = \mathrm{Bnd}(\perp) = \emptyset = \{\sigma(x) : x \in \mathrm{Bnd}(\perp)\}$$

Next we check that the property is true for $\phi = \phi_1 \to \phi_2$ if it is true for ϕ_1, ϕ_2:

$$
\begin{aligned}
\mathrm{Bnd}(\sigma(\phi)) &= \mathrm{Bnd}(\sigma(\phi_1 \to \phi_2)) \\
&= \mathrm{Bnd}(\sigma(\phi_1) \to \sigma(\phi_2)) \\
&= \mathrm{Bnd}(\sigma(\phi_1)) \cup \mathrm{Bnd}(\sigma(\phi_2)) \\
&= \{\,\sigma(x) : x \in \mathrm{Bnd}(\phi_1)\,\} \cup \{\,\sigma(x) : x \in \mathrm{Bnd}(\phi_2)\,\} \\
&= \{\,\sigma(x) : x \in \mathrm{Bnd}(\phi_1) \cup \mathrm{Bnd}(\phi_2)\,\} \\
&= \{\,\sigma(x) : x \in \mathrm{Bnd}(\phi_1 \to \phi_2)\,\} \\
&= \{\,\sigma(x) : x \in \mathrm{Bnd}(\phi)\,\}
\end{aligned}
$$

Finally we check that the property is true for $\phi = \forall x \phi_1$ if it is true for ϕ_1:

$$
\begin{aligned}
\mathrm{Bnd}(\sigma(\phi)) &= \mathrm{Bnd}(\sigma(\forall x \phi_1)) \\
&= \mathrm{Bnd}(\forall \sigma(x)\, \sigma(\phi_1)) \\
&= \{\,\sigma(x)\,\} \cup \mathrm{Bnd}(\sigma(\phi_1)) \\
&= \{\,\sigma(x)\,\} \cup \{\,\sigma(u) : u \in \mathrm{Bnd}(\phi_1)\,\} \\
&= \{\,\sigma(u) : u \in \{x\} \cup \mathrm{Bnd}(\phi_1)\,\} \\
&= \{\,\sigma(u) : u \in \mathrm{Bnd}(\forall x \phi_1)\,\} \\
&= \{\,\sigma(x) : x \in \mathrm{Bnd}(\phi)\,\}
\end{aligned}
$$

.

2.1.9 Valid Substitution of Variable

Suppose we had a parameterized integral $I(x) = \int f(x, y)dy$ defined for $x \in A$. Given some $a \in A$, we would naturally write $I(a) = \int f(a, y)dy$. However, if y was also an element of A, very few of us would dare to say $I(y) = \int f(y, y)dy$. Substituting the variable y in place of x is not valid, or in other words the substitution $[y/x]$ is not a valid substitution for the formula $\phi = \int f(x, y)dy$. Similarly, if we had the formula $\phi = \forall y(x \in y) \in \mathbf{P}(V)$ with $x \neq y$ which expresses some unary predicate $I(x)$, it would be a natural thing to write the formula $I(a) = \forall y(a \in y)$ whenever $a \neq y$, while referring to $\forall y(y \in y)$ as representing $I(y)$ would make no sense. Here again it is clear that the substitution

$[y/x]$ is not a valid substitution for the formula $\phi = \forall y(x \in y)$ when $x \neq y$. It is not clear at this stage how $I(y)$ should be defined but we certainly know it cannot be defined in terms of a substitution of variable which is not valid. At some point, it will be important for us to define $I(y)$ in order to claim that:

$$\forall x \forall y(x \in y) \to I(a)$$

is a legitimate axiom, including when $a = y$. We shall worry about this later. In this section, we want to formally define the notion of substitution $\sigma : V \to W$ which is valid for a formula $\phi \in \mathbf{P}(V)$. We are keeping W as an arbitrary set rather than $W = V$ to make this discussion as general as possible.

So suppose $\phi = \forall y(x \in y)$ with $x \neq y$ and $\sigma : V \to W$ is an arbitrary map. Then $\sigma(\phi) = \forall v(u \in v)$ where $u = \sigma(x)$ and $v = \sigma(y)$. The question we are facing is to determine which conditions should be imposed on σ to make it a valid substitution for ϕ. Since x is a free variable of $\forall y(x \in y)$, a natural condition seems to require that u be a free variable of $\forall v(u \in v)$. This can only happen when $u \neq v$ which leads to the condition $\sigma(x) \neq \sigma(y)$. So it seems that an injective σ would be a valid substitution for ϕ. In fact, we know from proposition (36) that $\sigma(\phi)$ only depends on the restriction $\sigma_{|\mathrm{Var}(\phi)}$ so we may require that $\sigma_{|\mathrm{Var}(\phi)}$ be injective rather than σ itself. However, does injectivity really matter? Suppose we had $\phi = \forall y[(x \in y) \to (y \in z)]$ with x, y, z distinct. There would be nothing wrong with a substitution σ leading to the formula $\forall v[(u \in v) \to (v \in u)]$ with $u \neq v$. There is nothing absurd in considering the binary predicate $I(x, z) = \forall y[(x \in y) \to (y \in z)]$ with $(x, z) = (u, u)$ (having changed the bound variable y by v). So injectivity does not matter. What matters is the fact that the free variables x and z of ϕ have been substituted by the free variable u in $\forall v[(u \in v) \to (v \in u)]$. In other words, when considering a formula $\phi = \forall y[\ \ldots\ x\ \ldots\ z\ \ldots\ ]$ with x and z free, what matters is not to end up with something like $\sigma(\phi) = \forall \sigma(y)[\ \ldots\ \sigma(x)\ \ldots\ \sigma(z)\ \ldots\ ]$ with $\sigma(x) = \sigma(y)$ or $\sigma(z) = \sigma(y)$. We do not want free variables of ϕ to become artificially bound by the substitution σ. So it seems that a possible condition for the substitution σ to be valid for ϕ is the following:

$$x \in \mathrm{Fr}(\phi) \ \Rightarrow\ \sigma(x) \in \mathrm{Fr}(\sigma(\phi))$$

So let us consider $\phi = \forall x \forall y(x \in y)$ with $x \neq y$ as a new example. In this case, the formula ϕ has no free variables and there is therefore no risk of having a free variable getting artificially bound by a substitution σ. So any substitution σ would seem to be valid for ϕ, which of course isn't the case. As a rule of thumb, a valid substitution σ is one which prevents a mathematician writing nonsense. If $\phi = \forall x \psi$ with $\psi = \forall y(x \in y)$, then we cannot hope $\sigma(\phi) = \forall \sigma(x) \sigma(\psi)$ to be a legitimate expression, unless $\sigma(\psi)$ itself is a legitimate expression. So yes, we do not want free variables to become artificially bound by the substitution σ, but these free variables are not so much the free variables of ϕ itself. There are also the free variables of ψ or more generally of any sub-formula of ϕ. So in the light of this discussion we shall attempt the following:

Definition 31 *Let V and W be sets and $\sigma : V \to W$ be a map. Let $\phi \in \mathbf{P}(V)$. We say that σ is* valid for ϕ *if and only if for every sub-formula $\psi \preceq \phi$ we have:*

$$x \in \mathrm{Fr}(\psi) \;\Rightarrow\; \sigma(x) \in \mathrm{Fr}(\sigma(\psi))$$

where $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ also denotes the associated substitution mapping.

Recall that the notion of sub-formula and the relation $\psi \preceq \phi$ are defined in definition (19) of page 57. An immediate consequence of definition (30) is:

Proposition 51 *Let V and W be sets and $\sigma : V \to W$ be a map. Let $\phi \in \mathbf{P}(V)$. Then σ is valid for ϕ if and only if it is valid for any sub-formula $\psi \preceq \phi$.*

Proof
Since $\phi \preceq \phi$, i.e. ϕ is a sub-formula of itself, the 'if' part of this proposition is clear. So we now prove the 'only if' part. So suppose σ is valid for ϕ and let $\psi \preceq \phi$. We need to show that σ is also valid for ψ. So let $\chi \preceq \psi$ and let $x \in \mathrm{Fr}(\chi)$. We need to show that $\sigma(x) \in \mathrm{Fr}(\sigma(\chi))$, which follows immediately from the validity of σ for ϕ and the fact (by transitivity) that $\chi \preceq \phi$, i.e. that χ is also a sub-formula of ϕ. **.**

Another immediate consequence of definition (30) is:

Proposition 52 *Let V and W be sets and $\sigma : V \to W$ be a map. Let $\phi \in \mathbf{P}(V)$. Then σ is valid for ϕ if and only if for every sub-formula $\psi \preceq \phi$ we have:*

$$\mathrm{Fr}(\sigma(\psi)) = \sigma(\mathrm{Fr}(\psi))$$

Proof
The substitution $\sigma : V \to W$ if valid for ϕ if and only if for all $\psi \preceq \phi$:

$$x \in \mathrm{Fr}(\psi) \;\Rightarrow\; \sigma(x) \in \mathrm{Fr}(\sigma(\psi))$$

This condition is clearly equivalent to $\sigma(\mathrm{Fr}(\psi)) \subseteq \mathrm{Fr}(\sigma(\psi))$, where $\sigma(\mathrm{Fr}(\psi))$ refers to the direct image of the set $\mathrm{Fr}(\psi)$ by the map $\sigma : V \to W$. From proposition (43) we know the reverse inclusion $\mathrm{Fr}(\sigma(\psi)) \subseteq \sigma(\mathrm{Fr}(\psi))$ is always true. **.**

As anticipated, if σ is injective on $\mathrm{Var}(\phi)$ then it is valid for ϕ:

Proposition 53 *Let V and W be sets and $\sigma : V \to W$ be a map. Let $\phi \in \mathbf{P}(V)$ such that $\sigma_{|\mathrm{Var}(\phi)}$ is an injective map. Then σ is valid for ϕ.*

Proof
Let $\sigma : V \to W$ be map and $\phi \in \mathbf{P}(V)$ such that the restriction $\sigma_{|\mathrm{Var}(\phi)}$ is an injective map. We need to show that σ is valid for ϕ. So let $\psi \preceq \phi$. Using proposition (52), we need to show that $\mathrm{Fr}(\sigma(\psi)) = \sigma(\mathrm{Fr}(\psi))$. From proposition (44), it is sufficient to prove that $\sigma_{|\mathrm{Var}(\psi)}$ is injective. Since $\sigma_{|\mathrm{Var}(\phi)}$ is injective, it is sufficient to show that $\mathrm{Var}(\psi) \subseteq \mathrm{Var}(\phi)$ which follows from $\psi \preceq \phi$ and proposition (34). **.**

If it is meaningful to speak of $\sigma(\phi_1)$ and $\sigma(\phi_2)$, it should also be meaningful to consider $\sigma(\phi_1) \to \sigma(\phi_2)$ which is the same as $\sigma(\phi_1 \to \phi_2)$. So in order to prove that a substitution σ is valid for $\phi = \phi_1 \to \phi_2$, it should be sufficient to establish its validity both for ϕ_1 and ϕ_2. The following proposition establishes that fact, which may be useful for structural induction arguments on $\mathbf{P}(V)$.

Proposition 54 *Let V and W be sets and $\sigma : V \to W$ be a map. Let $\phi \in \mathbf{P}(V)$ of the form $\phi = \phi_1 \to \phi_2$ with $\phi_1, \phi_2 \in \mathbf{P}(V)$. Then σ is valid for ϕ if and only if it is valid for both ϕ_1 and ϕ_2.*

Proof
Suppose σ is valid for $\phi = \phi_1 \to \phi_2$. From the equality:

$$\mathrm{Sub}(\phi) = \{\phi_1 \to \phi_2\} \cup \mathrm{Sub}(\phi_1) \cup \mathrm{Sub}(\phi_2) \tag{2.10}$$

we obtain $\phi_1 \in \mathrm{Sub}(\phi_1) \subseteq \mathrm{Sub}(\phi)$ and $\phi_2 \in \mathrm{Sub}(\phi_2) \subseteq \mathrm{Sub}(\phi)$. Hence we see that $\phi_1 \preceq \phi$ and $\phi_2 \preceq \phi$ i.e. both ϕ_1 and ϕ_2 are sub-formulas of ϕ. It follows from proposition (51) that σ is valid for both ϕ_1 and ϕ_2. Conversely, suppose σ is valid for ϕ_1 and ϕ_2. We need to show that σ is valid for $\phi = \phi_1 \to \phi_2$. So let $\psi \preceq \phi$ and $u \in \mathrm{Fr}(\psi)$. We need to show that $\sigma(u) \in \mathrm{Fr}(\sigma(\psi))$. From $\psi \preceq \phi$ we have $\psi \in \mathrm{Sub}(\phi)$. So from the above equation (2.10), we must have $\psi = \phi$ or $\psi \in \mathrm{Sub}(\phi_1)$ or $\psi \in \mathrm{Sub}(\psi_2)$. So we shall distinguish three cases: first we assume that $\psi \in \mathrm{Sub}(\phi_1)$. Then $\psi \preceq \phi_1$ and from $u \in \mathrm{Fr}(\psi)$ and the validity of σ for ϕ_1 we see that $\sigma(u) \in \mathrm{Fr}(\sigma(\psi))$. Next we assume that $\psi \in \mathrm{Sub}(\phi_2)$. Then a similar argument shows that $\sigma(u) \in \mathrm{Fr}(\sigma(\psi))$. Finally we assume that $\psi = \phi$. Then $\mathrm{Fr}(\psi) = \mathrm{Fr}(\phi_1 \to \phi_2) = \mathrm{Fr}(\phi_1) \cup \mathrm{Fr}(\phi_2)$ and from $u \in \mathrm{Fr}(\psi)$ we must have $u \in \mathrm{Fr}(\phi_1)$ or $u \in \mathrm{Fr}(\phi_2)$. So we shall distinguish two further cases: first we assume that $u \in \mathrm{Fr}(\phi_1)$. From $\phi_1 \preceq \phi_1$ and the validity of σ for ϕ_1 we obtain $\sigma(u) \in \mathrm{Fr}(\sigma(\phi_1))$. However, we have:

$$\begin{aligned} \mathrm{Fr}(\sigma(\phi_1)) &\subseteq \mathrm{Fr}(\sigma(\phi_1)) \cup \mathrm{Fr}(\sigma(\phi_2)) \\ &= \mathrm{Fr}(\sigma(\phi_1) \to \sigma(\phi_2)) \\ &= \mathrm{Fr}(\sigma(\phi_1 \to \phi_2)) \\ &= \mathrm{Fr}(\sigma(\psi)) \end{aligned}$$

Hence we see that $\sigma(u) \in \mathrm{Fr}(\sigma(\psi))$. Next we assume that $u \in \mathrm{Fr}(\phi_2)$. Then a similar argument shows that $\sigma(u) \in \mathrm{Fr}(\sigma(\psi))$. In all possible cases we have shown that $\sigma(u) \in \mathrm{Fr}(\sigma(\psi))$. **.**

The next proposition may also be useful for induction arguments on $\mathbf{P}(V)$. It establishes conditions for a substitution σ to be valid for a formula of the form $\phi = \forall x \phi_1$. As expected, the validity of σ for ϕ_1 is a prerequisite. However, we also require free variables of ϕ not to become artificially bound by the substitution σ. This naturally leads to the condition $u \in \mathrm{Fr}(\phi) \;\Rightarrow\; \sigma(u) \neq \sigma(x)$.

Proposition 55 *Let V and W be sets and $\sigma : V \to W$ be a map. Let $\phi \in \mathbf{P}(V)$ of the form $\phi = \forall x \phi_1$ with $\phi_1 \in \mathbf{P}(V)$ and $x \in V$. Then σ is valid for ϕ if and only if it is valid for ϕ_1 and for all $u \in V$ we have:*

$$u \in \mathrm{Fr}(\forall x \phi_1) \;\Rightarrow\; \sigma(u) \neq \sigma(x)$$

Proof
First we show the 'only if' part. So suppose σ is valid for $\phi = \forall x\phi_1$. From:

$$\mathrm{Sub}(\phi) = \{\forall x\phi_1\} \cup \mathrm{Sub}(\phi_1) \tag{2.11}$$

we obtain $\phi_1 \in \mathrm{Sub}(\phi_1) \subseteq \mathrm{Sub}(\phi)$ and consequently $\phi_1 \preceq \phi$ i.e. ϕ_1 is a sub-formula of ϕ. It follows from proposition (51) that σ is valid for ϕ_1. So let $u \in \mathrm{Fr}(\forall x\phi_1) = \mathrm{Fr}(\phi)$. It remains to show that $\sigma(u) \neq \sigma(x)$. Since $\phi \preceq \phi$ and $u \in \mathrm{Fr}(\phi)$ it follows from the validity of σ for ϕ that $\sigma(u) \in \mathrm{Fr}(\sigma(\phi))$. Hence $\sigma(u)$ is a free variable of $\sigma(\phi) = \forall\sigma(x)\sigma(\phi_1)$, so $\sigma(u) \neq \sigma(x)$ as requested.

We now prove the 'if' part. So suppose σ is valid for ϕ_1 and furthermore that $\sigma(u) \neq \sigma(x)$ whenever $u \in \mathrm{Fr}(\forall x\phi_1) = \mathrm{Fr}(\phi)$. We need to show that σ is valid for $\phi = \forall x\phi_1$. So let $\psi \preceq \phi$ and $u \in \mathrm{Fr}(\psi)$. We need to show that $\sigma(u) \in \mathrm{Fr}(\sigma(\psi))$. From $\psi \preceq \phi$ we have $\psi \in \mathrm{Sub}(\phi)$. So from the above equation (2.11), we must have $\psi = \phi$ or $\psi \in \mathrm{Sub}(\phi_1)$. So we shall distinguish two cases: first we assume that $\psi \in \mathrm{Sub}(\phi_1)$. Then $\psi \preceq \phi_1$ and from $u \in \mathrm{Fr}(\psi)$ and the validity of σ for ϕ_1 we see that $\sigma(u) \in \mathrm{Fr}(\sigma(\psi))$. Next we assume that $\psi = \phi$. Then $\mathrm{Fr}(\psi) = \mathrm{Fr}(\forall x\phi_1) = \mathrm{Fr}(\phi_1) \setminus \{x\}$ and from $u \in \mathrm{Fr}(\psi)$ we must have in particular $u \in \mathrm{Fr}(\phi_1)$. From $\phi_1 \preceq \phi_1$ and the validity of σ for ϕ_1 we obtain $\sigma(u) \in \mathrm{Fr}(\sigma(\phi_1))$. Furthermore, from $u \in \mathrm{Fr}(\psi)$ and $\psi = \phi$ we obtain $u \in \mathrm{Fr}(\phi)$ and this implies by assumption that $\sigma(u) \neq \sigma(x)$. Thus:

$$\begin{aligned} \sigma(u) \in \mathrm{Fr}(\sigma(\phi_1)) \setminus \{\sigma(x)\} &= \mathrm{Fr}(\forall\sigma(x)\sigma(\phi_1)) \\ &= \mathrm{Fr}(\sigma(\forall x\phi_1)) \\ &= \mathrm{Fr}(\sigma(\psi)) \end{aligned}$$

Hence we see that $\sigma(u) \in \mathrm{Fr}(\sigma(\psi))$ as requested. .

Looking back at definition (30), a substitution σ is valid for ϕ if and only if for all $\psi \in \mathbf{P}(V)$ we have the following property:

$$(\psi \preceq \phi) \;\Rightarrow\; [\; u \in \mathrm{Fr}(\psi) \;\Rightarrow\; \sigma(u) \in \mathrm{Fr}(\sigma(\psi)) \;]$$

In the next proposition, we offer another criterion for the validity of σ for ϕ:

$$(\forall x\phi_1 \preceq \phi) \;\Rightarrow\; [\; u \in \mathrm{Fr}(\forall x\phi_1) \;\Rightarrow\; \sigma(u) \neq \sigma(x) \;]$$

This criterion is arguably simpler as we no longer need to check every sub-formula $\psi \preceq \phi$, but instead can limit our attention to those sub-formula of the form $\psi = \forall x\phi_1$ with $\phi_1 \in \mathbf{P}(V)$ and $x \in V$. Furthermore, we no longer need to establish that $\sigma(u)$ is a free variable of $\sigma(\psi)$, but instead have to show that $\sigma(u) \neq \sigma(x)$ which is also a lot simpler.

Proposition 56 *Let V and W be sets and $\sigma : V \to W$ be a map. Let $\phi \in \mathbf{P}(V)$. Then σ is valid for ϕ if and only if for all $\phi_1 \in \mathbf{P}(V)$ and $x \in V$ we have:*

$$(\forall x\phi_1 \preceq \phi) \;\Rightarrow\; [\; u \in \mathrm{Fr}(\forall x\phi_1) \;\Rightarrow\; \sigma(u) \neq \sigma(x) \;]$$

Proof
First we show the 'only if' part: So suppose σ is valid for ϕ. Let $\phi_1 \in \mathbf{P}(V)$ and $x \in V$ such that $\psi = \forall x \phi_1 \preceq \phi$ and let $u \in \mathrm{Fr}(\psi)$. We need to show that $\sigma(u) \neq \sigma(x)$. However, from the validity of σ for ϕ we have $\sigma(u) \in \mathrm{Fr}(\sigma(\psi))$. So $\sigma(u)$ is a free variable of $\sigma(\psi) = \forall \sigma(x) \sigma(\phi_1)$ and $\sigma(u) \neq \sigma(x)$ as requested.

We now prove the 'if' part: Consider the property $P_\sigma(\phi)$ defined by:

$$\forall \phi_1 \forall x \; [\; (\forall x \phi_1 \preceq \phi) \;\Rightarrow\; [\; u \in \mathrm{Fr}(\forall x \phi_1) \;\Rightarrow\; \sigma(u) \neq \sigma(x) \;]\;]$$

Then we need to prove that $P_\sigma(\phi) \;\Rightarrow\; (\sigma \text{ valid for } \phi)$ for all $\phi \in \mathbf{P}(V)$. We shall do so by structural induction, using theorem (3) of page 31. First we assume that $\phi = (x \in y)$ for some $x, y \in V$. We need to show that the implication is true for ϕ. So suppose $P_\sigma(\phi)$ is true. We need to show that σ is valid for ϕ, which is always the case when $\phi = (x \in y)$. Next we assume that $\phi = \bot$. Then σ is once again always valid for ϕ and the implication is true. Next we assume that $\phi = \phi_1 \to \phi_2$ where the implication is true for $\phi_1, \phi_2 \in \mathbf{P}(V)$. We need to show that the implication is also true for ϕ. So we assume that $P_\sigma(\phi)$ is true. We need to show that σ is valid for $\phi = \phi_1 \to \phi_2$. Using proposition (54) it is sufficient to prove that σ is valid for both ϕ_1 and ϕ_2. Having assumed the implication is true for ϕ_1 and ϕ_2, it is therefore sufficient to prove that $P_\sigma(\phi_1)$ and $P_\sigma(\phi_2)$ are true. First we show that $P_\sigma(\phi_1)$ is true. So let $\psi \in \mathbf{P}(V)$ and $z \in V$ such that $\forall z \psi \preceq \phi_1$. Suppose $u \in \mathrm{Fr}(\forall z \psi)$. We need to show that $\sigma(u) \neq \sigma(z)$. Having assumed $P_\sigma(\phi)$ is true, it is sufficient to prove that $\forall z \psi \preceq \phi$, which follows immediately from $\forall z \psi \preceq \phi_1$ and $\phi_1 \preceq \phi$. So we have proved that $P_\sigma(\phi_1)$ is indeed true and a similar argument shows that $P_\sigma(\phi_2)$ is true. This concludes the case when $\phi = \phi_1 \to \phi_2$. Next we assume that $\phi = \forall x \phi_1$ where $x \in V$ and the implication is true for $\phi_1 \in \mathbf{P}(V)$. We need to show that the implication is also true for ϕ. So we assume that $P_\sigma(\phi)$ is true. We need to show that σ is valid for $\phi = \forall x \phi_1$. Using proposition (55) it is sufficient to prove that σ is valid for ϕ_1 and furthermore that $\sigma(u) \neq \sigma(x)$ whenever $u \in \mathrm{Fr}(\forall x \phi_1)$. First we show that σ is valid for ϕ_1. Having assumed the implication is true for ϕ_1, it is sufficient to prove that $P_\sigma(\phi_1)$ is true. So let $\psi \in \mathbf{P}(V)$ and $z \in V$ such that $\forall z \psi \preceq \phi_1$. Suppose $u \in \mathrm{Fr}(\forall z \psi)$. We need to show that $\sigma(u) \neq \sigma(z)$. Having assumed $P_\sigma(\phi)$ is true, it is sufficient to prove that $\forall z \psi \preceq \phi$, which follows immediately from $\forall z \psi \preceq \phi_1$ and $\phi_1 \preceq \phi$. So we have proved that $P_\sigma(\phi_1)$ is indeed true and σ is therefore valid for ϕ_1. Next we show that $\sigma(u) \neq \sigma(x)$ whenever $u \in \mathrm{Fr}(\forall x \phi_1)$. So let $u \in \mathrm{Fr}(\forall x \phi_1)$. We need to show that $\sigma(u) \neq \sigma(x)$. Having assumed $P_\sigma(\phi)$ is true, it is sufficient to prove that $\forall x \phi_1 \preceq \phi$ which is immediate since $\forall x \phi_1 = \phi$. **.**

The following proposition is a simple application of proposition (53):

Proposition 57 *Let V be a set and $x, y \in V$. Let $\phi \in \mathbf{P}(V)$. Then we have:*

$$y \notin \mathrm{Var}(\phi) \;\Rightarrow\; ([y/x] \textit{ valid for } \phi)$$

Proof
We assume that $y \notin \mathrm{Var}(\phi)$. We need to show that the substitution $[y/x]$ is

valid for ϕ. Using proposition (53), it is sufficient to prove that $[y/x]_{|\mathrm{Var}(\phi)}$ is an injective map. This follows immediately from $y \notin \mathrm{Var}(\phi)$ and proposition (38).
.

If U and V are sets and $\tau : U \to V$ is a valid substitution for $\phi \in \mathbf{P}(U)$, then our rule of thumb says it does make logical sense to speak of $\tau(\phi)$. So if W is another set and $\sigma : V \to W$ is a substitution which is valid for $\tau(\phi)$, it should make logical sense to speak of $\sigma(\tau(\phi)) = (\sigma \circ \tau)(\phi)$. So we should expect the substitution $\sigma \circ \tau$ to be valid for ϕ. Luckily, this happens to be true. In fact, the converse is also true: if $\sigma \circ \tau$ is valid for ϕ then not only is σ is valid for $\tau(\phi)$, but surprisingly τ itself is necessarily valid for ϕ.

Proposition 58 *Let U, V, W be sets and $\tau : U \to V$ and $\sigma : V \to W$ be maps. Then for all $\phi \in \mathbf{P}(U)$ we have the equivalence:*

$$(\tau \textit{ valid for } \phi) \wedge (\sigma \textit{ valid for } \tau(\phi)) \;\Leftrightarrow\; (\sigma \circ \tau \textit{ valid for } \phi)$$

where $\tau : \mathbf{P}(U) \to \mathbf{P}(V)$ also denotes the associated substitution mapping.

Proof
First we prove $\Rightarrow$: so we assume that τ is valid for $\phi \in \mathbf{P}(U)$ and σ is valid for $\tau(\phi)$. We need to show that $\sigma \circ \tau$ is valid for ϕ. So let $\psi \preceq \phi$. Using proposition (52) we need to show that $\mathrm{Fr}(\sigma \circ \tau(\psi)) = (\sigma \circ \tau)(\mathrm{Fr}(\psi))$:

$$\begin{array}{rcl}
\mathrm{Fr}(\sigma \circ \tau(\psi)) & = & \mathrm{Fr}(\sigma(\tau(\psi))) \\
(\tau(\psi) \preceq \tau(\phi)) \wedge (\sigma \text{ valid for } \tau(\phi)) \to & = & \sigma(\mathrm{Fr}(\tau(\psi))) \\
(\psi \preceq \phi) \wedge (\tau \text{ valid for } \phi) \to & = & \sigma(\tau(\mathrm{Fr}(\psi))) \\
 & = & (\sigma \circ \tau)(\mathrm{Fr}(\psi))
\end{array}$$

Note that $\tau(\psi) \preceq \tau(\phi)$ follows from $\psi \preceq \phi$ and proposition (30). We now prove $\Leftarrow$: So suppose $\sigma \circ \tau$ is valid for ϕ. We need to show that τ is valid for ϕ and σ is valid for $\tau(\phi)$. First we show that σ is valid for $\tau(\phi)$, having assumed τ is indeed valid for ϕ. So let $\chi \preceq \tau(\phi)$. Using proposition (52) we need to show that $\mathrm{Fr}(\sigma(\chi)) = \sigma(\mathrm{Fr}(\chi))$. However from proposition (30), there exists $\psi \preceq \phi$ such that $\chi = \tau(\psi)$. Hence we have the following equalities:

$$\begin{array}{rcl}
\mathrm{Fr}(\sigma(\chi)) & = & \mathrm{Fr}(\sigma(\tau(\psi)) \\
 & = & \mathrm{Fr}(\sigma \circ \tau(\psi)) \\
(\psi \preceq \phi) \wedge (\sigma \circ \tau \text{ valid for } \phi) \to & = & \sigma \circ \tau(\mathrm{Fr}(\psi)) \\
 & = & \sigma(\tau(\mathrm{Fr}(\psi))) \\
(\psi \preceq \phi) \wedge (\tau \text{ valid for } \phi) \to & = & \sigma(\mathrm{Fr}(\tau(\psi))) \\
 & = & \sigma(\mathrm{Fr}(\chi))
\end{array}$$

It remains to prove that τ is valid for ϕ. So consider the property:

$$(\sigma \circ \tau \text{ valid for } \phi) \;\Rightarrow\; (\tau \text{ valid for } \phi)$$

We need to show this property holds for all $\phi \in \mathbf{P}(U)$. We shall do so by a structural induction argument, using theorem (3) of page 31. First we assume that $\phi = (x \in y)$ for some $x, y \in U$. Then τ is always valid for ϕ and the property is true. Likewise, τ is always valid for $\phi = \perp$ and the property is true for $\perp$. So we assume that $\phi = \phi_1 \to \phi_2$ where $\phi_1, \phi_2 \in \mathbf{P}(U)$ satisfy the property. We need to show that same is true of ϕ. So we assume that $\sigma \circ \tau$ is valid for ϕ. We need to show that τ is valid for $\phi = \phi_1 \to \phi_2$. Using proposition (54) it is sufficient to prove that τ is valid for both ϕ_1 and ϕ_2. First we show that τ is valid for ϕ_1. Having assumed the property is true for ϕ_1 it is sufficient to show that $\sigma \circ \tau$ is valid for ϕ_1, which follows from the validity of $\sigma \circ \tau$ for $\phi = \phi_1 \to \phi_2$ and proposition (54). We prove similarly that τ is valid for ϕ_2 which completes the case when $\phi = \phi_1 \to \phi_2$. So we now assume that $\phi = \forall x \phi_1$ where $x \in U$ and $\phi_1 \in \mathbf{P}(U)$ satisfies our property. We need to show that same is true of ϕ. So we assume that $\sigma \circ \tau$ is valid for ϕ. We need to show that τ is valid for $\phi = \forall x \phi_1$. Using proposition (55) it is sufficient to show that τ is valid for ϕ_1 and furthermore that $u \in \mathrm{Fr}(\forall x \phi_1) \;\Rightarrow\; \tau(u) \neq \tau(x)$. First we show that τ is valid for ϕ_1. Having assumed the property is true for ϕ_1 it is sufficient to prove that $\sigma \circ \tau$ is valid for ϕ_1 which follows from the validity of $\sigma \circ \tau$ for $\phi = \forall x \phi_1$ and proposition (55). So we assume that $u \in \mathrm{Fr}(\forall x \phi_1)$ and it remains to show that $\tau(u) \neq \tau(x)$. So suppose to the contrary that $\tau(u) = \tau(x)$. Then in particular $\sigma \circ \tau(u) = \sigma \circ \tau(x)$ which contradicts the validity of $\sigma \circ \tau$ for $\phi = \forall x \phi_1$. **.**

Proposition 59 *Let V, W be sets and $\sigma, \tau : V \to W$ be maps. Let $\phi \in \mathbf{P}(V)$ such that the equality $\sigma(\phi) = \tau(\phi)$ holds. Then we have the equivalence:*

$$(\sigma \text{ valid for } \phi) \;\Leftrightarrow\; (\tau \text{ valid for } \phi)$$

Proof
So we assume that $\sigma(\phi) = \tau(\phi)$. It is sufficient to show the implication $\Rightarrow$. So we assume that σ is valid for ϕ. We need to show that τ is also valid for ϕ. So let $\psi \preceq \phi$ be a sub-formula of ϕ and $x \in \mathrm{Fr}(\psi)$. We need to show that $\tau(x) \in \mathrm{Fr}(\tau(\psi))$. However from proposition (36) and the equality $\sigma(\phi) = \tau(\phi)$ we see that σ and τ coincide on $\mathrm{Var}(\phi)$. Furthermore from proposition (34) we have $\mathrm{Var}(\psi) \subseteq \mathrm{Var}(\phi)$. It follows that σ and τ coincide on $\mathrm{Var}(\psi)$ and in particular $\sigma(x) = \tau(x)$. Using proposition (36) we also have $\sigma(\psi) = \tau(\psi)$. Hence we need to show that $\sigma(x) \in \mathrm{Fr}(\sigma(\psi))$ which follows from the validity of σ for ϕ. **.**

The following proposition will appear later as a useful criterion:

Proposition 60 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\phi \in \mathbf{P}(V)$. We assume that there exists a subset $V_0 \subseteq V$ with the following properties:*

$$\begin{array}{ll} (i) & \mathrm{Bnd}(\phi) \subseteq V_0 \\ (ii) & \sigma_{|V_0} \text{ is injective} \\ (iii) & \sigma(V_0) \cap \sigma(\mathrm{Var}(\phi) \setminus V_0) = \emptyset \end{array}$$

Then the map $\sigma : V \to W$ is valid for the formula $\phi \in \mathbf{P}(V)$.

Proof
Let $x \in V$ and $\phi_1 \in \mathbf{P}(V)$ such that $\forall x\phi_1 \preceq \phi$. Using proposition (56), given $u \in \text{Fr}(\forall x\phi_1)$ we need to show that $\sigma(u) \neq \sigma(x)$. However, from proposition (49) we have $\text{Bnd}(\forall x\phi_1) \subseteq \text{Bnd}(\phi)$ and consequently $x \in \text{Bnd}(\phi)$. From the assumption (i) it follows that $x \in V_0$. We shall now distinguish two cases: first we assume that $u \in V_0$. Then from assumption (ii), in order to show $\sigma(u) \neq \sigma(x)$ it is sufficient to prove that $u \neq x$ which follows from $u \in \text{Fr}(\forall x\phi_1)$. We now assume that $u \notin V_0$. However, from proposition (34) we have $\text{Var}(\forall x\phi_1) \subseteq \text{Var}(\phi)$ and consequently $u \in \text{Var}(\phi)$. It follows that $u \in \text{Var}(\phi) \setminus V_0$. Hence, we see that $\sigma(u) \neq \sigma(x)$ is a consequence of assumption (iii) and $x \in V_0$. **.**

2.1.10 Dual Substitution of Variable

Until now we have studied one type of mapping $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ which are the variable substitutions arising from a single mapping $\sigma : V \to W$, as per definition (24) of page 69. In this section, we wish to study another type of substitution $\tau : \mathbf{P}(V) \to \mathbf{P}(W)$ arising from two mappings $\tau_0, \tau_1 : V \to W$. The idea behind this new type is to allow us to move variables to different values, according to whether a given occurrence of the variable is free or bound. For example, suppose we had $\phi = \forall x(x \in y) \to (x \in y)$. We want to construct a *dual substitution mapping* $\tau : \mathbf{P}(V) \to \mathbf{P}(W)$ such that:

$$\tau(\phi) = \forall u^*(u^* \in v) \to (u \in v)$$

More generally given a mapping $\tau_0 : V \to W$ such that $\tau_0(x) = u$ and $\tau_0(y) = v$, and another mapping $\tau_1 : V \to W$ such that $\tau_1(x) = u^*$, we want to define $\tau : \mathbf{P}(V) \to \mathbf{P}(W)$ which will assign free occurrences of a variable according to τ_0 and bound occurrences according to τ_1.

One of the main motivations for introducing dual variable substitutions is to define a local inverse for the substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ associated with a single map $\sigma : V \to W$. Suppose we had $\phi = \forall x(x \in y) \to (z \in y)$ with x, y, z distinct and $\sigma = [x/z]$. Then $\sigma(\phi) = \forall x(x \in y) \to (x \in y)$ and there is no way to find a mapping $\tau : W \to V$ such that $\tau \circ \sigma(\phi) = \phi$. We need to go further.

So we are given $\tau_0, \tau_1 : V \to W$ and looking to define $\tau : \mathbf{P}(V) \to \mathbf{P}(W)$ which assigns free and bound occurrences of variables as specified by τ_0 and τ_1 respectively. The issue we have is that on the one hand we need to have some form of recursive definition, but on the other hand a sub-formula $x \in y$ has no knowledge of whether x and y will remain free occurrences of a given formula. One possible solution is to always assume that x and y will remain free and define $\tau(x \in y) = \tau_0(x) \in \tau_0(y)$ accordingly, while substituting the variable $\tau_0(x)$ by $\tau_1(x)$ whenever a quantification $\forall x$ arises by setting:

$$\tau(\forall x\phi_1) = \forall \tau_1(x)\tau(\phi_1)[\tau_1(x)/\tau_0(x)] \tag{2.12}$$

Unfortunately, this doesn't work. Suppose we have $\phi = \forall x(x \in y)$ with $x \neq y$. Take $\tau_0(x) = \tau_0(y) = u$ and $\tau_1(x) = u^*$. The formula we wish to obtain is

$\tau(\phi) = \forall u^*(u^* \in u)$. However, if we apply equation (2.12) we have:

$$\tau(\phi) = \forall u^*(u \in u)[u^*/u] = \forall u^*(u^* \in u^*)$$

Another idea is to define τ in two steps: first we define a map:

$$\tau^* : \mathbf{P}(V) \to [\mathcal{P}(V) \to \mathbf{P}(W)]$$

So given $\phi \in \mathbf{P}(V)$, we have a map $\tau^*(\phi) : \mathcal{P}(V) \to \mathbf{P}(W)$ which assigns to every subset $U \subseteq V$ a formula $\tau^*(\phi)(U) \in \mathbf{P}(W)$ which represents the formula obtained from ϕ by assuming all free variables are in U. Specifically, if we define $\tau_U(x) = \tau_0(x)$ if $x \in U$ and $\tau_U(x) = \tau_1(x)$ if $x \notin U$, we put:

$$\tau^*(x \in y)(U) = \tau_U(x) \in \tau_U(y)$$

In the case when $\phi = \forall x \phi_1$, we cannot easily define $\tau^*(\phi)(U)$ in terms of $\tau^*(\phi_1)(U)$ because we want the variable x to be tagged as *bound* in $\tau^*(\phi_1)$. So we need to consider the formula $\tau^*(\phi_1)(U \setminus \{x\})$ instead, having excluded the variable x from the set of possible free variables. Specifically we define:

$$\tau^*(\forall x \phi_1)(U) = \forall \tau_1(x) \tau^*(\phi_1)(U \setminus \{x\}) \tag{2.13}$$

Once we have defined $\tau^*(\phi) : \mathcal{P}(V) \to \mathbf{P}(W)$ we can just set $\tau(\phi) = \tau^*(\phi)(V)$ since all free variables of ϕ are possibly in V. So let us go back to our example of $\phi = \forall x(x \in y)$ with $x \neq y$, $\tau_0(x) = \tau_0(y) = u$ and $\tau_1(x) = u^*$. We obtain:

$$\tau(\phi) = \tau^*(\phi)(V) = \forall u^* \tau^*(x \in y)(V \setminus \{x\}) = \forall u^*(u^* \in u)$$

This is exactly what we want. So let's hope for the best and define:

Definition 32 *Let V, W be sets and $\tau_0, \tau_1 : V \to W$ be maps. We call* dual variable substitution *associated with (τ_0, τ_1) the map $\tau : \mathbf{P}(V) \to \mathbf{P}(W)$ defined by $\tau(\phi) = \tau^*(\phi)(V)$, where the map $\tau^* : \mathbf{P}(V) \to [\mathcal{P}(V) \to \mathbf{P}(W)]$ is defined by the following structural recursion, given $\phi \in \mathbf{P}(V)$ and $U \in \mathcal{P}(V)$:*

$$\tau^*(\phi)(U) = \begin{cases} \tau_U(x) \in \tau_U(y) & \text{if} \quad \phi = (x \in y) \\ \bot & \text{if} \quad \phi = \bot \\ \tau^*(\phi_1)(U) \to \tau^*(\phi_2)(U) & \text{if} \quad \phi = \phi_1 \to \phi_2 \\ \forall \tau_1(x) \tau^*(\phi_1)(U \setminus \{x\}) & \text{if} \quad \phi = \forall x \phi_1 \end{cases} \tag{2.14}$$

where $\tau_U(x) = \tau_0(x)$ if $x \in U$ and $\tau_U(x) = \tau_1(x)$ if $x \notin U$.

Proposition 61 *The structural recursion of* definition (31) *is legitimate.*

Proof
We need to prove the existence and uniqueness of $\tau^* : \mathbf{P}(V) \to [\mathcal{P}(V) \to \mathbf{P}(W)]$ satisfying equation (2.14). We shall do so using theorem (4) of page 42. So we take $X = \mathbf{P}(V)$, $X_0 = \mathbf{P}_0(V)$ and $A = [\mathcal{P}(V) \to \mathbf{P}(W)]$. We consider the map $g_0 : X_0 \to A$ defined by $g_0(x \in y)(U) = \tau_U(x) \in \tau_U(y)$. We define

$h(\perp) : A^0 \to A$ by setting $h(\perp)(0)(U) = \perp$ and $h(\to) : A^2 \to A$ by setting $h(\to)(v)(U) = v(0)(U) \to v(1)(U)$. Finally, we define $h(\forall x) : A^1 \to A$ with:

$$h(\forall x)(v)(U) = \forall \tau_1(x) v(0)(U \setminus \{x\})$$

From theorem (4) there exists a unique map $\tau^* : X \to A$ such that $\tau^*(\phi) = g_0(\phi)$ whenever $\phi = (x \in y)$ and $\tau^*(f(\phi)) = h(f)(\tau^*(\phi))$ for all $f = \perp, \to, \forall x$ and $\phi \in X^{\alpha(f)}$. So let us check that this works: from $\tau^*(\phi) = g_0(\phi)$ for $\phi = (x \in y)$ we obtain $\tau^*(\phi)(U) = g_0(x \in y)(U) = \tau_U(x) \in \tau_U(y)$ which is the first line of equation (2.14). Take $f = \perp$ and $\phi = \perp$. We obtain the equalities:

$$\begin{aligned}
\tau^*(\phi)(U) &= \tau^*(\perp)(U) \\
\text{proper notation } \to &= \tau^*(\perp(0))(U) \\
&= \tau^*(f(0))(U) \\
\tau^* : X^0 \to A^0 \ \to &= h(f)(\tau^*(0))(U) \\
&= h(f)(0)(U) \\
&= h(\perp)(0)(U) \\
&= \perp
\end{aligned}$$

which is the second line of equation (2.14). Recall that the τ^* which appears in the fourth equality refers to the unique mapping $\tau^* : X^0 \to A^0$. We now take $f = \to$ and $\phi = \phi_1 \to \phi_2$ for some $\phi_1, \phi_2 \in \mathbf{P}(V)$. Then we have:

$$\begin{aligned}
\tau^*(\phi)(U) &= \tau^*(\phi_1 \to \phi_2)(U) \\
\phi^*(0) = \phi_1,\ \phi^*(1) = \phi_2 \ \to &= \tau^*(f(\phi^*))(U) \\
\tau^* : X^2 \to A^2 \ \to &= h(f)(\tau^*(\phi^*))(U) \\
&= h(\to)(\tau^*(\phi^*))(U) \\
&= \tau^*(\phi^*)(0)(U) \to \tau^*(\phi^*)(1)(U) \\
&= \tau^*(\phi^*(0))(U) \to \tau^*(\phi^*(1))(U) \\
&= \tau^*(\phi_1)(U) \to \tau^*(\phi_2)(U)
\end{aligned}$$

This is the third line of equation (2.14). Finally consider $f = \forall x$ and $\phi = \forall x \phi_1$:

$$\begin{aligned}
\tau^*(\phi)(U) &= \tau^*(\forall x \phi_1)(U) \\
\phi^*(0) = \phi_1 \ \to &= \tau^*(f(\phi^*))(U) \\
\tau^* : X^1 \to A^1 \ \to &= h(f)(\tau^*(\phi^*))(U) \\
&= h(\forall x)(\tau^*(\phi^*))(U) \\
&= \forall \tau_1(x) \tau^*(\phi^*)(0)(U \setminus \{x\}) \\
&= \forall \tau_1(x) \tau^*(\phi^*(0))(U \setminus \{x\}) \\
&= \forall \tau_1(x) \tau^*(\phi_1)(U \setminus \{x\})
\end{aligned}$$

and this is the last line of equation (2.14). .

2.1.11 Local Inversion of Variable Substitution

Any map $\sigma : V \to W$ gives rise to a substitution mapping $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$. In general, this substitution mapping has little chance to be injective unless $\sigma : V \to W$ is itself injective. However even when σ is not injective, there may be cases where we can still argue the following implication is true:

$$\sigma(\phi) = \sigma(\psi) \;\Rightarrow\; \phi = \psi \tag{2.15}$$

For example, if $\mathrm{Var}(\phi) = \mathrm{Var}(\psi)$ it is sufficient that $\sigma_{|\mathrm{Var}(\phi)}$ be an injective map for (2.15) to be true. But this itself is not necessary. Consider the case when $\phi = \forall y(x \in y) \to (x \in z)$ with x, y, z distinct and $\sigma = [y/z]$. Then we have $\sigma(\phi) = \forall y(x \in y) \to (x \in y)$. Suppose we knew for some reason that $\mathrm{Bnd}(\psi) = \mathrm{Bnd}(\phi) = \{y\}$. Then this would exclude $\psi = \forall z(x \in z) \to (x \in z)$ and the implication (2.15) would hold, if not everywhere at least on the set:

$$\Gamma(\phi) = \{\psi \in \mathbf{P}(V) : \mathrm{Bnd}(\psi) = \mathrm{Bnd}(\phi)\}$$

However, if $\sigma = [y/x]$ then $\sigma(\phi) = \forall y(y \in y) \to (y \in z)$ and the implication (2.15) fails to be true even if $\psi \in \Gamma(\phi)$. As it turns out, the substitution σ is not valid for ϕ, and $\Gamma(\phi)$ is of little use if we mix up free and bound variables.

In this section, we wish to establish sufficient conditions for the implication (2.15) to hold, if not everywhere at least locally on a domain $\Gamma(\phi)$. One way to achieve this is to prove that the substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ has a left-inverse locally around ϕ, i.e. that there exists a subset $\Gamma \subseteq \mathbf{P}(V)$ and a map $\tau : \mathbf{P}(W) \to \mathbf{P}(V)$ such that $\tau \circ \sigma(\phi) = \phi$ for all $\phi \in \Gamma$. So if we happen to know that both ϕ and ψ are elements of Γ, we are guaranteed the implication (2.15) is true. So we are given a map $\sigma : V \to W$ and we want to design a map $\tau : \mathbf{P}(W) \to \mathbf{P}(V)$ which will reverse the effect of the substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$, at least locally on some interesting domain Γ. We cannot hope to achieve this for every σ, but we would like our result to be general enough. Suppose we knew our substitution σ behaved on free variables in a reversible way. Specifically, we would have $V_0 \subseteq V$ such that $\sigma_{|V_0}$ is an injective map and $\mathrm{Fr}(\phi) \subseteq V_0$. Suppose likewise that the impact on bound variables was also reversible. So we assume there is $V_1 \subseteq V$ such that $\sigma_{|V_1}$ is an injective map and $\mathrm{Bnd}(\phi) \subseteq V_1$. For example, if we go back to $\phi = \forall y(x \in y) \to (x \in z)$ with x, y, z distinct and $\sigma = [y/z]$, then σ is of course not injective but $\sigma_{|V_0}$ and $\sigma_{|V_1}$ are both injective with $V_0 = V \setminus \{y\}$ and $V_1 = V \setminus \{x, z\}$. As it turns out, we also have $\mathrm{Fr}(\phi) \subseteq V_0$ and $\mathrm{Bnd}(\phi) \subseteq V_1$. So σ behaves in a reversible way both on free and bound variables. Consider now $\tau_0, \tau_1 : W \to V$ which are left-inverse of σ on V_0 and V_1 respectively, i.e. such that:

$$\begin{aligned} &(i) \qquad u \in V_0 \;\Rightarrow\; \tau_0 \circ \sigma(u) = u \\ &(ii) \qquad u \in V_1 \;\Rightarrow\; \tau_1 \circ \sigma(u) = u \end{aligned}$$

Then we should hope to reverse the impact of $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ by acting separately on the free and bound variables of $\sigma(\phi)$ according to τ_0 and τ_1 respectively. Specifically, if we consider $\tau : \mathbf{P}(W) \to \mathbf{P}(V)$ the dual variable

substitution associated with the ordered pair (τ_0, τ_1) as per definition (31) of page 98, we should hope to obtain $\tau \circ \sigma(\phi) = \phi$ at least for all ϕ such that $\mathrm{Fr}(\phi) \subseteq V_0$ and $\mathrm{Bnd}(\phi) \subseteq V_1$. So let us see if this works in our case:

$$\begin{aligned}
\tau \circ \sigma(\phi) &= \tau \circ \sigma(\forall y(x \in y) \to (x \in z)) \\
\sigma = [y/z] \ \to \ &= \tau(\forall y(x \in y) \to (x \in y)) \\
W = V \text{ and definition (31)} \ \to \ &= \tau^*(\,\forall y(x \in y) \to (x \in y)\,)(V) \\
&= \tau^*(\,\forall y(x \in y)\,)(V) \to \tau^*(x \in y)(V) \\
&= \forall \tau_1(y) \tau^*(x \in y)(V \backslash \{y\}) \to (\tau_0(x) \in \tau_0(y)) \\
&= \forall \tau_1(y)(\tau_0(x) \in \tau_1(y)) \to (\tau_0(x) \in \tau_0(y)) \\
\text{A: to be proved} \ \to \ &= \forall y(x \in y) \to (x \in z) \\
&= \phi
\end{aligned}$$

So it remains to show that $\tau_1(y) = y$, $\tau_0(x) = x$ and $\tau_0(y) = z$. Since we have $V_0 = V \setminus \{y\}$ we obtain $x, z \in V_0$ and consequently from (i) above it follows that $\tau_0(x) = \tau_0 \circ [y/z](x) = x$ and $\tau_0(y) = \tau_0 \circ [y/z](z) = z$. Similarly, since $V_1 = V \setminus \{x, z\}$ we have $y \in V_1$ and consequently from (ii) above it follows that $\tau_1(y) = \tau_1 \circ [y/z](y) = y$ as requested. Hence we see that our inversion scheme is working, at least in this case. As it turns out, the substitution $\sigma = [y/z]$ is valid for the formula $\phi = \forall y(x \in y) \to (x \in z)$. But what if σ wasn't valid for ϕ? Well obviously, when the substitution σ is not valid for ϕ the free and bound variables of $\sigma(\phi)$ have been muddled up. We cannot expect our scheme to work any longer. So let us consider $\sigma = [y/x]$ instead which is clearly not valid for $\phi = \forall y(x \in y) \to (x \in z)$. Then $\sigma_{|V_0}$ and $\sigma_{|V_1}$ are still injective and we still have $\mathrm{Fr}(\phi) \subseteq V_0$ and $\mathrm{Bnd}(\phi) \subseteq V_1$. Of course the maps $\tau_0, \tau_1 : V \to V$ would need to be different but even assuming (i) and (ii) above, our scheme would fail:

$$\begin{aligned}
\tau \circ \sigma(\phi) &= \tau \circ \sigma(\forall y(x \in y) \to (x \in z)) \\
\sigma = [y/x] \ \to \ &= \tau(\forall y(y \in y) \to (y \in z)) \\
W = V \text{ and definition (31)} \ \to \ &= \tau^*(\,\forall y(y \in y) \to (y \in z)\,)(V) \\
&= \tau^*(\,\forall y(y \in y)\,)(V) \to \tau^*(y \in z)(V) \\
&= \forall \tau_1(y) \tau^*(y \in y)(V \backslash \{y\}) \to (\tau_0(y) \in \tau_0(z)) \\
&= \forall \tau_1(y)(\tau_1(y) \in \tau_1(y)) \to (\tau_0(y) \in \tau_0(z)) \\
\text{A: to be proved} \ \to \ &= \forall y(y \in y) \to (x \in z) \\
&\neq \phi
\end{aligned}$$

So it remains to show that $\tau_1(y) = y$, $\tau_0(y) = x$ and $\tau_0(z) = z$. Since we have $V_0 = V \setminus \{y\}$ we obtain $x, z \in V_0$ and consequently from (i) above it follows that $\tau_0(y) = \tau_0 \circ [y/x](x) = x$ and $\tau_0(z) = \tau_0 \circ [y/x](z) = z$. Similarly, since $V_1 = V \setminus \{x, z\}$ we have $y \in V_1$ and consequently from (ii) above it follows that $\tau_1(y) = \tau_1 \circ [y/x](y) = y$ as requested. Ok so we are now ready to proceed. We are given a map $\sigma : V \to W$ and $V_0, V_1 \subseteq V$ such that $\sigma_{|V_0}$ and $\sigma_{|V_1}$ are injective maps. We then consider $\Gamma \subseteq \mathbf{P}(V)$ defined by:

$$\Gamma = \{\phi \in \mathbf{P}(V) : (\mathrm{Fr}(\phi) \subseteq V_0) \wedge (\mathrm{Bnd}(\phi) \subseteq V_1) \wedge (\sigma \text{ valid for } \phi)\}$$

We are hoping the inversion scheme will work on Γ, namely that we can build a map $\tau : \mathbf{P}(W) \to \mathbf{P}(V)$ such that $\tau \circ \sigma(\phi) = \phi$ for all $\phi \in \Gamma$. This result is the object of theorem (10) of page 105 below. The proof of this theorem relies on a technical lemma for which we shall now provide a few words of explanations: proving the formula $\tau \circ \sigma(\phi) = \phi$ is in fact showing $\tau^*(\sigma(\phi))(W) = \phi$ as follows from definition (31). A structural induction with $\phi = \forall x \phi_1$ leads to:

$$\begin{array}{rcl} \tau^*(\sigma(\phi))(W) & = & \tau^*(\sigma(\forall x \phi_1))(W) \\ & = & \tau^*(\,\forall \sigma(x) \sigma(\phi_1)\,)(W) \\ & = & \forall \tau_1 \circ \sigma(x)\, \tau^*(\sigma(\phi_1))(W \setminus \{\sigma(x)\}) \\ x \in \mathrm{Bnd}(\phi) \subseteq V_1 \;\to & = & \forall x\, \tau^*(\sigma(\phi_1))(W \setminus \{\sigma(x)\}) \end{array}$$

So we are immediately confronted with two separate issues. One the one hand we cannot hope to carry out a successful induction argument relating to W only, since $W \setminus \{\sigma(x)\}$ appears on the right-hand-side of this equation. So we need to prove something which relates to some $\tau^*(\sigma(\phi))(W \setminus \sigma(U))$ rather than $\tau^*(\sigma(\phi))(W)$ where U is a possibly non-empty subset of V. On the other hand, the condition $\phi \in \Gamma$ is not very useful when $\phi = \forall x \phi_1$. From the equality $\mathrm{Fr}(\phi) = \mathrm{Fr}(\phi_1) \setminus \{x\}$, it is clear that the condition $\mathrm{Fr}(\phi) \subseteq V_0$ does not imply $\mathrm{Fr}(\phi_1) \subseteq V_0$. So it is possible to have $\phi \in \Gamma$ and yet $\phi_1 \notin \Gamma$. It is important for us to design an induction argument in such a way that if an assumption is made about $\phi = \forall x \phi_1$, this assumption is also satisfied by ϕ_1 so we can use our induction hypothesis. The following lemma addresses these two issues:

Lemma 9 *Let V, W be sets and $\sigma : V \to W$ be a map. Let V_0, V_1 be subsets of V and $\tau_0, \tau_1 : W \to V$ be maps such that for all $x \in V$:*

$$\begin{array}{ll} (i) & x \in V_0 \;\Rightarrow\; \tau_0 \circ \sigma(x) = x \\ (ii) & x \in V_1 \;\Rightarrow\; \tau_1 \circ \sigma(x) = x \end{array}$$

Let $\tau^* : \mathbf{P}(W) \to [\mathcal{P}(W) \to \mathbf{P}(V)]$ be the map associated with (τ_0, τ_1) as per definition (31). *Then for all $U \in \mathcal{P}(V)$ and $\phi \in \mathbf{P}(V)$ we have:*

$$\tau^*(\sigma(\phi))(W \setminus \sigma(U)) = \phi \tag{2.16}$$

provided U and ϕ satisfy the following properties:

$$\begin{array}{ll} (iii) & (\,\mathrm{Fr}(\phi) \setminus U \subseteq V_0\,) \wedge (\,\mathrm{Bnd}(\phi) \cup U \subseteq V_1\,) \\ (iv) & (\,\sigma \textit{ valid for } \phi\,) \wedge (\,\sigma(U) \cap \sigma(\mathrm{Fr}(\phi) \setminus U) = \emptyset\,) \end{array}$$

Proof
We assume $\sigma : V \to W$ is given together with the subsets V_0, V_1 and the maps $\tau_0, \tau_1 : W \to V$ satisfying (i) and (ii). Let $\tau^* : \mathbf{P}(W) \to [\mathcal{P}(W) \to \mathbf{P}(V)]$ be the map associated with the ordered pair (τ_0, τ_1) as per definition (31) of page 98. Given $U \subseteq V$ and $\phi \in \mathbf{P}(V)$ consider the property $q(U, \phi)$ defined by (iii) and (iv). Then we need to show that for all $\phi \in \mathbf{P}(V)$ we have the property:

$$\forall U \subseteq V\ ,\ [\,q(U, \phi)\ \Rightarrow\ \tau^*(\sigma(\phi))(W \setminus \sigma(U)) = \phi\,]$$

We shall do so by a structural induction argument, using theorem (3) of page 31. First we assume that $\phi = (x \in y)$ for some $x, y \in V$. Let $U \subseteq V$ and suppose $q(U, \phi)$ is true. We need to show that equation (2.16) holds. We have:

$$\begin{array}{rcl} \tau^*(\sigma(\phi))(W \setminus \sigma(U)) & = & \tau^*(\sigma(x \in y))(W \setminus \sigma(U)) \\ \text{define } U^* = W \setminus \sigma(U) \ \rightarrow & = & \tau^*(\sigma(x \in y))(U^*) \\ & = & \tau^*(\,\sigma(x) \in \sigma(y)\,)(U^*) \\ \text{definition (31)} \ \rightarrow & = & \tau_{U^*} \circ \sigma(x) \in \tau_{U^*} \circ \sigma(y) \\ \text{A: to be proved} \ \rightarrow & = & x \in y \\ & = & \phi \end{array}$$

So it remains to show that $\tau_{U^*} \circ \sigma(x) = x$ and $\tau_{U^*} \circ \sigma(y) = y$. First we show that $\tau_{U^*} \circ \sigma(x) = x$. We shall distinguish two cases: first we assume that $x \in U$. Then $\sigma(x) \in \sigma(U)$ and it follows that $\sigma(x) \notin U^*$. Thus, using definition (31) we have $\tau_{U^*} \circ \sigma(x) = \tau_1 \circ \sigma(x)$. From the property (ii) above we have $\tau_1 \circ \sigma(x) = x$ whenever $x \in V_1$. So we only need to show that $x \in V_1$. However, having assumed that $q(U, \phi)$ is true, in particular we have $\mathrm{Bnd}(\phi) \cup U \subseteq V_1$. So $x \in V_1$ follows immediately from our assumption $x \in U$. Next we assume that $x \notin U$. Since $\phi = (x \in y)$ we have $x \in \mathrm{Fr}(\phi)$. So it follows that $x \in \mathrm{Fr}(\phi) \setminus U$ and consequently $\sigma(x) \in \sigma(\mathrm{Fr}(\phi) \setminus U)$. Having assumed that $q(U, \phi)$ is true, in particular we have $\sigma(U) \cap \sigma(\mathrm{Fr}(\phi) \setminus U) = \emptyset$. Thus, from $\sigma(x) \in \sigma(\mathrm{Fr}(\phi) \setminus U)$ we obtain $\sigma(x) \notin \sigma(U)$ and we see that $\sigma(x) \in U^*$. Thus, using definition (31) we have $\tau_{U^*} \circ \sigma(x) = \tau_0 \circ \sigma(x)$. From the property (i) above we have $\tau_0 \circ \sigma(x) = x$ whenever $x \in V_0$. So it remains to show that $x \in V_0$. Having assumed that $q(U, \phi)$ is true, in particular we have $\mathrm{Fr}(\phi) \setminus U \subseteq V_0$. So $x \in V_0$ follows immediately from $x \in \mathrm{Fr}(\phi) \setminus U$ which we have already proved. This completes our proof of $\tau_{U^*} \circ \sigma(x) = x$. The proof of $\tau_{U^*} \circ \sigma(y) = y$ is identical so we are now done with the case $\phi = (x \in y)$. Next we assume that $\phi = \bot$. Let $U \subseteq V$ and suppose $q(U, \phi)$ is true. We need to show that equation (2.16) holds:

$$\tau^*(\sigma(\bot))(W \setminus \sigma(U)) = \tau^*(\bot)(W \setminus \sigma(U)) = \bot$$

Next we assume that $\phi = \phi_1 \rightarrow \phi_2$ where $\phi_1, \phi_2 \in \mathbf{P}(V)$ satisfy our desired property. We need to show that the same is true of ϕ. So let $U \subseteq V$ and suppose $q(U, \phi)$ is true. We need to show that equation (2.16) holds:

$$\begin{array}{rcl} \tau^*(\sigma(\phi))(W \setminus \sigma(U)) & = & \tau^*(\sigma(\phi_1 \rightarrow \phi_2))(W \setminus \sigma(U)) \\ \text{define } U^* = W \setminus \sigma(U) \ \rightarrow & = & \tau^*(\sigma(\phi_1 \rightarrow \phi_2))(U^*) \\ & = & \tau^*(\,\sigma(\phi_1) \rightarrow \sigma(\phi_2)\,)(U^*) \\ \text{definition (31)} \ \rightarrow & = & \tau^*(\sigma(\phi_1))(U^*) \rightarrow \tau^*(\sigma(\phi_2))(U^*) \\ \text{A: to be proved} \ \rightarrow & = & \phi_1 \rightarrow \phi_2 \\ & = & \phi \end{array}$$

So it remains to show that equation (2.16) holds for ϕ_1 and ϕ_2. However, from our induction hypothesis, our property is true for ϕ_1 and ϕ_2. Hence, it

is sufficient to prove that $q(U, \phi_1)$ and $q(U, \phi_2)$ are true. First we show that $q(U, \phi_1)$ is true. We need to prove that (iii) and (iv) above are true for ϕ_1:

$$\mathrm{Fr}(\phi_1) \setminus U \subseteq \mathrm{Fr}(\phi) \setminus U \subseteq V_0$$

where the second inclusion follows from our assumption of $q(U, \phi)$. Furthermore:

$$\mathrm{Bnd}(\phi_1) \cup U \subseteq \mathrm{Bnd}(\phi) \cup U \subseteq V_1$$

So (iii) is now established for ϕ_1. Also from $q(U, \phi)$ we obtain:

$$\sigma(U) \cap \sigma(\mathrm{Fr}(\phi_1) \setminus U) \subseteq \sigma(U) \cap \sigma(\mathrm{Fr}(\phi) \setminus U) = \emptyset$$

So it remains to show that σ is valid for ϕ_1, which follows immediately from proposition (54) and the validity of σ for $\phi = \phi_1 \to \phi_2$. This completes our proof of $q(U, \phi_1)$. The proof of $q(U, \phi_2)$ being identical, we are now done with the case $\phi = \phi_1 \to \phi_2$. So we now assume that $\phi = \forall x \phi_1$ where $x \in V$ and $\phi_1 \in \mathbf{P}(V)$ satisfy our induction hypothesis. We need to show the same is true for ϕ. So let $U \subseteq V$ and suppose $q(U, \phi)$ is true. We need to show that equation (2.16) holds for U, which goes as follows:

$$\begin{array}{rcl}
\tau^*(\sigma(\phi))(W \setminus \sigma(U)) & = & \tau^*(\sigma(\forall x \phi_1))(W \setminus \sigma(U)) \\
\text{define } U^* = W \setminus \sigma(U) \ \to & = & \tau^*(\sigma(\forall x \phi_1))(U^*) \\
& = & \tau^*(\,\forall \sigma(x) \sigma(\phi_1)\,)(U^*) \\
\text{definition (31)} \ \to & = & \forall \tau_1 \circ \sigma(x)\, \tau^*(\sigma(\phi_1))(\,U^* \setminus \{\sigma(x)\}\,) \\
(ii) \text{ and } x \in \mathrm{Bnd}(\phi) \subseteq V_1 \ \to & = & \forall x\, \tau^*(\sigma(\phi_1))(\,U^* \setminus \{\sigma(x)\}\,) \\
\text{define } U_1^* = U^* \setminus \{\sigma(x)\} \ \to & = & \forall x\, \tau^*(\sigma(\phi_1))(U_1^*) \\
\text{A: to be proved} \ \to & = & \forall x \phi_1 \\
& = & \phi
\end{array}$$

So it remains to show that $\tau^*(\sigma(\phi_1))(U_1^*) = \phi_1$. From $U^* = W \setminus \sigma(U)$ and $U_1^* = U^* \setminus \{\sigma(x)\}$ we obtain $U_1^* = W \setminus \sigma(U_1)$ where $U_1 = U \cup \{x\}$. So it remains to show that $\tau^*(\sigma(\phi_1))(W \setminus \sigma(U_1)) = \phi_1$, or equivalently that equation (2.16) holds for U_1 and ϕ_1. Having assumed ϕ_1 satisfies our induction hypothesis, it is therefore sufficient to prove that $q(U_1, \phi_1)$ is true. So we need to show that (iii) and (iv) above are true for U_1 and ϕ_1:

$$\begin{array}{rcl}
\mathrm{Fr}(\phi_1) \setminus U_1 & = & \mathrm{Fr}(\phi_1) \setminus \{x\} \setminus U \\
& = & \mathrm{Fr}(\phi) \setminus U \\
q(U, \phi) \ \to & \subseteq & V_0
\end{array}$$

Furthermore:

$$\begin{array}{rcl}
\mathrm{Bnd}(\phi_1) \cup U_1 & = & \mathrm{Bnd}(\phi_1) \cup \{x\} \cup U \\
& = & \mathrm{Bnd}(\phi) \cup U \\
q(U, \phi) \ \to & \subseteq & V_1
\end{array}$$

and:

$$\begin{aligned}
\sigma(U_1) \cap \sigma(\mathrm{Fr}(\phi_1) \setminus U_1) &= \sigma(U_1) \cap \sigma(\,\mathrm{Fr}(\phi_1) \setminus \{x\} \setminus U\,) \\
&= \sigma(U_1) \cap \sigma(\mathrm{Fr}(\phi) \setminus U) \\
&= (\sigma(U) \cup \{\sigma(x)\}) \cap \sigma(\mathrm{Fr}(\phi) \setminus U) \\
q(U,\phi) \;\rightarrow\; &= \{\sigma(x)\} \cap \sigma(\mathrm{Fr}(\phi) \setminus U) \\
&\subseteq \{\sigma(x)\} \cap \sigma(\mathrm{Fr}(\phi)) \\
\text{A: to be proved} \;\rightarrow\; &= \emptyset
\end{aligned}$$

So we need to show that $\sigma(u) \neq \sigma(x)$ whenever $u \in \mathrm{Fr}(\phi)$, which follows immediately from proposition (55) and the validity of σ for $\phi = \forall x \phi_1$, itself a consequence of our assumption $q(U, \phi)$. So we are almost done proving $q(U_1, \phi_1)$ and it remains to show that σ is valid for ϕ_1, which is another immediate consequence of proposition (55). This completes our induction argument. **.**

Theorem 10 *Let V, W be sets and $\sigma : V \to W$ be a map. Let V_0, V_1 be subsets of V such that $\sigma_{|V_0}$ and $\sigma_{|V_1}$ are injective maps. Let Γ be the subset of $\mathbf{P}(V)$:*

$$\Gamma = \{\phi \in \mathbf{P}(V) : (\mathrm{Fr}(\phi) \subseteq V_0) \wedge (\mathrm{Bnd}(\phi) \subseteq V_1) \wedge (\sigma \textit{ valid for } \phi)\}$$

Then, there exits $\tau : \mathbf{P}(W) \to \mathbf{P}(V)$ such that:

$$\forall \phi \in \Gamma \;,\; \tau \circ \sigma(\phi) = \phi$$

where $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ also denotes the associated substitution mapping.

Proof
Let $\sigma : V \to W$ be a map and $V_0, V_1 \subseteq V$ be such that $\sigma_{|V_0}$ and $\sigma_{|V_1}$ are injective maps. We shall distinguish two cases: first we assume that $V = \emptyset$. Then for all $\phi \in \mathbf{P}(V)$ the inclusions $\mathrm{Fr}(\phi) \subseteq V_0$ and $\mathrm{Bnd}(\phi) \subseteq V_1$ are always true. Furthermore, from definition (30) the substitution σ is always valid for ϕ. Hence we have $\Gamma = \mathbf{P}(V)$ and we need to find $\tau : \mathbf{P}(W) \to \mathbf{P}(V)$ such that $\tau \circ \sigma(\phi) = \phi$ for all $\phi \in \mathbf{P}(V)$. We define τ with the following recursion:

$$\tau(\psi) = \begin{cases} \bot & \text{if} \quad \psi = (u \in v) \\ \bot & \text{if} \quad \psi = \bot \\ \tau(\psi_1) \to \tau(\psi_2) & \text{if} \quad \psi = \psi_1 \to \psi_2 \\ \bot & \text{if} \quad \psi = \forall u \psi_1 \end{cases} \tag{2.17}$$

We shall now prove that $\tau \circ \sigma(\phi) = \phi$ using a structural induction argument. Since $V = \emptyset$ there is nothing to check in the case when $\phi = (x \in y)$. So we assume that $\phi = \bot$. Then $\sigma(\phi) = \bot$ and $\tau \circ \sigma(\phi) = \bot$ as requested. Next we assume that $\phi = \phi_1 \to \phi_2$ with $\tau \circ \sigma(\phi_1) = \phi_1$ and $\tau \circ \sigma(\phi_2) = \phi_2$. Then:

$$\begin{aligned}
\tau \circ \sigma(\phi) &= \tau \circ \sigma(\phi_1 \to \phi_2) \\
&= \tau(\,\sigma(\phi_1) \to \sigma(\phi_2)\,) \\
&= \tau \circ \sigma(\phi_1) \to \tau \circ \sigma(\phi_2) \\
&= \phi_1 \to \phi_2 \\
&= \phi
\end{aligned}$$

Since $V = \emptyset$ there is nothing to check in the case when $\phi = \forall x \phi_1$. So this completes our proof when $V = \emptyset$, and we now assume that $V \neq \emptyset$. Let $x_0 \in V$ and consider $\tau_0 : \sigma(V_0) \to V$ and $\tau_1 : \sigma(V_1) \to V$ to be the inverse mappings of $\sigma_{|V_0}$ and $\sigma_{|V_1}$ respectively. Extend τ_0 and τ_1 to the whole of W by setting $\tau_0(u) = x_0$ if $u \notin \sigma(V_0)$ and $\tau_1(u) = x_0$ if $u \notin \sigma(V_1)$. Then $\tau_0, \tau_1 : W \to V$ are left-inverse of σ on V_0 and V_1 respectively, i.e. we have:

$$\begin{aligned} (i) \qquad & x \in V_0 \;\Rightarrow\; \tau_0 \circ \sigma(x) = x \\ (ii) \qquad & x \in V_1 \;\Rightarrow\; \tau_1 \circ \sigma(x) = x \end{aligned}$$

Let $\tau : \mathbf{P}(W) \to \mathbf{P}(V)$ be the dual variable substitution associated with the ordered pair (τ_0, τ_1) as per definition (31). We shall complete the proof of the theorem by showing that $\tau \circ \sigma(\phi) = \phi$ for all $\phi \in \Gamma$ where:

$$\Gamma = \{\phi \in \mathbf{P}(V) : (\mathrm{Fr}(\phi) \subseteq V_0) \wedge (\mathrm{Bnd}(\phi) \subseteq V_1) \wedge (\sigma \text{ valid for } \phi)\}$$

So let $\phi \in \Gamma$. Then in particular ϕ satisfies property (iii) and (iv) of lemma (9) in the particular case when $U = \emptyset$. So applying lemma (9) for $U = \emptyset$, we see that $\tau^*(\sigma(\phi))(W \setminus \sigma(\emptyset)) = \phi$ where $\tau^* : \mathbf{P}(W) \to [\mathcal{P}(W) \to \mathbf{P}(V)]$ is the map associated with τ. Hence we conclude that $\tau \circ \sigma(\phi) = \tau^*(\sigma(\phi))(W) = \phi$. .

2.2 The Substitution Congruence

2.2.1 Preliminaries

Before we start, we would like to say a few words to the more expert readers. The notion of *substitution congruence* seems to be commonly known as *α-equivalence* in the computer science literature, especially within the context of λ-calculus. We decided to use the phrase *substitution congruence* partly out of ignorance and partly because first order logic does not have the notion of β-equivalence and η-equivalence as far as we can tell. Instead, we shall consider other congruences on $\mathbf{P}(V)$ which are the *permutation*, the *absorption* and the *propositional* congruence which have no obvious counterpart in λ-calculus. So we were tempted to change our terminology out of due respect for established traditions, but decided otherwise in the end. The notion of α-equivalence and the more general issue of variable binding in formal languages, has already received some academic attention. For example, the interested reader may wish to refer to Murdoch J. Gabbay [22] and Murdoch J. Gabbay and Aad Mathijssen [23]. These references also focus on *capture-avoiding substitutions* which we feel is an important topic, intimately linked to α-equivalence. Our own treatment of *capture-avoiding substitutions* will give rise to *essential substitutions*.

2.2.2 The Strong Substitution Congruence

We all know that $\forall x(x \in z)$ and $\forall y(y \in z)$ should be identical mathematical statements when $z \notin \{x, y\}$. In this section, we shall attempt to formally define

a congruence $\sim$ on $\mathbf{P}(V)$ such that $\forall x(x \in z) \sim \forall y(y \in z)$ is satisfied for all $z \notin \{x, y\}$. More generally, given a set V and a formula $\phi_1 \in \mathbf{P}(V)$, we would like our congruence $\sim$ to be such that $\forall x\phi_1 \sim \forall y\phi_1[y/x]$ for all $x, y \in V$. In other words, if we were to replace the variable x by the variable y in the formula $\phi = \forall x\phi_1$, the formula $\psi = \forall y\phi_1[y/x]$ resulting from the substitution should have the same *meaning* as that of ϕ. One of the difficulties in pinning down a formal definition for the congruence $\sim$ is to know exactly what we want. If $\phi_1 = (x \in y)$ with $x \neq y$, then $\phi = \forall x(x \in y)$ while $\psi = \forall y(y \in y)$ and it is clear that ϕ and ψ do not represent the same mathematical statement. It would therefore be inappropriate to require that $\forall x\phi_1 \sim \forall y\phi_1[y/x]$ for all $x, y \in V$, without some form of restriction on the variables x and y. Looking back at the example of $\phi_1 = (x \in y)$, the problem arises from the fact that the substitution $[y/x]$ is not a valid substitution for $\forall x\phi_1$. It is therefore tempting to require that $\forall x\phi_1 \sim \forall y\phi_1[y/x]$ for all $x, y \in V$ such that $[y/x]$ is valid for $\forall x\phi_1$. From proposition (57), we can easily check that $[y/x]$ is automatically valid for $\forall x\phi_1$ whenever the condition $y \notin \mathrm{Var}(\phi_1)$ is satisfied. So we could also require that $\forall x\phi_1 \sim \forall y\phi_1[y/x]$ solely when the condition $y \notin \mathrm{Var}(\phi_1)$ is met. This is obviously simpler as it does not require the concept of valid substitution, and it is also in line with the existing literature (e.g. see Donald W. Barnes, John M. Mack [4] page 28). As it turns out, whether we decide to go for the condition $y \notin \mathrm{Var}(\phi_1)$ or $[y/x]$ *is valid for* $\forall x\phi_1$ will lead to the same congruence, as can be seen from proposition (94). So the question is settled: we shall require that $\forall x\phi_1 \sim \forall y\phi_1[y/x]$ whenever $y \notin \mathrm{Var}(\phi_1)$. Since a congruence is always reflexive, there is no harm in imposing that $x \neq y$. We shall define our congruence in terms of a generator, in the sense of definition (18). Such a congruence exists and is unique by virtue of theorem (6) of page 52. However despite our best efforts, it will appear later that the congruence $\sim$ is not the right one. It will in fact be too strong when the set V is a finite set. For this reason, the congruence presented in this section will be called the *strong substitution congruence*. In later parts of this document, we shall alter our definition slightly so as to reach what we believe is a definitive notion of *substitution congruence* working equally well for V finite and V infinite. Despite its minor flaws, the *strong substitution congruence* deserves to be studied in its own right, as it seems to be the one studied in every known textbook (which usually assumes an infinite set V).

Definition 33 *Let V be a set. We call* strong substitution congruence on $\mathbf{P}(V)$ *the congruence on $\mathbf{P}(V)$ generated by the following set $R_0 \subseteq \mathbf{P}(V) \times \mathbf{P}(V)$:*

$$R_0 = \{\, (\, \forall x\phi_1 \,,\, \forall y\, \phi_1[y/x]\,) : \phi_1 \in \mathbf{P}(V) \ ,\ x, y \in V \ ,\ x \neq y \ ,\ y \notin \mathrm{Var}(\phi_1)\,\}$$

where $[y/x]$ denotes the substitution of y in place of x as per definition (26).

2.2.3 Free Variable and Strong Substitution Congruence

The strong substitution congruence is designed in such a way that if you take a formula ϕ and replace its bound variables by other variables, you obtain a formula ψ which is equivalent to ϕ, provided the variable substitution is valid.

The strong substitution congruence is also designed to be the smallest congruence on $\mathbf{P}(V)$ with such property. So one would expect two equivalent formulas to be identical in all respects, except possibly in relation to their bound variables. In particular, if a formula ϕ is equivalent to a formula ψ, we should expect both formulas to have the same free variables. This is indeed the case, as the following proposition shows. Since we already know from proposition (46) that $\mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$ defines a congruence on $\mathbf{P}(V)$, the proof reduces to making sure that every ordered pair (ϕ, ψ) belonging to the generator R_0 of the strong substitution congruence, is such that $\mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$.

Proposition 62 *Let $\sim$ be the strong substitution congruence on $\mathbf{P}(V)$ where V is a set. Then for all $\phi, \psi \in \mathbf{P}(V)$ we have the implication:*

$$\phi \sim \psi \;\Rightarrow\; \mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$$

Proof
Let $\equiv$ be the relation on $\mathbf{P}(V)$ defined by $\phi \equiv \psi \;\Leftrightarrow\; \mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$. We need to show that $\phi \sim \psi \;\Rightarrow\; \phi \equiv \psi$ or equivalently that the inclusion $\sim \subseteq \equiv$ holds. Since $\sim$ is the strong substitution congruence on $\mathbf{P}(V)$, it is the smallest congruence on $\mathbf{P}(V)$ which contains the set R_0 of definition (32). In order to show the inclusion $\sim \subseteq \equiv$ it is therefore sufficient to show that $\equiv$ is a congruence on $\mathbf{P}(V)$ such that $R_0 \subseteq \equiv$. However, we already know from proposition (46) that $\equiv$ is a congruence on $\mathbf{P}(V)$. So it remains to show that $R_0 \subseteq \equiv$. So let $\phi_1 \in \mathbf{P}(V)$ and $x, y \in V$ be such that $x \neq y$ and $y \notin \mathrm{Var}(\phi_1)$. Define the two formulas $\phi = \forall x \phi_1$ and $\psi = \forall y\, \phi_1[y/x]$. We need to show that $\phi \equiv \psi$ or equivalently that $\mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$. We shall distinguish two cases. First we assume that $x \notin \mathrm{Fr}(\phi_1)$. From the assumption $y \notin \mathrm{Var}(\phi_1)$ and proposition (45) we obtain $\mathrm{Fr}(\phi_1[y/x]) = \mathrm{Fr}(\phi_1)$. Furthermore, since $\mathrm{Fr}(\phi_1) \subseteq \mathrm{Var}(\phi_1)$, we also have $y \notin \mathrm{Fr}(\phi_1)$. It follows that:

$$\begin{aligned}
\mathrm{Fr}(\psi) &= \mathrm{Fr}(\forall y\, \phi_1[y/x]) \\
&= \mathrm{Fr}(\phi_1[y/x]) \setminus \{y\} \\
&= \mathrm{Fr}(\phi_1) \setminus \{y\} \\
&= \mathrm{Fr}(\phi_1) \\
&= \mathrm{Fr}(\phi_1) \setminus \{x\} \\
&= \mathrm{Fr}(\forall x \phi_1) \\
&= \mathrm{Fr}(\phi)
\end{aligned}$$

We now consider the case when $x \in \mathrm{Fr}(\phi_1)$. From the assumption $y \notin \mathrm{Var}(\phi_1)$ and proposition (45) we obtain $\mathrm{Fr}(\phi_1[y/x]) = \mathrm{Fr}(\phi_1) \setminus \{x\} \cup \{y\}$, and so:

$$\begin{aligned}
\mathrm{Fr}(\psi) &= \mathrm{Fr}(\forall y\, \phi_1[y/x]) \\
&= \mathrm{Fr}(\phi_1[y/x]) \setminus \{y\} \\
&= (\,\mathrm{Fr}(\phi_1) \setminus \{x\} \cup \{y\}\,) \setminus \{y\} \\
&= (\,\mathrm{Fr}(\phi_1) \setminus \{x\}\,) \setminus \{y\}
\end{aligned}$$

$$\begin{aligned} &= \mathrm{Fr}(\phi_1) \setminus \{x\} \\ &= \mathrm{Fr}(\forall x \phi_1) \\ &= \mathrm{Fr}(\phi) \end{aligned}$$

.

2.2.4 Substitution and Strong Substitution Congruence

Given a substitution mapping $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ arising from an injective map $\sigma : V \to W$, and given an arbitrary congruence $\sim$ on $\mathbf{P}(W)$, we showed in proposition (31) that the relation $\equiv$ on $\mathbf{P}(V)$ defined by $\phi \equiv \psi$ if and only if $\sigma(\phi) \sim \sigma(\psi)$ is a congruence on $\mathbf{P}(V)$. We now apply this fact to the strong substitution congruence on $\mathbf{P}(W)$ to show that $\sigma(\phi) \sim \sigma(\psi)$ whenever we have $\phi \sim \psi$, where $\sim$ also denotes the strong substitution congruence on $\mathbf{P}(V)$. In other words, substitution mappings arising from injective substitution preserve the strong substitution congruence. Since we know that $\equiv$ is a congruence on $\mathbf{P}(V)$, the proof simply consists in showing that $R_0 \subseteq \equiv$, where R_0 is the generator of the strong substitution congruence on $\mathbf{P}(V)$ as per definition (32).

Proposition 63 *Let V and W be sets and $\sigma : V \to W$ be an injective map. Let $\sim$ be the strong substitution congruence both on $\mathbf{P}(V)$ and $\mathbf{P}(W)$. Then:*

$$\phi \sim \psi \;\Rightarrow\; \sigma(\phi) \sim \sigma(\psi)$$

for all $\phi, \psi \in \mathbf{P}(V)$, where $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is also the substitution mapping.

Proof
Let $\equiv$ be the relation on $\mathbf{P}(V)$ defined by $\phi \equiv \psi \;\Leftrightarrow\; \sigma(\phi) \sim \sigma(\psi)$. We need to show that $\phi \sim \psi \;\Rightarrow\; \phi \equiv \psi$ or equivalently that the inclusion $\sim \subseteq \equiv$ holds. Since $\sim$ is the strong substitution congruence on $\mathbf{P}(V)$, it is the smallest congruence on $\mathbf{P}(V)$ which contains the set R_0 of definition (32). In order to show the inclusion $\sim \subseteq \equiv$ it is therefore sufficient to show that $\equiv$ is a congruence on $\mathbf{P}(V)$ such that $R_0 \subseteq \equiv$. However, we already know from proposition (31) that $\equiv$ is a congruence on $\mathbf{P}(V)$. So it remains to show that $R_0 \subseteq \equiv$. So let $\phi_1 \in \mathbf{P}(V)$ and $x, y \in V$ be such that $x \neq y$ and $y \notin \mathrm{Var}(\phi_1)$. Define $\phi = \forall x \phi_1$ and $\psi = \forall y\, \phi_1[y/x]$. We need to show that $\phi \equiv \psi$ or equivalently that $\sigma(\phi) \sim \sigma(\psi)$. In order to do so, it is sufficient to show that the ordered pair $(\sigma(\phi), \sigma(\psi))$ belongs to the generator R_0' of the strong substitution congruence on $\mathbf{P}(W)$ as per definition (32). In other words, it is sufficient to show the existence of $\phi_1' \in \mathbf{P}(W)$ and $x', y' \in W$ with $x' \neq y'$ and $y' \notin \mathrm{Var}(\phi_1')$, such that $\sigma(\phi) = \forall x' \phi_1'$ and $\sigma(\psi) = \forall y'\, \phi_1'[y'/x']$. Take $\phi_1' = \sigma(\phi_1) \in \mathbf{P}(W)$ together with $x' = \sigma(x) \in W$ and $y' = \sigma(y) \in W$. Then, we have:

$$\sigma(\phi) = \sigma(\forall x \phi_1) = \forall \sigma(x)\, \sigma(\phi_1) = \forall x' \phi_1'$$

Furthermore, if we accept for now that $\sigma \circ [y/x] = [\sigma(y)/\sigma(x)] \circ \sigma$, we have:

$$\sigma(\psi) \;=\; \sigma(\forall y\, \phi_1[y/x])$$

$$
\begin{aligned}
&= \forall\sigma(y)\,\sigma(\phi_1[y/x]) \\
&= \forall y'\,\sigma([y/x](\phi_1)) \\
&= \forall y'\,\sigma\circ[y/x]\,(\phi_1) \\
&= \forall y'\,[\sigma(y)/\sigma(x)]\circ\sigma\,(\phi_1) \\
&= \forall y'\,[y'/x'](\phi_1') \\
&= \forall y'\,\phi_1'[y'/x']
\end{aligned}
$$

So it remains to show that $\sigma\circ[y/x] = [\sigma(y)/\sigma(x)]\circ\sigma$ is indeed true, and furthermore that $x' \neq y'$ and $y' \notin \mathrm{Var}(\phi_1')$. Since $\sigma : V \to W$ is an injective map, $x' \neq y'$ follows immediately from $x \neq y$. We now show that $y' \notin \mathrm{Var}(\phi_1')$. So suppose to the contrary that $y' \in \mathrm{Var}(\phi_1')$. We shall arrive at a contradiction. Since $\phi_1' = \sigma(\phi_1)$, from proposition (35) we have:

$$\mathrm{Var}(\phi_1') = \{\sigma(u) : u \in \mathrm{Var}(\phi_1)\}$$

It follows that there exists $u \in \mathrm{Var}(\phi_1)$ such that $y' = \sigma(u)$. However, $y' = \sigma(y)$ and $\sigma : V \to W$ is an injective map. Hence we see that $u = y$ and consequently $y \in \mathrm{Var}(\phi_1)$ which contradicts our initial assumption of $y \notin \mathrm{Var}(\phi_1)$. We shall complete the proof of this proposition by showing that $\sigma\circ[y/x] = [\sigma(y)/\sigma(x)]\circ\sigma$. So let $u \in V$, and suppose first that $u \neq x$. Then:

$$
\begin{aligned}
\sigma\circ[y/x](u) &= \sigma([y/x](u)) \\
&= \sigma(u) \\
&= [\sigma(y)/\sigma(x)](\sigma(u)) \\
&= [\sigma(y)/\sigma(x)]\circ\sigma(u)
\end{aligned}
$$

where the third equality crucially depends on $\sigma(u) \neq \sigma(x)$ which itself follows from the injectivity of σ and $u \neq x$. We now assume that $u = x$. Then:

$$
\begin{aligned}
\sigma\circ[y/x](u) &= \sigma([y/x](u)) \\
&= \sigma(y) \\
&= [\sigma(y)/\sigma(x)](\sigma(u)) \\
&= [\sigma(y)/\sigma(x)]\circ\sigma(u)
\end{aligned}
$$

In both cases $u \neq x$ and $u = x$ we see that $\sigma\circ[y/x](u) = [\sigma(y)/\sigma(x)]\circ\sigma(u)$. .

We now wish to apply proposition (63) to the substitution mapping $[y/x]$ which is not injective when $x \neq y$. The trick is to consider the permutation mapping $[y\,{:}\,x]$ and argue that $\phi[y/x]$ coincides with $\phi[y\,{:}\,x]$ while $\psi[y/x]$ coincides with $\psi[y\,{:}\,x]$, provided the condition $y \notin \mathrm{Var}(\phi)\cup\mathrm{Var}(\psi)$ is satisfied.

Proposition 64 *Let $\sim$ be the strong substitution congruence on $\mathbf{P}(V)$ where V is a set. Let $\phi, \psi \in \mathbf{P}(V)$ and $x, y \in V$ such that $y \notin \mathrm{Var}(\phi)\cup\mathrm{Var}(\psi)$. Then:*

$$\phi \sim \psi \;\Rightarrow\; \phi[y/x] \sim \psi[y/x]$$

Proof
We assume that $\phi \sim \psi$. We need to show that $\phi[y/x] \sim \psi[y/x]$. Unfortunately, the map $[y/x] : V \to V$ is not injective when $x \neq y$ since $[y/x](x) = y = [y/x](y)$. So we cannot argue directly from proposition (63) that $\phi[y/x] \sim \psi[y/x]$. Instead, we shall consider the permutation $[y : x] : V \to V$ as per definition (27). Since $[y : x]$ is injective, from proposition (63) we have $\phi[y : x] \sim \psi[y : x]$. We shall complete the proof of the proposition by proving $\phi[y : x] = \phi[y/x]$ and $\psi[y : x] = \psi[y/x]$. But this follows immediately from proposition (39) and the assumption $y \notin \mathrm{Var}(\phi) \cup \mathrm{Var}(\psi)$. **.**

As can be seen from definition (32), the strong substitution congruence was defined so as to ensure that $\forall x \phi_1$ is always equivalent to $\forall y \phi_1[y/x]$ when $x \neq y$, provided we have $y \notin \mathrm{Var}(\phi_1)$. The fundamental idea is that if we replace a variable x which is not free, by a variable y which is not already present in a formula, then we do not change the *meaning* of the formula. We now check that this property is indeed true. The proof is done by structural induction.

Proposition 65 *Let $\sim$ be the strong substitution congruence on $\mathbf{P}(V)$ where V is a set. Let $\phi \in \mathbf{P}(V)$, $x, y \in V$ such that $y \notin \mathrm{Var}(\phi)$ and $x \notin \mathrm{Fr}(\phi)$. Then:*

$$\phi[y/x] \sim \phi$$

Proof
We assume $x, y \in V$ given. For all $\phi \in \mathbf{P}(V)$, we need to show the implication $(y \notin \mathrm{Var}(\phi)) \wedge (x \notin \mathrm{Fr}(\phi)) \;\Rightarrow\; \phi[y/x] \sim \phi$. We shall do so by structural induction, using theorem (3) of page 31. Since $\mathbf{P}_0(V)$ is a generator of $\mathbf{P}(V)$, we show first that the property is true on $\mathbf{P}_0(V)$. So let $\phi = (u \in v) \in \mathbf{P}_0(V)$, where $u, v \in V$. We assume that $y \notin \mathrm{Var}(\phi)$ and $x \notin \mathrm{Fr}(\phi)$, and we need to show that $\phi[y/x] \sim \phi$. Since $\mathrm{Var}(\phi) = \mathrm{Fr}(\phi) = \{u, v\}$, we have $x, y \notin \{u, v\}$. In particular, $x \notin \{u, v\}$ and consequently we have:

$$\phi[y/x] = (\,[y/x](u) \;\in\; [y/x](v)\,) = (u \in v) = \phi$$

In particular $\phi[y/x] \sim \phi$. Next we check that the property is true for $\bot \in \mathbf{P}(V)$:

$$\bot[y/x] = [y/x](\bot) = \bot$$

and in particular $\bot[y/x] \sim \bot$. Next we check that the property is true for $\phi = \phi_1 \to \phi_2$, if it is true for $\phi_1, \phi_2 \in \mathbf{P}(V)$. So we assume that $y \notin \mathrm{Var}(\phi)$ and $x \notin \mathrm{Fr}(\phi)$, and we need to show that $\phi[y/x] \sim \phi$. From the equality $\mathrm{Var}(\phi) = \mathrm{Var}(\phi_1) \cup \mathrm{Var}(\phi_2)$ we see that $y \notin \mathrm{Var}(\phi_1)$ and $y \notin \mathrm{Var}(\phi_2)$. Likewise, from $\mathrm{Fr}(\phi) = \mathrm{Fr}(\phi_1) \cup \mathrm{Fr}(\phi_2)$ we obtain $x \notin \mathrm{Fr}(\phi_1)$ and $x \notin \mathrm{Fr}(\phi_2)$. Having assumed the property is true for ϕ_1 and ϕ_2, it follows that $\phi_1[y/x] \sim \phi_1$ and $\phi_2[y/x] \sim \phi_2$. The strong substitution congruence being a congruent relation:

$$\phi[y/x] \;=\; \phi_1[y/x] \to \phi_2[y/x] \;\sim\; \phi_1 \to \phi_2 \;=\; \phi$$

Finally we check that the property is true for $\phi = \forall u \phi_1$, if it is true for ϕ_1. So we assume that $y \notin \mathrm{Var}(\phi)$ and $x \notin \mathrm{Fr}(\phi)$, and we need to show that $\phi[y/x] \sim \phi$.

We shall distinguish two cases. First we assume that $x \neq u$. Then, we have:

$$\phi[y/x] = [y/x](\forall u \phi_1) = \forall\, [y/x](u)\, \phi_1[y/x] = \forall u \phi_1[y/x]$$

So we need to show that $\forall u \phi_1[y/x] \sim \forall u \phi_1$. The strong substitution congruence being a congruent relation, it is sufficient to prove that $\phi_1[y/x] \sim \phi_1$. Having assumed the property is true for ϕ_1, it is therefore sufficient to show $y \notin \mathrm{Var}(\phi_1)$ and $x \notin \mathrm{Fr}(\phi_1)$. Since $y \notin \mathrm{Var}(\phi)$ and $\mathrm{Var}(\phi) = \{u\} \cup \mathrm{Var}(\phi_1)$, it is clear that $y \notin \mathrm{Var}(\phi_1)$. So we need to show that $x \notin \mathrm{Fr}(\phi_1)$. So suppose to the contrary that $x \in \mathrm{Fr}(\phi_1)$. Since $\mathrm{Fr}(\phi) = \mathrm{Fr}(\phi_1) \setminus \{u\}$ and $x \neq u$, we obtain $x \in \mathrm{Fr}(\phi)$ which contradicts our initial assumption of $x \notin \mathrm{Fr}(\phi)$. This completes our proof in the case when $x \neq u$. We now assume $x = u$. Then:

$$\phi[y/x] = [y/x](\forall u \phi_1) = \forall\, [y/x](u)\, \phi_1[y/x] = \forall y \phi_1[y/x]$$

So we need to show that $\forall y \phi_1[y/x] \sim \forall x \phi_1$. We shall consider two cases. First we assume that $x = y$. So we need to show that $\forall x \phi_1[x/x] \sim \forall x \phi_1$, for which it is sufficient to prove that $\phi_1[x/x] = \phi_1$ which follows from proposition (29) and the fact that $[x/x] : V \to V$ is the identity mapping. We now assume that $x \neq y$. It is sufficient to prove that the ordered pair $(\forall x \phi_1, \forall y \phi_1[y/x])$ belongs to the generator R_0 of the strong substitution congruence on $\mathbf{P}(V)$ as per definition (32). Since $x \neq y$, it remains to show that $y \notin \mathrm{Var}(\phi_1)$ which follows immediately from $y \notin \mathrm{Var}(\phi)$ and $\mathrm{Var}(\phi) = \{x\} \cup \mathrm{Var}(\phi_1)$. .

2.2.5 Characterization of the Strong Congruence

In definition (32) the strong substitution congruence was defined in terms of a generator. This makes it very convenient to show that two given formulas ϕ and ψ are equivalent. For instance, if $\phi = \forall x \forall y (x \in y)$ and $\psi = \forall y \forall x (y \in x)$, if there is $u \in V$ such that $u \notin \{x, y\}$, the proof that $\phi \sim \psi$ would go as follows:

$$\begin{aligned} \forall x \forall y (x \in y) &\sim \forall u \forall y (u \in y) \\ &\sim \forall u \forall x (u \in x) \\ &\sim \forall y \forall x (y \in x) \end{aligned}$$

The first and third equivalence stem directly from definition (32), as does the equivalence $\forall y (u \in y) \sim \forall x (u \in x)$. Knowing that $\sim$ is a congruent relation allows us to establish the second equivalence, while knowing that $\sim$ is a transitive relation allows us to conclude that $\phi \sim \psi$. More generally, the knowledge of the generator R_0 of definition (32) gives us the equivalence $\phi \sim \psi$ immediately, for many pairs (ϕ, ψ). Using the congruent property, reflexivity, symmetry and transitivity of the relation $\sim$, we readily obtain this equivalence for many more pairs. So showing that $\phi \sim \psi$ is usually the easy part.

What is more difficult is proving that an equivalence $\phi \sim \psi$ does not hold. For instance, if $\phi = (x \in y)$ and $\psi = \bot$, we would like to think that ϕ is not equivalent to ψ. However, definition (32) does not give us an immediate tool to prove that $\phi \not\sim \psi$. Fortunately, we showed in proposition (62) that if $\phi \sim \psi$

then we must have $\mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$. Since $\mathrm{Fr}(\phi) = \{x, y\}$ while $\mathrm{Fr}(\psi) = \emptyset$ we are able in this case to conclude that ϕ is not equivalent to ψ. But if $\phi = (x \in y)$ while $\psi = (y \in x)$ with $x \neq y$, then the implication $\phi \sim \psi \;\Rightarrow\; \mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$ does not help us to conclude that $\phi \not\sim \psi$. Somehow we need something sharper.

So we need to prove an implication $\phi \sim \psi \;\Rightarrow\; \phi \simeq \psi$, having chosen a relation $\simeq$ which tells us a bit more about the formulas ϕ and ψ, than the simple $\mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$. In fact, we shall choose the relation $\simeq$ so as to have the equivalence $\phi \sim \psi \;\Leftrightarrow\; \phi \simeq \psi$, as a way of ensuring that the statement $\phi \simeq \psi$ tells us as much as possible about the formulas ϕ and ψ. So before we prove anything, our first task is to choose a sensible relation $\simeq$.

So let us assume that $\phi \sim \psi$. We know from theorem (2) of page 21 that any formula of first order predicate logic is either of the form $(x \in y)$, or is the contradiction constant $\bot$, or is an implication $\phi_1 \to \phi_2$ or is a quantification $\forall x \phi_1$. Let us review all these four cases in relation to ϕ: so suppose first that $\phi = (x \in y)$ with $\phi \sim \psi$. Clearly we would expect the formula ψ to be equal to the formula ϕ. Suppose now that $\phi = \bot$. Then we would expect the formula ψ to be equal to $\bot$. Suppose now that ϕ is an implication $\phi = \phi_1 \to \phi_2$. If $\phi \sim \psi$ we would also expect the formula ψ to be an implication $\psi = \psi_1 \to \psi_2$. Furthermore, we would expect to have $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$.

Suppose now that ϕ is a quantification $\phi = \forall x \phi_1$. Then we would also expect the formula ψ to be a quantification $\psi = \forall y \psi_1$. However, we would not expect the variables x and y to be the same in general. If $x = y$ then we would expect to have $\phi_1 \sim \psi_1$, but if $x \neq y$ then the relationship between ϕ_1 and ψ_1 should be more complex. Informally, we would expect the formula ψ_1 to be the *same mathematical statement* as the formula ϕ_1, but with the variable x replaced by the variable y. Of course we cannot hope to have $\psi_1 = \phi_1[y/x]$ in general, as there may have been other *changes of variable* within the formulas ϕ_1 and ψ_1. However, we would expect to have the equivalence $\psi_1 \sim \phi_1[y/x]$.

Unfortunately, this does not quite work. We already know from definition (32) that considering the formula $\phi_1[y/x]$ is not very safe unless we have $y \notin \mathrm{Var}(\phi_1)$. We have made no mention of this fact so far, so it is likely that the simple condition $\psi_1 \sim \phi_1[y/x]$ is doomed, without further qualification. In fact, consider the case when $\phi = \forall x \forall y (x \in y)$ and $\psi = \forall y \forall x (y \in x)$ with $x \neq y$. Then $\phi_1 = \forall y (x \in y)$ and $\psi_1 = \forall x (y \in x)$. So we obtain $\phi_1[y/x] = \forall y (y \in y)$ and we certainly expect the equivalence $\psi_1 \sim \phi_1[y/x]$ to be false. So we need to look for something more complicated. Suppose there exists $u \in V$ such that $u \notin \{x, y\}$. Defining the formula $\theta = \forall u (x \in u)$ the condition $y \notin \mathrm{Var}(\theta)$ is now satisfied and we can safely consider the formula $\theta[y/x] = \forall u (y \in u)$. From definition (32) we obtain immediately $\phi_1 \sim \theta$ and $\psi_1 \sim \theta[y/x]$. So this may be the relationship we are looking for between the formula ϕ_1 and the formula ψ_1: the existence of a third formula θ such that $\phi_1 \sim \theta$ and $\psi_1 \sim \theta[y/x]$, with the additional condition $y \notin \mathrm{Var}(\theta)$. Note that we cannot hope to make this relationship simpler in general. We have already established that $\phi_1 = \theta$ and $\psi_1 \sim \theta[y/x]$, (or indeed $\phi_1 = \theta$ and $\psi_1 = \theta[y/x]$) fails to work. The condition $\phi_1 \sim \theta$ and $\psi_1 = \theta[y/x]$ does not work in general either: from proposition (41) we know that x can never be a variable of $\theta[y/x]$ when $x \neq y$, and consequently we cannot

hope to have the equality $\psi_1 = \theta[y/x]$ in the case when $\psi_1 = \forall x(y \in x)$. In the light of these comments, we can now venture a sensible guess for our relation $\simeq$.

Definition 34 *Let $\sim$ be the strong substitution congruence on $\mathbf{P}(V)$ where V is a set. Let $\phi, \psi \in \mathbf{P}(V)$. We say that ϕ is* almost strongly equivalent to ψ *and we write $\phi \simeq \psi$, if and only if one of the following is the case:*

(i) $\quad \phi \in \mathbf{P}_0(V)\ ,\ \psi \in \mathbf{P}_0(V)\ ,\ \textit{and}\ \phi = \psi$

(ii) $\quad \phi = \bot\ \textit{and}\ \psi = \bot$

(iii) $\quad \phi = \phi_1 \to \phi_2\ ,\ \psi = \psi_1 \to \psi_2\ ,\ \phi_1 \sim \psi_1\ \textit{and}\ \phi_2 \sim \psi_2$

(iv) $\quad \phi = \forall x \phi_1\ ,\ \psi = \forall x \psi_1\ \textit{and}\ \phi_1 \sim \psi_1$

(v) $\quad \phi = \forall x \phi_1\ ,\ \psi = \forall y \psi_1\ ,\ x \neq y\ ,\ \phi_1 \sim \theta\ ,\ \psi_1 \sim \theta[y/x]\ ,\ y \notin \mathrm{Var}(\theta)$

It should be noted that (v) of definition (33) is a notational shortcut for the more detailed statement $\phi = \forall x \phi_1\ ,\ \psi = \forall y \psi_1\ ,\ x \neq y$ and *there exists a formula* $\theta \in \mathbf{P}(V)$ such that $\phi_1 \sim \theta\ ,\ \psi_1 \sim \theta[y/x]\ ,\ y \notin \mathrm{Var}(\theta)$.

Proposition 66 $(i), (ii), (iii), (iv), (v)$ *of* definition (33) *are mutually exclusive.*

Proof
This is an immediate consequence of theorem (2) of page 21 applied to the free universal algebra $\mathbf{P}(V)$ with free generator $\mathbf{P}_0(V)$, where a formula $\phi \in \mathbf{P}(V)$ is either an element of $\mathbf{P}_0(V)$, or the contradiction constant $\phi = \bot$, or an implication $\phi = \phi_1 \to \phi_2$, or a quantification $\phi = \forall x \phi_1$, but cannot be equal to any two of those things simultaneously. Since (v) can only occur with $x \neq y$, it also follows from theorem (2) that (v) cannot occur at the same time as (iv). **.**

So we have defined our relation $\simeq$ and it remains to prove the equivalence:

$$\phi \sim \psi \ \Leftrightarrow\ \phi \simeq \psi$$

As we will soon discover, the difficult part is showing the implication $\Rightarrow$. In order to do so, we shall need to show that $\simeq$ is a congruence on $\mathbf{P}(V)$ which contains the generator R_0 of definition (32). So we start by proving $R_0 \subseteq \simeq$.

Proposition 67 *Let $\simeq$ be the almost strong equivalence relation on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ contains the generator R_0 of* definition (32).

Proof
Suppose $x, y \in V$ and $\phi_1 \in \mathbf{P}(V)$ are such that $x \neq y$ and $y \notin \mathrm{Var}(\phi_1)$. Note that this cannot happen unless V has at least two elements. We define $\phi = \forall x \phi_1$ and $\psi = \forall y\, \phi_1[y/x]$. We need to show that $\phi \simeq \psi$. We shall do so by proving that (v) of proposition (33) is the case. Define $\theta = \phi_1$ and $\psi_1 = \phi_1[y/x] = \theta[y/x]$. Since the strong substitution congruence $\sim$ is reflexive on $\mathbf{P}(V)$, we have $\phi_1 \sim \theta$ and $\psi_1 \sim \theta[y/x]$. It follows that $\phi = \forall x \phi_1$, $\psi = \forall y \psi_1$, $x \neq y$, $\phi_1 \sim \theta$, $\psi_1 \sim \theta[y/x]$ and $y \notin \mathrm{Var}(\theta)$. **.**

We now need to show that $\simeq$ is a congruence on $\mathbf{P}(V)$. In particular, it is an equivalence relation, i.e. a relation on $\mathbf{P}(V)$ which is reflexive, symmetric and transitive. We first deal with the reflexivity.

Proposition 68 *Let $\simeq$ be the almost strong equivalence relation on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ is a reflexive relation on $\mathbf{P}(V)$.*

Proof
Let $\phi \in \mathbf{P}(V)$. We need to show that $\phi \simeq \phi$. From theorem (2) of page 21 we know that ϕ is either an element of $\mathbf{P}_0(V)$, or $\phi = \bot$ or $\phi = \phi_1 \to \phi_2$ or $\phi = \forall x \phi_1$ for some $\phi_1, \phi_2 \in \mathbf{P}(V)$ and $x \in V$. We shall consider these four mutually exclusive cases separately. Suppose first that $\phi \in \mathbf{P}_0(V)$: then from $\phi = \phi$ we obtain $\phi \simeq \phi$. Suppose next that $\phi = \bot$: then it is clear that $\phi \simeq \phi$. Suppose now that $\phi = \phi_1 \to \phi_2$. Since the strong substitution congruence $\sim$ is reflexive, we have $\phi_1 \sim \phi_1$ and $\phi_2 \sim \phi_2$. It follows from (iii) of definition (33) that $\phi \simeq \phi$. Suppose finally that $\phi = \forall x \phi_1$. From $\phi_1 \sim \phi_1$ and (iv) of definition (33) we conclude that $\phi \simeq \phi$. In all cases, we have proved that $\phi \simeq \phi$. **.**

Proposition 69 *Let $\simeq$ be the almost strong equivalence relation on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ is a symmetric relation on $\mathbf{P}(V)$.*

Proof
Let $\phi, \psi \in \mathbf{P}(V)$ be such that $\phi \simeq \psi$. We need to show that $\psi \simeq \phi$. We shall consider the five possible cases of definition (33): suppose first that $\phi \in \mathbf{P}_0(V)$, $\psi \in \mathbf{P}_0(V)$ and $\phi = \psi$. Then it is clear that $\psi \simeq \phi$. Suppose next that $\phi = \bot$ and $\psi = \bot$. Then we also have $\psi \simeq \phi$. We now assume that $\phi = \phi_1 \to \phi_2$ and $\psi = \psi_1 \to \psi_2$ with $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$. Since the strong substitution congruence on $\mathbf{P}(V)$ is symmetric, we have $\psi_1 \sim \phi_1$ and $\psi_2 \sim \phi_2$. Hence we have $\psi \simeq \phi$. We now assume that $\phi = \forall x \phi_1$ and $\psi = \forall x \psi_1$ with $\phi_1 \sim \psi_1$. Then once again by symmetry of the strong substitution congruence we have $\psi_1 \sim \phi_1$ and consequently $\psi \simeq \phi$. We finally consider the last possible case of $\phi = \forall x \phi_1$, $\psi = \forall y \psi_1$ with $x \neq y$ and we assume the existence of $\theta \in \mathbf{P}(V)$ such that $\phi_1 \sim \theta$, $\psi_1 \sim \theta[y/x]$ and $y \notin \mathrm{Var}(\theta)$. Define $\theta^* = \theta[y/x]$. In order to show that $\psi \simeq \phi$ it is sufficient to prove that $\phi_1 \sim \theta^*[x/y]$ and $x \notin \mathrm{Var}(\theta^*)$. First we show that $x \notin \mathrm{Var}(\theta^*)$. So we need to show that $x \notin \mathrm{Var}(\theta[y/x])$ which in fact follows immediately from proposition (41) and $x \neq y$. We now show that $\phi_1 \sim \theta^*[x/y] = \theta[y/x][x/y]$. Since $\phi_1 \sim \theta$ and the strong substitution congruence on $\mathbf{P}(V)$ is a transitive relation, it is sufficient to prove that:

$$\theta \sim \theta[y/x][x/y]$$

In fact, the strong substitution congruence being reflexive, it is sufficient to prove that $\theta = \theta[y/x][x/y]$. From proposition (40), since $y \notin \mathrm{Var}(\theta)$ we obtain $\theta[x/x] = \theta[y/x][x/y]$. Since $[x/x] : V \to V$ is the identity mapping, we conclude from proposition (29) that $\theta[x/x] = \theta$ and finally $\theta = \theta[y/x][x/y]$. **.**

Having shown that $\simeq$ is a reflexive and symmetric relation on $\mathbf{P}(V)$, we now prove that it is also a transitive relation. This is by far the most difficult result of this section as many technical details need to be checked.

Proposition 70 *Let $\simeq$ be the almost strong equivalence relation on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ is a transitive relation on $\mathbf{P}(V)$.*

Proof
Let ϕ, ψ and $\chi \in \mathbf{P}(V)$ be such that $\phi \simeq \psi$ and $\psi \simeq \chi$. We need to show that $\phi \simeq \chi$. We shall consider the five possible cases of definition (33) in relation to $\phi \simeq \psi$. Suppose first that $\phi, \psi \in \mathbf{P}_0(V)$ and $\phi = \psi$. Then from $\psi \simeq \chi$ we obtain $\psi, \chi \in \mathbf{P}_0(V)$ and $\psi = \chi$. It follows that $\phi, \chi \in \mathbf{P}_0(V)$ and $\phi = \chi$. Hence we see that $\phi \simeq \chi$. We now assume that $\phi = \psi = \perp$. Then from $\psi \simeq \chi$ we obtain $\psi = \chi = \perp$. It follows that $\phi = \chi = \perp$ and consequently $\phi \simeq \chi$. We now assume that $\phi = \phi_1 \to \phi_2$ and $\psi = \psi_1 \to \psi_2$ with $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$. From $\psi \simeq \chi$ we obtain $\chi = \chi_1 \to \chi_2$ with $\psi_1 \sim \chi_1$ and $\psi_2 \sim \chi_2$. The strong substitution congruence being transitive, it follows that $\phi_1 \sim \chi_1$ and $\phi_2 \sim \chi_2$. Hence we see that $\phi \simeq \chi$. We now assume that $\phi = \forall x \phi_1$ and $\psi = \forall x \psi_1$ with $\phi_1 \sim \psi_1$, for some $x \in V$. From $\psi \simeq \chi$ only the cases (iv) and (v) of definition (33) are possible. First we assume that (iv) is the case. Then $\chi = \forall x \chi_1$ with $\psi_1 \sim \chi_1$. The strong substitution congruence being transitive, we obtain $\phi_1 \sim \chi_1$ and consequently $\phi \simeq \chi$. We now assume that (v) is the case. Then $\chi = \forall y \chi_1$ for some $y \in V$ with $x \neq y$, and there exists $\theta \in \mathbf{P}(V)$ such that $\psi_1 \sim \theta$, $\chi_1 \sim \theta[y/x]$ and $y \notin \mathrm{Var}(\theta)$. The strong substitution congruence being transitive, we obtain $\phi_1 \sim \theta$ and consequently $\phi \simeq \chi$. It remains to consider the last possible case of definition (33). So we assume that $\phi = \forall x \phi_1$ and $\psi = \forall y \psi_1$ with $x \neq y$, and we assume the existence of $\theta \in \mathbf{P}(V)$ such that $\phi_1 \sim \theta$, $\psi_1 \sim \theta[y/x]$ and $y \notin \mathrm{Var}(\theta)$. From $\psi \simeq \chi$ only the cases (iv) and (v) of definition (33) are possible. First we assume that (iv) is the case. Then $\chi = \forall y \chi_1$ with $\psi_1 \sim \chi_1$. The strong substitution congruence being transitive, we obtain $\chi_1 \sim \theta[y/x]$ and consequently $\phi \simeq \chi$. We now assume that (v) is the case. Then $\chi = \forall z \chi_1$ for some $z \in V$ with $y \neq z$, and there exists $\theta^* \in \mathbf{P}(V)$ such that $\psi_1 \sim \theta^*$, $\chi_1 \sim \theta^*[z/y]$ and $z \notin \mathrm{Var}(\theta^*)$. We shall now distinguish two cases. First we assume that $x = z$. Then $\phi = \forall x \phi_1$ and $\chi = \forall x \chi_1$ and in order to show that $\phi \simeq \chi$ it is sufficient to prove that $\phi_1 \sim \chi_1$. Since $\phi_1 \sim \theta$ and $\chi_1 \sim \theta^*[z/y]$, using the symmetry and transitivity of the strong substitution congruence, it remains to show that $\theta \sim \theta^*[z/y]$. Having assumed that $x = z$, we have to prove that $\theta \sim \theta^*[x/y]$. Since $y \notin \mathrm{Var}(\theta)$, from proposition (40) we have $\theta[y/x][x/y] = \theta[x/x]$ and from proposition (29) we obtain $\theta[x/x] = \theta$. It follows that $\theta[y/x][x/y] = \theta$ and it remains to prove that $\theta[y/x][x/y] \sim \theta^*[x/y]$. Using proposition (64), it is sufficient to prove that $\theta[y/x] \sim \theta^*$ and $x \notin \mathrm{Var}(\theta[y/x]) \cup \mathrm{Var}(\theta^*)$. The fact that $\theta[y/x] \sim \theta^*$ follows from $\psi_1 \sim \theta[y/x]$ and $\psi_1 \sim \theta^*$, using the symmetry and transitivity of the strong substitution congruence on $\mathbf{P}(V)$. The fact that $x \notin \mathrm{Var}(\theta[y/x])$ follows from proposition (41) and the assumption $x \neq y$. The fact that $x \notin \mathrm{Var}(\theta^*)$ follows from the assumptions $x = z$ and $z \notin \mathrm{Var}(\theta^*)$. This completes our proof in the case when $x = z$. We now assume that $x \neq z$. So we have $x \neq y$, $y \neq z$ and $x \neq z$, with $\phi = \forall x \phi_1$, $\psi = \forall y \psi_1$ and $\chi = \forall z \chi_1$. Furthermore, there exist θ and $\theta^* \in \mathbf{P}(V)$ such that $\phi_1 \sim \theta$, $\psi_1 \sim \theta[y/x]$, $\psi_1 \sim \theta^*$ and $\chi_1 \sim \theta^*[z/y]$. Finally, we have $y \notin \mathrm{Var}(\theta)$ and $z \notin \mathrm{Var}(\theta^*)$, and we need to show that $\phi \simeq \chi$. Define $\eta = \theta[y/z]$. It is sufficient to show that $\phi_1 \sim \eta$ and $\chi_1 \sim \eta[z/x]$ with $z \notin \mathrm{Var}(\eta)$. The fact that $z \notin \mathrm{Var}(\eta)$ is a direct consequence of proposition (41) and $y \neq z$. So it remains to show that $\phi_1 \sim \eta$ and $\chi_1 \sim \eta[z/x]$. First we show

that $\phi_1 \sim \eta$. Since $\phi_1 \sim \theta$ and $\eta = \theta[y/z]$, from the symmetry and transitivity of the strong substitution congruence on $\mathbf{P}(V)$ it is sufficient to prove that $\theta[y/z] \sim \theta$, which itself follows from proposition (65) provided we show that $y \notin \mathrm{Var}(\theta)$ and $z \notin \mathrm{Fr}(\theta)$. We already know that $y \notin \mathrm{Var}(\theta)$, so it remains to prove that $z \notin \mathrm{Fr}(\theta)$. In order to do so, we shall first prove the implication:

$$z \in \mathrm{Fr}(\theta) \;\Rightarrow\; z \in \mathrm{Fr}(\theta[y/x]) \tag{2.18}$$

using proposition (45) and the assumption $y \notin \mathrm{Var}(\theta)$. In the case $x \notin \mathrm{Fr}(\theta)$, we obtain $\mathrm{Fr}(\theta[y/x]) = \mathrm{Fr}(\theta)$ and the implication (2.18) is clear. In the case when $x \in \mathrm{Fr}(\theta)$, we obtain $\mathrm{Fr}(\theta[y/x]) = \mathrm{Fr}(\theta) \setminus \{x\} \cup \{y\}$, and the implication (2.18) follows immediately from the fact that $z \neq x$. Having proved the implication (2.18), we can now show that $z \notin \mathrm{Fr}(\theta)$ by instead proving that $z \notin \mathrm{Fr}(\theta[y/x])$. Since $\psi_1 \sim \theta[y/x]$ and $\psi_1 \sim \theta^*$ it follows from the symmetry and transitivity of the strong substitution congruence on $\mathbf{P}(V)$ that $\theta[y/x] \sim \theta^*$. Thus, from proposition (62) we obtain $\mathrm{Fr}(\theta[y/x]) = \mathrm{Fr}(\theta^*)$, and it is therefore sufficient to prove that $z \notin \mathrm{Fr}(\theta^*)$, which follows immediately from $z \notin \mathrm{Var}(\theta^*)$ and $\mathrm{Fr}(\theta^*) \subseteq \mathrm{Var}(\theta^*)$, the latter being a consequence of proposition (48). This completes our proof of $\phi_1 \sim \eta$. It remains to show that $\chi_1 \sim \eta[z/x]$. Since $\chi_1 \sim \theta^*[z/y]$ and $\eta = \theta[y/z]$ we have to show:

$$\theta[y/z][z/x] \sim \theta^*[z/y] \tag{2.19}$$

We shall prove the equivalence (2.19) by proving the following two results:

$$\theta[y/z][z/x] \sim \theta[y/z][z/x][x/y] \tag{2.20}$$

$$\theta^*[z/y] \sim \theta[y/x][x/z][z/y] \tag{2.21}$$

Suppose for now that (2.20) and (2.21) have been proved. Comparing with the equivalence (2.19), it is sufficient to show that:

$$\theta[y/z][z/x][x/y] = \theta[y/x][x/z][z/y] \tag{2.22}$$

So we shall now prove equation (2.22). From proposition (36) it is sufficient to show that the maps $[x/y] \circ [z/x] \circ [y/z]$ and $[z/y] \circ [x/z] \circ [y/x]$ coincide on $\mathrm{Var}(\theta)$. So let $u \in \mathrm{Var}(\theta)$. In particular $u \neq y$ and we have to show that:

$$[x/y] \circ [z/x] \circ [y/z](u) = [z/y] \circ [x/z] \circ [y/x](u) \tag{2.23}$$

We shall distinguish three cases. First we assume that $u \notin \{x, y, z\}$. Then it is clear that the equality (2.23) holds. Next we assume that $u = x$:

$$[x/y] \circ [z/x] \circ [y/z](u) = [x/y] \circ [z/x](u) = [x/y](z) = z$$

and:

$$[z/y] \circ [x/z] \circ [y/x](u) = [z/y] \circ [x/z](y) = [z/y](y) = z$$

So the equality (2.23) holds. Finally we assume that $u = z$:

$$[x/y] \circ [z/x] \circ [y/z](u) = [x/y] \circ [z/x](y) = [x/y](y) = x$$

and:

$$[z/y] \circ [x/z] \circ [y/x](u) = [z/y] \circ [x/z](u) = [z/y](x) = x$$

So the equality (2.23) holds again. This completes our proof of (2.23) and (2.22). It remains to show that the equivalence (2.20) and (2.21) are true. First we show the equivalence (2.20). Using proposition (65), it is sufficient to show that we have both $x \notin \mathrm{Var}(\theta[y/z][z/x])$ and $y \notin \mathrm{Fr}(\theta[y/z][z/x])$. The fact that $x \notin \mathrm{Var}(\theta[y/z][z/x])$ is a consequence of proposition (41) and $x \neq z$. So we need to show that $y \notin \mathrm{Fr}(\theta[y/z][z/x])$. We shall do so by applying proposition (45) from which we obtain, provided we show $z \notin \mathrm{Var}(\theta[y/z])$:

$$\mathrm{Fr}(\theta[y/z][z/x]) = \begin{cases} \mathrm{Fr}(\theta[y/z]) \setminus \{x\} \cup \{z\} & \text{if} \quad x \in \mathrm{Fr}(\theta[y/z]) \\ \mathrm{Fr}(\theta[y/z]) & \text{if} \quad x \notin \mathrm{Fr}(\theta[y/z]) \end{cases} \tag{2.24}$$

However, before we can use equation (2.24) we need to check $z \notin \mathrm{Var}(\theta[y/z])$, which in fact immediately follows from proposition (41) and $y \neq z$. Having justified equation (2.24), it is now clear that in order to prove $y \notin \mathrm{Fr}(\theta[y/z][z/x])$, it is sufficient to prove that $y \notin \mathrm{Fr}(\theta[y/z])$. Since $y \notin \mathrm{Var}(\theta)$, we can apply proposition (45) once more, and having already shown $z \notin \mathrm{Fr}(\theta)$ while proving the equivalence $\phi_1 \sim \eta$, we obtain $\mathrm{Fr}(\theta[y/z]) = \mathrm{Fr}(\theta)$. Hence, it is sufficient to prove that $y \notin \mathrm{Fr}(\theta)$ which follows immediately from $y \notin \mathrm{Var}(\theta)$ and $\mathrm{Fr}(\theta) \subseteq \mathrm{Var}(\theta)$. This completes our proof of the equivalence (2.20). It remains to show that the equivalence (2.21) is true. Using proposition (64), it is sufficient to prove that $\theta^* \sim \theta[y/x][x/z]$ and $z \notin \mathrm{Var}(\theta^*) \cup \mathrm{Var}(\theta[y/x][x/z])$. We already know that $z \notin \mathrm{Var}(\theta^*)$, and $z \notin \mathrm{Var}(\theta[y/x][x/z])$ is an immediate consequence of proposition (41) and $x \neq z$. So we need to show that $\theta^* \sim \theta[y/x][x/z]$. From $\psi_1 \sim \theta[y/x]$ and $\psi_1 \sim \theta^*$ we obtain $\theta[y/x] \sim \theta^*$ and it is therefore sufficient to prove that $\theta[y/x] \sim \theta[y/x][x/z]$. Using proposition (65), it is sufficient to show that $x \notin \mathrm{Var}(\theta[y/x])$ and $z \notin \mathrm{Fr}(\theta[y/x])$. The fact that $x \notin \mathrm{Var}(\theta[y/x])$ is an immediate consequence of proposition (41) and $x \neq y$. So it remains to show that $z \notin \mathrm{Fr}(\theta[y/x])$, which in fact was already proved in the course of proving the equivalence $\phi_1 \sim \eta$. **.**

Having shown that $\simeq$ is a reflexive, symmetric and transitive relation on $\mathbf{P}(V)$, it remains to prove that it is also a congruent relation on $\mathbf{P}(V)$. However, this cannot be done before we show the implication $\phi \simeq \psi \ \Rightarrow \ \phi \sim \psi$.

Proposition 71 *Let $\simeq$ be the almost strong equivalence and $\sim$ be the strong substitution congruence on $\mathbf{P}(V)$, where V is a set. For all $\phi, \psi \in \mathbf{P}(V)$:*

$$\phi \simeq \psi \ \Rightarrow \ \phi \sim \psi$$

Proof
Let $\phi, \psi \in \mathbf{P}(V)$ such that $\phi \simeq \psi$. We need to show that $\phi \sim \psi$. We shall consider the five possible cases of definition (33) in relation to $\phi \simeq \psi$. Suppose first that $\phi = \psi \in \mathbf{P}_0(V)$. From the reflexivity of the strong substitution congruence, it is clear that $\phi \sim \psi$. Suppose next that $\phi = \psi = \bot$. Then we also have $\phi \sim \psi$. We now assume that $\phi = \phi_1 \to \phi_2$ and $\psi = \psi_1 \to \psi_2$

where $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$. The strong substitution congruence being a congruent relation on $\mathbf{P}(V)$, we obtain $\phi \sim \psi$. Next we assume that $\phi = \forall x \phi_1$ and $\psi = \forall x \psi_1$ where $\phi_1 \sim \psi_1$ and $x \in V$. Again, the strong substitution congruence being a congruent relation we obtain $\phi \sim \psi$. Finally we assume that $\phi = \forall x \phi_1$ and $\psi = \forall y \psi_1$ where $x \neq y$, and there exists $\theta \in \mathbf{P}(V)$ such that $\phi_1 \sim \theta$, $\psi_1 \sim \theta[y/x]$ and $y \notin \mathrm{Var}(\theta)$. Using once again the fact that the strong substitution congruence is a congruent relation, we see that $\phi \sim \forall x\, \theta$ and $\psi \sim \forall y\, \theta[y/x]$. By symmetry and transitivity of the strong substitution congruence, it is therefore sufficient to show that $\forall x\, \theta \sim \forall y\, \theta[y/x]$ which follows immediately from $x \neq y$, $y \notin \mathrm{Var}(\theta)$ and definition (32). **.**

We are now in a position to show that $\simeq$ is a congruent relation, which is the last part missing before we can conclude that $\simeq$ is a congruence on $\mathbf{P}(V)$.

Proposition 72 *Let $\simeq$ be the almost strong equivalence relation on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ is a congruent relation on $\mathbf{P}(V)$.*

Proof
From proposition (68), the almost strong equivalence $\simeq$ is reflexive and so $\bot \simeq \bot$. We now assume that $\phi = \phi_1 \to \phi_2$ and $\psi = \psi_1 \to \psi_2$ where $\phi_1 \simeq \psi_1$ and $\phi_2 \simeq \psi_2$. We need to show that $\phi \simeq \psi$. However from proposition (71) we have $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$ and it follows from definition (33) that $\phi \simeq \psi$. We now assume that $\phi = \forall x \phi_1$ and $\psi = \forall x \psi_1$ where $\phi_1 \simeq \psi_1$ and $x \in V$. We need to show that $\phi \simeq \psi$. Once again from proposition (71) we have $\phi_1 \sim \psi_1$ and consequently from definition (33) we obtain $\phi \simeq \psi$. **.**

Proposition 73 *Let $\simeq$ be the almost strong equivalence relation on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ is a congruence on $\mathbf{P}(V)$.*

Proof
We need to show that $\simeq$ is reflexive, symmetric, transitive and that it is a congruent relation on $\mathbf{P}(V)$. From proposition (68), the relation $\simeq$ is reflexive. From proposition (69) it is symmetric while from proposition (70) it is transitive. Finally from proposition (72) the relation $\simeq$ is a congruent relation. **.**

So $\simeq$ is a congruence on $\mathbf{P}(V)$ such that $R_0 \subseteq \simeq$. We conclude this section with the equivalence $\phi \sim \psi \;\Leftrightarrow\; \phi \simeq \psi$ and summarize with theorem (11) below.

Proposition 74 *Let $\simeq$ be the almost strong equivalence and $\sim$ be the strong substitution congruence on $\mathbf{P}(V)$, where V is a set. For all $\phi, \psi \in \mathbf{P}(V)$:*

$$\phi \simeq \psi \;\Leftrightarrow\; \phi \sim \psi$$

Proof
From proposition (71) it is sufficient to show the implication $\Leftarrow$ or equivalently the inclusion $\sim \subseteq \simeq$. Since $\sim$ is the strong substitution congruence on $\mathbf{P}(V)$, it is the smallest congruence on $\mathbf{P}(V)$ which contains the set R_0 of definition (32). In order to show the inclusion $\sim \subseteq \simeq$ it is therefore sufficient to show that $\simeq$ is a congruence on $\mathbf{P}(V)$ such that $R_0 \subseteq \simeq$. The fact that it is a congruence stems from proposition (73). The fact that $R_0 \subseteq \simeq$ follows from proposition (67). **.**

We are now ready to provide a characterization of the strong substitution congruence. It should be noted that (v) of theorem (11) below is a notational shortcut for the more detailed statement $\phi = \forall x \phi_1$, $\psi = \forall y \psi_1$, $x \neq y$ and *there exists a formula* $\theta \in \mathbf{P}(V)$ such that $\phi_1 \sim \theta$, $\psi_1 \sim \theta[y/x]$, $y \notin \mathrm{Var}(\theta)$.

Theorem 11 *Let $\sim$ be the strong substitution congruence on $\mathbf{P}(V)$ where V is a set. For all $\phi, \psi \in \mathbf{P}(V)$, $\phi \sim \psi$ if and only if one of the following is the case:*

(i) $\phi \in \mathbf{P}_0(V)$, $\psi \in \mathbf{P}_0(V)$, *and* $\phi = \psi$

(ii) $\phi = \bot$ *and* $\psi = \bot$

(iii) $\phi = \phi_1 \to \phi_2$, $\psi = \psi_1 \to \psi_2$, $\phi_1 \sim \psi_1$ *and* $\phi_2 \sim \psi_2$

(iv) $\phi = \forall x \phi_1$, $\psi = \forall x \psi_1$ *and* $\phi_1 \sim \psi_1$

(v) $\phi = \forall x \phi_1$, $\psi = \forall y \psi_1$, $x \neq y$, $\phi_1 \sim \theta$, $\psi_1 \sim \theta[y/x]$, $y \notin \mathrm{Var}(\theta)$

Proof
Immediately follows from proposition (74) and definition (33). **.**

2.2.6 Counterexamples of the Strong Congruence

A fair amount of work has been devoted to the study of the strong substitution congruence, culminating with its characterization in the form of theorem (11). Unfortunately, most of this work was done vain. As we shall now discover, the strong substitution congruence is not the appropriate notion to study. It may give us insight and will certainly help us in the forthcoming developments, it may be commonly referred to in the literature, but it is marred by a major flaw. The problem is as follows: when $V = \{x, y\}$ with $x \neq y$, i.e. when V has only two elements, the formulas $\phi = \forall x \forall y (x \in y)$ and $\psi = \forall y \forall x (y \in x)$ are not equivalent. This is highly disappointing. If there is one thing we would expect of a *substitution congruence*, it is certainly to be such that ϕ and ψ be equivalent. This leaves us with a painful alternative: we either give up on the possibility of finite sets of variables V, or we abandon the notion of strong substitution congruence and all the work that has gone along with it. As already hinted, we are not prepared to accept that nothing interesting can be said with finite sets V. There must be an appropriate notion of *substitution congruence* to be defined on $\mathbf{P}(V)$, and we shall therefore continue our search for it. But before we resume our quest, we shall first prove that the problem truly exists:

Proposition 75 *Let $\sim$ be the strong substitution congruence on $\mathbf{P}(V)$ where $V = \{x, y\}$ and $x \neq y$. Then, we have:*

$$\forall x \forall y \, (x \in y) \not\sim \forall y \forall x \, (y \in x)$$

Proof
Define $\phi_1 = \forall y (x \in y)$ and $\psi_1 = \forall x (y \in x)$. We need to show that $\forall x \phi_1 \not\sim \forall y \psi_1$. Suppose to the contrary that $\forall x \phi_1 \sim \forall y \psi_1$. We shall derive a contradiction. Since $x \neq y$, from theorem (11) of page 120 there exists $\theta \in \mathbf{P}(V)$ such that

$\phi_1 \sim \theta$, $\psi_1 \sim \theta[y/x]$ and $y \notin \mathrm{Var}(\theta)$. From $\phi_1 \sim \theta$ we see that $\forall y(x \in y) \sim \theta$, and applying theorem (11) once more, since $V = \{x, y\}$ we see that θ must be of the form $\theta = \forall x\theta_1$ or $\theta = \forall y\theta_1$. However the case $\theta = \forall y\theta_1$ is impossible since $y \notin \mathrm{Var}(\theta)$. Suppose now that $\theta = \forall x\theta_1$ for some $\theta_1 \in \mathbf{P}(V)$. Then $x \notin \mathrm{Fr}(\theta) = \mathrm{Fr}(\theta_1) \setminus \{x\}$. However we have $\forall y(x \in y) \sim \theta$ from proposition (62) we have $\{x\} = \mathrm{Fr}(\,\forall y(x \in y)\,) = \mathrm{Fr}(\theta)$. This is our desired contradiction. .

As we have just seen, the strong substitution congruence is inadequate when V has two elements. In fact, it is also inadequate when V has three elements as the following proposition shows. We do not intend to spend too much time proving negative results, but we certainly believe the strong substitution congruence on $\mathbf{P}(V)$ will fail whenever V is a finite set.

Proposition 76 *Let $\sim$ be the strong substitution congruence on $\mathbf{P}(V)$ where $V = \{x, y, z\}$ and $x \neq y$, $y \neq z$ and $x \neq z$. Then, we have:*

$$\forall x\forall y\forall z\,[(x \in y) \to (y \in z)] \not\sim \forall y\forall z\forall x\,[(y \in z) \to (z \in x)]$$

Proof
Define $\phi_1 = \forall y\forall z\,[(x \in y) \to (y \in z)]$ and $\psi_1 = \forall z\forall x\,[(y \in z) \to (z \in x)]$. We need to show that $\forall x\phi_1 \not\sim \forall y\psi_1$. Suppose to the contrary that $\forall x\phi_1 \sim \forall y\psi_1$. We shall derive a contradiction. Since $x \neq y$, from theorem (11) of page 120 there exists $\theta \in \mathbf{P}(V)$ such that $\phi_1 \sim \theta$, $\psi_1 \sim \theta[y/x]$ and $y \notin \mathrm{Var}(\theta)$. From $\phi_1 \sim \theta$ we see that $\forall y\forall z\,[(x \in y) \to (y \in z)] \sim \theta$, and applying theorem (11) once more, since $V = \{x, y, z\}$ we see that θ must be of the form $\theta = \forall x\,\theta_1$, $\theta = \forall y\,\theta_1$ or $\theta = \forall z\,\theta_1$. However the case $\theta = \forall y\,\theta_1$ is impossible since $y \notin \mathrm{Var}(\theta)$. Furthermore, the case $\theta = \forall x\,\theta_1$ is also impossible since this would imply that $x \notin \mathrm{Fr}(\theta)$, while from $\forall y\forall z\,[(x \in y) \to (y \in z)] \sim \theta$ and proposition (62):

$$\{x\} = \mathrm{Fr}(\,\forall y\forall z\,[(x \in y) \to (y \in z)]\,) = \mathrm{Fr}(\theta)$$

It follows that $\theta = \forall z\,\theta_1$ for some $\theta_1 \in \mathbf{P}(V)$. Hence we see that:

$$\forall y\forall z\,[(x \in y) \to (y \in z)] \sim \forall z\,\theta_1$$

Applying theorem (11) once more, there exists $\eta \in \mathbf{P}(V)$ such that we have $\forall z\,[(x \in y) \to (y \in z)] \sim \eta$, $\theta_1 \sim \eta[z/y]$ and $z \notin \mathrm{Var}(\eta)$. From the strong equivalence $\forall z\,[(x \in y) \to (y \in z)] \sim \eta$ and yet another application of theorem (11), since $V = \{x, y, z\}$ we see that η must be of the form $\eta = \forall x\,\eta_1$, $\eta = \forall y\,\eta_1$ or $\eta = \forall z\,\eta_1$. However, the case $\eta = \forall z\,\eta_1$ is impossible since $z \notin \mathrm{Var}(\eta)$. Suppose now that $\eta = \forall x\,\eta_1$. Then $x \notin \mathrm{Fr}(\eta)$, contradicting the equality:

$$\{x, y\} = \mathrm{Fr}(\,\forall z\,[(x \in y) \to (y \in z)]\,) = \mathrm{Fr}(\eta)$$

obtained from $\forall z\,[(x \in y) \to (y \in z)] \sim \eta$ and proposition (62). Since $y \in \mathrm{Fr}(\eta)$ we conclude similarly that $\eta = \forall y\,\eta_1$ is equally impossible. .

2.2.7 The Substitution Congruence

Prior to defining the strong substitution congruence in page 107, we discussed what we believed were the requirements a *substitution congruence* ought to meet. Unfortunately, despite our best efforts, we failed to define the right notion. So we are back to our starting point, enquiring about the appropriate definition of a *substitution congruence*. In proposition (65) we showed that given a formula ϕ, we have the equivalence $\phi[y/x] \sim \phi$ provided $y \notin \text{Var}(\phi)$ and $x \notin \text{Fr}(\phi)$. The key idea underlying this proposition is that some substitution should not affect the *meaning* of a formula. This may give us a new angle of attack. In this section, we define those substitutions σ which we believe should have this invariance property of not altering the equivalence class of a given formula ϕ, i.e. such that $\sigma(\phi) \sim \phi$. We shall then define a new substitution congruence.

In proposition (65) we required that $x \notin \text{Fr}(\phi)$. This condition ensures the substitution $[y/x]$ does not affect free variables of the formula ϕ. There is clearly a good reason for this. A substitution congruence is all about potentially differing quantification variables. We cannot expect to have $\sigma(\phi) \sim \phi$ unless the free variables of ϕ are invariant under the substitution σ. Furthermore, proposition (65) also required $y \notin \text{Var}(\phi)$. This condition guarantees the substitution $[y/x]$ is valid for ϕ. This motivates the following definition:

Definition 35 *Let V be a set and $\sigma : V \to V$ be a map. Let $\phi \in \mathbf{P}(V)$. We say that σ is an* admissible substitution for ϕ *if and only if it satisfies:*

$$\begin{array}{ll} (i) & \sigma \text{ valid for } \phi \\ (ii) & \forall u \in \text{Fr}(\phi)\ ,\ \sigma(u) = u \end{array}$$

Having defined admissible substitutions with respect to a formula ϕ, our belief is that an appropriate *substitution congruence* $\sim$ should be such that $\sigma(\phi) \sim \phi$ whenever σ is admissible for ϕ. If we consider $\phi = \forall x \forall y (x \in y)$ and the permutation $\sigma = [y{:}x]$ for $x \neq y$, then σ is clearly admissible for ϕ. Yet we know from proposition (75) that the equivalence $\sigma(\phi) \sim \phi$ fails when $V = \{x, y\}$ and $\sim$ is the strong substitution congruence on $\mathbf{P}(V)$. To remedy this failure, we may conjecture that an appropriate definition of a *substitution congruence* should be made in reference to ordered pairs $(\phi, \sigma(\phi))$ where σ is admissible for ϕ. In other words, if we define:

$$R_1 = \{\, (\, \phi\, ,\, \sigma(\phi)\,) : \phi \in \mathbf{P}(V)\ ,\ \sigma : V \to V \text{ admissible for } \phi\}$$

the *right* substitution congruence should simply be defined as the congruence on $\mathbf{P}(V)$ generated by R_1. As it turns out, we shall adopt a different but equivalent definition of the substitution congruence, in terms of a generator R_0 which is a lot smaller than R_1. In effect, rather than considering all possible ordered pair $(\phi, \sigma(\phi))$ where σ is admissible for ϕ, we restrict our attention to the case when $\phi = \forall x \phi_1$ and $\sigma = [y{:}x]$ for $x \neq y$ and $y \notin \text{Fr}(\phi_1)$, thereby obtaining a definition of the substitution congruence which is formally very similar to definition (32) of the strong substitution congruence.

Definition 36 *Let V be a set. We call* substitution congruence on $\mathbf{P}(V)$ *the congruence on $\mathbf{P}(V)$ generated by the following set $R_0 \subseteq \mathbf{P}(V) \times \mathbf{P}(V)$:*

$$R_0 = \{\, (\, \forall x \phi_1 \,,\, \forall y \, \phi_1[y{:}x] \,) : \phi_1 \in \mathbf{P}(V) \;,\; x, y \in V \;,\; x \neq y \;,\; y \notin \mathrm{Fr}(\phi_1) \,\}$$

where $[y{:}x]$ denotes the permutation of x and y as per definition (27)*.*

We have now defined what we hope will be a definitive notion of *substitution congruence*. However, the definition (35) we chose does not make reference to ordered pairs $(\phi, \sigma(\phi))$ where σ is an admissible substitution for ϕ. One of our first task is to make sure definition (35) is equivalent to having defined the substitution congruence as generated by these ordered pairs. We start by showing that $\phi \sim \sigma(\phi)$ whenever σ is admissible for ϕ.

Proposition 77 *Let $\sim$ be the substitution congruence on $\mathbf{P}(V)$ where V is a set. Let $\phi \in \mathbf{P}(V)$ and $\sigma : V \to V$ be an admissible substitution for ϕ. Then:*

$$\phi \sim \sigma(\phi)$$

Proof
We need to show the property $\forall \sigma [\, (\sigma \text{ admissible for } \phi) \;\Rightarrow\; \phi \sim \sigma(\phi) \,]$ for all $\phi \in \mathbf{P}(V)$. We shall do so by structural induction, using theorem (3) of page 31. Since $\mathbf{P}_0(V)$ is a generator of $\mathbf{P}(V)$, we shall first show that the property is true on $\mathbf{P}_0(V)$. So let $\phi = (x \in y) \in \mathbf{P}_0(V)$ where $x, y \in V$. We assume that $\sigma : V \to V$ is an admissible substitution for ϕ. We need to show that $\phi \sim \sigma(\phi)$. However since $\mathrm{Fr}(\phi) = \{x, y\}$ and σ is an admissible substitution for ϕ, we have $\sigma(x) = x$ and $\sigma(y) = y$ and consequently:

$$\sigma(\phi) = \sigma(x \in y) = (\, \sigma(x) \in \sigma(y) \,) = (x \in y) = \phi$$

and in particular we see that $\phi \sim \sigma(\phi)$. We now check that the property is true for $\phi = \bot$. Note that any map $\sigma : V \to V$ is an admissible substitution for $\bot$. Since we always have $\bot = \sigma(\bot)$, it follows that $\bot \sim \sigma(\bot)$. We now check that the property is true for $\phi = \phi_1 \to \phi_2$ if it is true for $\phi_1, \phi_2 \in \mathbf{P}(V)$. So we assume that $\sigma : V \to V$ is an admissible substitution for ϕ. We need to show that $\phi \sim \sigma(\phi)$. Since $\phi = \phi_1 \to \phi_2$ and $\sigma(\phi) = \sigma(\phi_1) \to \sigma(\phi_2)$, the substitution congruence being a congruent relation on $\mathbf{P}(V)$, it is sufficient to show that $\phi_1 \sim \sigma(\phi_1)$ and $\phi_2 \sim \sigma(\phi_2)$. First we show that $\phi_1 \sim \sigma(\phi_1)$. Having assumed the property is true for ϕ_1, it is sufficient to show that σ is an admissible substitution for ϕ_1. Since σ admissible for ϕ, in particular it is valid for ϕ and it follows from proposition (54) that it is also valid for ϕ_1. So it remains to show that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\phi_1)$ which follows immediately from $\mathrm{Fr}(\phi) = \mathrm{Fr}(\phi_1) \cup \mathrm{Fr}(\phi_2)$ and the fact that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\phi)$. So we have proved that $\phi_1 \sim \sigma(\phi_1)$ and we show similarly that $\phi_2 \sim \sigma(\phi_2)$. We now need to check that the property is true for $\phi = \forall x \phi_1$ if it is true for $\phi_1 \in \mathbf{P}(V)$. So we assume that $\sigma : V \to V$ is an admissible substitution for ϕ. We need to show that $\phi \sim \sigma(\phi)$. We shall distinguish two cases: first we assume that $\sigma(x) = x$. Then $\sigma(\phi) = \forall x \, \sigma(\phi_1)$ and in order to show $\phi \sim \sigma(\phi)$, the

substitution congruence being a congruent relation on $\mathbf{P}(V)$, it is sufficient to show that $\phi_1 \sim \sigma(\phi_1)$. Having assumed the property is true for ϕ_1, it is therefore sufficient to prove that σ is an admissible substitution for ϕ_1. Since σ admissible for ϕ, in particular it is valid for ϕ and it follows from proposition (55) that it is also valid for ϕ_1. So it remains to show that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\phi_1)$. We shall distinguish two further cases: first we assume that $u = x$. Then $\sigma(u) = u$ is true from our assumption $\sigma(x) = x$. So we assume that $u \neq x$. It follows that $u \in \mathrm{Fr}(\phi_1) \setminus \{x\} = \mathrm{Fr}(\phi)$, and since σ is admissible for ϕ, we conclude that $\sigma(u) = u$. This completes our proof of $\phi \sim \sigma(\phi)$ in the case when $\sigma(x) = x$. We now assume that $\sigma(x) \neq x$. Let $y = \sigma(x)$. Then $\sigma(\phi) = \forall y\, \sigma(\phi_1)$ and we need to show that $\forall x \phi_1 \sim \forall y\, \sigma(\phi_1)$. However, since $[y : x] \circ [y : x]$ is the identity mapping we have $\sigma = [y{:}x] \circ \sigma^*$ where the map $\sigma^* : V \to V$ is defined as $\sigma^* = [y : x] \circ \sigma$. It follows that $\sigma(\phi_1) = \sigma^*(\phi_1)[y : x]$ and we need to show that $\forall x \phi_1 \sim \forall y \sigma^*(\phi_1)[y : x]$. Let us accept for now that $y \notin \mathrm{Fr}(\sigma^*(\phi_1))$. Then from definition (35) we obtain $\forall x \sigma^*(\phi_1) \sim \forall y \sigma^*(\phi_1)[y : x]$, and it is therefore sufficient to prove that $\forall x \phi_1 \sim \forall x \sigma^*(\phi_1)$. So we see that it is sufficient to prove $\phi_1 \sim \sigma^*(\phi_1)$ provided we can justify the fact that $y \notin \mathrm{Fr}(\sigma^*(\phi_1))$. First we show that $\phi_1 \sim \sigma^*(\phi_1)$. Having assumed our property is true for ϕ_1 it is sufficient to prove that σ^* is admissible for ϕ_1. However, we have already seen that σ is valid for ϕ_1. Furthermore, since $[y{:}x]$ is an injective map, from proposition (53) it is a valid substitution for $\sigma(\phi_1)$. It follows from proposition (58) that $\sigma^* = [y{:}x] \circ \sigma$ is valid for ϕ_1. So in order to prove that σ^* is admissible for ϕ_1, it remains to show that $\sigma^*(u) = u$ for all $u \in \mathrm{Fr}(\phi_1)$. So let $u \in \mathrm{Fr}(\phi_1)$. We shall distinguish two cases: first we assume that $u = x$. Then $\sigma^*(u) = [y : x](\sigma(x)) = [y : x](y) = x = u$. Next we assume that $u \neq x$. Then u is in fact an element of $\mathrm{Fr}(\phi)$. Having assumed σ is admissible for ϕ we obtain $\sigma(u) = u$. We also obtain the fact that σ is valid for $\phi = \forall x \phi_1$ and consequently $\sigma(u) \neq \sigma(x)$, i.e. $u \neq y$. Thus $\sigma^*(u) = [y : x](\sigma(u)) = [y : x](u) = u$. This completes our proof that σ^* is admissible for ϕ_1 and $\phi_1 \sim \sigma^*(\phi_1)$. It remains to show that $y \notin \mathrm{Fr}(\sigma^*(\phi_1))$. So suppose to the contrary that $y \in \mathrm{Fr}(\sigma^*(\phi_1))$. We shall obtain a contradiction. Using proposition (43) there exists $u \in \mathrm{Fr}(\phi_1)$ such that $y = \sigma^*(u)$. Having proven that σ^* is admissible for ϕ_1 we have $\sigma^*(u) = u$ and consequently $y = u \in \mathrm{Fr}(\phi_1)$. From the assumption $y = \sigma(x) \neq x$ we in fact have $y \in \mathrm{Fr}(\phi)$. So from the admissibility of σ for ϕ we obtain $\sigma(y) = y$ and furthermore from the validity of σ for $\phi = \forall x \phi_1$ we obtain $\sigma(y) \neq \sigma(x)$. So we conclude that $y \neq \sigma(x)$ which contradicts our very definition of y. **.**

We are now in a position to check that the substitution congruence is also generated by the set of ordered pairs $(\phi, \sigma(\phi))$ where σ is admissible for ϕ.

Proposition 78 *Let V be a set. Then the substitution congruence on $\mathbf{P}(V)$ is also generated by the following set $R_1 \subseteq \mathbf{P}(V) \times \mathbf{P}(V)$:*

$$R_1 = \{\, (\, \phi\, ,\, \sigma(\phi)\,) : \phi \in \mathbf{P}(V)\ ,\ \sigma : V \to V \ \textit{admissible for}\ \phi\}$$

Proof
Let $\sim$ denote the substitution congruence on $\mathbf{P}(V)$ and $\equiv$ be the congruence on $\mathbf{P}(V)$ generated by R_1. We need to show that $\sim = \equiv$. First we show that

$\sim \subseteq \equiv$. Since $\sim$ is the smallest congruence on $\mathbf{P}(V)$ which contains the set R_0 of definition (35), in order to prove $\sim \subseteq \equiv$ it is sufficient to prove that $R_0 \subseteq \equiv$. So let $\phi_1 \in \mathbf{P}(V)$ and $x, y \in V$ be such that $x \neq y$ and $y \notin \mathrm{Fr}(\phi_1)$. Define $\phi = \forall x \phi_1$ and $\psi = \forall y\, \phi_1[y:x]$. We need to show that $\phi \equiv \psi$. The congruence $\equiv$ being generated by R_1 it is sufficient to prove that $(\phi, \psi) \in R_1$. However, if we define $\sigma : V \to V$ by setting $\sigma = [y:x]$ we have:

$$\psi = \forall y\, \phi_1[y:x] = \forall \sigma(x)\, \sigma(\phi_1) = \sigma(\forall x \phi_1) = \sigma(\phi)$$

Hence, in order to show $(\phi, \psi) \in R_1$, it is sufficient to prove that σ is an admissible substitution for ϕ. Being injective, it is clear from proposition (53) that σ is valid for ϕ. So we need to prove that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\phi)$. So let $u \in \mathrm{Fr}(\phi)$. It is sufficient to prove that $u \notin \{x, y\}$. The fact that $u \neq x$ is clear from $u \in \mathrm{Fr}(\phi) = \mathrm{Fr}(\phi_1) \setminus \{x\}$. The fact that $u \neq y$ follows from $u \in \mathrm{Fr}(\phi) \subseteq \mathrm{Fr}(\phi_1)$ and the assumption $y \notin \mathrm{Fr}(\phi_1)$. We now show that $\equiv \subseteq \sim$. Since $\equiv$ is the smallest congruence on $\mathbf{P}(V)$ which contains the set R_1, it is sufficient to show that $R_1 \subseteq \sim$. So let $\phi \in \mathbf{P}(V)$ and $\sigma : V \to V$ be an admissible substitution for ϕ. We need to show that $\phi \sim \sigma(\phi)$. But this follows immediately from proposition (77). **.**

2.2.8 Free Variable and Substitution Congruence

A lot of the work which was done for the strong substitution congruence needs to be done all over again for the substitution congruence. We start by showing that equivalent formulas have the same free variables. The following proposition is the counterpart of proposition (62) of the strong substitution congruence.

Proposition 79 *Let $\sim$ denote the substitution congruence on $\mathbf{P}(V)$ where V is a set. Then for all $\phi, \psi \in \mathbf{P}(V)$ we have the implication:*

$$\phi \sim \psi \;\Rightarrow\; \mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$$

Proof
Let $\equiv$ be the relation on $\mathbf{P}(V)$ defined by $\phi \equiv \psi \;\Leftrightarrow\; \mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$. We need to show that $\phi \sim \psi \;\Rightarrow\; \phi \equiv \psi$ or equivalently that the inclusion $\sim \subseteq \equiv$ holds. Since $\sim$ is the substitution congruence on $\mathbf{P}(V)$, it is the smallest congruence on $\mathbf{P}(V)$ which contains the set R_1 of proposition (78). In order to show the inclusion $\sim \subseteq \equiv$ it is therefore sufficient to show that $\equiv$ is a congruence on $\mathbf{P}(V)$ such that $R_1 \subseteq \equiv$. However, we already know from proposition (46) that $\equiv$ is a congruence on $\mathbf{P}(V)$. So it remains to show that $R_1 \subseteq \equiv$. So let $\phi \in \mathbf{P}(V)$ and $\sigma : V \to V$ be an admissible substitution for ϕ. We need to show that $\phi \equiv \sigma(\phi)$ or equivalently that $\mathrm{Fr}(\phi) = \mathrm{Fr}(\sigma(\phi))$. However, since σ is valid for ϕ, from proposition (52) we have $\mathrm{Fr}(\sigma(\phi)) = \sigma(\mathrm{Fr}(\phi))$ so we need to show that $\mathrm{Fr}(\phi) = \sigma(\mathrm{Fr}(\phi))$ which follows from the fact that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\phi)$. **.**

Proposition 80 *Let $\sim$ denote the substitution congruence on $\mathbf{P}(V)$ where V is a set. Then for all $\phi_1 \in \mathbf{P}(V)$ and $x, y \in V$ such that $x, y \notin \mathrm{Fr}(\phi_1)$ we have:*

$$\forall x \phi_1 \sim \forall y \phi_1$$

Proof
From $y \notin \mathrm{Fr}(\phi_1)$ and definition (35) we see that $\forall x\phi_1 \sim \forall y\phi_1[y:x]$. So we need to show that $\forall y\phi_1[y:x] \sim \forall y\phi_1$. Hence it is sufficient to prove that $\phi_1[y:x] \sim \phi_1$. Using proposition (77), we simply need to argue that $[y:x]$ is an admissible substitution for ϕ_1. Being injective, from proposition (53) it is a valid substitution for ϕ_1. So it remains to show that $[y:x](u) = u$ for all $u \in \mathrm{Fr}(\phi_1)$ which follows immediately from $x, y \notin \mathrm{Fr}(\phi_1)$. .

2.2.9 Substitution and Substitution Congruence

We now show that equivalence between formulas is invariant under injective substitution. The following proposition is the counterpart of proposition (63) of the strong substitution congruence.

Proposition 81 *Let V and W be sets and $\sigma : V \to W$ be an injective map. Let $\sim$ be the substitution congruence both on $\mathbf{P}(V)$ and $\mathbf{P}(W)$. Then:*

$$\phi \sim \psi \;\Rightarrow\; \sigma(\phi) \sim \sigma(\psi)$$

for all $\phi, \psi \in \mathbf{P}(V)$, where $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is also the substitution mapping.

Proof
Let $\equiv$ be the relation on $\mathbf{P}(V)$ defined by $\phi \equiv \psi \;\Leftrightarrow\; \sigma(\phi) \sim \sigma(\psi)$. We need to show that $\phi \sim \psi \;\Rightarrow\; \phi \equiv \psi$ or equivalently that the inclusion $\sim \subseteq \equiv$ holds. Since $\sim$ is the substitution congruence on $\mathbf{P}(V)$, it is the smallest congruence on $\mathbf{P}(V)$ which contains the set R_0 of definition (35). In order to show the inclusion $\sim \subseteq \equiv$ it is therefore sufficient to show that $\equiv$ is a congruence on $\mathbf{P}(V)$ such that $R_0 \subseteq \equiv$. However, we already know from proposition (31) that $\equiv$ is a congruence on $\mathbf{P}(V)$. So it remains to show that $R_0 \subseteq \equiv$. So let $\phi_1 \in \mathbf{P}(V)$ and $x, y \in V$ be such that $x \neq y$ and $y \notin \mathrm{Fr}(\phi_1)$. Define $\phi = \forall x\phi_1$ and $\psi = \forall y\, \phi_1[y:x]$. We need to show that $\phi \equiv \psi$ or equivalently that $\sigma(\phi) \sim \sigma(\psi)$. In order to do so, it is sufficient to show that the ordered pair $(\sigma(\phi), \sigma(\psi))$ belongs to the generator R_0' of the substitution congruence on $\mathbf{P}(W)$ as per definition (35). In other words, it is sufficient to show the existence of $\phi_1' \in \mathbf{P}(W)$ and $x', y' \in W$ with $x' \neq y'$ and $y' \notin \mathrm{Fr}(\phi_1')$, such that $\sigma(\phi) = \forall x'\phi_1'$ and $\sigma(\psi) = \forall y'\, \phi_1'[y':x']$. Take $\phi_1' = \sigma(\phi_1) \in \mathbf{P}(W)$ together with $x' = \sigma(x) \in W$ and $y' = \sigma(y) \in W$. Then:

$$\sigma(\phi) = \sigma(\forall x\phi_1) = \forall\sigma(x)\, \sigma(\phi_1) = \forall x'\phi_1'$$

Furthermore, from proposition (37) we have $\sigma \circ [y:x] = [\sigma(y):\sigma(x)] \circ \sigma$ and so:

$$\begin{aligned}
\sigma(\psi) &= \sigma(\forall y\, \phi_1[y:x]) \\
&= \forall\sigma(y)\, \sigma(\phi_1[y:x]) \\
&= \forall y'\, \sigma([y:x](\phi_1)) \\
&= \forall y'\, \sigma \circ [y:x]\,(\phi_1) \\
&= \forall y'\, [\sigma(y):\sigma(x)] \circ \sigma\,(\phi_1) \\
&= \forall y'\, [y':x'](\phi_1') \\
&= \forall y'\, \phi_1'[y':x']
\end{aligned}$$

So it remains to show that $x' \neq y'$ and $y' \notin \mathrm{Fr}(\phi_1')$. Since $\sigma : V \to W$ is an injective map, $x' \neq y'$ follows immediately from $x \neq y$. We now show that $y' \notin \mathrm{Fr}(\phi_1')$. So suppose to the contrary that $y' \in \mathrm{Fr}(\phi_1')$. We shall arrive at a contradiction. Since $\phi_1' = \sigma(\phi_1)$, from proposition (44) we have:

$$\mathrm{Fr}(\phi_1') = \{\sigma(u) : u \in \mathrm{Fr}(\phi_1)\}$$

It follows that there exists $u \in \mathrm{Fr}(\phi_1)$ such that $y' = \sigma(u)$. However, $y' = \sigma(y)$ and $\sigma : V \to W$ is an injective map. Hence we see that $u = y$ and consequently $y \in \mathrm{Fr}(\phi_1)$ which contradicts our initial assumption of $y \notin \mathrm{Fr}(\phi_1)$. .

2.2.10 Characterization of the Substitution Congruence

Just like the strong substitution congruence, the substitution congruence was defined in terms of a generator. This makes it convenient to prove an equivalence $\phi \sim \psi$, but inconvenient when it comes to proving this equivalence does not hold. We shall therefore follow a similar strategy to that leading up to theorem (11) of page 120. We refer the reader to the discussion preceding definition (33). We shall define a new relation $\simeq$ on $\mathbf{P}(V)$ and prove that $\phi \sim \psi \;\Leftrightarrow\; \phi \simeq \psi$. The point of the relation $\simeq$ is to give us more insight about the formulas ϕ and ψ whenever we have $\phi \sim \psi$. Most of the hard work consists in proving that $\simeq$ is a transitive relation. However, this will be a lot simpler than in the case of the strong substitution congruence. In fact comparing definition (36) below to its counterpart definition (33), we see that these definitions are formally identical with a difference occurring solely in (v). For the strong substitution congruence:

$$(v) \qquad \phi = \forall x \phi_1 \ , \ \psi = \forall y \psi_1 \ , \ x \neq y \ , \ \phi_1 \sim \theta \ , \ \psi_1 \sim \theta[y/x] \ , \ y \notin \mathrm{Var}(\theta)$$

while for the substitution congruence we have:

$$(v) \qquad \phi = \forall x \phi_1 \ , \ \psi = \forall y \psi_1 \ , \ x \neq y \ , \ \psi_1 \sim \phi_1[y{:}x] \ , \ y \notin \mathrm{Fr}(\phi_1)$$

This is the beauty of the substitution congruence. Not only does it work equally well for V finite and V infinite or so we believe, but it is also a lot simpler in many respects. It involves the injective permutation $[y : x]$ rather than the non-injective substitution $[y/x]$. It makes no reference to the existence of a third formula θ in the case of (v) but directly gives us $\psi_1 \sim \phi_1[y : x]$ instead. The proofs in the case of the substitution congruence are simpler than their counterparts of the strong substitution congruence.

Definition 37 *Let $\sim$ be the substitution congruence on $\mathbf{P}(V)$ where V is a set. Let $\phi, \psi \in \mathbf{P}(V)$. We say that ϕ is* almost equivalent to *ψ and we write $\phi \simeq \psi$, if and only if one of the following is the case:*

$$(i) \qquad \phi \in \mathbf{P}_0(V) \ , \ \psi \in \mathbf{P}_0(V) \ , \ \textit{and } \phi = \psi$$

$$(ii) \qquad \phi = \bot \textit{ and } \psi = \bot$$

$$(iii) \qquad \phi = \phi_1 \to \phi_2 \ , \ \psi = \psi_1 \to \psi_2 \ , \ \phi_1 \sim \psi_1 \textit{ and } \phi_2 \sim \psi_2$$

$$(iv) \qquad \phi = \forall x \phi_1 \ , \ \psi = \forall x \psi_1 \textit{ and } \phi_1 \sim \psi_1$$

$$(v) \qquad \phi = \forall x \phi_1 \ , \ \psi = \forall y \psi_1 \ , \ x \neq y \ , \ \psi_1 \sim \phi_1[y{:}x] \ , \ y \notin \mathrm{Fr}(\phi_1)$$

Proposition 82 $(i), (ii), (iii), (iv), (v)$ *of* def. (36) *are mutually exclusive.*

Proof
This is an immediate consequence of theorem (2) of page 21 applied to the free universal algebra $\mathbf{P}(V)$ with free generator $\mathbf{P}_0(V)$, where a formula $\phi \in \mathbf{P}(V)$ is either an element of $\mathbf{P}_0(V)$, or the contradiction constant $\phi = \bot$, or an implication $\phi = \phi_1 \to \phi_2$, or a quantification $\phi = \forall x \phi_1$, but cannot be equal to any two of those things simultaneously. Since (v) can only occur with $x \neq y$, it also follows from theorem (2) that (v) cannot occur at the same time as (iv). **.**

Having defined the relation $\simeq$, we now proceed to prove the equivalence $\phi \sim \psi \;\Leftrightarrow\; \phi \simeq \psi$. The strategy is the same as the one adopted for the strong substitution congruence. The difficult part is to show the inclusion $\sim \subseteq \simeq$, which we achieve by showing $R_0 \subseteq \simeq$ together with the fact that $\simeq$ is a congruence.

Proposition 83 *Let $\simeq$ be the almost equivalence relation on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ contains the generator R_0 of* definition (35)*.*

Proof
Suppose $x, y \in V$ and $\phi_1 \in \mathbf{P}(V)$ are such that $x \neq y$ and $y \notin \mathrm{Fr}(\phi_1)$. Note that this cannot happen unless V has at least two elements. We define $\phi = \forall x \phi_1$ and $\psi = \forall y\, \phi_1[y:x]$. We need to show that $\phi \simeq \psi$. We shall do so by proving that (v) of definition (36) is the case. Define $\psi_1 = \phi_1[y:x]$. Then we have $\phi = \forall x \phi_1$, $\psi = \forall y \psi_1$, $x \neq y$ and $y \notin \mathrm{Fr}(\phi_1)$. So it remains to show that $\psi_1 \sim \phi_1[y:x]$ which is immediate from the reflexivity of $\sim$. **.**

Proposition 84 *Let $\simeq$ be the almost equivalence relation on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ is a reflexive relation on $\mathbf{P}(V)$.*

Proof
Let $\phi \in \mathbf{P}(V)$. We need to show that $\phi \simeq \phi$. From theorem (2) of page 21 we know that ϕ is either an element of $\mathbf{P}_0(V)$, or $\phi = \bot$ or $\phi = \phi_1 \to \phi_2$ or $\phi = \forall x \phi_1$ for some $\phi_1, \phi_2 \in \mathbf{P}(V)$ and $x \in V$. We shall consider these four mutually exclusive cases separately. Suppose first that $\phi \in \mathbf{P}_0(V)$: then from $\phi = \phi$ we obtain $\phi \simeq \phi$. Suppose next that $\phi = \bot$: then it is clear that $\phi \simeq \phi$. Suppose now that $\phi = \phi_1 \to \phi_2$. Since the substitution congruence $\sim$ is reflexive, we have $\phi_1 \sim \phi_1$ and $\phi_2 \sim \phi_2$. It follows from (iii) of definition (36) that $\phi \simeq \phi$. Suppose finally that $\phi = \forall x \phi_1$. From $\phi_1 \sim \phi_1$ and (iv) of definition (36) we conclude that $\phi \simeq \phi$. In all cases, we have proved that $\phi \simeq \phi$. **.**

Proposition 85 *Let $\simeq$ be the almost equivalence relation on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ is a symmetric relation on $\mathbf{P}(V)$.*

Proof
Let $\phi, \psi \in \mathbf{P}(V)$ be such that $\phi \simeq \psi$. We need to show that $\psi \simeq \phi$. We shall consider the five possible cases of definition (36): suppose first that $\phi \in \mathbf{P}_0(V)$, $\psi \in \mathbf{P}_0(V)$ and $\phi = \psi$. Then it is clear that $\psi \simeq \phi$. Suppose next that $\phi = \bot$ and $\psi = \bot$. Then we also have $\psi \simeq \phi$. We now assume that $\phi = \phi_1 \to \phi_2$ and $\psi = \psi_1 \to \psi_2$ with $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$. Since the substitution congruence

on $\mathbf{P}(V)$ is symmetric, we have $\psi_1 \sim \phi_1$ and $\psi_2 \sim \phi_2$. Hence we have $\psi \simeq \phi$. We now assume that $\phi = \forall x\phi_1$ and $\psi = \forall x\psi_1$ with $\phi_1 \sim \psi_1$. Then once again by symmetry of the substitution congruence we have $\psi_1 \sim \phi_1$ and consequently $\psi \simeq \phi$. We finally consider the last possible case of $\phi = \forall x\phi_1$, $\psi = \forall y\psi_1$ with $x \neq y$, $\psi_1 \sim \phi_1[y:x]$ and $y \notin \mathrm{Fr}(\phi_1)$. We need to show that $\phi_1 \sim \psi_1[x:y]$ and $x \notin \mathrm{Fr}(\psi_1)$. First we show that $\phi_1 \sim \psi_1[x:y]$. Note that $[x:y]$ and $[y:x]$ are in fact the same substitutions. So we need to show that $\phi_1 \sim \psi_1[y:x]$. Since $\psi_1 \sim \phi_1[y:x]$ and $[y:x] : V \to V$ is injective, from proposition (81) we obtain:

$$\psi_1[y:x] \sim \phi_1[y:x][y:x]$$

It is therefore sufficient to show that $\phi_1 \sim \phi_1[y:x][y:x]$ which follows from proposition (29) and the fact that $[y:x] \circ [y:x]$ is the identity mapping. We now show that $x \notin \mathrm{Fr}(\psi_1)$. From $\psi_1 \sim \phi_1[y:x]$ and proposition (79) we obtain $\mathrm{Fr}(\psi_1) = \mathrm{Fr}(\phi_1[y:x])$. So we need to show that $x \notin \mathrm{Fr}(\phi_1[y:x])$. So suppose to the contrary that $x \in \mathrm{Fr}(\phi_1[y:x])$. We shall derive a contradiction. Since $[y:x]$ is injective, from proposition (44) we have $\mathrm{Fr}(\phi_1[y:x]) = [y:x](\mathrm{Fr}(\phi_1))$ and consequently there exists $u \in \mathrm{Fr}(\phi_1)$ such that $x = [y:x](u)$. It follows that $u = y$ which contradicts the assumption $y \notin \mathrm{Fr}(\phi_1)$. .

Showing that $\simeq$ is a transitive relation is the difficult part of this section. The following proposition is the counterpart of proposition (70) of the strong substitution congruence. Its proof is however a lot simpler.

Proposition 86 *Let $\simeq$ be the almost equivalence relation on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ is a transitive relation on $\mathbf{P}(V)$.*

Proof
Let ϕ, ψ and $\chi \in \mathbf{P}(V)$ be such that $\phi \simeq \psi$ and $\psi \simeq \chi$. We need to show that $\phi \simeq \chi$. We shall consider the five possible cases of definition (36) in relation to $\phi \simeq \psi$. Suppose first that $\phi, \psi \in \mathbf{P}_0(V)$ and $\phi = \psi$. Then from $\psi \simeq \chi$ we obtain $\psi, \chi \in \mathbf{P}_0(V)$ and $\psi = \chi$. It follows that $\phi, \chi \in \mathbf{P}_0(V)$ and $\phi = \chi$. Hence we see that $\phi \simeq \chi$. We now assume that $\phi = \psi = \bot$. Then from $\psi \simeq \chi$ we obtain $\psi = \chi = \bot$. It follows that $\phi = \chi = \bot$ and consequently $\phi \simeq \chi$. We now assume that $\phi = \phi_1 \to \phi_2$ and $\psi = \psi_1 \to \psi_2$ with $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$. From $\psi \simeq \chi$ we obtain $\chi = \chi_1 \to \chi_2$ with $\psi_1 \sim \chi_1$ and $\psi_2 \sim \chi_2$. The substitution congruence being transitive, it follows that $\phi_1 \sim \chi_1$ and $\phi_2 \sim \chi_2$. Hence we see that $\phi \simeq \chi$. We now assume that $\phi = \forall x\phi_1$ and $\psi = \forall x\psi_1$ with $\phi_1 \sim \psi_1$, for some $x \in V$. From $\psi \simeq \chi$ only the cases (iv) and (v) of definition (36) are possible. First we assume that (iv) is the case. Then $\chi = \forall x\chi_1$ with $\psi_1 \sim \chi_1$. The substitution congruence being transitive, we obtain $\phi_1 \sim \chi_1$ and consequently $\phi \simeq \chi$. We now assume that (v) is the case. Then $\chi = \forall y\chi_1$ for some $y \in V$ with $x \neq y$, $\chi_1 \sim \psi_1[y:x]$ and $y \notin \mathrm{Fr}(\psi_1)$. In order to prove $\phi \simeq \chi$ it is sufficient to show that $\chi_1 \sim \phi_1[y:x]$ and $y \notin \mathrm{Fr}(\phi_1)$. First we show that $\chi_1 \sim \phi_1[y:x]$. It is sufficient to prove that $\phi_1[y:x] \sim \psi_1[y:x]$ which follows from $\phi_1 \sim \psi_1$, using proposition (81) and the fact that $[y:x] : V \to V$ is injective. We now show that $y \notin \mathrm{Fr}(\phi_1)$. From $\phi_1 \sim \psi_1$ and proposition (79) we obtain $\mathrm{Fr}(\phi_1) = \mathrm{Fr}(\psi_1)$. Hence it is sufficient to show that $y \notin \mathrm{Fr}(\psi_1)$ which is true by assumption. It

remains to consider the last possible case of definition (36). So we assume that $\phi = \forall x \phi_1$ and $\psi = \forall y \psi_1$ with $x \neq y$, $\psi_1 \sim \phi_1[y:x]$ and $y \notin \mathrm{Fr}(\phi_1)$. From $\psi \simeq \chi$ only the cases (iv) and (v) of definition (36) are possible. First we assume that (iv) is the case. Then $\chi = \forall y \chi_1$ with $\psi_1 \sim \chi_1$. The substitution congruence being transitive, we obtain $\chi_1 \sim \phi_1[y:x]$ and consequently $\phi \simeq \chi$. We now assume that (v) is the case. Then $\chi = \forall z \chi_1$ for some $z \in V$ with $y \neq z$, $\chi_1 \sim \psi_1[z:y]$ and $z \notin \mathrm{Fr}(\psi_1)$. We shall now distinguish two cases. First we assume that $x = z$. Then $\phi = \forall x \phi_1$ and $\chi = \forall x \chi_1$ and in order to show that $\phi \simeq \chi$ it is sufficient to prove that $\phi_1 \sim \chi_1$. From $\chi_1 \sim \psi_1[z:y]$ and $z = x$ we obtain $\chi_1 \sim \psi_1[y:x]$ and it is therefore sufficient to prove that $\phi_1 \sim \psi_1[y:x]$. However, we know that $\psi_1 \sim \phi_1[y:x]$ and since $[y:x] : V \to V$ is injective, from proposition (81) we obtain $\psi_1[y:x] \sim \phi_1[y:x][y:x]$. It is therefore sufficient to show that $\phi_1 \sim \phi_1[y:x][y:x]$ which follows from proposition (29) and the fact that $[y:x] \circ [y:x]$ is the identity mapping. This completes our proof in the case when $x = z$. We now assume that $x \neq z$. So we have $x \neq y$, $y \neq z$ and $x \neq z$, with $\phi = \forall x \phi_1$, $\psi = \forall y \psi_1$ and $\chi = \forall z \chi_1$. Furthermore, $\psi_1 \sim \phi_1[y:x]$ and $\chi_1 \sim \psi_1[z:y]$ while we have $y \notin \mathrm{Fr}(\phi_1)$ and $z \notin \mathrm{Fr}(\psi_1)$, and we need to show that $\phi \simeq \chi$. So we need to prove that $\chi_1 \sim \phi_1[z:x]$ and $z \notin \mathrm{Fr}(\phi_1)$. First we show that $z \notin \mathrm{Fr}(\phi_1)$. So suppose to the contrary that $z \in \mathrm{Fr}(\phi_1)$. We shall derive a contradiction. Since $[y:x]$ is injective, from proposition (44) we have $\mathrm{Fr}(\phi_1[y:x]) = [y:x](\mathrm{Fr}(\phi_1))$. It follows that $z = [y:x](z)$ is also an element of $\mathrm{Fr}(\phi_1[y:x])$. However we have $\psi_1 \sim \phi_1[y:x]$ and consequently from proposition (79) we obtain $\mathrm{Fr}(\psi_1) = \mathrm{Fr}(\phi_1[y:x])$. Hence we see that $z \in \mathrm{Fr}(\psi_1)$ which is our desired contradiction. We shall now prove that $\chi_1 \sim \phi_1[z:x]$. Since $\chi_1 \sim \psi_1[z:y]$, it is sufficient to show that $\psi_1[z:y] \sim \phi_1[z:x]$. However we know that $\psi_1 \sim \phi_1[y:x]$ and since $[z:y] : V \to V$ is injective, from proposition (81) we obtain $\psi_1[z:y] \sim \phi_1[y:x][z:y]$. It is therefore sufficient to show that $\phi_1[y:x][z:y] \sim \phi_1[z:x]$. Let us accept for now:

$$[z:x] = [y:x] \circ [z:y] \circ [y:x] \tag{2.25}$$

Then we simply need to show that $\phi_1[y:x][z:y] \sim \phi_1[y:x][z:y][y:x]$. Using proposition (77), it is therefore sufficient to prove that $[y:x]$ is an admissible substitution for $\phi_1[y:x][z:y]$. Since $[y:x] : V \to V$ is injective, from proposition (53) it is valid for $\phi_1[y:x][z:y]$. So it remains to show that $[y:x](u) = u$ for all $u \in \mathrm{Fr}(\phi_1[y:x][z:y])$. It is therefore sufficient to prove that neither x nor y are elements of $\mathrm{Fr}(\phi_1[y:x][z:y])$. However, since $[z:y] \circ [y:x] : V \to V$ is injective, from proposition (44) we have $\mathrm{Fr}(\phi_1[y:x][z:y]) = [z:y] \circ [y:x](\mathrm{Fr}(\phi_1))$. So we need to show that x and y do not belong to $[z:y] \circ [y:x](\mathrm{Fr}(\phi_1))$. First we do this for x. Suppose $x = [z:y] \circ [y:x](u)$ for some $u \in \mathrm{Fr}(\phi_1)$. By injectivity we must have $u = y$, contradicting the assumption $y \notin \mathrm{Fr}(\phi_1)$. We now deal with y. So suppose $y = [z:y] \circ [y:x](u)$ for some $u \in \mathrm{Fr}(\phi_1)$. By injectivity we must have $u = z$, contradicting the fact that $z \notin \mathrm{Fr}(\phi_1)$ which we have already proven. It remains to prove that equation (2.25) holds. So let $u \in V$. We need:

$$[z:x](u) = [y:x] \circ [z:y] \circ [y:x](u)$$

This is clearly the case when $u \notin \{x, y, z\}$. The cases $u = x$, $u = y$ and $u = z$ are easily checked. .

The implication $\phi \simeq \psi \;\Rightarrow\; \phi \sim \psi$ is the simple one. We need to prove it now in order to show that $\simeq$ is a congruent relation.

Proposition 87 *Let $\simeq$ be the almost equivalence and $\sim$ be the substitution congruence on $\mathbf{P}(V)$, where V is a set. For all $\phi, \psi \in \mathbf{P}(V)$:*

$$\phi \simeq \psi \;\Rightarrow\; \phi \sim \psi$$

Proof
Let $\phi, \psi \in \mathbf{P}(V)$ such that $\phi \simeq \psi$. We need to show that $\phi \sim \psi$. We shall consider the five possible cases of definition (36) in relation to $\phi \simeq \psi$. Suppose first that $\phi = \psi \in \mathbf{P}_0(V)$. From the reflexivity of the substitution congruence, it is clear that $\phi \sim \psi$. Suppose next that $\phi = \psi = \bot$. Then we also have $\phi \sim \psi$. We now assume that $\phi = \phi_1 \to \phi_2$ and $\psi = \psi_1 \to \psi_2$ where $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$. The substitution congruence being a congruent relation on $\mathbf{P}(V)$, we obtain $\phi \sim \psi$. Next we assume that $\phi = \forall x \phi_1$ and $\psi = \forall x \psi_1$ where $\phi_1 \sim \psi_1$ and $x \in V$. Again, the substitution congruence being a congruent relation we obtain $\phi \sim \psi$. Finally we assume that $\phi = \forall x \phi_1$ and $\psi = \forall y \psi_1$ where $x \neq y$, $\psi_1 \sim \phi_1[y : x]$ and $y \notin \mathrm{Fr}(\phi_1)$. For the last time, the substitution congruence being a congruent relation we obtain $\psi \sim \forall y\, \phi_1[y : x]$. Hence in order to show $\phi \sim \psi$ it is sufficient to show that $\forall x \phi_1 \sim \forall y\, \phi_1[y : x]$ which follows immediately from $x \neq y$, $y \notin \mathrm{Fr}(\phi_1)$ and definition (35). .

Proposition 88 *Let $\simeq$ be the almost equivalence relation on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ is a congruent relation on $\mathbf{P}(V)$.*

Proof
From proposition (84), the almost equivalence $\simeq$ is reflexive and so $\bot \simeq \bot$. We now assume that $\phi = \phi_1 \to \phi_2$ and $\psi = \psi_1 \to \psi_2$ where $\phi_1 \simeq \psi_1$ and $\phi_2 \simeq \psi_2$. We need to show that $\phi \simeq \psi$. However from proposition (87) we have $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$ and it follows from definition (36) that $\phi \simeq \psi$. We now assume that $\phi = \forall x \phi_1$ and $\psi = \forall x \psi_1$ where $\phi_1 \simeq \psi_1$ and $x \in V$. We need to show that $\phi \simeq \psi$. Once again from proposition (87) we have $\phi_1 \sim \psi_1$ and consequently from definition (36) we obtain $\phi \simeq \psi$. .

Proposition 89 *Let $\simeq$ be the almost equivalence relation on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ is a congruence on $\mathbf{P}(V)$.*

Proof
We need to show that $\simeq$ is reflexive, symmetric, transitive and that it is a congruent relation on $\mathbf{P}(V)$. From proposition (84), the relation $\simeq$ is reflexive. From proposition (85) it is symmetric while from proposition (86) it is transitive. Finally from proposition (88) the relation $\simeq$ is a congruent relation. .

So we have shown that $\simeq$ is a congruence on $\mathbf{P}(V)$ which contains the generator R_0 of the substitution congruence. The equality $\simeq = \sim$ follows immediately.

Proposition 90 *Let $\simeq$ be the almost equivalence and $\sim$ be the substitution congruence on $\mathbf{P}(V)$, where V is a set. For all $\phi, \psi \in \mathbf{P}(V)$:*

$$\phi \simeq \psi \;\Leftrightarrow\; \phi \sim \psi$$

Proof
From proposition (87) it is sufficient to show the implication $\Leftarrow$ or equivalently the inclusion $\sim \subseteq \simeq$. Since $\sim$ is the substitution congruence on $\mathbf{P}(V)$, it is the smallest congruence on $\mathbf{P}(V)$ which contains the set R_0 of definition (35). In order to show the inclusion $\sim \subseteq \simeq$ it is therefore sufficient to show that $\simeq$ is a congruence on $\mathbf{P}(V)$ such that $R_0 \subseteq \simeq$. The fact that it is a congruence stems from proposition (89). The fact that $R_0 \subseteq \simeq$ follows from proposition (83). .

We have no need to remember the relation $\simeq$. The equality $\simeq = \sim$ is wrapped up in the following theorem for future reference. This is the counterpart of theorem (11) of page 120 of the strong substitution congruence.

Theorem 12 *Let $\sim$ be the substitution congruence on $\mathbf{P}(V)$ where V is a set. For all $\phi, \psi \in \mathbf{P}(V)$, $\phi \sim \psi$ if and only if one of the following is the case:*

$$\begin{array}{ll}
(i) & \phi \in \mathbf{P}_0(V)\ ,\ \psi \in \mathbf{P}_0(V)\ ,\ \textit{and}\ \phi = \psi \\
(ii) & \phi = \bot\ \textit{and}\ \psi = \bot \\
(iii) & \phi = \phi_1 \to \phi_2\ ,\ \psi = \psi_1 \to \psi_2\ ,\ \phi_1 \sim \psi_1\ \textit{and}\ \phi_2 \sim \psi_2 \\
(iv) & \phi = \forall x \phi_1\ ,\ \psi = \forall x \psi_1\ \textit{and}\ \phi_1 \sim \psi_1 \\
(v) & \phi = \forall x \phi_1\ ,\ \psi = \forall y \psi_1\ ,\ x \neq y\ ,\ \psi_1 \sim \phi_1[y:x]\ ,\ y \notin \mathrm{Fr}(\phi_1)
\end{array}$$

Proof
Immediately follows from proposition (90) and definition (36). .

2.2.11 Substitution Congruence vs Strong Congruence

In definition (32) we initially defined the strong substitution congruence thinking it was the appropriate notion to study. We then realized in proposition (75) and proposition (76) that the strong substitution congruence is in fact unsatisfactory in the case when the set of variables V has two or three elements. For example, when $V = \{x, y\}$ with $x \neq y$, we saw that the formulas $\phi = \forall x \forall y (x \in y)$ and $\psi = \forall y \forall x (y \in x)$ failed to be equivalent. It is easy to believe that similar failures can be uncovered whenever V is a finite set. So we decided to search for a new notion of *substitution congruence* which led to definition (35). In this section, we shall attempt to show that this new substitution congruence has all the advantages of the strong substitution congruence, but without its flaws.

First we look at the paradox of proposition (75). So let $V = \{x, y\}$ with $x \neq y$ and $\phi = \forall x \forall y (x \in y)$ with $\psi = \forall y \forall x (y \in x)$. Then setting $\phi_1 = \forall y (x \in y)$ we have $\phi = \forall x \phi_1$ and $\psi = \forall y\, \phi_1[y:x]$. Since $x \neq y$ and $y \notin \mathrm{Fr}(\phi_1)$ we conclude from definition (35) that $\phi \sim \psi$ where $\sim$ denotes the substitution congruence. So the paradox of proposition (75) is lifted. Suppose now that $V = \{x, y, z\}$ where x, y and z are distinct, and define $\phi = \forall x \forall y \forall z\, [(x \in y) \to (y \in z)]$

and $\psi = \forall y \forall z \forall x\,[(y \in z) \rightarrow (z \in x)]$. We claim that $\phi \sim \psi$. If this is the case, then the paradox of proposition (76) is also lifted. Let χ be the formula defined by $\chi = \forall y \forall x \forall z\,[(y \in x) \rightarrow (x \in z)]$. Then χ is simply the formula obtained from ϕ by permuting the variables x and y. In order to show $\phi \sim \psi$ it is sufficient to prove that $\phi \sim \chi$ and $\chi \sim \psi$. First we show that $\phi \sim \chi$. Defining $\phi_1 = \forall y \forall z\,[(x \in y) \rightarrow (y \in z)]$ we have $\phi = \forall x \phi_1$ and $\chi = \forall y \phi_1[y:x]$. Since $x \neq y$ and $y \notin \mathrm{Fr}(\phi_1)$ we conclude from definition (35) that $\phi \sim \chi$. We now show that $\chi \sim \psi$. Setting $\theta = \forall x \forall z\,[(y \in x) \rightarrow (x \in z)]$ together with $\theta^* = \forall z \forall x\,[(y \in z) \rightarrow (z \in x)]$ we have $\chi = \forall y \theta$ and $\psi = \forall y \theta^*$. It is therefore sufficient to show that $\theta \sim \theta^*$. Defining $\theta_1 = \forall z\,[(y \in x) \rightarrow (x \in z)]$ we obtain $\theta = \forall x \theta_1$ and $\theta^* = \forall z \theta_1[z:x]$. Since $x \neq z$ and $z \notin \mathrm{Fr}(\theta_1)$ we conclude from definition (35) that $\theta \sim \theta^*$. So we have proved that the substitution congruence is not subject to the paradoxes of proposition (75) and proposition (76).

Having reviewed the known shortcomings of the strong substitution congruence, we shall now establish that the new substitution congruence is in fact pretty much the same notion as the old. Specifically, we shall see that both congruences coincide when V is an infinite set. Furthermore, even when V is a finite set we shall see that two formulas ϕ and ψ which are simply equivalent with respect to the substitution congruence, are in fact strongly equivalent provided ϕ and ψ do not use up all the variables in V, i.e. $\mathrm{Var}(\phi) \neq V$ or $\mathrm{Var}(\psi) \neq V$. First we check that the strong substitution congruence is indeed a relation which is *stronger* than the substitution congruence:

Proposition 91 *Let $\sim$ be the substitution congruence and $\simeq$ be the strong substitution congruence on $\mathbf{P}(V)$ where V is a set. Then for all $\phi, \psi \in \mathbf{P}(V)$:*

$$\phi \simeq \psi \;\Rightarrow\; \phi \sim \psi$$

Proof
We need to show the inclusion $\simeq \subseteq \sim$. However, using definition (32) the strong substitution congruence $\simeq$ is generated by the following set:

$$R_0 = \{\, (\, \forall x \phi_1\,,\, \forall y\, \phi_1[y/x]\,) : \phi_1 \in \mathbf{P}(V)\ ,\ x, y \in V\ ,\ x \neq y\ ,\ y \notin \mathrm{Var}(\phi_1)\,\}$$

while from definition (35) the congruence $\sim$ is generated by the set:

$$R_1 = \{\, (\, \forall x \phi_1\,,\, \forall y\, \phi_1[y:x]\,) : \phi_1 \in \mathbf{P}(V)\ ,\ x, y \in V\ ,\ x \neq y\ ,\ y \notin \mathrm{Fr}(\phi_1)\,\}$$

So it is sufficient to show that $R_0 \subseteq R_1$ which follows from the fact that $\phi_1[y/x] = \phi_1[y:x]$ whenever $y \notin \mathrm{Var}(\phi_1)$ as can be seen from proposition (39).
.

Proposition 92 *Let $\simeq$ be the strong substitution congruence on $\mathbf{P}(V)$ where V is a set. Let $\phi \in \mathbf{P}(V)$ such that $y \notin \mathrm{Fr}(\phi)$ and $\mathrm{Var}(\phi) \neq V$. Then we have:*

$$\forall x\, \phi \simeq \forall y\, \phi[y:x]$$

Proof
Suppose for now that $y \notin \mathrm{Var}(\phi)$. From proposition (39) we have the equality $\phi[y:x] = \phi[y/x]$ and the strong equivalence $\forall x\, \phi \simeq \forall y\, \phi[y:x]$ is therefore a of consequence $y \notin \mathrm{Var}(\phi)$ and definition (32). So the conclusion of the proposition follows easily with the simple assumption $y \notin \mathrm{Var}(\phi)$. Thus we may assume that $y \in \mathrm{Var}(\phi)$ from now on. Suppose now that $\psi \in \mathbf{P}(V)$ is such that $y \notin \mathrm{Var}(\psi)$ and $\phi \simeq \psi$. Then for the reasons just indicated we obtain $\forall x\, \psi \simeq \forall y\, \psi[y:x]$. Furthermore, the strong substitution congruence being a congruent relation on $\mathbf{P}(V)$, from $\phi \simeq \psi$ we have $\forall x\, \phi \simeq \forall x\, \psi$ and $\forall y\, \phi[y:x] \simeq \forall y\, \psi[y:x]$, where we have used the fact that $\phi[y:x] \simeq \psi[y:x]$ which itself follows from the injectivity of $[y:x] : V \to V$ and proposition (63). By transitivity it follows that $\forall x\, \phi \simeq \forall y\, \phi[y:x]$ and the proposition is proved. Thus, it is sufficient to show the existence of $\psi \in \mathbf{P}(V)$ with $y \notin \mathrm{Var}(\psi)$ and $\phi \simeq \psi$. Having assumed the existence of $z \in V$ such that $z \notin \mathrm{Var}(\phi)$, let $\psi \in \mathbf{P}(V)$ be defined as $\psi = \phi[z/y]$. Note in particular that $z \neq y$ since we have assumed $y \in \mathrm{Var}(\phi)$. The fact that $y \notin \mathrm{Var}(\psi)$ follows immediately from $z \neq y$ and proposition (41). So it remains to show that $\phi \simeq \psi$ or equivalently that $\phi \simeq \phi[z/y]$ which is a consequence of proposition (65) and the facts that $z \notin \mathrm{Var}(\phi)$ and $y \notin \mathrm{Fr}(\phi)$. **.**

Proposition 93 *Let $\sim$ be the substitution congruence and $\simeq$ be the strong substitution congruence on $\mathbf{P}(V)$ where V is a set. Let $\phi, \psi \in \mathbf{P}(V)$ be such that $\mathrm{Var}(\phi) \neq V$. Then we have the equivalence:*

$$\phi \simeq \psi \;\Leftrightarrow\; \phi \sim \psi$$

Proof
The implication $\Rightarrow$ follows from proposition (91). So we need to prove $\Leftarrow$. Specifically, given $\phi \in \mathbf{P}(V)$, we need to show that ϕ satisfies the property:

$$\mathrm{Var}(\phi) \neq V \;\Rightarrow\; \forall \psi [\, \phi \sim \psi \;\Rightarrow\; \phi \simeq \psi \,]$$

We shall do so by a structural induction argument, using theorem (3) of page 31. First we assume that $\phi = (x \in y)$ for some $x, y \in V$. As we shall see the condition $\mathrm{Var}(\phi) \neq V$ will not be used here. So let $\psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$. It is sufficient to prove that $\phi \simeq \psi$. In fact it is sufficient to show that $\phi = \psi$ which follows immediately from $\phi = (x \in y)$ and $\phi \sim \psi$, using theorem (12) of page 132. So we now assume that $\phi = \bot$. Then again from theorem (12) the condition $\phi \sim \psi$ implies that $\phi = \psi$ and we are done. So we now assume that $\phi = \phi_1 \to \phi_2$ where $\phi_1, \phi_2 \in \mathbf{P}(V)$ satisfy our property. We need to show the same is true of ϕ. So we assume that $\mathrm{Var}(\phi) \neq V$ and we consider $\psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$. We need to show that $\phi \simeq \psi$. However, using theorem (12) once more the condition $\phi \sim \psi$ implies that ψ must be of the form $\psi = \psi_1 \to \psi_2$ where $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$. Hence the strong substitution $\simeq$ being a congruent relation, in order to show $\phi \simeq \psi$ it is sufficient to prove that $\phi_1 \simeq \psi_1$ and $\phi_2 \simeq \psi_2$. Having assumed our induction property is true for ϕ_1, it follows from $\mathrm{Var}(\phi_1) \subseteq \mathrm{Var}(\phi)$ that $\mathrm{Var}(\phi_1) \neq V$ and $\phi_1 \simeq \psi_1$ is therefore an immediate consequence of $\phi_1 \sim \psi_1$. We prove similarly that $\phi_2 \simeq \psi_2$ which

completes the case when $\phi = \phi_1 \rightarrow \phi_2$. We now assume that $\phi = \forall x \phi_1$ where $x \in V$ and $\phi_1 \in \mathbf{P}(V)$ satisfies our property. We need to show the same is true for ϕ. So we assume that $\mathrm{Var}(\phi) \neq V$ and consider $\psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$. We need to show that $\phi \simeq \psi$. From theorem (12), the condition $\phi \sim \psi$ leads to two possible cases: ψ must be of the form $\psi = \forall x \psi_1$ with $\phi_1 \sim \psi_1$, or it must be of the form $\psi = \forall y \psi_1$ with $x \neq y$, $\psi_1 \sim \phi_1[y:x]$ and $y \notin \mathrm{Fr}(\phi_1)$. First we assume that $\psi = \forall x \psi_1$ which $\phi_1 \sim \psi_1$. Then in order to show that $\phi \simeq \psi$ it is sufficient to prove that $\phi_1 \simeq \psi_1$. Having assumed our induction property is true for ϕ_1, it follows from $\mathrm{Var}(\phi_1) \subseteq \mathrm{Var}(\phi)$ that $\mathrm{Var}(\phi_1) \neq V$ and $\phi_1 \simeq \psi_1$ is therefore an immediate consequence of $\phi_1 \sim \psi_1$. So we now consider the second case when $\psi = \forall y \psi_1$ with $x \neq y$, $\psi_1 \sim \phi_1[y:x]$ and $y \notin \mathrm{Fr}(\phi_1)$. We need to show that $\phi \simeq \psi$. However, using proposition (81) and the fact that $[y:x] : V \rightarrow V$ is an injective map such that $[y:x] \circ [y:x]$ is the identity mapping, we obtain immediately $\psi_1[y:x] \sim \phi_1$. Having assumed our property is true for ϕ_1, from $\mathrm{Var}(\phi_1) \neq V$ we obtain $\psi_1[y:x] \simeq \phi_1$. Composing once again on both side by $[y:x]$ we now argue from proposition (63) that $\psi_1 \simeq \phi_1[y:x]$. Thus in order to show that $\phi \simeq \psi$ it is sufficient to prove that $\forall x \phi_1 \simeq \forall y \phi_1[y:x]$ which follows immediately from proposition (92), $y \notin \mathrm{Fr}(\phi_1)$ and $\mathrm{Var}(\phi_1) \neq V$. **.**

So it is now clear that the substitution congruence and strong substitution congruence are pretty much the same thing. We just need to bear in mind that an equivalence $\phi \sim \psi$ may fail to imply a strong equivalence $\phi \simeq \psi$ in the case when all variables of V have been used up by both ϕ and ψ. We shall conclude this section by providing counterparts to proposition (77) and proposition (78) for the strong substitution congruence.

Proposition 94 *Let $\simeq$ be the strong substitution congruence on $\mathbf{P}(V)$ where V is a set. Let $\phi \in \mathbf{P}(V)$ and $\sigma : V \rightarrow V$ be an admissible substitution for ϕ such that $\mathrm{Var}(\sigma(\phi)) \neq V$. Then, we have:*

$$\phi \simeq \sigma(\phi)$$

Proof
Let $\sim$ be the substitution congruence on $\mathbf{P}(V)$. Having assumed σ is admissible for ϕ, using proposition (77) we obtain $\phi \sim \sigma(\phi)$. Since $\mathrm{Var}(\sigma(\phi)) \neq V$ we conclude from proposition (93) that $\phi \simeq \sigma(\phi)$. **.**

Proposition (94) allows us to state another characterization of the strong substitution congruence as the following proposition shows. In definition (32), the strong substitution congruence was defined in terms of a generator:

$$R_0 = \{(\phi, \sigma(\phi)) \ : \ \phi = \forall x \phi_1 \ , \ \sigma = [y/x] \ , x \neq y \ , \ y \notin \mathrm{Var}(\phi_1)\}$$

As we shall soon discover, this generator is in fact a subset of the set R_1 of ordered pairs $(\phi, \sigma(\phi))$ where σ is admissible for ϕ and such that $\mathrm{Var}(\sigma(\phi)) \neq V$. Since we now know from proposition (94) that R_1 is itself a subset of the strong substitution congruence, it follows that R_1 is also a generator of the strong substitution congruence, which we shall now prove formally:

Proposition 95 *Let V be a set. Then the strong substitution congruence on $\mathbf{P}(V)$ is also generated by the following set $R_1 \subseteq \mathbf{P}(V) \times \mathbf{P}(V)$:*

$$R_1 = \{ (\phi, \sigma(\phi)) : \phi \in \mathbf{P}(V) \ , \ \sigma : V \to V \text{ admissible for } \phi \ , \ \mathrm{Var}(\sigma(\phi)) \neq V \}$$

Proof
Let $\simeq$ denote the strong substitution congruence on $\mathbf{P}(V)$ and $\equiv$ be the congruence on $\mathbf{P}(V)$ generated by R_1. We need to show that $\simeq = \equiv$. First we show that $\simeq \subseteq \equiv$. Since $\simeq$ is the smallest congruence on $\mathbf{P}(V)$ which contains the set R_0 of definition (32), in order to prove $\simeq \subseteq \equiv$ it is sufficient to prove that $R_0 \subseteq \equiv$. So let $\phi_1 \in \mathbf{P}(V)$ and $x, y \in V$ be such that $x \neq y$ and $y \notin \mathrm{Var}(\phi_1)$. Define $\phi = \forall x \phi_1$ and $\psi = \forall y \, \phi_1[y/x]$. We need to show that $\phi \equiv \psi$. The congruence $\equiv$ being generated by R_1 it is sufficient to prove that $(\phi, \psi) \in R_1$. However, if we define $\sigma : V \to V$ by setting $\sigma = [y/x]$ we have:

$$\psi = \forall y \, \phi_1[y/x] = \forall \sigma(x) \, \sigma(\phi_1) = \sigma(\forall x \phi_1) = \sigma(\phi)$$

Hence, in order to show $(\phi, \psi) \in R_1$, it is sufficient to prove that σ is an admissible substitution for ϕ and furthermore that $\mathrm{Var}(\sigma(\phi)) \neq V$. The fact that $\mathrm{Var}(\sigma(\phi)) \neq V$ follows immediately from $x \notin \mathrm{Var}(\phi[y/x])$, which is itself a consequence of $x \neq y$ and proposition (41). So we need to show that σ is an admissible substitution for ϕ. First we show that σ is valid for $\phi = [y/x]$. This follows immediately from proposition (57) and the fact that y is not an element of $\mathrm{Var}(\phi) = \mathrm{Var}(\phi_1) \cup \{x\}$. Next we show that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\phi)$. So let $u \in \mathrm{Fr}(\phi) = \mathrm{Fr}(\phi_1) \setminus \{x\}$. Then in particular $u \neq x$ and consequently $\sigma(u) = [y/x](u) = u$. This completes our proof of $\simeq \subseteq \equiv$. We now show that $\equiv \subseteq \simeq$. Since $\equiv$ is the smallest congruence on $\mathbf{P}(V)$ which contains the set R_1, it is sufficient to show that $R_1 \subseteq \simeq$. So let $\phi \in \mathbf{P}(V)$ and $\sigma : V \to V$ be an admissible substitution for ϕ such that $\mathrm{Var}(\sigma(\phi)) \neq V$. We need to show that $\phi \simeq \sigma(\phi)$. But this follows immediately from proposition (94). **.**

From proposition (95) the strong substitution congruence is generated by the set of ordered pairs $(\phi, \sigma(\phi))$ where σ is admissible for ϕ and such that $\mathrm{Var}(\sigma(\phi)) \neq V$. This is also a flaw of the strong substitution congruence as we feel the condition $\mathrm{Var}(\sigma(\phi)) \neq V$ should not be there. In contrast, as can be seen from proposition (78), the substitution congruence does not suffer from this condition, as it is simply generated by the set of ordered pairs $(\phi, \sigma(\phi))$ where σ is admissible for ϕ. Whichever way we look at it, it is clear that the substitution congruence is a better notion to look at than the strong substitution congruence. In many respects, it is also a lot simpler. Before we close this section, we may go back to a question we raised before defining the strong substitution congruence in page 107. We decided to define the strong substitution in terms of ordered pairs $(\forall x \phi_1, \forall y \phi_1[y/x])$ where $x \neq y$ and $y \notin \mathrm{Var}(\phi_1)$. What if we had opted for the condition '$[y/x]$ *valid for* $\forall x \phi_1$' rather than '$y \notin \mathrm{Var}(\phi_1)$'? It is now clear from proposition (94) that this would have yielded a congruence identical to the strong substitution congruence. So we did well to keep it simple.

2.3 Essential Substitution of Variable

2.3.1 Preliminaries

The notion of *essential substitution* arises from the more general issue of *capture-avoiding substitutions* in formal languages with variable binding. This question is already dealt with in the computer science literature of which by and large, we are sadly unaware. It is therefore very difficult for us to give due credit to the work that has already been done. However, we would like to mention the papers of Murdoch J. Gabbay [22] and Murdoch J. Gabbay and Aad Mathijssen [23], whose existence came to our attention, and which deal with *capture-avoiding substitutions*. Our own approach we think is original, but of course we cannot be sure. The whole question of *capture-avoiding substitutions* arises from the fact that most substitutions $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ associated with a map $\sigma : V \to W$ are not *capture-avoiding*. We introduced the notion of *valid substitutions* in definition (30) so as to distinguish those cases when $\sigma(\phi)$ is *capture-avoiding* and those when it is not. This was clearly a step forward but we were still very short of defining a total map $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ which would somehow be associated to $\sigma : V \to W$, while avoiding capture for every $\phi \in \mathbf{P}(V)$. Our solution to the problem relies on the introduction of the *minimal transform mapping* $\mathcal{M} : \mathbf{P}(V) \to \mathbf{P}(\bar{V})$ where $\bar{V} = V \oplus \mathbf{N}$ is the direct sum of V and $\mathbf{N}$. In considering the *minimal extension* $\bar{V}$ of the set V, we are effectively adding a new set of variables specifically for the purpose of variable binding, an idea which bears some resemblance with the introduction of *atoms* in the *nominal set* approach of Murdoch J. Gabbay. The *minimal transform mapping* replaces all bound variables from the set V to the set $\mathbf{N}$. The benefit of doing so is immediate as given a map $\sigma : V \to W$, the obvious extension $\bar{\sigma} : \bar{V} \to \bar{W}$ applied to the minimal transform $\mathcal{M}(\phi)$ is now *capture-avoiding* for all ϕ. In other words, the formula $\bar{\sigma} \circ \mathcal{M}(\phi)$ is always logically meaningful. However, this formula belongs to the space $\mathbf{P}(\bar{W})$ and we are still short of defining *an essential substitution* $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$. The breakthrough consists in noting that, provided the set W is infinite or larger than the set V, it is always possible to express the formula $\bar{\sigma} \circ \mathcal{M}(\phi)$ as the *minimal transform* $\mathcal{M}(\psi)$ for some formula $\psi \in \mathbf{P}(W)$. Using the axiom of choice, an *essential substitution* $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ associated with the map $\sigma : V \to W$ is simply defined in terms of $\mathcal{M} \circ \sigma = \bar{\sigma} \circ \mathcal{M}$, and is uniquely characterized modulo α-equivalence, i.e. the substitution congruence. Of course, anyone interested in computer science and computability in general will not look favorably upon the use of the axiom of choice. We are dealing with arbitrary sets V and W of arbitrary cardinality. In practice, a computer scientist will have sets of variables which are well-ordered, and it is not difficult to find some $\psi \in \mathbf{P}(W)$ such that $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M}(\psi)$ in a way which is deterministic.

2.3.2 Minimal Transform of Formula

There will come a point when we will want to invoke $\forall x \phi_1 \to \phi_1[a]$ as an instance of the specialization axioms to argue that $\phi_1[a]$ must be true if we

know that $\forall x \phi_1$ is itself true. In doing so, the formula $\phi_1[a]$ should be some form of *evaluation* of the formula ϕ_1, where the free variable x of ϕ_1 has been replaced by a. For example, when $\phi_1 = \forall y(x \in y)$ with $x \neq y$, it would be natural to define $\phi_1[a] = \forall y(a \in y)$, provided $a \neq y$. In the case when $a = y$ such definition would not work. So we have a problem. It is important for us to argue that $\forall x \phi_1 \to \phi_1[a]$ is a legitimate axiom even in the case when $a = y$. If we fail to do so, our deductive system will be too weak and we will most likely have a very hard time attempting to prove Gödel's completeness theorem.

There are no doubt several ways to solve our problem. One of them is to abandon the aim of defining $\phi_1[a]$ as a formula and define it instead as an equivalence class. So $\phi_1[y]$ would not be defined as $\forall u(y \in u)$ for an arbitrary $u \neq y$ but rather as the full equivalence class of $\forall u(y \in u)$ (modulo the substitution congruence for example). It is always an ugly thing to do to define a mapping $a \to \phi_1[a]$ in terms of a randomly chosen $u \neq y$. By viewing $\phi_1[a]$ as an equivalence class we eliminate this dependency in u, which is aesthetically far more pleasing. On the negative side, if we are later to attempt defining a *deductive congruence* by setting $\phi \sim \psi$ whenever both $\phi \to \psi$ and $\psi \to \phi$ are provable from our deductive system, having $\phi_1[a]$ defined as an equivalence class would mean our deductive congruence fails to be decoupled from the substitution congruence. It would be very nice to define a deductive congruence which has no dependency to a substitution congruence.

There is possibly another approach to resolve our problem which is the one pursued in this section. The formula $\phi_1 = \forall y(x \in y)$ is a problem to us simply because it has y as a variable. The way we have defined the algebra $\mathbf{P}(V)$ has a major drawback: we are using the same set of variables V to represent variables which are free and those which are not. Things would be so much simpler if we had $\forall * (x \in *)$ or $\forall 0 (x \in 0)$ instead of $\forall y(x \in y)$. Life would be a lot easier if we had an algebra where the free variables and the bound variables were taken from different sets, more specifically sets with empty intersection.

Definition 38 *Let V be a set. We call* minimal extension *of V the set $\bar{V}$ defined as the disjoint union of V and $\mathbf{N}$, that is:*

$$\bar{V} = \{0\} \times V \cup \{1\} \times \mathbf{N}$$

So now we have a set of variables $\bar{V}$ with fundamentally two types of elements. We can use the elements of the form $(0, x)$ with $x \in V$ to represent free variables of a formula, and the elements of the form $(1, n)$ with $n \in \mathbf{N}$ to represent variables which are not free. Furthermore, since we have two obvious embeddings $i : V \to \bar{V}$ and $j : \mathbf{N} \to \bar{V}$ there is no point writing $(0, x)$ or $(1, n)$ and we can simply represent elements of $\bar{V}$ as x and n, having in mind the inclusions $V \subseteq \bar{V}$ and $\mathbf{N} \subseteq \bar{V}$ with $V \cap \mathbf{N} = \emptyset$. So we can now represent elements of $\mathbf{P}(\bar{V})$ as $\bar{\phi} = \forall 0 (x \in 0)$ without ambiguity. Of course, the formula $\bar{\phi} = \forall x(0 \in x)$ is also an element of $\mathbf{P}(\bar{V})$ which is contrary to the spirit of why we have defined $\bar{V}$ in the first place: we want free variables of any formula to be chosen from V and bound variables to be chosen from $\mathbf{N}$. So not every

element of $\mathbf{P}(\bar{V})$ will be interesting to us. We will need to restrict our attention to a meaningful subset of $\mathbf{P}(\bar{V})$. We shall do so by defining a mapping $\mathcal{M} : \mathbf{P}(V) \to \mathbf{P}(\bar{V})$ which will make sure the formula $\mathcal{M}(\phi) \in \mathbf{P}(\bar{V})$ abides to the right variable conventions, for all $\phi \in \mathbf{P}(V)$. The range of this mapping $\mathcal{M}(\mathbf{P}(V)) \subseteq \mathbf{P}(\bar{V})$ will hopefully be an interesting algebra to look at.

So how should our mapping $\mathcal{M} : \mathbf{P}(V) \to \mathbf{P}(\bar{V})$ look like? Given $x, y \in V$ we would probably want to have $\mathcal{M}(x \in y) = x \in y \in \mathbf{P}(\bar{V})$. We would also request that $\mathcal{M}(\bot) = \bot$ and $\mathcal{M}(\phi_1 \to \phi_2) = \mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2)$. The real question is to determine how $\mathcal{M}(\forall x \phi_1)$ should be defined, given $\phi_1 \in \mathbf{P}(V)$ and $x \in V$. The whole idea of the mapping $\mathcal{M} : \mathbf{P}(V) \to \mathbf{P}(\bar{V})$ is to replace bound variables in V of a formula $\phi \in \mathbf{P}(V)$ with nice looking variables $0, 1, 2, 3 \ldots$ in the formula $\mathcal{M}(\phi)$. So $\mathcal{M}(\forall x \phi_1)$ should be defined as:

$$\mathcal{M}(\forall x \phi_1) = \forall n \mathcal{M}(\phi_1)[n/x]$$

where $n \in \mathbf{N} \subseteq \bar{V}$. With such definition, we start from the formula $\mathcal{M}(\phi_1)$ which has been adequately transformed until now, and then replace the free variable x (if applicable) with an integer variable n so as to obtain $\mathcal{M}(\phi_1)[n/x]$, and we finally substitute the quantification $\forall x$ with the corresponding $\forall n$. This is all looking good. The only thing left to determine is how to choose the integer n. We know from our study of valid substitutions defined in page 91 that we cannot just pick any n. It would not make sense to consider $\mathcal{M}(\phi_1)[n/x]$ unless the substitution $[n/x]$ is valid for $\mathcal{M}(\phi_1)$. For example, suppose $\phi = \forall x \forall y (x \in y)$, i.e. $\phi_1 = \forall y (x \in y)$. It is acceptable to define $\mathcal{M}(\phi_1) = \forall 0 \, (x \in 0)$ and choose $n = 0$ or indeed $\mathcal{M}(\phi_1) = \forall 7 \, (x \in 7)$ is also fine, since $[n/y]$ is always valid for $(x \in y)$ regardless of the particular choice of n. However, having decided upon $\mathcal{M}(\phi_1) = \forall 0 \, (x \in 0)$, we cannot define $\mathcal{M}(\phi) = \forall 0 \forall 0 \, (0 \in 0)$ as this would make no sense. The substitution $[0/x]$ is not valid for $\forall 0 \, (x \in 0)$. We have to choose a different integer and set $\mathcal{M}(\phi) = \forall 1 \forall 0 \, (1 \in 0)$. The substitution $[n/x]$ should be valid for the formula $\mathcal{M}(\phi_1)$. In fact, the obvious choice of integer is to pick n as the smallest integer for which $[n/x]$ is valid for $\mathcal{M}(\phi_1)$. Note that such an integer always exists: we know that $\mathcal{M}(\phi_1)$ has a finite number of variables, so there exists $n \in \mathbf{N}$ which is not a variable of $\mathcal{M}(\phi_1)$. Having chosen such an n, we see from proposition (57) that $[n/x]$ is valid for $\mathcal{M}(\phi_1)$.

Definition 39 *Let V be a set with minimal extension $\bar{V}$. We call* minimal transform mapping on $\mathbf{P}(V)$ *the map $\mathcal{M} : \mathbf{P}(V) \to \mathbf{P}(\bar{V})$ defined by:*

$$\forall \phi \in \mathbf{P}(V) \ , \ \mathcal{M}(\phi) = \begin{cases} (x \in y) & \text{if} \quad \phi = (x \in y) \\ \bot & \text{if} \quad \phi = \bot \\ \mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2) & \text{if} \quad \phi = \phi_1 \to \phi_2 \\ \forall n \mathcal{M}(\phi_1)[n/x] & \text{if} \quad \phi = \forall x \phi_1 \end{cases} \tag{2.26}$$

where $n = \min\{k \in \mathbf{N} : [k/x]$ valid for $\mathcal{M}(\phi_1)\}$.

Given $\phi \in \mathbf{P}(V)$ we call $\mathcal{M}(\phi)$ the *minimal transform* of ϕ.

Proposition 96 *The structural recursion of* definition (38) *is legitimate.*

Proof
We need to prove that there exists a unique map $\mathcal{M} : \mathbf{P}(V) \to \mathbf{P}(\bar{V})$ which satisfies equation (2.26). We shall do so using theorem (4) or page 42. So take $X = \mathbf{P}(V)$, $X_0 = \mathbf{P}_0(V)$ and $A = \mathbf{P}(\bar{V})$. Define $g_0 : X_0 \to A$ by setting $g_0(x \in y) = (x \in y)$. Define $h(\perp) : A^0 \to A$ by setting $h(\perp)(0) = \perp$ and $h(\to) : A^2 \to A$ by setting $h(\to)(\phi_1, \phi_2) = \phi_1 \to \phi_2$. Finally, given $x \in V$, define $h(\forall x) : A^1 \to A$ by setting $h(\forall x)(\phi_1) = \forall n \phi_1[n/x]$ where:

$$n = n(\forall x)(\phi_1) = \min\{k \in \mathbf{N} : [k/x] \text{ valid for } \phi_1\}$$

Then applying theorem (4), there exists a unique map $\mathcal{M} : X \to A$ satisfying the following conditions: first we have $\mathcal{M}(x \in y) = g_0(x \in y) = (x \in y)$ which is the first line of equation (2.26). Next we have $\mathcal{M}(\perp) = h(\perp)(0) = \perp$ which is the second line. Next we have:

$$\mathcal{M}(\phi_1 \to \phi_2) = h(\to)(\mathcal{M}(\phi_1), \mathcal{M}(\phi_2)) = \mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2)$$

which is the third line. Finally, given $x \in V$ we have:

$$\mathcal{M}(\forall x \phi_1) = h(\forall x)(\mathcal{M}(\phi_1)) = \forall n \mathcal{M}(\phi_1)[n/x]$$

where $n = \min\{k \in \mathbf{N} : [k/x] \text{ valid for } \mathcal{M}(\phi_1)\}$ and this is the fourth line. **.**

The variables of the minimal transform $\mathcal{M}(\phi)$ are what we expect:

Proposition 97 *Let V be a set and $\phi \in \mathbf{P}(V)$. Then we have:*

$$\text{Fr}(\mathcal{M}(\phi)) = \text{Var}(\mathcal{M}(\phi)) \cap V = \text{Fr}(\phi) \tag{2.27}$$

where $\mathcal{M}(\phi) \in \mathbf{P}(\bar{V})$ is the minimal transform of $\phi \in \mathbf{P}(V)$.

Proof
We shall prove equation (2.27) with a structural induction argument, using theorem (3) of page 31. First we assume that $\phi = (x \in y)$ with $x, y \in V$. We need to show the equation is true for ϕ. However, we have $\mathcal{M}(\phi) = (x \in y)$ and consequently $\text{Fr}(\mathcal{M}(\phi)) = \{x, y\} = \text{Var}(\mathcal{M}(\phi))$. So the equation is clearly true. Next we assume that $\phi = \perp$. Then $\mathcal{M}(\phi) = \perp$ and $\text{Fr}(\mathcal{M}(\phi)) = \emptyset = \text{Var}(\mathcal{M}(\phi))$. So the equation is also clearly true. Next we assume that $\phi = \phi_1 \to \phi_2$ where the equation is true for $\phi_1, \phi_2 \in \mathbf{P}(V)$. We need to show the equation is also true for ϕ. On the one hand we have:

$$\begin{aligned}
\text{Var}(\mathcal{M}(\phi)) \cap V &= \text{Var}(\mathcal{M}(\phi_1 \to \phi_2)) \cap V \\
&= \text{Var}(\mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2)) \cap V \\
&= [\,\text{Var}(\mathcal{M}(\phi_1)) \cup \text{Var}(\mathcal{M}(\phi_2))\,] \cap V \\
&= [\text{Var}(\mathcal{M}(\phi_1)) \cap V] \cup [\text{Var}(\mathcal{M}(\phi_2)) \cap V] \\
&= \text{Fr}(\phi_1) \cup \text{Fr}(\phi_2) \\
&= \text{Fr}(\phi_1 \to \phi_2) \\
&= \text{Fr}(\phi)
\end{aligned}$$

and on the other hand:

$$\begin{aligned}
\mathrm{Fr}(\mathcal{M}(\phi)) &= \mathrm{Fr}(\mathcal{M}(\phi_1 \to \phi_2)) \\
&= \mathrm{Fr}(\mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2)) \\
&= \mathrm{Fr}(\mathcal{M}(\phi_1)) \cup \mathrm{Fr}(\mathcal{M}(\phi_2)) \\
&= \mathrm{Fr}(\phi_1) \cup \mathrm{Fr}(\phi_2) \\
&= \mathrm{Fr}(\phi_1 \to \phi_2) \\
&= \mathrm{Fr}(\phi)
\end{aligned}$$

So the equation is indeed true for $\phi = \phi_1 \to \phi_2$. Next we assume that $\phi = \forall x \phi_1$ where $x \in V$ and the equation is true for $\phi_1 \in \mathbf{P}(V)$. We need to show the equation is also true for ϕ. Since $\mathcal{M}(\phi) = \forall n \mathcal{M}(\phi_1)[n/x]$ for some $n \in \mathbf{N}$:

$$\begin{aligned}
\mathrm{Var}(\mathcal{M}(\phi)) \cap V &= \mathrm{Var}(\,\forall n \mathcal{M}(\phi_1)[n/x]\,) \cap V \\
&= (\,\{n\} \cup \mathrm{Var}(\,\mathcal{M}(\phi_1)[n/x]\,)\,) \cap V \\
V \cap \mathbf{N} = \emptyset \text{ in } \bar{V} \;\to\; &= \mathrm{Var}(\,\mathcal{M}(\phi_1)[n/x]\,) \cap V \\
&= \mathrm{Var}(\,[n/x](\,\mathcal{M}(\phi_1)\,)\,) \cap V \\
\text{prop. (35)} \;\to\; &= [n/x](\,\mathrm{Var}(\,\mathcal{M}(\phi_1)\,)\,) \cap V \\
[n/x](x) = n \notin V \;\to\; &= [n/x](\,\mathrm{Var}(\,\mathcal{M}(\phi_1)\,) \setminus \{x\}\,) \cap V \\
[n/x](u) = u \text{ if } u \neq x \;\to\; &= (\,\mathrm{Var}(\,\mathcal{M}(\phi_1)\,) \setminus \{x\}\,) \cap V \\
&= (\,\mathrm{Var}(\mathcal{M}(\phi_1)) \cap V\,) \setminus \{x\} \\
&= \mathrm{Fr}(\phi_1) \setminus \{x\} \\
&= \mathrm{Fr}(\forall x \phi_1) \\
&= \mathrm{Fr}(\phi)
\end{aligned}$$

Furthermore, since $[n/x]$ is valid for $\mathcal{M}(\phi_1)$, we have:

$$\begin{aligned}
\mathrm{Fr}(\mathcal{M}(\phi)) &= \mathrm{Fr}(\,\forall n \mathcal{M}(\phi_1)[n/x]\,) \\
&= \mathrm{Fr}(\,\mathcal{M}(\phi_1)[n/x]\,) \setminus \{n\} \\
&= \mathrm{Fr}(\,[n/x](\,\mathcal{M}(\phi_1)\,)\,) \setminus \{n\} \\
\text{prop. (52), } [n/x] \text{ valid for } \mathcal{M}(\phi_1) \;\to\; &= [n/x](\,\mathrm{Fr}(\,\mathcal{M}(\phi_1)\,)\,) \setminus \{n\} \\
[n/x](x) = n \;\to\; &= [n/x](\,\mathrm{Fr}(\,\mathcal{M}(\phi_1)\,) \setminus \{x\}\,) \setminus \{n\} \\
[n/x](u) = u \text{ if } u \neq x \;\to\; &= \mathrm{Fr}(\,\mathcal{M}(\phi_1)\,) \setminus \{x\} \setminus \{n\} \\
&= \mathrm{Fr}(\phi_1) \setminus \{x\} \setminus \{n\} \\
\mathrm{Fr}(\phi_1) \subseteq V,\, n \in \mathbf{N} \;\to\; &= \mathrm{Fr}(\phi_1) \setminus \{x\} \\
&= \mathrm{Fr}(\forall x \phi_1) \\
&= \mathrm{Fr}(\phi)
\end{aligned}$$

So we see that equation (2.27) is also true for $\phi = \forall x \phi_1$. **.**

Proposition 98 *Let V be a set and $\phi \in \mathbf{P}(V)$. Then we have:*

$$\mathrm{Bnd}(\mathcal{M}(\phi)) = \mathrm{Var}(\mathcal{M}(\phi)) \cap \mathbf{N} \tag{2.28}$$

where $\mathcal{M}(\phi) \in \mathbf{P}(\bar{V})$ is the minimal transform of $\phi \in \mathbf{P}(V)$.

Proof
We shall prove equation (2.28) with a structural induction argument, using theorem (3) of page 31. First we assume that $\phi = (x \in y)$ with $x, y \in V$. We need to show the equation is true for ϕ. However, we have $\mathcal{M}(\phi) = (x \in y)$ and consequently $\mathrm{Bnd}(\mathcal{M}(\phi)) = \emptyset = \mathrm{Var}(\mathcal{M}(\phi)) \cap \mathbf{N}$. So the equation is true. Next we assume that $\phi = \bot$. Then $\mathcal{M}(\phi) = \bot$ and $\mathrm{Bnd}(\mathcal{M}(\phi)) = \emptyset = \mathrm{Var}(\mathcal{M}(\phi))$. So the equation is also true. Next we assume that $\phi = \phi_1 \to \phi_2$ where the equation is true for $\phi_1, \phi_2 \in \mathbf{P}(V)$. We need to show it is also true for ϕ:

$$\begin{aligned}
\mathrm{Bnd}(\mathcal{M}(\phi)) &= \mathrm{Bnd}(\mathcal{M}(\phi_1 \to \phi_2)) \\
&= \mathrm{Bnd}(\mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2)) \\
&= \mathrm{Bnd}(\mathcal{M}(\phi_1)) \cup \mathrm{Bnd}(\mathcal{M}(\phi_2)) \\
&= (\mathrm{Var}(\mathcal{M}(\phi_1)) \cap \mathbf{N}) \cup (\mathrm{Var}(\mathcal{M}(\phi_2)) \cap \mathbf{N}) \\
&= (\,\mathrm{Var}(\mathcal{M}(\phi_1)) \cup \mathrm{Var}(\mathcal{M}(\phi_2))\,) \cap \mathbf{N} \\
&= \mathrm{Var}(\mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2)) \cap \mathbf{N} \\
&= \mathrm{Var}(\mathcal{M}(\phi_1 \to \phi_2)) \cap \mathbf{N} \\
&= \mathrm{Var}(\mathcal{M}(\phi)) \cap \mathbf{N}
\end{aligned}$$

So the equation is indeed true for $\phi = \phi_1 \to \phi_2$. Next we assume that $\phi = \forall x \phi_1$ where $x \in V$ and the equation is true for $\phi_1 \in \mathbf{P}(V)$. We need to show the equation is also true for ϕ. Since $\mathcal{M}(\phi) = \forall n \mathcal{M}(\phi_1)[n/x]$ for some $n \in \mathbf{N}$:

$$\begin{aligned}
\mathrm{Bnd}(\mathcal{M}(\phi)) &= \mathrm{Bnd}(\,\forall n \mathcal{M}(\phi_1)[n/x]\,) \\
&= \{n\} \cup \mathrm{Bnd}(\mathcal{M}(\phi_1)[n/x]) \\
&= \{n\} \cup \mathrm{Bnd}(\,[n/x](\mathcal{M}(\phi_1))\,) \\
\text{prop. (50)} \;\to\; &= \{n\} \cup [n/x](\,\mathrm{Bnd}(\mathcal{M}(\phi_1))\,) \\
[n/x](x) = n \;\to\; &= \{n\} \cup [n/x](\,\mathrm{Bnd}(\mathcal{M}(\phi_1)) \setminus \{x\}\,) \\
[n/x](u) = u \text{ if } u \neq x \;\to\; &= \{n\} \cup \mathrm{Bnd}(\mathcal{M}(\phi_1)) \setminus \{x\} \\
&= \{n\} \cup (\,\mathrm{Var}(\mathcal{M}(\phi_1)) \cap \mathbf{N}\,) \setminus \{x\} \\
&= (\,\{n\} \cup \mathrm{Var}(\mathcal{M}(\phi_1)) \setminus \{x\}\,) \cap \mathbf{N} \\
[n/x](u) = u \text{ if } u \neq x \;\to\; &= (\,\{n\} \cup [n/x](\,\mathrm{Var}(\mathcal{M}(\phi_1)) \setminus \{x\}\,)\,) \cap \mathbf{N} \\
[n/x](x) = n \;\to\; &= (\,\{n\} \cup [n/x](\,\mathrm{Var}(\mathcal{M}(\phi_1))\,)\,) \cap \mathbf{N} \\
\text{prop. (35)} \;\to\; &= (\,\{n\} \cup \mathrm{Var}(\,[n/x](\mathcal{M}(\phi_1))\,)\,) \cap \mathbf{N} \\
&= (\,\{n\} \cup \mathrm{Var}(\,\mathcal{M}(\phi_1)[n/x]\,)\,) \cap \mathbf{N} \\
&= \mathrm{Var}(\forall n \mathcal{M}(\phi_1)[n/x]) \cap \mathbf{N} \\
&= \mathrm{Var}(\mathcal{M}(\phi)) \cap \mathbf{N}
\end{aligned}$$

So we see that equation (2.28) is also true for $\phi = \forall x \phi_1$. **.**

Given $\phi \in \mathbf{P}(V)$ the minimal transform $\mathcal{M}(\phi)$ is an element of $\mathbf{P}(\bar{V})$. So it is difficult to argue that both formulas ϕ and $\mathcal{M}(\phi)$ are substitution equivalent

as they do not sit on the same space. However, if we consider the inclusion map $i : V \to \bar{V}$, it is possible to regard ϕ as an element of $\mathbf{P}(\bar{V})$ and ask whether both formulas are equivalent. Indeed, we have:

Proposition 99 *Let V be a set and $i : V \to \bar{V}$ be the inclusion map. We denote $\sim$ the substitution congruence on $\mathbf{P}(\bar{V})$. Then for all $\phi \in \mathbf{P}(V)$ we have:*

$$\mathcal{M}(\phi) \sim i(\phi)$$

Proof
We shall prove the equivalence $\mathcal{M}(\phi) \sim i(\phi)$ by a structural induction argument, using theorem (3) of page 31. First we assume that $\phi = (x \in y)$ for some $x, y \in V$. Then we have the equality $\mathcal{M}(\phi) = (x \in y) = i(\phi)$ and the equivalence is clear. Next we assume that $\phi = \bot$. Then we have $\mathcal{M}(\phi) = \bot = i(\phi)$ and the equivalence is also clear. So we assume that $\phi = \phi_1 \to \phi_2$ where $\phi_1, \phi_2 \in \mathbf{P}(V)$ satisfy the equivalence. Then we have:

$$\begin{array}{rcl} \mathcal{M}(\phi) & = & \mathcal{M}(\phi_1 \to \phi_2) \\ & = & \mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2) \\ & \sim & i(\phi_1) \to i(\phi_2) \\ & = & i(\phi_1 \to \phi_2) \\ & = & i(\phi) \end{array}$$

Finally we assume that $\phi = \forall x \phi_1$ where $x \in V$ and $\phi_1 \in \mathbf{P}(V)$ satisfies the equivalence. In this case we have:

$$\begin{array}{rcl} \mathcal{M}(\phi) & = & \mathcal{M}(\forall x \phi_1) \\ n = \min\{k : [k/x] \text{ valid for } \mathcal{M}(\phi_1)\} \to & = & \forall n \mathcal{M}(\phi_1)[n/x] \\ & = & [n/x](\forall x \mathcal{M}(\phi_1)) \\ \text{A: to be proved} \to & \sim & \forall x \mathcal{M}(\phi_1) \\ & \sim & \forall x\, i(\phi_1) \\ & = & \forall i(x)\, i(\phi_1) \\ & = & i(\forall x \phi_1) \\ & = & i(\phi) \end{array}$$

So it remains to show that $[n/x](\forall x \mathcal{M}(\phi_1)) \sim \forall x \mathcal{M}(\phi_1)$. Hence, from proposition (77) it is sufficient to prove that $[n/x]$ is an admissible substitution for $\forall x \mathcal{M}(\phi_1)$. We already know that $[n/x]$ is valid for $\mathcal{M}(\phi_1)$. Using proposition (55), given $u \in \mathrm{Fr}(\forall x \mathcal{M}(\phi_1))$, in order to prove that $[n/x]$ is valid for $\forall x \mathcal{M}(\phi_1)$ we need to show that $[n/x](u) \neq [n/x](x)$. So it is sufficient to show that $[n/x](u) \neq n$. Since $u \in \mathrm{Fr}(\forall x \mathcal{M}(\phi_1))$, in particular we have $u \neq x$. Hence, we have to show that $u \neq n$. Using proposition (97) we have:

$$u \in \mathrm{Fr}(\forall x \mathcal{M}(\phi_1)) \subseteq \mathrm{Fr}(\mathcal{M}(\phi_1)) \subseteq V$$

and consequently from $V \cap \mathbf{N} = \emptyset$ we conclude that $u \neq n$. In order to show that $[n/x]$ is an admissible substitution for $\forall x \mathcal{M}(\phi_1)$ it remains to prove that $[n/x](u) = u$ for all $u \in \mathrm{Fr}(\forall x \mathcal{M}(\phi_1))$, which follows from $u \neq x$. **.**

2.3.3 Minimal Transform and Valid Substitution

In the previous section, we hinted at the difficulty of defining the *evaluation* $\phi[a]$ when $\phi = \forall y(x \in y)$ and $a = y$. The issue is that the substitution $[y/x]$ is not valid for the formula ϕ (when $x \neq y$), making it impossible to write:

$$\forall a \in V \ , \ \phi[a] = \phi[a/x]$$

We defined the minimal transform mapping $\mathcal{M} : \mathbf{P}(V) \to \mathbf{P}(\bar{V})$ with this problem in mind. Now from definition (38), the minimal transform of ϕ is $\mathcal{M}(\phi) = \forall 0 \, (x \in 0)$ and it is clear that $[a/x]$ is now valid for $\mathcal{M}(\phi)$ for all $a \in V$. So it would be sensible to define:

$$\forall a \in V \ , \ \phi[a] = \mathcal{M}(\phi)[a/x]$$

Of course such a definition would lead to $\phi[a] = \forall 0 \, (a \in 0)$ which is an element of $\mathbf{P}(\bar{V})$ and not an element of $\mathbf{P}(V)$. So it may not be what we want, but we are certainly moving forward. More generally suppose $\phi \in \mathbf{P}(V)$ is an arbitrary formula and $\sigma : V \to W$ is an arbitrary map. We would like to define the formula $\sigma(\phi)$ in $\mathbf{P}(W)$ but in a way which is sensible, rather than following blindly the details of definition (24). The problem is that the substitution σ may not be valid for the formula ϕ. This doesn't mean we shouldn't be interested in $\sigma(\phi)$. In many cases we may only care about what happens to the free variables. Bound variables are not interesting. We do not mind having them moved around, provided the basic structure of the formula remains. So when σ is valid for ϕ, this is what happens when using $\sigma(\phi)$ as per definition (24). However when σ is not valid for ϕ, we need to find another way to move the free variables of ϕ without making a mess of it. So consider the minimal transform $\mathcal{M}(\phi)$. There is no longer any conflicts between the free and he bound variables. If $\sigma : V \to W$ is an arbitrary map, we can move the free variables of $\mathcal{M}(\phi)$ according to the substitution σ without creating nonsense. To make this idea precise, we define:

Definition 40 *Let V and W be sets. Let $\sigma : V \to W$ be a map. We call* minimal extension *of σ the map $\bar{\sigma} : \bar{V} \to \bar{W}$ defined by:*

$$\forall u \in \bar{V} \ , \ \bar{\sigma}(u) = \begin{cases} \sigma(u) & \text{if} \quad u \in V \\ u & \text{if} \quad u \in \mathbf{N} \end{cases}$$

where $\bar{V}$ and $\bar{W}$ are the minimal extensions of V and W respectively.

So the map $\bar{\sigma} : \bar{V} \to \bar{W}$ is the map moving the free variables of $\mathcal{M}(\phi)$ according to σ, without touching the bound variables. As expected we have:

Proposition 100 *Let $\sigma : V \to W$ be a map. Then for all $\phi \in \mathbf{P}(V)$ the minimal extension $\bar{\sigma} : \bar{V} \to \bar{W}$ is valid for the minimal transform $\mathcal{M}(\phi)$.*

Proof
We need to check the three properties of proposition (60) are met in relation

to $\bar{\sigma} : \bar{V} \to \bar{W}$ and $\mathcal{M}(\phi)$ with $V_0 = \mathbf{N}$. First we show property (i): we need to show that $\mathrm{Bnd}(\mathcal{M}(\phi)) \subseteq \mathbf{N}$ which follows from proposition (98). Next we show property (ii): we need to show that $\bar{\sigma}_{|\mathbf{N}}$ is injective which is clear from definition (39). We finally show property (iii): we need to show that $\bar{\sigma}(\mathbf{N}) \cap \bar{\sigma}(\mathrm{Var}(\mathcal{M}(\phi)) \setminus \mathbf{N}) = \emptyset$. This follows from $\bar{\sigma}(\mathbf{N}) \subseteq \mathbf{N}$ and $\bar{\sigma}(\mathrm{Var}(\mathcal{M}(\phi)) \setminus \mathbf{N}) \subseteq \bar{\sigma}(V) = \sigma(V) \subseteq W$, while $W \cap \mathbf{N} = \emptyset$. .

So here we are. Given $\phi \in \mathbf{P}(V)$ and an arbitrary map $\sigma : V \to W$ we cannot safely consider $\sigma(\phi)$ unless σ is valid for ϕ. However, there is no issues in looking at $\bar{\sigma} \circ \mathcal{M}(\phi)$ instead, since $\bar{\sigma}$ is always valid for $\mathcal{M}(\phi)$. Of course $\bar{\sigma} \circ \mathcal{M}(\phi)$ is an element of $\mathbf{P}(\bar{W})$ and not $\mathbf{P}(W)$. It is however a lot better to have a meaningful element of $\mathbf{P}(\bar{W})$, rather than a nonsensical formula $\sigma(\phi)$ of $\mathbf{P}(W)$. But what if σ was a valid substitution for ϕ? Then $\sigma(\phi)$ would be meaningful. There would not be much point in considering $\bar{\sigma} \circ \mathcal{M}(\phi)$ as a general scheme for substituting free variables, unless it coincided with $\sigma(\phi)$ in the particular case when σ is valid for ϕ. Since $\sigma(\phi) \in \mathbf{P}(W)$ while $\bar{\sigma} \circ \mathcal{M}(\phi) \in \mathbf{P}(\bar{W})$, we cannot expect these formulas to match. However, after we take the minimal transform $\mathcal{M} \circ \sigma(\phi)$ we should expect it to be equal to $\bar{\sigma} \circ \mathcal{M}(\phi)$. This is indeed the case, and is the object theorem (13) below. For now, we shall establish a couple of lemmas:

Lemma 10 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\phi = \forall x \phi_1$ where $\phi_1 \in \mathbf{P}(V)$ and $x \in V$ such that $\sigma(x) \notin \sigma(\mathrm{Fr}(\phi))$. Then for all $n \in \mathbf{N}$ we have:*

$$\bar{\sigma} \circ [n/x] \circ \mathcal{M}(\phi_1) = [n/\sigma(x)] \circ \bar{\sigma} \circ \mathcal{M}(\phi_1)$$

where $\bar{\sigma} : \bar{V} \to \bar{W}$ is the minimal extension of $\sigma : V \to W$.

Proof
Using proposition (36), we only need to show that the mappings $\bar{\sigma} \circ [n/x]$ and $[n/\sigma(x)] \circ \bar{\sigma}$ coincide on $\mathrm{Var}(\mathcal{M}(\phi_1))$. So let $u \in \mathrm{Var}(\mathcal{M}(\phi_1)) \subseteq \bar{V}$. We want:

$$\bar{\sigma} \circ [n/x](u) = [n/\sigma(x)] \circ \bar{\sigma}(u) \tag{2.29}$$

Since $\bar{V}$ is the disjoint union of V and $\mathbf{N}$, we shall distinguish two cases: first we assume that $u \in \mathbf{N}$. From $V \cap \mathbf{N} = \emptyset$ we obtain $u \neq x$ and consequently $\bar{\sigma} \circ [n/x](u) = \bar{\sigma}(u) = u$. From $W \cap \mathbf{N} = \emptyset$ we obtain $u \neq \sigma(x)$ and consequently $[n/\sigma(x)] \circ \bar{\sigma}(u) = [n/\sigma(x)](u) = u$. So equation (2.29) is indeed satisfied. Next we assume that $u \in V$. We shall distinguish two further cases: first we assume that $u = x$. Then $\bar{\sigma} \circ [n/x](u) = \bar{\sigma}(n) = n$ and $[n/\sigma(x)] \circ \bar{\sigma}(u) = [n/\sigma(x)](\sigma(x)) = n$ and we see that equation (2.29) is again satisfied. Next we assume that $u \neq x$. Then $\bar{\sigma} \circ [n/x](u) = \bar{\sigma}(u) = \sigma(u)$, and furthermore $[n/\sigma(x)] \circ \bar{\sigma}(u) = [n/\sigma(x)](\sigma(u))$. In order to establish equation (2.29), it is therefore sufficient to prove that $\sigma(u) \neq \sigma(x)$. However, since $u \in \mathrm{Var}(\mathcal{M}(\phi_1))$ and $u \in V$, it follows from proposition (97) that $u \in \mathrm{Fr}(\phi_1)$. Having assumed that $u \neq x$ we in fact have $u \in \mathrm{Fr}(\forall x \phi_1) = \mathrm{Fr}(\phi)$. Having assumed that $\sigma(x) \notin \sigma(\mathrm{Fr}(\phi))$ it follows that $\sigma(u) \neq \sigma(x)$ as requested. .

Lemma 11 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\phi = \forall x \phi_1$ where $\phi_1 \in \mathbf{P}(V)$ and $x \in V$ such that $\sigma(x) \notin \sigma(\mathrm{Fr}(\phi))$. Then for all $k \in \mathbf{N}$ we have:*

$$[k/x] \text{ valid for } \mathcal{M}(\phi_1) \;\Leftrightarrow\; [k/\sigma(x)] \text{ valid for } \bar{\sigma} \circ \mathcal{M}(\phi_1)$$

where $\bar{\sigma} : \bar{V} \to \bar{W}$ is the minimal extension of $\sigma : V \to W$.

Proof
First we show $\Leftarrow$: So we assume that $[k/\sigma(x)]$ is valid for $\bar{\sigma} \circ \mathcal{M}(\phi_1)$. We need to show that $[k/x]$ is valid for $\mathcal{M}(\phi_1)$. However, we know from proposition (100) that $\bar{\sigma}$ is valid for $\mathcal{M}(\phi_1)$. Hence, from the validity of $[k/\sigma(x)]$ for $\bar{\sigma} \circ \mathcal{M}(\phi_1)$ and proposition (58) we see that $[k/\sigma(x)] \circ \bar{\sigma}$ is valid for $\mathcal{M}(\phi_1)$. Furthermore, having assumed $\sigma(x) \notin \sigma(\mathrm{Fr}(\phi))$, we can use lemma (10) to obtain:

$$\bar{\sigma} \circ [k/x] \circ \mathcal{M}(\phi_1) = [k/\sigma(x)] \circ \bar{\sigma} \circ \mathcal{M}(\phi_1) \tag{2.30}$$

It follows from proposition (59) that $\bar{\sigma} \circ [k/x]$ is valid for $\mathcal{M}(\phi_1)$, and in particular, using proposition (58) once more, we conclude that $[k/x]$ is valid for $\mathcal{M}(\phi_1)$ as requested. We now show $\Rightarrow$: so we assume that $[k/x]$ is valid for $\mathcal{M}(\phi_1)$. We need to show that $[k/\sigma(x)]$ is valid for $\bar{\sigma} \circ \mathcal{M}(\phi_1)$. However, from proposition (58) it is sufficient to prove that $[k/\sigma(x)] \circ \bar{\sigma}$ is valid for $\mathcal{M}(\phi_1)$. Using equation (2.30) and proposition (59) once more, we simply need to show that $\bar{\sigma} \circ [k/x]$ is valid for $\mathcal{M}(\phi_1)$. Having assumed that $[k/x]$ is valid for $\mathcal{M}(\phi_1)$, from proposition (58) it is sufficient to show that $\bar{\sigma}$ is valid for $[k/x] \circ \mathcal{M}(\phi_1)$. We shall do so with an application of proposition (60) to $V_0 = \mathbf{N}$. First we need to check that $\mathrm{Bnd}(\, [k/x] \circ \mathcal{M}(\phi_1)\,) \subseteq \mathbf{N}$. However, from proposition (50) we have $\mathrm{Bnd}(\, [k/x] \circ \mathcal{M}(\phi_1)\,) = [k/x](\, \mathrm{Bnd}(\mathcal{M}(\phi_1))\,)$ and from proposition (98) we have $\mathrm{Bnd}(\mathcal{M}(\phi_1)) \subseteq \mathbf{N}$. So the desired inclusion follows. Next we need to show that $\bar{\sigma}_{|\mathbf{N}}$ is injective which is clear from definition (39). Finally, we need to check that $\bar{\sigma}(\mathbf{N}) \cap \bar{\sigma}(\, \mathrm{Var}([k/x] \circ \mathcal{M}(\phi_1)) \setminus \mathbf{N}\,) = \emptyset$. This follows from $\bar{\sigma}(\mathbf{N}) \subseteq \mathbf{N}$ and $\bar{\sigma}(\, \mathrm{Var}([k/x] \circ \mathcal{M}(\phi_1)) \setminus \mathbf{N}\,) \subseteq \bar{\sigma}(V) = \sigma(V) \subseteq W$, while $W \cap \mathbf{N} = \emptyset$. **.**

Theorem 13 *Let V and W be sets. Let $\sigma : V \to W$ be a map. Let $\phi \in \mathbf{P}(V)$. If σ is valid for ϕ, then it commutes with minimal transforms, specifically:*

$$\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M} \circ \sigma(\phi) \tag{2.31}$$

where $\bar{\sigma} : \bar{V} \to \bar{W}$ is the minimal extension of $\sigma : V \to W$.

Proof
Before we start, it should be noted that σ in equation (2.31) refers to the substitution mapping $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ while the $\mathcal{M}$ on the right-hand-side refers to the minimal transform mapping $\mathcal{M} : \mathbf{P}(W) \to \mathbf{P}(\bar{W})$. The other $\mathcal{M}$ which appears on the left-hand-side refers to the minimal transform mapping $\mathcal{M} : \mathbf{P}(V) \to \mathbf{P}(\bar{V})$, and $\bar{\sigma}$ is the substitution mapping $\bar{\sigma} : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{W})$. So everything makes sense. For all $\phi \in \mathbf{P}(V)$, we need to show the property:

$$(\sigma \text{ valid for } \phi) \;\Rightarrow\; \bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M} \circ \sigma(\phi)$$

We shall do so by structural induction using theorem (3) of page 31. First we assume that $\phi = (x \in y)$ where $x, y \in V$. Then any σ is valid for ϕ and we need to show equation (2.31). This goes as follows:

$$\begin{aligned}
\bar{\sigma} \circ \mathcal{M}(\phi) &= \bar{\sigma} \circ \mathcal{M}(x \in y) \\
&= \bar{\sigma}(x \in y) \\
&= \bar{\sigma}(x) \in \bar{\sigma}(y) \\
&= \sigma(x) \in \sigma(y) \\
&= \mathcal{M}(\sigma(x) \in \sigma(y)) \\
&= \mathcal{M}(\sigma(x \in y)) \\
&= \mathcal{M} \circ \sigma(x \in y) \\
&= \mathcal{M} \circ \sigma(\phi)
\end{aligned}$$

Next we assume that $\phi = \bot$. Then we have $\bar{\sigma} \circ \mathcal{M}(\phi) = \bot = \mathcal{M} \circ \sigma(\phi)$ and the property is also true. Next we assume that $\phi = \phi_1 \to \phi_2$ where the property is true for $\phi_1, \phi_2 \in \mathbf{P}(V)$. We need to show the property is also true for ϕ. So we assume that σ is valid for ϕ. We need to show equation (2.31) holds for ϕ. However, from proposition (54), the substitution σ is valid for both ϕ_1 and ϕ_2. Having assumed the property is true for ϕ_1 and ϕ_2, it follows that equation (2.31) holds for ϕ_1 and ϕ_2. Hence, we have:

$$\begin{aligned}
\bar{\sigma} \circ \mathcal{M}(\phi) &= \bar{\sigma} \circ \mathcal{M}(\phi_1 \to \phi_2) \\
&= \bar{\sigma}(\mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2)) \\
&= \bar{\sigma}(\mathcal{M}(\phi_1)) \to \bar{\sigma}(\mathcal{M}(\phi_2)) \\
&= \mathcal{M}(\sigma(\phi_1)) \to \mathcal{M}(\sigma(\phi_2)) \\
&= \mathcal{M}(\sigma(\phi_1) \to \sigma(\phi_2)) \\
&= \mathcal{M}(\sigma(\phi_1 \to \phi_2)) \\
&= \mathcal{M} \circ \sigma(\phi)
\end{aligned}$$

Finally we assume that $\phi = \forall x \phi_1$ where $x \in V$ and the property is true for $\phi_1 \in \mathbf{P}(V)$. We need to show the property is also true for ϕ. So we assume that σ is valid for ϕ. We need to show equation (2.31) holds for ϕ. However, from proposition (55), the substitution σ is also valid for ϕ_1. Having assumed the property is true for ϕ_1, it follows that equation (2.31) holds for ϕ_1. Hence:

$$\begin{aligned}
\bar{\sigma} \circ \mathcal{M}(\phi) &= \bar{\sigma} \circ \mathcal{M}(\forall x \phi_1) \\
n = \min\{k : [k/x] \text{ valid for } \mathcal{M}(\phi_1)\} \ \to \ &= \bar{\sigma}(\, \forall n \mathcal{M}(\phi_1)[n/x]\,) \\
&= \forall \bar{\sigma}(n) \bar{\sigma}(\, \mathcal{M}(\phi_1)[n/x]\,) \\
&= \forall n\, \bar{\sigma} \circ [n/x] \circ \mathcal{M}(\phi_1) \\
\text{A: to be proved} \ \to \ &= \forall n\, [n/\sigma(x)] \circ \bar{\sigma} \circ \mathcal{M}(\phi_1) \\
&= \forall n\, [n/\sigma(x)] \circ \mathcal{M} \circ \sigma(\phi_1) \\
&= \forall n\, \mathcal{M}[\sigma(\phi_1)][n/\sigma(x)]
\end{aligned}$$

$$\begin{array}{rcl} \text{B: to be proved } \rightarrow & = & \forall m\, \mathcal{M}[\sigma(\phi_1)][m/\sigma(x)] \\ m = \min\{k : [k/\sigma(x)] \text{ valid for } \mathcal{M}[\sigma(\phi_1)]\} \rightarrow & = & \mathcal{M}(\forall\sigma(x)\sigma(\phi_1)) \\ & = & \mathcal{M}(\sigma(\forall x\phi_1)) \\ & = & \mathcal{M}\circ\sigma(\phi) \end{array}$$

So we have two more points A and B to justify. First we deal with point A. It is sufficient for us to prove the equality:

$$\bar{\sigma}\circ[n/x]\circ\mathcal{M}(\phi_1) = [n/\sigma(x)]\circ\bar{\sigma}\circ\mathcal{M}(\phi_1)$$

Using lemma (10) it is sufficient to show that $\sigma(x) \notin \sigma(\mathrm{Fr}(\phi))$. So suppose to the contrary that $\sigma(x) \in \sigma(\mathrm{Fr}(\phi))$. Then there exists $u \in \mathrm{Fr}(\phi)$ such that $\sigma(u) = \sigma(x)$. This contradicts proposition (55) and the fact that σ is valid for ϕ, which completes the proof of point A. So we now turn to point B. We need to prove that $n = m$, for which it is sufficient to show the equivalence:

$$[k/x] \text{ valid for } \mathcal{M}(\phi_1) \;\Leftrightarrow\; [k/\sigma(x)] \text{ valid for } \mathcal{M}[\sigma(\phi_1)]$$

This follows from lemma (11) and the fact that $\sigma(x) \notin \sigma(\mathrm{Fr}(\phi))$, together with the induction hypothesis $\bar{\sigma}\circ\mathcal{M}(\phi_1) = \mathcal{M}\circ\sigma(\phi_1)$. .

2.3.4 Minimal Transform and Substitution Congruence

Let $\phi = \forall x\forall y(x \in y)$ and $\psi = \forall y\forall x(y \in x)$, where $x \neq y$. We know that $\phi \sim \psi$ where $\sim$ denotes the substitution congruence on $\mathbf{P}(V)$. The quickest way to see this is to define $\phi_1 = \forall y(x \in y)$ and argue using definition (35) of page 123 that $\phi = \forall x\phi_1$ while $\psi = \forall y\phi_1[y:x]$ with $y \notin \mathrm{Fr}(\phi_1)$. If we now look at minimal transforms, since $\mathcal{M}(\phi_1) = \forall\, 0\,(x \in 0)$ and $\mathcal{M}(\phi_1[y:x]) = \forall\, 0\,(y \in 0)$ we obtain:

$$\mathcal{M}(\phi) = \forall\, 1\forall\, 0\,(1 \in 0) = \mathcal{M}(\psi)$$

So here is a case of two equivalent formulas with identical minimal transforms. Of course, this is hardly surprising. We designed the minimal transform so as to replace the bound variables with a unique and sensible choice. In fact, we should expect the equality $\mathcal{M}(\phi) = \mathcal{M}(\psi)$ to hold whenever $\phi \sim \psi$. Conversely, suppose $\chi \in \mathbf{P}(V)$ is a formula with minimal transform:

$$\mathcal{M}(\chi) = \forall\, 1\forall\, 0\,(1 \in 0)$$

It is hard to imagine a formula χ which is not equivalent to ϕ and ψ. It seems pretty obvious that χ would need to be of the form $\chi = \forall u\forall v(u \in v)$ and it would not be possible to have $u = v$. Hence:

$$\chi = \forall u\forall v(u \in v) \sim \forall u\forall y(u \in y) \sim \forall x\forall y(x \in y) = \phi$$

The main theorem of this section will show that $\phi \sim \psi$ is indeed equivalent to $\mathcal{M}(\phi) = \mathcal{M}(\psi)$. As a preamble, we shall prove:

Proposition 101 *Let V be a set and $\equiv$ be the relation on $\mathbf{P}(V)$ defined by:*

$$\phi \equiv \psi \;\Leftrightarrow\; \mathcal{M}(\phi) = \mathcal{M}(\psi)$$

for all $\phi, \psi \in \mathbf{P}(V)$. Then $\equiv$ is a congruence on $\mathbf{P}(V)$.

Proof
The relation $\equiv$ is clearly reflexive, symmetric and transitive. So it is an equivalence relation on $\mathbf{P}(V)$ and we simply need to prove that it is a congruent relation, as per definition (15) of page 49. We already know that $\bot \equiv \bot$. So let $\phi = \phi_1 \to \phi_2$ and $\psi = \psi_1 \to \psi_2$ where $\phi_1 \equiv \psi_1$ and $\phi_2 \equiv \psi_2$. We need to show that $\phi \equiv \psi$. This goes as follows:

$$\begin{array}{rcl} \mathcal{M}(\phi) & = & \mathcal{M}(\phi_1 \to \phi_2) \\ & = & \mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2) \\ (\phi_1 \equiv \psi_1) \wedge (\phi_2 \equiv \psi_2) \;\to & = & \mathcal{M}(\psi_1) \to \mathcal{M}(\psi_2) \\ & = & \mathcal{M}(\psi_1 \to \psi_2) \\ & = & \mathcal{M}(\psi) \end{array}$$

Next we assume that $\phi = \forall x \phi_1$ and $\psi = \forall x \psi_1$ where $x \in V$ and $\phi_1 \equiv \psi_1$. We need to show that $\phi \equiv \psi$. This goes as follows:

$$\begin{array}{rcl} \mathcal{M}(\phi) & = & \mathcal{M}(\forall x \phi_1) \\ n = \min\{k : [k/x] \text{ valid for } \mathcal{M}(\phi_1)\} \;\to & = & \forall n \mathcal{M}(\phi_1)[n/x] \\ \phi_1 \equiv \psi_1 \;\to & = & \forall n \mathcal{M}(\psi_1)[n/x] \\ \phi_1 \equiv \psi_1 \;\to & = & \forall m \mathcal{M}(\psi_1)[m/x] \\ m = \min\{k : [k/x] \text{ valid for } \mathcal{M}(\psi_1)\} \;\to & = & \mathcal{M}(\forall x \psi_1) \\ & = & \mathcal{M}(\psi) \end{array}$$

.

Theorem 14 *Let $\sim$ be the substitution congruence on $\mathbf{P}(V)$ where V is a set. Then for all $\phi, \psi \in \mathbf{P}(V)$ we have the equivalence:*

$$\phi \sim \psi \;\Leftrightarrow\; \mathcal{M}(\phi) = \mathcal{M}(\psi)$$

where $\mathcal{M}(\phi)$ and $\mathcal{M}(\psi)$ are the minimal transforms as per definition (38).

Proof
First we show $\Rightarrow$: consider the relation $\equiv$ on $\mathbf{P}(V)$ defined by $\phi \equiv \psi$ if and only if $\mathcal{M}(\phi) = \mathcal{M}(\psi)$. We need to show the inclusion $\sim \subseteq \equiv$. However, we know from proposition (101) that $\equiv$ is a congruence on $\mathbf{P}(V)$ and furthermore from proposition (78) that $\sim$ is generated by the set:

$$R_1 = \{\, (\, \phi\, ,\, \sigma(\phi)\,) : \phi \in \mathbf{P}(V)\ ,\ \sigma : V \to V \text{ admissible for } \phi\}$$

It is therefore sufficient to prove the inclusion $R_1 \subseteq \equiv$. So let $\sigma : V \to V$ be an admissible substitution for ϕ as per definition (34) of page 122. We need to

show that $\phi \equiv \sigma(\phi)$, i.e. that $\mathcal{M}(\phi) = \mathcal{M} \circ \sigma(\phi)$. Let $\bar{\sigma} : \bar{V} \to \bar{V}$ be the minimal extension of σ as per definition (39) of page 144. Since σ is admissible for ϕ, in particular σ is valid for ϕ. So we can apply theorem (13) of page 146 from which we obtain $\mathcal{M} \circ \sigma(\phi) = \bar{\sigma} \circ \mathcal{M}(\phi)$. It is therefore sufficient to prove that $\mathcal{M}(\phi) = \bar{\sigma} \circ \mathcal{M}(\phi)$. Let $i : \bar{V} \to \bar{V}$ be the identity mapping. We need to show that $i \circ \mathcal{M}(\phi) = \bar{\sigma} \circ \mathcal{M}(\phi)$ and from proposition (36) it is sufficient to prove that i and $\bar{\sigma}$ coincide on $\mathrm{Var}(\mathcal{M}(\phi))$. So let $u \in \mathrm{Var}(\mathcal{M}(\phi))$. We need to show that $\bar{\sigma}(u) = u$. Since $\bar{V}$ is the disjoint union of V and $\mathbf{N}$, we shall distinguish two cases: first we assume that $u \in \mathbf{N}$. Then $\bar{\sigma}(u) = u$ is immediate from definition (39). Next we assume that $u \in V$. Then from $u \in \mathrm{Var}(\mathcal{M}(\phi))$ and proposition (97) it follows that $u \in \mathrm{Fr}(\phi)$. Having assumed that σ is admissible for ϕ we conclude that $\bar{\sigma}(u) = \sigma(u) = u$ as requested. We now prove $\Leftarrow$: we need to show that every $\phi \in \mathbf{P}(V)$ satisfies the property:

$$\forall \psi \in \mathbf{P}(V) \ , \ [\, \mathcal{M}(\phi) = \mathcal{M}(\psi) \ \Rightarrow \ \phi \sim \psi \,]$$

We shall do so by a structural induction argument using theorem (3) of page 31. First we assume that $\phi = (x \in y)$ for some $x, v \in V$. Let $\psi \in \mathbf{P}(V)$ such that $\mathcal{M}(\phi) = (x \in y) = \mathcal{M}(\psi)$. We need to show that $\phi \sim \psi$. So it is sufficient to prove that $\phi = \psi$. From theorem (2) of page 21 the formula ψ can be of one and only one of four types: first it can be of the form $\psi = (u \in v)$ for some $u, v \in V$. Next, it can be of the form $\psi = \bot$, and possibly of the form $\psi = \psi_1 \to \psi_2$ with $\psi_1, \psi_2 \in \mathbf{P}(V)$. Finally, it can be of the form $\psi = \forall u \psi_1$ for some $u \in V$ and $\psi_1 \in \mathbf{P}(V)$. Looking at definition (38) we see that the minimal transform $\mathcal{M}(\psi)$ has the same basic structure as ψ. Thus, from the equality $\mathcal{M}(\psi) = (x \in y)$ it follows that ψ can only be of the form $\psi = (u \in v)$. So we obtain $\mathcal{M}(\psi) = (u \in v) = (x \in y)$ and consequently $u = x$ and $v = y$ which implies that $\psi = (x \in y) = \phi$ as requested. We now assume that $\phi = \bot$. Let $\psi \in \mathbf{P}(V)$ such that $\mathcal{M}(\phi) = \bot = \mathcal{M}(\psi)$. We need to show that $\phi \sim \psi$. Once again it is sufficient to prove that $\phi = \psi$. From $\mathcal{M}(\psi) = \bot$ we see that ψ can only be of the form $\psi = \bot$. So $\phi = \psi$ as requested. We now assume that $\phi = \phi_1 \to \phi_2$ where $\phi_1, \phi_2 \in \mathbf{P}(V)$ satisfy our property. We need to show the same if true of ϕ. So let $\psi \in \mathbf{P}(V)$ such that $\mathcal{M}(\phi) = \mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2) = \mathcal{M}(\psi)$. We need to show that $\phi \sim \psi$. From $\mathcal{M}(\psi) = \mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2)$ we see that ψ can only be of the form $\psi = \psi_1 \to \psi_2$. It follows that $\mathcal{M}(\psi) = \mathcal{M}(\psi_1) \to \mathcal{M}(\psi_2)$ and consequently we obtain $\mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2) = \mathcal{M}(\psi_1) \to \mathcal{M}(\psi_2)$. Thus, using theorem (2) of page 21 we have $\mathcal{M}(\phi_1) = \mathcal{M}(\psi_1)$ and $\mathcal{M}(\phi_2) = \mathcal{M}(\psi_2)$. Having assumed ϕ_1 and ϕ_2 satisfy our induction property, it follows that $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$ and consequently $\phi_1 \to \phi_2 \sim \psi_1 \to \psi_2$. So we have proved that $\phi \sim \psi$ as requested. We now assume that $\phi = \forall x \phi_1$ where $x \in V$ and $\phi_1 \in \mathbf{P}(V)$ satisfy our property. We need to show the same is true of ϕ. So let $\psi \in \mathbf{P}(V)$ such that $\mathcal{M}(\phi) = \mathcal{M}(\psi)$. We need to show that $\phi \sim \psi$. We have:

$$\mathcal{M}(\phi) = \forall n \mathcal{M}(\phi_1)[n/x] \tag{2.32}$$

where $n = \min\{k \in \mathbf{N} : [k/x] \text{ valid for } \mathcal{M}(\phi_1)\}$. Hence from the equality $\mathcal{M}(\phi) = \mathcal{M}(\psi)$ we see that ψ can only be of the form $\psi = \forall y \psi_1$ for some $y \in V$

and $\psi_1 \in \mathbf{P}(V)$. We shall distinguish two cases: first we assume that $y = x$. Then we need to show that $\forall x\phi_1 \sim \forall x\psi_1$ and it is therefore sufficient to prove that $\phi_1 \sim \psi_1$. Having assumed ϕ_1 satisfy our property, we simply need to show that $\mathcal{M}(\phi_1) = \mathcal{M}(\psi_1)$. However we have the equality:

$$\mathcal{M}(\psi) = \forall m\mathcal{M}(\psi_1)[m/x] \tag{2.33}$$

where $m = \min\{k \in \mathbf{N} : [k/x] \text{ valid for } \mathcal{M}(\psi_1)\}$. Comparing (2.32) and (2.33), from $\mathcal{M}(\phi) = \mathcal{M}(\psi)$ and theorem (2) of page 21 we obtain $n = m$ and thus:

$$\mathcal{M}(\phi_1)[n/x] = \mathcal{M}(\psi_1)[n/x] \tag{2.34}$$

Consider the substitution $\sigma : \bar{V} \to \bar{V}$ defined by $\sigma = [n/x]$. We shall conclude that $\mathcal{M}(\phi_1) = \mathcal{M}(\psi_1)$ by inverting equation (2.34) using the local inversion theorem (10) of page 105 on the substitution σ. So consider the sets $V_0 = V$ and $V_1 = \mathbf{N}$. It is clear that both $\sigma_{|V_0}$ and $\sigma_{|V_1}$ are injective maps. Define:

$$\Gamma = \{\chi \in \mathbf{P}(\bar{V}) : (\mathrm{Fr}(\chi) \subseteq V_0) \wedge (\mathrm{Bnd}(\chi) \subseteq V_1) \wedge (\sigma \text{ valid for } \chi)\}$$

Then using theorem (10) there exits $\tau : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{V})$ such that $\tau \circ \sigma(\chi) = \chi$ for all $\chi \in \Gamma$. Hence from equation (2.34) it is sufficient to prove that $\mathcal{M}(\phi_1) \in \Gamma$ and $\mathcal{M}(\psi_1) \in \Gamma$. First we show that $\mathcal{M}(\phi_1) \in \Gamma$. We already know that $\sigma = [n/x]$ is a valid substitution for $\mathcal{M}(\phi_1)$. The fact that $\mathrm{Fr}(\mathcal{M}(\phi_1)) \subseteq V_0$ follows from proposition (97). The fact that $\mathrm{Bnd}(\mathcal{M}(\phi_1)) \subseteq V_1$ follows from proposition (98). So we have proved that $\mathcal{M}(\phi_1) \in \Gamma$ as requested. The proof of $\mathcal{M}(\psi_1) \in \Gamma$ is identical, which completes our proof of $\phi \sim \psi$ in the case when $\psi = \forall y\psi_1$ and $y = x$. We now assume that $y \neq x$. Consider the formula $\psi^* = \forall x\psi_1[x:y]$ where $[x:y]$ is the permutation mapping as per definition (27) of page 79. Suppose we have proved the equivalence $\psi \sim \psi^*$. Then in order to prove $\phi \sim \psi$ it is sufficient by transitivity to show that $\phi \sim \psi^*$. However, having already proved the implication $\Rightarrow$ of this theorem, we know that $\psi \sim \psi^*$ implies $\mathcal{M}(\psi) = \mathcal{M}(\psi^*)$. Hence, if we have $\psi \sim \psi^*$, it is sufficient to prove $\phi \sim \psi^*$ knowing that $\mathcal{M}(\phi) = \mathcal{M}(\psi^*)$ and $\psi^* = \forall x\psi_1^*$ where $\psi_1^* = \psi_1[x:y]$. So we are back to the case when $y = x$, a case we have already dealt with. It follows that we can complete our induction argument simply by showing $\psi \sim \psi^*$. Since $\psi = \forall y\psi_1$ and $\psi^* = \forall x\psi_1[x:y]$ with $x \neq y$, from definition (35) of page 123 we simply need to check that $x \notin \mathrm{Fr}(\psi_1)$. So suppose to the contrary that $x \in \mathrm{Fr}(\psi_1)$. Since $x \neq y$ we obtain $x \in \mathrm{Fr}(\psi)$. From proposition (97) it follows that $x \in \mathrm{Fr}(\mathcal{M}(\psi))$. Having assumed that $\mathcal{M}(\phi) = \mathcal{M}(\psi)$ we obtain $x \in \mathrm{Fr}(\mathcal{M}(\phi))$ and finally using proposition (97) once more, we obtain $x \in \mathrm{Fr}(\phi)$. This is our desired contradiction since $\phi = \forall x\phi_1$. .

We conclude this section with an immediate consequence of theorem (13) of page 146 and theorem (14). From proposition (81) we know that $\sigma(\phi) \sim \sigma(\psi)$ follows from $\phi \sim \psi$ whenever $\sigma : V \to W$ is injective. We can now loosen the hypothesis by requiring that σ be simply valid for ϕ and ψ. Note that this result is not true if $\sim$ denotes the strong substitution congruence rather than the substitution congruence. Take $V = \{x, y, z\}$ and $W = \{x, y\}$ with x, y, z distinct and $\phi = \forall x\forall y(x \in y)$ while $\psi = \forall y\forall x(y \in x)$ with $\sigma(x) = x$ and $\sigma(y) = y$. Then σ is valid for ϕ and ψ but $\sigma(\phi) \sim \sigma(\psi)$ fails to be true.

Theorem 15 *Let V and W be sets and $\sigma : V \to W$ be a map. Let $\sim$ be the substitution congruence on $\mathbf{P}(V)$ and $\mathbf{P}(W)$. Then if σ is valid for ϕ and ψ:*

$$\phi \sim \psi \;\Rightarrow\; \sigma(\phi) \sim \sigma(\psi)$$

for all $\phi, \psi \in \mathbf{P}(V)$, where $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is also the substitution mapping.

Proof
We assume that $\phi \sim \psi$ and $\sigma : V \to W$ is valid for ϕ and ψ. We need to show that $\sigma(\phi) \sim \sigma(\psi)$. Using theorem (14) it is sufficient to prove that $\mathcal{M} \circ \sigma(\phi) = \mathcal{M} \circ \sigma(\psi)$. Since σ is valid for ϕ and ψ, using theorem (13) of page 146 it is therefore sufficient to prove that $\bar{\sigma} \circ \mathcal{M}(\phi) = \bar{\sigma} \circ \mathcal{M}(\psi)$, which follows immediately from $\mathcal{M}(\phi) = \mathcal{M}(\psi)$, itself a consequence of $\phi \sim \psi$. **.**

2.3.5 Isomorphic Representation Modulo Substitution

One of our goals in defining the minimal transform mapping $\mathcal{M} : \mathbf{P}(V) \to \mathbf{P}(\bar{V})$ in page 139 was to design an algebra $\mathbf{Q}(V)$ where the free and bound variables would be chosen from different sets. We now pursue this idea further. Given a set V, we defined the minimal extension $\bar{V}$ by adding to V a disjoint copy of $\mathbf{N}$, giving us plenty of bound variables to choose from. Unfortunately in spite of this, the free algebra $\mathbf{P}(\bar{V})$ is not very interesting to us, as it contains too many formulas, including those such as $\phi = \forall x(0 \in x)$ which contravene our desired convention of keeping free variables in V and bound variables in $\mathbf{N}$. So we need to restrict our attention to a smaller subset of $\mathbf{P}(\bar{V})$ and the obvious choice is to pick $\mathbf{Q}(V) = \mathcal{M}(\mathbf{P}(V))$ i.e. to choose $\mathbf{Q}(V)$ as the range of the minimal transform mapping. From proposition (97) and proposition (98) this guarantees all formulas have free variables in V and bound variables in $\mathbf{N}$. So we have the right set of formulas. However $\mathbf{Q}(V)$ is not yet an algebra, as it is not a universal sub-algebra of $\mathbf{P}(\bar{V})$. Indeed, given $x \in V$ and $\phi \in \mathbf{Q}(V)$, the formula $\forall x\phi$ is not an element of $\mathbf{Q}(V)$. Somehow we would like $\mathbf{Q}(V)$ to be an algebra. But of which type? The free universal algebras $\mathbf{P}(V)$ and $\mathbf{P}(\bar{V})$ do not have the same type. The algebra $\mathbf{P}(\bar{V})$ has many more quantification operators $\forall n$ for $n \in \mathbf{N}$ which $\mathbf{P}(V)$ does not have. So what do we want for $\mathbf{Q}(V)$? All elements of $\mathbf{Q}(V)$ have free variables in V. It does not add any value to quantify a formula with respect to a variable which is not free. So it is clear the unary operators $\forall n$ for $n \in \mathbf{N}$ should not be part of $\mathbf{Q}(V)$, and $\mathbf{Q}(V)$ should be of the same type of universal algebra as $\mathbf{P}(V)$. So let's endow $\mathbf{Q}(V)$ with the appropriate structure of universal algebra: First we need an operator $\perp : \mathbf{Q}(V)^0 \to \mathbf{Q}(V)$. Since $\perp = \mathcal{M}(\perp) \in \mathbf{Q}(V)$ we should keep the structure induced by $\mathbf{P}(\bar{V})$ and define $\perp(0) = \perp \in \mathbf{Q}(V)$. Next we need a binary operator $\to : \mathbf{Q}(V)^2 \to \mathbf{Q}(V)$. Since for all $\phi_1, \phi_2 \in \mathbf{P}(V)$, we have:

$$\mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2) = \mathcal{M}(\phi_1 \to \phi_2)$$

we see that $\mathbf{Q}(V)$ is closed under the operator $\to$ of $\mathbf{P}(\bar{V})$. So we should keep that too. Finally given $x \in V$, we need a unary operator $\forall \mathbf{x} : \mathbf{Q}(V)^1 \to \mathbf{Q}(V)$.

In this case the operator $\forall x$ of $\mathbf{P}(\bar{V})$ is not suitable for our purpose, as $\mathbf{Q}(V)$ is not closed under $\forall x$. So we need to define a new operator which we denote $\forall \mathbf{x}$ (with the letter $\mathbf{x}$ in bold) to avoid any possible confusion. Let us pick:

$$\forall \phi \in \mathbf{Q}(V) \ , \ \forall \mathbf{x} \phi = \forall n \phi[n/x] \tag{2.35}$$

where $n = \min\{k \in \mathbf{N} : [k/x] \text{ valid for } \phi\}$ and the $\forall n$ on the right-hand-side of equation (2.35) is the usual quantification operator of $\mathbf{P}(\bar{V})$. We need to check that this definition does indeed yield an operator $\forall \mathbf{x} : \mathbf{Q}(V)^1 \to \mathbf{Q}(V)$, specifically that $\forall \mathbf{x} \phi \in \mathbf{Q}(V)$ for all $\phi \in \mathbf{Q}(V)$. So let $\phi \in \mathbf{Q}(V)$. There exists $\phi_1 \in \mathbf{P}(V)$ such that $\phi = \mathcal{M}(\phi_1)$ and consequently we have:

$$\forall \mathbf{x} \phi = \forall n \phi[n/x] = \forall n \mathcal{M}(\phi_1)[n/x] = \mathcal{M}(\forall x \phi_1) \in \mathbf{Q}(V)$$

where the last equality follows from definition (38) and:

$$n = \min\{k \in \mathbf{N} : [k/x] \text{ valid for } \mathcal{M}(\phi_1)\}$$

So $\mathbf{Q}(V)$ is now a universal algebra of the same type as $\mathbf{P}(V)$ which is what we set out to achieve. Note that this algebra is not free in general since:

$$\forall \mathbf{x} \forall \mathbf{y} (x \in y) = \forall 1 \forall 0 \, (1 \in 0) = \forall \mathbf{y} \forall \mathbf{x} (y \in x)$$

whenever x and y are two distinct elements of V. This contradicts the uniqueness principle of theorem (2) of page 21 which prevails in free universal algebras.

Definition 41 *Let V be a set with first order logic type α. We call* minimal transform algebra *associated with V, the universal algebra $\mathbf{Q}(V)$ of type α:*

$$\mathbf{Q}(V) = \mathcal{M}(\mathbf{P}(V)) \subseteq \mathbf{P}(\bar{V})$$

where $\mathcal{M} : \mathbf{P}(V) \to \mathbf{P}(\bar{V})$ is the minimal transform mapping, and the operators $\perp, \to$ are induced from $\mathbf{P}(\bar{V})$ while for all $x \in V$ and $\phi \in \mathbf{Q}(V)$ we have:

$$\forall \mathbf{x} \phi = \forall n \phi[n/x]$$

where $n = \min\{k \in \mathbf{N} : [k/x] \text{ valid for } \phi\}$.

Proposition 102 *Let V be a set with minimal transform algebra $\mathbf{Q}(V)$. Then, the minimal transform mapping $\mathcal{M} : \mathbf{P}(V) \to \mathbf{Q}(V)$ is a surjective morphism.*

Proof
The minimal transform mapping $\mathcal{M} : \mathbf{P}(V) \to \mathbf{Q}(V)$ is clearly surjective by definition (40) of $\mathbf{Q}(V)$. So it remains to show it is a morphism. From definition (38) of page 139 we have $\mathcal{M}(\perp) = \perp$ and for all $\phi_1, \phi_2 \in \mathbf{P}(V)$:

$$\mathcal{M}(\phi_1 \to \phi_2) = \mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2)$$

So it remains to show that $\mathcal{M}(\forall x\phi_1) = \forall \mathbf{x}\mathcal{M}(\phi_1)$ for all $x \in V$ and $\phi_1 \in \mathbf{P}(V)$. However, defining $n = \min\{k \in \mathbf{N} : [k/x] \text{ valid for } \mathcal{M}(\phi_1)\}$ we have:

$$\mathcal{M}(\forall x\phi_1) = \forall n\mathcal{M}(\phi_1)[n/x] = \forall \mathbf{x}\mathcal{M}(\phi_1)$$

where the two equalities follow from definitions (38) and (40) respectively. **.**

So from proposition (102) we have a morphism $\mathcal{M} : \mathbf{P}(V) \to \mathbf{Q}(V)$ which is surjective, while from theorem (14) we have the equivalence:

$$\mathcal{M}(\phi) = \mathcal{M}(\psi) \;\Leftrightarrow\; \phi \sim \psi$$

So the kernel of this morphism is exactly the substitution congruence on $\mathbf{P}(V)$.

Theorem 16 *Let V be a set with minimal transform algebra $\mathbf{Q}(V)$, and let the quotient universal algebra of $\mathbf{P}(V)$ modulo the substitution congruence be denoted $[\mathbf{P}(V)]$ as per* theorem (7)*. Let $\mathcal{M}^* : [\mathbf{P}(V)] \to \mathbf{Q}(V)$ be defined as:*

$$\forall \phi \in \mathbf{P}(V)\ ,\ \mathcal{M}^*([\phi]) = \mathcal{M}(\phi)$$

where $\mathcal{M}$ is the minimal transform mapping. Then $\mathcal{M}^*$ is an isomorphism.

Proof
From proposition (102) $\mathcal{M} : \mathbf{P}(V) \to \mathbf{Q}(V)$ is a surjective morphism and from theorem (14), the kernel $\ker(\mathcal{M})$ coincides with the substitution congruence on $\mathbf{P}(V)$. Hence the fact that $\mathcal{M}^* : [\mathbf{P}(V)] \to \mathbf{Q}(V)$ is an isomorphism follows immediately from the first isomorphism theorem (8) of page 55. **.**

2.3.6 Substitution Rank of Formula

When V and W are sets and $\sigma : V \to W$ is a map, given $\phi \in \mathbf{P}(V)$ our motivating force in the last few sections has been to define a map $\sigma(\phi)$ even in the case when σ is not a valid substitution for ϕ. Our strategy so far has been to *step outside* of $\mathbf{P}(W)$ into the bigger space $\mathbf{P}(\bar{W})$, and define $\sigma(\phi)$ as $\bar{\sigma} \circ \mathcal{M}(\phi)$ where $\mathcal{M}(\phi)$ is the minimal transform of ϕ and $\bar{\sigma} : \bar{V} \to \bar{W}$ is the minimal extension of σ, as per definitions (38) and (39) respectively. In this section and the next, we wish to go further than this and define $\sigma(\phi)$ as an actual element of $\mathbf{P}(W)$. This shouldn't be too hard. Indeed, when computing the minimal transform $\mathcal{M}(\phi)$, all the bound variables have been ordered and rationalized in a given way. The effect of $\bar{\sigma}$ on $\mathcal{M}(\phi)$ is simply to move the free variables from V to W which should have no impact of the configuration of the bound variables. It is therefore not unreasonable to think that the formula $\bar{\sigma} \circ \mathcal{M}(\phi)$ is still properly configured so to speak, in other words that $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M}(\psi)$ for some $\psi \in \mathbf{P}(W)$. If this is the case, we can simply define $\sigma(\phi) = \psi$. This definition would not uniquely characterize the formula $\sigma(\phi)$, but it would certainly define a unique class modulo the substitution congruence, by virtue of theorem (14) of page 149. So let's have a look at an example with $\phi = \forall y(x \in y)$ and $x \neq y$. Assuming $\sigma(x) = u$ we obtain $\bar{\sigma} \circ \mathcal{M}(\phi) = \forall\, 0(u \in 0)$, and sure enough this is indeed the minimal transform of $\forall v(u \in v)$ where $v \in W$ and

$u \neq v$. So our strategy is clear: all we need to do is prove that $\bar{\sigma} \circ \mathcal{M}(\phi)$ is indeed equal to the minimal transform $\mathcal{M}(\psi)$ for some $\psi \in \mathbf{P}(W)$. There is however a glitch: the set W may be too small. Our example was successful because we assumed the existence of $v \in W$ such that $u \neq v$. This need not be the case. We cannot have $W = \emptyset$ as otherwise there would be no map $\sigma : V \to W$ when $\{x, y\} \subseteq V \neq \emptyset$, but it is possible that W be limited to the singleton $W = \{u\}$. When this is the case, there exists no $\psi \in \mathbf{P}(W)$ such that $\mathcal{M}(\psi) = \forall 0(u \in 0)$. So it is clear we cannot hope to achieve $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M}(\psi)$ in general unless W has sufficiently many variables to *accommodate* the formula $\bar{\sigma} \circ \mathcal{M}(\phi)$. It appears the formula $\forall 0(u \in 0)$ requires at least two variables. This is also the case for $\forall 1 \forall 0(0 \in 1)$ or $(u \in v)$ with $u \neq v$, while $\forall 0(0 \in 0)$ requires one variable only. As for the formula $\bot \to (\bot \to \bot)$, it requires no variable at all. So we need to make this idea precise: given the formula $\bar{\sigma} \circ \mathcal{M}(\phi)$ we have to define the minimum required number of variables in W so the formula can be *squeezed* into $\mathbf{P}(W)$. This motivates the following definition:

Definition 42 *Let V be a set and $\sim$ be the substitution congruence on $\mathbf{P}(V)$. For all $\phi \in \mathbf{P}(V)$ we call* substitution rank *of ϕ the integer* $\mathrm{rnk}(\phi)$ *defined by:*

$$\mathrm{rnk}(\phi) = \min\{\, |\mathrm{Var}(\psi)| \;:\; \psi \in \mathbf{P}(V) \;,\; \phi \sim \psi \,\}$$

where $|\mathrm{Var}(\psi)|$ denotes the cardinal of the set $\mathrm{Var}(\psi)$, for all $\psi \in \mathbf{P}(V)$.

Given a set A, it is customary to use the notation $|A|$ to refer to the *cardinal number* of A. We have not formally defined the notion of ordinal and cardinal numbers at this stage, but for all $\psi \in \mathbf{P}(V)$ the set $\mathrm{Var}(\psi)$ is finite and $|\mathrm{Var}(\psi)|$ is simply the number of elements it has. So this should be enough for now. Given a formula $\phi \in \mathbf{P}(V)$, we defined $\mathrm{rnk}(\phi)$ as the smallest number of variables used by a formula ψ, which is equivalent to ϕ modulo the substitution congruence. Our hope is that provided $\mathrm{rnk}(\,\bar{\sigma} \circ \mathcal{M}(\phi)\,) \leq |W|$, there should be enough variables in W for us to find $\psi \in \mathbf{P}(W)$ such that $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M}(\psi)$. So let us see if this works: in the case $\bar{\sigma} \circ \mathcal{M}(\phi) = \bot$, the condition $\mathrm{rnk}(\,\bar{\sigma} \circ \mathcal{M}(\phi)\,) \leq |W|$ becomes $0 \leq |W|$ and it is clear we do not require W to have any element. In the case when $\bar{\sigma} \circ \mathcal{M}(\phi) = \forall 0(0 \in 0)$ the condition becomes $1 \leq |W|$ and it is clear W should have at least one variable. If $\bar{\sigma} \circ \mathcal{M}(\phi) = \forall 0(u \in 0)$ then the condition becomes $2 \leq |W|$ which is another success. A more interesting example is $\bar{\sigma} \circ \mathcal{M}(\phi) = \forall 1 \forall 0(1 \in 0) \to (u \in v)$ with $u \neq v$. This formula is equivalent to $\psi = \forall u \forall v(u \in v) \to (u \in v)$ and consequently we have $\mathrm{rnk}(\,\bar{\sigma} \circ \mathcal{M}(\phi)\,) = 2$. So the condition becomes $2 \leq |W|$ which is indeed the correct condition to impose on W since we do not need more than two variables, as $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M}(\psi)$ with $\psi = \forall u \forall v(u \in v) \to (u \in v)$. Hence we believe definition (41) refers to the correct notion and we shall endeavor to prove the existence of $\psi \in \mathbf{P}(W)$ such that $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M}(\psi)$ whenever the condition $\mathrm{rnk}(\,\bar{\sigma} \circ \mathcal{M}(\phi)\,) \leq |W|$ is satisfied. For now, we shall establish some of the rank's properties:

Proposition 103 *Let V be a set and $\phi \in \mathbf{P}(V)$. Then, we have:*

$$|\mathrm{Fr}(\phi)| \leq \mathrm{rnk}(\phi) \leq |\mathrm{Var}(\phi)|$$

Proof
The inequality $\mathrm{rnk}(\phi) \leq |\mathrm{Var}(\phi)|$ follows immediately from definition (41). So it remains to show that $|\mathrm{Fr}(\phi)| \leq \mathrm{rnk}(\phi)$. So let $\psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$ where $\sim$ is the substitution congruence. We need to show $|\mathrm{Fr}(\phi)| \leq |\mathrm{Var}(\psi)|$. From proposition (79) we have $\mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$. Hence we need to show that $|\mathrm{Fr}(\psi)| \leq |\mathrm{Var}(\psi)|$ which follows from $\mathrm{Fr}(\psi) \subseteq \mathrm{Var}(\psi)$. .

Given $\phi \in \mathbf{P}(V)$, we know from definition (41) that $\mathrm{rnk}(\phi) = |\mathrm{Var}(\psi)|$ for some $\psi \sim \phi$. Given a suitably large subset $V_0 \subseteq V$, the following proposition allows us to choose such a ψ with the additional property $\mathrm{Var}(\psi) \subseteq V_0$ provided $\mathrm{Fr}(\phi) \subseteq V_0$. Obviously we cannot hope to have $\mathrm{Var}(\psi) \subseteq V_0$ unless V_0 is large enough and $\mathrm{Fr}(\phi) \subseteq V_0$ since two substitution equivalent formulas have the same free variables. Being able to find a ψ with $\mathrm{Var}(\psi) \subseteq V_0$ is crucially important for us. If we go back to the case when $\bar{\sigma} \circ \mathcal{M}(\phi) = \forall\, 0(u \in 0)$, our first step in proving the existence of ψ such that $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M}(\psi)$ will be to show the existence of $\psi_1 = \forall v(u \in v)$, which is a ψ_1 with $\mathrm{Var}(\psi_1) \subseteq V_0$ where $V_0 = W \subseteq \bar{W}$. When V_0 is not large enough, we cannot hope to find a ψ with $\mathrm{Var}(\psi) \subseteq V_0$. However, we can ensure that $V_0 \subseteq \mathrm{Var}(\psi)$ which will also be a useful property when calculating the substitution rank of $\phi_1 \to \phi_2$.

Proposition 104 *Let V be a set and $\phi \in \mathbf{P}(V)$ such that $\mathrm{Fr}(\phi) \subseteq V_0$ for some $V_0 \subseteq V$. Let $\sim$ denote the substitution congruence on $\mathbf{P}(V)$. Then there exists $\psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$ and $|\mathrm{Var}(\psi)| = \mathrm{rnk}(\phi)$ such that:*

$$(i) \qquad \mathrm{rnk}(\phi) \leq |V_0| \;\Rightarrow\; \mathrm{Var}(\psi) \subseteq V_0$$
$$(ii) \qquad |V_0| \leq \mathrm{rnk}(\phi) \;\Rightarrow\; V_0 \subseteq \mathrm{Var}(\psi)$$

Proof
Without loss of generality, we may assume that $|\mathrm{Var}(\phi)| = \mathrm{rnk}(\phi)$. Indeed, suppose the proposition has been established with the additional assumption $|\mathrm{Var}(\phi)| = \mathrm{rnk}(\phi)$. We need to show it is then true in the general case. So given $V_0 \subseteq V$, consider $\phi \in \mathbf{P}(V)$ such that $\mathrm{Fr}(\phi) \subseteq V_0$. From definition (41) there exists $\phi_1 \in \mathbf{P}(V)$ such that $\phi \sim \phi_1$ with the equality $|\mathrm{Var}(\phi_1)| = \mathrm{rnk}(\phi)$. From proposition (79) we obtain $\mathrm{Fr}(\phi) = \mathrm{Fr}(\phi_1)$ and so $\mathrm{Fr}(\phi_1) \subseteq V_0$. Hence we see that ϕ_1 satisfies the assumption of the proposition with the additional property $|\mathrm{Var}(\phi_1)| = \mathrm{rnk}(\phi_1)$. Having assumed the proposition is true in this case, we obtain the existence of $\psi \in \mathbf{P}(V)$ such that $\phi_1 \sim \psi$, $|\mathrm{Var}(\psi)| = \mathrm{rnk}(\phi_1)$ and which satisfies (i) and (ii) where ϕ is replaced by ϕ_1. However $\mathrm{rnk}(\phi_1) = \mathrm{rnk}(\phi)$ and replacing ϕ by ϕ_1 in (i) and (ii) has no impact. So ψ satisfies (i) and (ii). Hence we have $\phi \sim \psi$ and $|\mathrm{Var}(\psi)| = \mathrm{rnk}(\phi)$ together with (i) and (ii) which establishes the proposition in the general case. So we now assume without loss of generality that $|\mathrm{Var}(\phi)| = \mathrm{rnk}(\phi)$ and $\mathrm{Fr}(\phi) \subseteq V_0$. We need to show the existence of $\psi \sim \phi$ such that $|\mathrm{Var}(\psi)| = |\mathrm{Var}(\phi)|$ and which satisfies (i) and (ii). Note that if $V = \emptyset$ then $V_0 = \emptyset$ and we can take $\psi = \phi$. So we assume $V \neq \emptyset$. We shall first consider the case when $\mathrm{rnk}(\phi) \leq |V_0|$ and show the existence of ψ such that $\mathrm{Var}(\psi) \subseteq V_0$. Since $\mathrm{Fr}(\phi) \subseteq V_0$ the set V_0 is the disjoint union of $\mathrm{Fr}(\phi)$ and $V_0 \setminus \mathrm{Fr}(\phi)$, giving us the equality $|V_0| = |\mathrm{Fr}(\phi)| + |V_0 \setminus \mathrm{Fr}(\phi)|$. Since we

also have $|\mathrm{Var}(\phi)| = |\mathrm{Fr}(\phi)| + |\mathrm{Var}(\phi) \setminus \mathrm{Fr}(\phi)|$, we obtain from $|\mathrm{Var}(\phi)| \leq |V_0|$:

$$|\mathrm{Fr}(\phi)| + |\mathrm{Var}(\phi) \setminus \mathrm{Fr}(\phi)| \leq |\mathrm{Fr}(\phi)| + |V_0 \setminus \mathrm{Fr}(\phi)|$$

Since $|\mathrm{Fr}(\phi)|$ is a finite cardinal it follows that $|\mathrm{Var}(\phi) \setminus \mathrm{Fr}(\phi)| \leq |V_0 \setminus \mathrm{Fr}(\phi)|$. Hence, there is an injection mapping $i : \mathrm{Var}(\phi) \setminus \mathrm{Fr}(\phi) \to V_0 \setminus \mathrm{Fr}(\phi)$. Having assumed $V \neq \emptyset$ consider $x^* \in V$ and define the map $\sigma : V \to V$ as follows:

$$\forall u \in V \ , \ \sigma(u) = \begin{cases} u & \text{if} \quad u \in \mathrm{Fr}(\phi) \\ i(u) & \text{if} \quad u \in \mathrm{Var}(\phi) \setminus \mathrm{Fr}(\phi) \\ x^* & \text{if} \quad u \notin \mathrm{Var}(\phi) \end{cases}$$

Define $\psi = \sigma(\phi)$. It remains to show that ψ has the desired properties, namely that $\psi \sim \phi$, $|\mathrm{Var}(\psi)| = |\mathrm{Var}(\phi)|$ and $\mathrm{Var}(\psi) \subseteq V_0$. First we show $\psi \sim \phi$. Using proposition (77) it is sufficient to prove that σ is an admissible substitution for ϕ. It is clear that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\phi)$. So it remains to show that σ is valid for ϕ. From proposition (53) it is sufficient to prove that $\sigma_{|\mathrm{Var}(\phi)}$ is an injective map. So let $u, v \in \mathrm{Var}(\phi)$ such that $\sigma(u) = \sigma(v)$. We need to show that $u = v$. We shall distinguish four cases: first we assume that $u \in \mathrm{Fr}(\phi)$ and $v \in \mathrm{Fr}(\phi)$. Then the equality $\sigma(u) = \sigma(v)$ leads to $u = v$. Next we assume that $u \notin \mathrm{Fr}(\phi)$ and $v \notin \mathrm{Fr}(\phi)$. Then we obtain $i(u) = i(v)$ which also leads to $u = v$ since $i : \mathrm{Var}(\phi) \setminus \mathrm{Fr}(\phi) \to V_0 \setminus \mathrm{Fr}(\phi)$ is an injective map. So we now assume that $u \in \mathrm{Fr}(\phi)$ and $v \notin \mathrm{Fr}(\phi)$. Then from $\sigma(u) = \sigma(v)$ we obtain $u = i(v)$ which is in fact impossible since $u \in \mathrm{Fr}(\phi)$ and $i(v) \in V_0 \setminus \mathrm{Fr}(\phi)$. The last case $u \notin \mathrm{Fr}(\phi)$ and $v \in \mathrm{Fr}(\phi)$ is equally impossible which completes our proof of $\psi \sim \phi$. So we now prove that $|\mathrm{Var}(\psi)| = |\mathrm{Var}(\phi)|$. From proposition (35) we have $\mathrm{Var}(\psi) = \mathrm{Var}(\sigma(\phi)) = \sigma(\mathrm{Var}(\phi))$. So we need $|\sigma(\mathrm{Var}(\phi))| = |\mathrm{Var}(\phi)|$ which is clear since $\sigma_{|\mathrm{Var}(\phi)} : \mathrm{Var}(\phi) \to \sigma(\mathrm{Var}(\phi))$ is a bijection. So it remains to show that $\mathrm{Var}(\psi) \subseteq V_0$, or equivalently that $\sigma(\mathrm{Var}(\phi)) \subseteq V_0$. So let $u \in \mathrm{Var}(\phi)$. We need to show that $\sigma(u) \in V_0$. We shall distinguish two cases: first we assume that $u \in \mathrm{Fr}(\phi)$. Then $\sigma(u) = u$ and the property $\sigma(u) \in V_0$ follows from the inclusion $\mathrm{Fr}(\phi) \subseteq V_0$. Next we assume that $u \notin \mathrm{Fr}(\phi)$. Then we have $\sigma(u) = i(u) \in V_0 \setminus \mathrm{Fr}(\phi) \subseteq V_0$. So in the case when $\mathrm{rnk}(\phi) \leq |V_0|$ we have been able to prove the existence of ψ satisfying (i). In fact we claim that ψ also satisfies (ii). So let us assume that $|V_0| \leq \mathrm{rnk}(\phi)$. Then we must have $\mathrm{rnk}(\phi) = |V_0|$ and we need to show that $V_0 \subseteq \mathrm{Var}(\psi)$. However, we have $|\mathrm{Var}(\psi)| = \mathrm{rnk}(\phi)$ and consequently $|\mathrm{Var}(\psi)| = |V_0|$ together with $\mathrm{Var}(\psi) \subseteq V_0$. Two finite subsets ordered by inclusion and with the same cardinal must be equal. So $\mathrm{Var}(\psi) = V_0$. We now consider the case when $|V_0| < \mathrm{rnk}(\phi)$. We need to show the existence of $\psi \sim \phi$ such that $|\mathrm{Var}(\psi)| = |\mathrm{Var}(\phi)|$ satisfying (i) and (ii). In the case when $|V_0| < \mathrm{rnk}(\phi)$, (i) is vacuously true, so we simply need to ensure that $V_0 \subseteq \mathrm{Var}(\psi)$. Since $|V_0| < |\mathrm{Var}(\phi)|$ we obtain:

$$\begin{aligned} |V_0 \setminus \mathrm{Var}(\phi)| &= |V_0| - |V_0 \cap \mathrm{Var}(\phi)| \\ &< |\mathrm{Var}(\phi)| - |V_0 \cap \mathrm{Var}(\phi)| \\ &= |\mathrm{Var}(\phi) \setminus V_0| \end{aligned}$$

So there is an injective map $i : V_0 \setminus \mathrm{Var}(\phi) \to \mathrm{Var}(\phi) \setminus V_0$. Given $x^* \in V$, define:

$$\forall u \in V \ , \ \sigma(u) = \begin{cases} u & \text{if} \quad u \in \mathrm{Var}(\phi) \setminus i(\, V_0 \setminus \mathrm{Var}(\phi)\,) \\ i^{-1}(u) & \text{if} \quad u \in i(\, V_0 \setminus \mathrm{Var}(\phi)\,) \\ x^* & \text{if} \quad u \notin \mathrm{Var}(\phi) \end{cases}$$

Let $\psi = \sigma(\phi)$. It remains to show that $\psi \sim \phi$, $|\mathrm{Var}(\psi)| = |\mathrm{Var}(\phi)|$ and $V_0 \subseteq \mathrm{Var}(\psi)$. First we show that $\psi \sim \phi$. Using proposition (77) it is sufficient to prove that σ is an admissible substitution for ϕ. So let $u \in \mathrm{Fr}(\phi)$. We need to show that $\sigma(u) = u$. So it is sufficient to prove that $u \notin i(\, V_0 \setminus \mathrm{Var}(\phi)\,)$ which follows from the fact that $u \in V_0$, itself a consequence of $\mathrm{Fr}(\phi) \subseteq V_0$. In order to show that σ is also valid for ϕ, from proposition (53) it is sufficient to prove that σ is injective on $\mathrm{Var}(\phi)$. So let $u, v \in \mathrm{Var}(\phi)$ such that $\sigma(u) = \sigma(v)$. We need to prove that $u = v$. The only case when this may not be clear is when $\sigma(u) = u$ and $\sigma(v) = i^{-1}(v)$ or vice versa. So we assume that $u \in \mathrm{Var}(\phi) \setminus i(\, V_0 \setminus \mathrm{Var}(\phi)\,)$ and $v \in i(\, V_0 \setminus \mathrm{Var}(\phi)\,)$. Then we see that $\sigma(u) = u \in \mathrm{Var}(\phi)$ while $\sigma(v) = i^{-1}(v) \in V_0 \setminus \mathrm{Var}(\phi)$. So the equality $\sigma(u) = \sigma(v)$ is in fact impossible, which completes our proof of $\psi \sim \phi$. As before, the fact that $|\mathrm{Var}(\psi)| = |\mathrm{Var}(\phi)|$ follows from the injectivity of $\sigma_{|\mathrm{Var}(\phi)}$ and it remains to prove that $V_0 \subseteq \mathrm{Var}(\psi)$. So let $u \in V_0$ we need to show that $u \in \mathrm{Var}(\psi) = \sigma(\mathrm{Var}(\phi))$ and we shall distinguish two cases: first we assume that $u \in \mathrm{Var}(\phi)$. Since $u \in V_0$, it cannot be an element of $i(\, V_0 \setminus \mathrm{Var}(\phi)\,)$. It follows that $u \in \mathrm{Var}(\phi) \setminus i(\, V_0 \setminus \mathrm{Var}(\phi)\,)$ and consequently $u = \sigma(u) \in \sigma(\mathrm{Var}(\phi)) = \mathrm{Var}(\psi)$. Next we assume that $u \in V_0 \setminus \mathrm{Var}(\phi)$. Then $i(u)$ is an element of $i(\, V_0 \setminus \mathrm{Var}(\phi)\,)$ and therefore $\sigma(i(u)) = i^{-1}(i(u)) = u$. Since $i(u)$ is an element of $\mathrm{Var}(\phi) \setminus V_0$ we conclude that $u = \sigma(i(u)) \in \sigma(\mathrm{Var}(\phi)) = \mathrm{Var}(\psi)$, which completes our proof. **.**

The substitution rank of a formula is essentially the minimum number of variables needed to describe a representative of its class modulo substitution. We should expect injective variable substitutions to have no effect on the rank.

Proposition 105 *Let V, W be sets and $\sigma : V \to W$ be a map. Then for all $\phi \in \mathbf{P}(V)$, if $\sigma_{|\mathrm{Var}(\phi)}$ is an injective map, we have the equality:*

$$\mathrm{rnk}(\sigma(\phi)) = \mathrm{rnk}(\phi)$$

where $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ denotes the associated substitution mapping.

Proof

Let $\sigma : V \to W$ and $\phi \in \mathbf{P}(V)$ such that $\sigma_{|\mathrm{Var}(\phi)}$ is an injective map. We need to show that $\mathrm{rnk}(\sigma(\phi)) = \mathrm{rnk}(\phi)$. First we shall show $\mathrm{rnk}(\sigma(\phi)) \leq \mathrm{rnk}(\phi)$. Using proposition (104) with $V_0 = \mathrm{Var}(\phi)$, since we have $\mathrm{Fr}(\phi) \subseteq \mathrm{Var}(\phi)$ and $\mathrm{rnk}(\phi) \leq |\mathrm{Var}(\phi)|$, there exists $\psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$, $|\mathrm{Var}(\psi)| = \mathrm{rnk}(\phi)$ and $\mathrm{Var}(\psi) \subseteq \mathrm{Var}(\phi)$. Having assumed σ is injective on $\mathrm{Var}(\phi)$, it is therefore injective on both $\mathrm{Var}(\phi)$ and $\mathrm{Var}(\psi)$. From proposition (53) it follows that σ is a valid substitution for both ϕ and ψ. Hence from theorem (15) of page 152 we obtain $\sigma(\phi) \sim \sigma(\psi)$ and consequently using proposition (35) :

$$\mathrm{rnk}(\sigma(\phi)) \leq |\mathrm{Var}(\sigma(\psi))| = |\sigma(\mathrm{Var}(\psi))| = |\mathrm{Var}(\psi)| = \mathrm{rnk}(\phi)$$

So it remains to show that $\text{rnk}(\phi) \leq \text{rnk}(\sigma(\phi))$. If $V = \emptyset$ then $\text{rnk}(\phi) = 0$ and we are done. So we may assume that $V \neq \emptyset$. So let $x^* \in V$ and define:

$$\forall u \in W \ , \ \tau(u) = \begin{cases} \sigma^{-1}(u) & \text{if} \quad u \in \sigma(\text{Var}(\phi)) \\ x^* & \text{if} \quad u \notin \sigma(\text{Var}(\phi)) \end{cases}$$

Then $\tau : W \to V$ is injective on $\text{Var}(\sigma(\phi)) = \sigma(\text{Var}(\phi))$ and hence:

$$\text{rnk}(\ \tau(\sigma(\phi))\ ) \leq \text{rnk}(\sigma(\phi))$$

So it suffices for us to show that $\tau \circ \sigma(\phi) = \phi$. From proposition (36) it is thus sufficient to show that $\tau \circ \sigma(x) = x$ for all $x \in \text{Var}(\phi)$, which is clear. .

If $\phi \in \mathbf{P}(V)$ we know from proposition (99) that $\mathcal{M}(\phi)$ is substitution equivalent to $i(\phi)$ where $i : V \to \bar{V}$ is the inclusion map. Hence we have:

Proposition 106 *Let V be a set and $\phi \in \mathbf{P}(V)$. Then the formula ϕ and its minimal transform have equal substitution rank, i.e.:*

$$\text{rnk}(\mathcal{M}(\phi)) = \text{rnk}(\phi)$$

Proof
Let $\sim$ denote the substitution congruence on $\mathbf{P}(\bar{V})$ and $i : V \to \bar{V}$ be the inclusion map. From proposition (99) we have $\mathcal{M}(\phi) \sim i(\phi)$ and consequently $\text{rnk}(\mathcal{M}(\phi)) = \text{rnk}(i(\phi))$. So we need to show that $\text{rnk}(i(\phi)) = \text{rnk}(\phi)$ which follows from proposition (105) and the fact that $i : V \to \bar{V}$ is injective. .

We have already established that an injective variable substitution does not change the rank of a formula. If $\phi \in \mathbf{P}(V)$ and $\sigma : V \to V$ is an admissible substitution for ϕ, we also know from proposition (77) that $\phi \sim \sigma(\phi)$. Hence if $\sigma : V \to V$ is valid for ϕ while leaving the free variables unchanged, it will not change the rank of the formula ϕ either. It is not unreasonable to think that this property will remain true if we only impose that σ be injective on $\text{Fr}(\phi)$. In fact, this should also apply to any $\sigma : V \to W$, without assuming $W = V$.

Proposition 107 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\phi \in \mathbf{P}(V)$. We assume that σ is valid for ϕ and $\sigma_{|\text{Fr}(\phi)}$ is an injective map. Then:*

$$\text{rnk}(\sigma(\phi)) = \text{rnk}(\phi)$$

where $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ denotes the associated substitution mapping.

Proof
We shall proceed in two steps: first we shall prove the proposition is true in the case when $W = V$. We shall then extend the result to arbitrary W. So let us assume $W = V$. Let $\sigma : V \to V$ valid for $\phi \in \mathbf{P}(V)$ such that $\sigma_{|\text{Fr}(\phi)}$ is an injective map. We need to show that $\text{rnk}(\sigma(\phi)) = \text{rnk}(\phi)$. If $V = \emptyset$ then $\sigma : V \to V$ is the map with empty domain, namely the empty set which is injective on $\text{Var}(\phi) = \emptyset$ and $\text{rnk}(\sigma(\phi)) = \text{rnk}(\phi)$ follows from proposition (105). So we assume that $V \neq \emptyset$. The idea of the proof is to write $\sigma(\phi) = \tau_1 \circ \tau_0(\phi)$

where each substitution τ_0, τ_1 is rank preserving. Having assumed σ injective on $\mathrm{Fr}(\phi)$, we have the equality $|\sigma(\mathrm{Fr}(\phi)| = |\mathrm{Fr}(\phi)|$ and consequently:

$$\begin{aligned} |\mathrm{Var}(\phi) \setminus \mathrm{Fr}(\phi)| &= |\mathrm{Var}(\phi)| - |\mathrm{Fr}(\phi)| \\ &\leq |V| - |\mathrm{Fr}(\phi)| \\ &= |V| - |\,\sigma(\mathrm{Fr}(\phi))\,| \\ &= |\,V \setminus \sigma(\mathrm{Fr}(\phi))\,| \end{aligned}$$

So let $i : \mathrm{Var}(\phi) \setminus \mathrm{Fr}(\phi) \to V \setminus \sigma(\mathrm{Fr}(\phi))$ be an injective map. Let $x^* \in V$ and define the substitution $\tau_0 : V \to V$ as follows:

$$\forall x \in V \ , \ \tau_0(x) = \begin{cases} \sigma(x) & \text{if} \quad x \in \mathrm{Fr}(\phi) \\ i(x) & \text{if} \quad x \in \mathrm{Var}(\phi) \setminus \mathrm{Fr}(\phi) \\ x^* & \text{if} \quad x \notin \mathrm{Var}(\phi) \end{cases}$$

Let us accept for now that τ_0 is injective on $\mathrm{Var}(\phi)$. Then using proposition (105) we obtain $\mathrm{rnk}(\tau_0(\phi)) = \mathrm{rnk}(\phi)$. So consider $\tau_1 : V \to V$:

$$\forall u \in V \ , \ \tau_1(u) = \begin{cases} u & \text{if} \quad u \in \sigma(\mathrm{Fr}(\phi)) \\ \sigma \circ i^{-1}(u) & \text{if} \quad u \in i(\,\mathrm{Var}(\phi) \setminus \mathrm{Fr}(\phi)\,) \\ x^* & \text{otherwise} \end{cases}$$

Note that τ_1 is well defined since $\sigma(\mathrm{Fr}(\phi)) \cap i(\,\mathrm{Var}(\phi) \setminus \mathrm{Fr}(\phi)\,) = \emptyset$. So let us accept for now that τ_1 is admissible for $\tau_0(\phi)$. Then using proposition (77) we obtain $\tau_1 \circ \tau_0(\phi) \sim \tau_0(\phi)$ where $\sim$ is the substitution congruence on $\mathbf{P}(V)$. Hence in particular we have $\mathrm{rnk}(\tau_1 \circ \tau_0(\phi)) = \mathrm{rnk}(\tau_0(\phi)) = \mathrm{rnk}(\phi)$. So in order to show that the proposition is true in the case when $W = V$, it remains to prove that τ_0 is injective on $\mathrm{Var}(\phi)$, τ_1 is admissible for $\tau_0(\phi)$ and furthermore that $\tau_1 \circ \tau_0(\phi) = \sigma(\phi)$. First we show that τ_0 is injective on $\mathrm{Var}(\phi)$. So let $x, y \in \mathrm{Var}(\phi)$ such that $\tau_0(x) = \tau_0(y)$. We need to show that $x = y$. We shall distinguish four cases: first we assume that $x \in \mathrm{Fr}(\phi)$ and $y \in \mathrm{Fr}(\phi)$. Then the equality $\tau_0(x) = \tau_0(y)$ leads to $\sigma(x) = \sigma(y)$. Having assumed $\sigma_{|\mathrm{Fr}(\phi)}$ is an injective map, we obtain $x = y$. Next we assume that $x \in \mathrm{Var}(\phi) \setminus \mathrm{Fr}(\phi)$ and $y \in \mathrm{Var}(\phi) \setminus \mathrm{Fr}(\phi)$. Then the equality $\tau_0(x) = \tau_0(y)$ leads to $i(x) = i(y)$ and consequently $x = y$. So we now assume that $x \in \mathrm{Fr}(\phi)$ and $y \in \mathrm{Var}(\phi) \setminus \mathrm{Fr}(\phi)$. Then $\tau_0(x) = \sigma(x) \in \sigma(\mathrm{Fr}(\phi))$ and $\tau_0(y) = i(y) \in V \setminus \sigma(\mathrm{Fr}(\phi))$. So the equality $\tau_0(x) = \tau_0(y)$ is in fact impossible. We show similarly that the final case $x \in \mathrm{Var}(\phi) \setminus \mathrm{Fr}(\phi)$ and $y \in \mathrm{Fr}(\phi)$ is also impossible which completes the proof that τ_0 is injective on $\mathrm{Var}(\phi)$. We shall now show that $\tau_1 \circ \tau_0(\phi) = \sigma(\phi)$. From proposition (36) it is sufficient to prove that $\tau_1 \circ \tau_0(x) = \sigma(x)$ for all $x \in \mathrm{Var}(\phi)$. We shall distinguish two cases: first we assume that $x \in \mathrm{Fr}(\phi)$. Then $\tau_0(x) = \sigma(x) \in \sigma(\mathrm{Fr}(\phi))$ and consequently $\tau_1 \circ \tau_0(x) = \sigma(x)$ as requested. Next we assume that $x \in \mathrm{Var}(\phi) \setminus \mathrm{Fr}(\phi)$. Then $\tau_0(x) = i(x) \in i(\,\mathrm{Var}(\phi) \setminus \mathrm{Fr}(\phi)\,)$ and consequently $\tau_1 \circ \tau_0(x) = \sigma \circ i^{-1}(i(x)) = \sigma(x)$. So it remains to show that τ_1 is admissible for $\tau_0(\phi)$, i.e. that it is valid for $\tau_0(\phi)$ and $\tau_1(u) = u$ for all $u \in \mathrm{Fr}(\tau_0(\phi))$. So let $u \in \mathrm{Fr}(\tau_0(\phi))$. We need to show that $\tau_1(u) = u$. So

it is sufficient to prove that $u \in \sigma(\mathrm{Fr}(\phi))$. However from proposition (43) we have $\mathrm{Fr}(\tau_0(\phi)) \subseteq \tau_0(\mathrm{Fr}(\phi))$ and consequently there exists $x \in \mathrm{Fr}(\phi)$ such that $u = \tau_0(x) = \sigma(x)$. It follows that $u \in \sigma(\mathrm{Fr}(\phi))$ as requested and it remains to show that τ_1 is valid for $\tau_0(\phi)$. From proposition (58) it is sufficient to show that $\tau_1 \circ \tau_0$ is valid for ϕ. However, having proved that $\tau_1 \circ \tau_0(\phi) = \sigma(\phi)$ from proposition (59) it is sufficient to prove that σ is valid for ϕ which is in fact true by assumption. This completes our proof of the proposition in the case when $W = V$. We shall now prove the proposition in the general case. So we assume that $\sigma : V \to W$ is a map and $\phi \in \mathbf{P}(V)$ is such that σ is valid for ϕ and $\sigma_{|\mathrm{Fr}(\phi)}$ is an injective map. We need to prove that $\mathrm{rnk}(\sigma(\phi)) = \mathrm{rnk}(\phi)$. Let U be the disjoint union of the sets V and W, specifically:

$$U = \{0\} \times V \uplus \{1\} \times W$$

Let $i : V \to U$ and $j : W \to U$ be the corresponding inclusion maps. Consider the formula $\phi^* = i(\phi) \in \mathbf{P}(U)$ and let $\sigma^* : U \to U$ be defined as:

$$\forall u \in U \ , \ \sigma^*(u) = \begin{cases} j \circ \sigma(u) & \text{if} \quad u \in V \\ u & \text{if} \quad u \in W \end{cases}$$

Let us accept for now that σ^* is valid for ϕ^* and that $\sigma^*_{|\mathrm{Fr}(\phi^*)}$ is an injective map. Having proved the proposition in the case when $W = V$, it can be applied to $\sigma^* : U \to U$ and $\phi^* \in \mathbf{P}(U)$. Hence, since i and j are injective maps, using proposition (105) we obtain the following equalities:

$$\begin{aligned} \mathrm{rnk}(\sigma(\phi)) &= \mathrm{rnk}(j \circ \sigma(\phi)) \\ \text{A: to be proved} \ \rightarrow \ &= \mathrm{rnk}(\sigma^*(\phi^*)) \\ \text{case } W = V \ \rightarrow \ &= \mathrm{rnk}(\phi^*) \\ &= \mathrm{rnk}(i(\phi)) \\ \text{prop. (105)} \ \rightarrow \ &= \mathrm{rnk}(\phi) \end{aligned}$$

So it remains to show that $j \circ \sigma(\phi) = \sigma^*(\phi^*)$ and furthermore that σ^* is valid for ϕ^* while $\sigma^*_{|\mathrm{Fr}(\phi^*)}$ is an injective map. First we show that $j \circ \sigma(\phi) = \sigma^*(\phi^*)$. Since $\phi^* = i(\phi)$ from proposition (36) it is sufficient to prove that $j \circ \sigma(u) = \sigma^* \circ i(u)$ for all $u \in \mathrm{Var}(\phi)$. So let $u \in \mathrm{Var}(\phi)$. In particular $u \in V$ and consequently $i(u) \in i(V) \subseteq U$. From the above definition of σ^* we obtain immediately $\sigma^*(i(u)) = j \circ \sigma(u)$ as requested. So we now prove that σ^* is valid for $\phi^* = i(\phi)$. Using proposition (58) it is sufficient to prove that $\sigma^* \circ i$ is valid for ϕ. However, having proved that $\sigma^* \circ i(\phi) = j \circ \sigma(\phi)$, from proposition (59) it is sufficient to prove that $j \circ \sigma$ is valid for ϕ. Having assumed that σ is valid for ϕ, using proposition (58) once more it remains to show that j is valid for $\sigma(\phi)$ which follows from the injectivity of j and proposition (53). So it remains to prove that $\sigma^*_{|\mathrm{Fr}(\phi^*)}$ is an injective map. So let $u, v \in \mathrm{Fr}(\phi^*)$ such that $\sigma^*(u) = \sigma^*(v)$. We need to show that $u = v$. However since $\phi^* = i(\phi)$, from proposition (43) we have $\mathrm{Fr}(\phi^*) \subseteq i(\mathrm{Fr}(\phi))$. Hence, there exists $x, y \in \mathrm{Fr}(\phi)$ such that $u = i(x)$

and $v = i(y)$. Having proved that $j \circ \sigma = \sigma^* \circ i$ on $\mathrm{Var}(\phi)$, from the equality $\sigma^*(u) = \sigma^*(v)$ we obtain $j \circ \sigma(x) = j \circ \sigma(y)$. It follows from the injectivity of j that $\sigma(x) = \sigma(y)$. Having assumed that σ is injective on $\mathrm{Fr}(\phi)$ we conclude that $x = y$ and finally that $u = v$ as requested. **.**

As with anything involving the algebra $\mathbf{P}(V)$, it is difficult to establish deeper properties without resorting to some form of structural induction argument. Hence if we want to say anything more substantial about the substitution rank of a formula $\phi \in \mathbf{P}(V)$ we need to relate the rank of $\phi_1 \to \phi_2$ and $\forall x \phi_1$ to the ranks of ϕ_1 and ϕ_2. These relationships are not as simple as one would wish.

Proposition 108 *Let V be a set and $\phi \in \mathbf{P}(V)$ of the form $\phi = \phi_1 \to \phi_2$ where $\phi_1, \phi_2 \in \mathbf{P}(V)$. Then the substitution ranks of ϕ, ϕ_1 and ϕ_2 satisfy the equality:*

$$\mathrm{rnk}(\phi) = \max(\, |\mathrm{Fr}(\phi)|\,,\, \mathrm{rnk}(\phi_1)\,,\, \mathrm{rnk}(\phi_2)\,)$$

Proof
First we show that $\max(\, |\mathrm{Fr}(\phi)|\,,\, \mathrm{rnk}(\phi_1)\,,\, \mathrm{rnk}(\phi_2)\,) \leq \mathrm{rnk}(\phi)$. From proposition (103) we already know that $|\mathrm{Fr}(\phi)| \leq \mathrm{rnk}(\phi)$. So it remains to show that $\mathrm{rnk}(\phi_1) \leq \mathrm{rnk}(\phi)$ and $\mathrm{rnk}(\phi_2) \leq \mathrm{rnk}(\phi)$. So let $\sim$ be the substitution congruence on $\mathbf{P}(V)$ and $\psi \sim \phi$. We need to show that $\mathrm{rnk}(\phi_1) \leq |\mathrm{Var}(\psi)|$ and $\mathrm{rnk}(\phi_2) \leq |\mathrm{Var}(\psi)|$. However, from $\psi \sim \phi = \phi_1 \to \phi_2$ and theorem (12) of page 132 we see that ψ must be of the form $\psi = \psi_1 \to \psi_2$ where $\psi_1 \sim \phi_1$ and $\psi_2 \sim \phi_2$. Hence we have $\mathrm{rnk}(\phi_1) \leq |\mathrm{Var}(\psi_1)| \leq |\mathrm{Var}(\psi)|$ and similarly $\mathrm{rnk}(\phi_2) \leq |\mathrm{Var}(\psi_2)| \leq |\mathrm{Var}(\psi)|$. So it remains to show the inequality $\mathrm{rnk}(\phi) \leq \max(\, |\mathrm{Fr}(\phi)|\,,\, \mathrm{rnk}(\phi_1)\,,\, \mathrm{rnk}(\phi_2)\,)$. We shall distinguish two cases: first we assume that $\max(\mathrm{rnk}(\phi_1), \mathrm{rnk}(\phi_2)) \leq |\mathrm{Fr}(\phi)|$. Since $\mathrm{Fr}(\phi_1) \subseteq \mathrm{Fr}(\phi)$ and $\mathrm{Fr}(\phi_2) \subseteq \mathrm{Fr}(\phi)$ using proposition (104) we obtain the existence of $\psi_1 \sim \phi_1$ and $\psi_2 \sim \phi_2$ such that $|\mathrm{Var}(\psi_1)| = \mathrm{rnk}(\phi_1)$ and $|\mathrm{Var}(\psi_2)| = \mathrm{rnk}(\phi_2)$ with the inclusions $\mathrm{Var}(\psi_1) \subseteq \mathrm{Fr}(\phi)$ and $\mathrm{Var}(\psi_2) \subseteq \mathrm{Fr}(\phi)$. Since $\phi \sim \psi_1 \to \psi_2$:

$$\begin{array}{rcl} \mathrm{rnk}(\phi) & \leq & |\mathrm{Var}(\psi_1 \to \psi_2)| \\ & = & |\mathrm{Var}(\psi_1) \cup \mathrm{Var}(\psi_2)| \\ \mathrm{Var}(\psi_i) \subseteq \mathrm{Fr}(\phi) \;\to & \leq & |\mathrm{Fr}(\phi)| \\ & = & \max(\, |\mathrm{Fr}(\phi)|\,,\, \mathrm{rnk}(\phi_1)\,,\, \mathrm{rnk}(\phi_2)\,) \end{array}$$

Next we assume that $|\mathrm{Fr}(\phi)| \leq \max(\mathrm{rnk}(\phi_1), \mathrm{rnk}(\phi_2))$. We shall distinguish two further cases: first we assume that $\mathrm{rnk}(\phi_1) \leq \mathrm{rnk}(\phi_2)$. Since we have both $\mathrm{Fr}(\phi_2) \subseteq \mathrm{Fr}(\phi)$ and $|\mathrm{Fr}(\phi)| \leq \mathrm{rnk}(\phi_2)$, from proposition (104) we can find $\psi_2 \sim \phi_2$ such that $|\mathrm{Var}(\psi_2)| = \mathrm{rnk}(\phi_2)$ and $\mathrm{Fr}(\phi) \subseteq \mathrm{Var}(\psi_2)$. In particular we obtain the inclusion $\mathrm{Fr}(\phi_1) \subseteq \mathrm{Var}(\psi_2)$ and applying proposition (104) once more, from $\mathrm{rnk}(\phi_1) \leq \mathrm{rnk}(\phi_2) = |\mathrm{Var}(\psi_2)|$ we obtain the existence of $\psi_1 \sim \phi_1$ such that $|\mathrm{Var}(\psi_1)| = \mathrm{rnk}(\phi_1)$ and $\mathrm{Var}(\psi_1) \subseteq \mathrm{Var}(\psi_2)$. It follows that:

$$\begin{array}{rcl} \mathrm{rnk}(\phi) & \leq & |\mathrm{Var}(\psi_1 \to \psi_2)| \\ & = & |\mathrm{Var}(\psi_1) \cup \mathrm{Var}(\psi_2)| \\ \mathrm{Var}(\psi_1) \subseteq \mathrm{Var}(\psi_2) \;\to & = & |\mathrm{Var}(\psi_2)| \end{array}$$

$$\begin{aligned} &= \mathrm{rnk}(\phi_2) \\ &= \max(\,|\mathrm{Fr}(\phi)|\,,\,\mathrm{rnk}(\phi_1)\,,\,\mathrm{rnk}(\phi_2)\,) \end{aligned}$$

The case $\mathrm{rnk}(\phi_2) \leq \mathrm{rnk}(\phi_1)$ is dealt with similarly. .

Proposition 109 *Let V be a set and $\phi \in \mathbf{P}(V)$ of the form $\phi = \forall x \phi_1$ where $\phi_1 \in \mathbf{P}(V)$ and $x \in V$. Then the substitution ranks of ϕ and ϕ_1 satisfy:*

$$\mathrm{rnk}(\phi) = \mathrm{rnk}(\phi_1) + \epsilon$$

where $\epsilon \in 2 = \{0, 1\}$ is given by the equivalence $\epsilon = 1$ if and only if:

$$(\, x \notin \mathrm{Fr}(\phi_1)\,) \wedge (\,|\mathrm{Fr}(\phi_1)| = \mathrm{rnk}(\phi_1)\,)$$

Proof
Let $\phi = \forall x \phi_1$ where $\phi_1 \in \mathbf{P}(V)$ and $x \in V$. Define $\epsilon = \mathrm{rnk}(\phi) - \mathrm{rnk}(\phi_1)$. Then ϵ is an integer, possibly negative. In order to prove that $\epsilon \in 2$ it is therefore sufficient to prove that the following inequalities hold:

$$\mathrm{rnk}(\phi_1) \leq \mathrm{rnk}(\phi) \leq \mathrm{rnk}(\phi_1) + 1 \tag{2.36}$$

This will be the first part of our proof. Next we shall show the equivalence:

$$(\epsilon = 1) \;\Leftrightarrow\; (\, x \notin \mathrm{Fr}(\phi_1)\,) \wedge (\,|\mathrm{Fr}(\phi_1)| = \mathrm{rnk}(\phi_1)\,) \tag{2.37}$$

So first we show that $\mathrm{rnk}(\phi_1) \leq \mathrm{rnk}(\phi)$. Let $\psi \sim \phi$ where $\sim$ denotes the substitution congruence on $\mathbf{P}(V)$. We need to show that $\mathrm{rnk}(\phi_1) \leq |\mathrm{Var}(\psi)|$. Using theorem (12) of page 132, from the equivalence $\psi \sim \phi$ we see that ψ is either of the form $\psi = \forall x \psi_1$ where $\psi_1 \sim \phi_1$, or ψ is of the form $\psi = \forall y \psi_1$ where $\psi_1 \sim \phi_1[y:x]$, $x \neq y$ and $y \notin \mathrm{Fr}(\phi_1)$. First we assume that $\psi = \forall x \psi_1$ where $\psi_1 \sim \phi_1$. Then we have the following inequalities:

$$\begin{aligned} \mathrm{rnk}(\phi_1) &\leq |\mathrm{Var}(\psi_1)| \\ &\leq |\{x\} \cup \mathrm{Var}(\psi_1)| \\ &= |\mathrm{Var}(\forall x \psi_1)| \\ &= |\mathrm{Var}(\psi)| \end{aligned}$$

Next we assume that $\psi = \forall y \psi_1$ where $\psi_1 \sim \phi_1[y:x]$, $x \neq y$ and $y \notin \mathrm{Fr}(\phi_1)$. The permutation $[y:x]$ being injective, from proposition (81) we obtain $\psi_1^* \sim \phi_1$ where $\psi_1^* = \psi_1[y:x]$. Furthermore, defining $\psi^* = \forall x \psi_1^*$ we have $\psi = \psi^*[y:x]$. Using the injectivity of $[y:x]$ once more and proposition (35) we obtain:

$$|\mathrm{Var}(\psi)| = |\mathrm{Var}(\psi^*[y:x])| = |\,[y:x](\mathrm{Var}(\psi^*))\,| = |\mathrm{Var}(\psi^*)|$$

So we need to prove that $\mathrm{rnk}(\phi_1) \leq |\mathrm{Var}(\psi^*)|$ where $\psi^* = \forall x \psi_1^*$ and $\psi_1^* \sim \phi_1$. Hence we are back to our initial case and we have proved that $\mathrm{rnk}(\phi_1) \leq \mathrm{rnk}(\phi)$.

Next we show that $\mathrm{rnk}(\phi) \leq \mathrm{rnk}(\phi_1)+1$. So let $\psi_1 \sim \phi_1$. We need to show that $\mathrm{rnk}(\phi) - 1 \leq |\mathrm{Var}(\psi_1)|$ or equivalently that $\mathrm{rnk}(\phi) \leq |\mathrm{Var}(\psi_1)| + 1$:

$$\begin{array}{rcl} \mathrm{rnk}(\phi) & = & \mathrm{rnk}(\forall x \phi_1) \\ \forall x \phi_1 \sim \forall x \psi_1 \ \rightarrow & \leq & |\mathrm{Var}(\forall x \psi_1)| \\ & = & |\{x\} \cup \mathrm{Var}(\psi_1)| \\ & \leq & |\mathrm{Var}(\psi_1)| + 1 \end{array}$$

So we are done proving the inequalities (2.36). We shall complete the proof of this proposition by showing the equivalence (2.37). First we show $\Rightarrow$: so we assume that $\epsilon = 1$. We need to show that $x \notin \mathrm{Fr}(\phi_1)$ and furthermore that $|\mathrm{Fr}(\phi_1)| = \mathrm{rnk}(\phi_1)$. First we show that $x \notin \mathrm{Fr}(\phi_1)$. So suppose to the contrary that $x \in \mathrm{Fr}(\phi_1)$. We shall obtain a contradiction by showing $\epsilon = 0$, that is $\mathrm{rnk}(\phi_1) = \mathrm{rnk}(\phi)$. We already know that $\mathrm{rnk}(\phi_1) \leq \mathrm{rnk}(\phi)$. So we need to show that $\mathrm{rnk}(\phi) \leq \mathrm{rnk}(\phi_1)$. So let $\psi_1 \sim \phi_1$. We need to show that $\mathrm{rnk}(\phi) \leq |\mathrm{Var}(\psi_1)|$. However, from $\psi_1 \sim \phi_1$ and proposition (79) we obtain $\mathrm{Fr}(\psi_1) = \mathrm{Fr}(\phi_1)$ and in particular $x \in \mathrm{Fr}(\psi_1)$. It follows that:

$$\begin{array}{rcl} \mathrm{rnk}(\phi) & = & \mathrm{rnk}(\forall x \phi_1) \\ \forall x \phi_1 \sim \forall x \psi_1 \ \rightarrow & \leq & |\mathrm{Var}(\forall x \psi_1)| \\ & = & |\{x\} \cup \mathrm{Var}(\psi_1)| \\ x \in \mathrm{Fr}(\psi_1) \subseteq \mathrm{Var}(\psi_1) \ \rightarrow & = & |\mathrm{Var}(\psi_1)| \end{array}$$

This is our desired contradiction and we conclude that $x \notin \mathrm{Fr}(\phi_1)$. It remains to show that $|\mathrm{Fr}(\phi_1)| = \mathrm{rnk}(\phi_1)$. So suppose this equality does not hold. We shall obtain a contradiction by showing $\epsilon = 0$, that is $\mathrm{rnk}(\phi) \leq \mathrm{rnk}(\phi_1)$. So let $\psi_1 \sim \phi_1$. We need to show once again that $\mathrm{rnk}(\phi) \leq |\mathrm{Var}(\psi_1)|$. However, having assumed the equality $|\mathrm{Fr}(\phi_1)| = \mathrm{rnk}(\phi_1)$ does not hold, from proposition (103) we obtain $|\mathrm{Fr}(\phi_1)| < \mathrm{rnk}(\phi_1)$ and consequently from $\psi_1 \sim \phi_1$ we have:

$$|\mathrm{Fr}(\psi_1)| = |\mathrm{Fr}(\phi_1)| < \mathrm{rnk}(\phi_1) \leq |\mathrm{Var}(\psi_1)|$$

It follows that the set $\mathrm{Var}(\psi_1) \setminus \mathrm{Fr}(\psi_1)$ cannot be empty, and there exists $y \in \mathrm{Var}(\psi_1) \setminus \mathrm{Fr}(\psi_1)$. From $x \notin \mathrm{Fr}(\phi_1)$ and $y \notin \mathrm{Fr}(\psi_1) = \mathrm{Fr}(\phi_1)$ using proposition (80) we obtain the equivalence $\forall x \phi_1 \sim \forall y \phi_1$. Hence we also have the equivalence $\forall x \phi_1 \sim \forall y \psi_1$ and consequently:

$$\begin{array}{rcl} \mathrm{rnk}(\phi) & = & \mathrm{rnk}(\forall x \phi_1) \\ \forall x \phi_1 \sim \forall y \psi_1 \ \rightarrow & \leq & |\mathrm{Var}(\forall y \psi_1)| \\ & = & |\{y\} \cup \mathrm{Var}(\psi_1)| \\ y \in \mathrm{Var}(\psi_1) \ \rightarrow & = & |\mathrm{Var}(\psi_1)| \end{array}$$

which is our desired contradiction and we conclude that $|\mathrm{Fr}(\phi_1)| = \mathrm{rnk}(\phi_1)$. This completes our proof of $\Rightarrow$ in the equivalence (2.37). We now prove $\Leftarrow$:

so we assume that $x \notin \mathrm{Fr}(\phi_1)$ and $|\mathrm{Fr}(\phi_1)| = \mathrm{rnk}(\phi_1)$. We need to show that $\epsilon = 1$, that is $\mathrm{rnk}(\phi) = \mathrm{rnk}(\phi_1) + 1$. We already have the inequality $\mathrm{rnk}(\phi) \leq \mathrm{rnk}(\phi_1) + 1$. So it remains to show that $\mathrm{rnk}(\phi_1) + 1 \leq \mathrm{rnk}(\phi)$ or equivalently $\mathrm{rnk}(\phi_1) < \mathrm{rnk}(\phi)$. So let $\psi \sim \phi$. We need to show that $\mathrm{rnk}(\phi_1) < |\mathrm{Var}(\psi)|$. Once again, using theorem (12) of page 132, from the equivalence $\psi \sim \phi$ we see that ψ is either of the form $\psi = \forall x \psi_1$ where $\psi_1 \sim \phi_1$, or ψ is of the form $\psi = \forall y \psi_1$ where $\psi_1 \sim \phi_1[y:x]$, $x \neq y$ and $y \notin \mathrm{Fr}(\phi_1)$. First we assume that $\psi = \forall x \psi_1$ where $\psi_1 \sim \phi_1$. Hence $\mathrm{rnk}(\phi_1) \leq |\mathrm{Var}(\psi_1)|$ and we shall distinguish two further cases: first we assume that $\mathrm{rnk}(\phi_1) = |\mathrm{Var}(\psi_1)|$. Having assumed that $|\mathrm{Fr}(\phi_1)| = \mathrm{rnk}(\phi_1)$ we obtain:

$$|\mathrm{Fr}(\psi_1)| = |\mathrm{Fr}(\phi_1)| = \mathrm{rnk}(\phi_1) = |\mathrm{Var}(\psi_1)|$$

from which we see that $\mathrm{Var}(\psi_1) = \mathrm{Fr}(\psi_1)$ and consequently it follows that $x \notin \mathrm{Fr}(\phi_1) = \mathrm{Fr}(\psi_1) = \mathrm{Var}(\psi_1)$. Hence we see that:

$$\begin{array}{rcl} \mathrm{rnk}(\phi_1) & \leq & |\mathrm{Var}(\psi_1)| \\ x \notin \mathrm{Var}(\psi_1) \ \rightarrow & < & |\{x\} \cup \mathrm{Var}(\psi_1)| \\ & = & |\mathrm{Var}(\forall x \psi_1)| \\ & = & |\mathrm{Var}(\psi)| \end{array}$$

So we now assume that $\mathrm{rnk}(\phi_1) < |\mathrm{Var}(\psi_1)|$, in which case we obtain:

$$\begin{array}{rcl} \mathrm{rnk}(\phi_1) & < & |\mathrm{Var}(\psi_1)| \\ & \leq & |\{x\} \cup \mathrm{Var}(\psi_1)| \\ & = & |\mathrm{Var}(\forall x \psi_1)| \\ & = & |\mathrm{Var}(\psi)| \end{array}$$

We now consider the case when $\psi = \forall y \psi_1$ where $\psi_1 \sim \phi_1[y:x]$, $x \neq y$ and $y \notin \mathrm{Fr}(\phi_1)$. Once again, defining $\psi_1^* = \psi_1[y:x]$ and $\psi^* = \forall x \psi_1^*$ we obtain the equivalence $\psi_1^* \sim \phi_1$ and $|\mathrm{Var}(\psi^*)| = |\mathrm{Var}(\psi)|$. So we need to prove that $\mathrm{rnk}(\phi_1) < |\mathrm{Var}(\psi^*)|$ knowing that $\psi_1^* \sim \phi_1$ which follows from our initial case.
.

As already discussed, our objective is to show the existence of a $\psi \in \mathbf{P}(W)$ such that $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M}(\psi)$ provided we have $\mathrm{rnk}(\bar{\sigma} \circ \mathcal{M}(\phi)) \leq |W|$. Assuming we prove this result, it will be important for us to have a way of telling whether the condition $\mathrm{rnk}(\bar{\sigma} \circ \mathcal{M}(\phi)) \leq |W|$ is satisfied. The following proposition allows us to do this. Given any map $\sigma : V \rightarrow W$, the associated variable substitution $\sigma : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$ cannot increase the substitution rank of a formula. Hence:

$$\mathrm{rnk}(\bar{\sigma} \circ \mathcal{M}(\phi)) \leq \mathrm{rnk}(\mathcal{M}(\phi)) = \mathrm{rnk}(\phi) \leq |\mathrm{Var}(\phi)| \leq |V|$$

So we see for example that the condition $|V| \leq |W|$ is a sufficient condition. Note the following proposition makes no assumption on the validity of σ for ϕ.

Proposition 110 *Let V, W be sets and $\sigma : V \rightarrow W$ be a map. Let $\phi \in \mathbf{P}(V)$:*

$$\mathrm{rnk}(\sigma(\phi)) \leq \mathrm{rnk}(\phi)$$

where $\sigma : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$ denotes the associated substitution mapping.

Proof
We shall prove $\mathrm{rnk}(\sigma(\phi)) \leq \mathrm{rnk}(\phi)$ by structural induction using theorem (3) of page 31. First we assume that $\phi = (x \in y)$ for some $x, y \in V$. Then we have:

$$\mathrm{rnk}(\sigma(\phi)) = |\,\{\sigma(x), \sigma(y)\}\,| \leq |\,\{x, y\}\,| = \mathrm{rnk}(\phi)$$

Next we assume that $\phi = \bot$. Then $\mathrm{rnk}(\sigma(\phi)) = \mathrm{rnk}(\bot) = 0 = \mathrm{rnk}(\phi)$. So we now assume that $\phi = \phi_1 \to \phi_2$ where $\phi_1, \phi_2 \in \mathbf{P}(V)$ satisfy our property:

$$\begin{array}{rcl}
\mathrm{rnk}(\sigma(\phi)) & = & \mathrm{rnk}(\sigma(\phi_1 \to \phi_2)) \\
& = & \mathrm{rnk}(\sigma(\phi_1) \to \sigma(\phi_2)) \\
\text{prop. (108)} \;\to & = & \max(\,|\,\mathrm{Fr}(\sigma(\phi))\,|\,,\, \mathrm{rnk}(\sigma(\phi_1))\,,\, \mathrm{rnk}(\sigma(\phi_2))\,) \\
& \leq & \max(\,|\,\mathrm{Fr}(\sigma(\phi))\,|\,,\, \mathrm{rnk}(\phi_1)\,,\, \mathrm{rnk}(\phi_2)\,) \\
\text{prop. (43)} \;\to & \leq & \max(\,|\,\sigma(\mathrm{Fr}(\phi))\,|\,,\, \mathrm{rnk}(\phi_1)\,,\, \mathrm{rnk}(\phi_2)\,) \\
& \leq & \max(\,|\mathrm{Fr}(\phi)|\,,\, \mathrm{rnk}(\phi_1)\,,\, \mathrm{rnk}(\phi_2)\,) \\
\text{prop. (108)} \;\to & = & \mathrm{rnk}(\phi)
\end{array}$$

Finally we assume that $\phi = \forall x \phi_1$ where $x \in V$ and $\phi_1 \in \mathbf{P}(V)$ satisfy our induction property. Then $\sigma(\phi) = \forall \sigma(x) \sigma(\phi_1)$. Let $\epsilon = \mathrm{rnk}(\phi) - \mathrm{rnk}(\phi_1)$ and let $\eta = \mathrm{rnk}(\sigma(\phi)) - \mathrm{rnk}(\sigma(\phi_1))$. From proposition (109) we know that $\epsilon, \eta \in 2$. We shall distinguish two cases: first we assume that $\eta = 0$. Then we have:

$$\mathrm{rnk}(\sigma(\phi)) = \mathrm{rnk}(\sigma(\phi_1)) \leq \mathrm{rnk}(\phi_1) \leq \mathrm{rnk}(\phi)$$

Next we assume that $\eta = 1$. We shall distinguish two further cases: if $\epsilon = 1$:

$$\mathrm{rnk}(\sigma(\phi)) = 1 + \mathrm{rnk}(\sigma(\phi_1)) \leq 1 + \mathrm{rnk}(\phi_1) = \mathrm{rnk}(\phi)$$

So it remains to deal with the last possibility when $\eta = 1$ and $\epsilon = 0$. Using proposition (109), from $\epsilon = 0$ we see that $x \in \mathrm{Fr}(\phi_1)$ or $|\mathrm{Fr}(\phi_1)| < \mathrm{rnk}(\phi_1)$. So we shall distinguish two further cases. These cases may not be exclusive of one another but we don't need them to be. So first we assume $x \in \mathrm{Fr}(\phi_1)$. Using proposition (109) again, from $\eta = 1$ we obtain $|\mathrm{Fr}(\sigma(\phi_1))| = \mathrm{rnk}(\sigma(\phi_1))$ and furthermore $\sigma(x) \notin \mathrm{Fr}(\sigma(\phi_1))$. Having assumed that $x \in \mathrm{Fr}(\phi_1)$ it follows that $\sigma(x)$ is an element of $\sigma(\mathrm{Fr}(\phi_1))$ but not an element of $\mathrm{Fr}(\sigma(\phi_1))$. Hence, we see that the inclusion $\mathrm{Fr}(\sigma(\phi_1)) \subseteq \sigma(\mathrm{Fr}(\phi_1))$ which we know is true from proposition (43) is in fact a strict inclusion. So we have a strict inequality between the finite cardinals $|\mathrm{Fr}(\sigma(\phi_1))| < |\sigma(\mathrm{Fr}(\phi_1))|$. Thus:

$$\begin{array}{rcl}
\mathrm{rnk}(\sigma(\phi)) & = & 1 + \mathrm{rnk}(\sigma(\phi_1)) \\
|\mathrm{Fr}(\sigma(\phi_1))| = \mathrm{rnk}(\sigma(\phi_1)) \;\to & = & 1 + |\mathrm{Fr}(\sigma(\phi_1))| \\
|\mathrm{Fr}(\sigma(\phi_1))| < |\sigma(\mathrm{Fr}(\phi_1))| \;\to & \leq & |\sigma(\mathrm{Fr}(\phi_1))| \\
& \leq & |\mathrm{Fr}(\phi_1)| \\
\text{prop. (103)} \;\to & \leq & \mathrm{rnk}(\phi_1) \\
\epsilon = 0 \;\to & = & \mathrm{rnk}(\phi)
\end{array}$$

So we now assume that $|\mathrm{Fr}(\phi_1)| < \mathrm{rnk}(\phi_1)$. In this case we have:

$$\begin{array}{rcl} \mathrm{rnk}(\sigma(\phi)) & = & 1 + \mathrm{rnk}(\sigma(\phi_1)) \\ |\mathrm{Fr}(\sigma(\phi_1))| = \mathrm{rnk}(\sigma(\phi_1)) \ \rightarrow & = & 1 + |\mathrm{Fr}(\sigma(\phi_1))| \\ \text{prop. (43)} \ \rightarrow & \leq & 1 + |\sigma(\mathrm{Fr}(\phi_1))| \\ & \leq & 1 + |\mathrm{Fr}(\phi_1)| \\ |\mathrm{Fr}(\phi_1)| < \mathrm{rnk}(\phi_1) \ \rightarrow & \leq & \mathrm{rnk}(\phi_1) \\ \epsilon = 0 \ \rightarrow & = & \mathrm{rnk}(\phi) \end{array}$$

.

Proposition 111 *Let V be a set and $n \in \mathbf{N}$ such that $n \leq |V|$. Then there exists a formula $\phi \in \mathbf{P}(V)$ such that $\mathrm{Fr}(\phi) = \emptyset$ and $\mathrm{rnk}(\phi) = n$.*

Proof
From the inequality $n \leq |V|$ there exists an injective map $u : n \to V$. Define $\psi_0 = \perp$ and $\psi_{k+1} = (u(k) \in u(k)) \to \psi_k$ for $k \in n$. Let $\psi = \psi_n$. For example, in the case when $n = 2$ the formula ψ is given by:

$$\psi = (\, u(1) \in u(1)\,) \to [\,(\, u(0) \in u(0)\,) \to \perp\,]$$

Define $\phi_0 = \psi$ and $\phi_{k+1} = \forall u(k)\, \phi_k$ for $k \in n$. Let $\phi = \phi_n$. We shall complete the proof of this proposition by showing that $\mathrm{Fr}(\phi) = \emptyset$ and $\mathrm{rnk}(\phi) = n$. First we prove that $\mathrm{Fr}(\phi) = \emptyset$. From the recursion $\psi_{k+1} = (u(k) \in u(k)) \to \psi_k$:

$$\mathrm{Fr}(\psi_{k+1}) = \{u(k)\} \cup \mathrm{Fr}(\psi_k)\ ,\ k \in n$$

Since $\mathrm{Fr}(\psi_0) = \mathrm{Fr}(\perp) = \emptyset$ an easy induction argument shows that we have $\mathrm{Fr}(\psi_k) = u[k]$ for all $k \in n+1$. Note that $u[k]$ denotes the image of the set k by u, i.e. the range of the restricted map $u_{|k}$. We are using the square brackets $[\,.\,]$ to avoid any confusion between $u[k]$ and $u(k)$. In particular for $k = n$ we see that $\mathrm{Fr}(\psi) = \mathrm{Fr}(\psi_n) = u[n] = \mathrm{rng}(u)$. Furthermore, from the recursion formula $\phi_{k+1} = \forall u(k)\, \phi_k$ we obtain the equality:

$$\mathrm{Fr}(\phi_{k+1}) = \mathrm{Fr}(\phi_k) \setminus \{u(k)\}\ ,\ k \in n$$

Since $\mathrm{Fr}(\phi_0) = \mathrm{Fr}(\psi) = \mathrm{rng}(u)$, an easy induction argument shows that $\mathrm{Fr}(\phi_k) = \mathrm{rng}(u) \setminus u[k]$ for all $k \in n+1$. In particular for $k = n$ we have the equality $\mathrm{Fr}(\phi) = \mathrm{Fr}(\phi_n) = \mathrm{rng}(u) \setminus u[n] = \emptyset$ as requested. So it remains to show that $rnk(\phi) = n$. Using proposition (109), from the recursion formula $\phi_{k+1} = \forall u(k)\, \phi_k$ and the fact that $u(k) \in \mathrm{rng}(u) \setminus u[k] = \mathrm{Fr}(\phi_k)$ we obtain $\mathrm{rnk}(\phi_k) = \mathrm{rnk}(\phi_{k+1})$. Note that $u(k) \in \mathrm{rng}(u) \setminus u[k]$ is true since u is injective. Hence we see that $\mathrm{rnk}(\psi) = \mathrm{rnk}(\phi_0) = \mathrm{rnk}(\phi)$ and it is sufficient to prove that $\mathrm{rnk}(\psi) = n$. However having proved $\mathrm{Fr}(\psi_k) = u[k]$, it follows from the injectivity of u that $|\mathrm{Fr}(\psi_k)| = k$ for all $k \in n + 1$. From the recursion formula $\psi_{k+1} = (u(k) \in u(k)) \to \psi_k$ using proposition (108) we obtain:

$$\mathrm{rnk}(\psi_{k+1}) = \max(\, |\mathrm{Fr}(\psi_{k+1})|\,,\, \mathrm{rnk}(u(k) \in u(k))\,,\, \mathrm{rnk}(\psi_k)\,)$$

that is $\text{rnk}(\psi_{k+1}) = \max(k+1, 1, \text{rnk}(\psi_k))$ for all $k \in n$. Since $\text{rnk}(\psi_0) = 0$, a simple induction argument shows that $\text{rnk}(\psi_k) = k$ for all $k \in n+1$. In particular for $k = n$ we obtain $\text{rnk}(\psi) = \text{rnk}(\psi_n) = n$ as requested. **.**

2.3.7 Existence of Essential Substitution

Given a map $\sigma : V \to W$ we would like to prove the existence of an *essential substitution mapping*, namely a map as defined below. Recall that the minimal transform and minimal extension can be found in definitions (38) and (39):

Definition 43 *Let V, W be sets and $\sigma : V \to W$ be a map. We call* essential substitution mapping *associated with σ, any map $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ such that:*

$$\mathcal{M} \circ \sigma^* = \bar{\sigma} \circ \mathcal{M} \tag{2.38}$$

where $\bar{\sigma} : \bar{V} \to \bar{W}$ is the minimal extension and $\mathcal{M}$ is the minimal transform.

We cannot expect an essential substitution mapping to be uniquely defined. If $\sim$ denotes the substitution congruence on $\mathbf{P}(W)$ then from theorem (14) of page 149, any other map $\tau^* : \mathbf{P}(V) \to \mathbf{P}(W)$ satisfying $\tau^*(\phi) \sim \sigma^*(\phi)$ for all $\phi \in \mathbf{P}(V)$ will also satisfy equation (2.38). However, if $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ does indeed satisfy equation (2.38), then for all $\phi \in \mathbf{P}(V)$ the equivalence class of $\sigma^*(\phi)$ modulo the substitution congruence is uniquely determined. This is the best we can do. The notion of an *essential substitution mapping* σ^* associated with a map σ we feel plays an important role. If $\phi \in \mathbf{P}(V)$ is such that σ is valid for ϕ, then it follows from theorem (13) of page 146 that $\sigma^*(\phi) \sim \sigma(\phi)$ where $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ denotes the usual variable substitution mapping of definition (24). So σ^* can be viewed as a natural extension of $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ which thanks to equation (2.38), assigns a meaningful formula $\sigma^*(\phi)$ even in the case when σ is not a valid substitution for ϕ. This fundamentally allows us to write $\forall x\phi \to \phi[y/x]^*$ as a valid instance of the specialization axioms for all $y \in V$, without having to worry whether the substitution $[y/x]$ is valid for ϕ. For example, if $\phi = \forall y(x \in y)$ with $x \neq y$, we shall now be able to claim that $\forall x\phi \to \forall x(y \in x)$ is a legitimate axiom. So our aim is to prove the existence of an essential substitution mapping $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ associated with σ, at least when W is a large enough set. Given $\phi \in \mathbf{P}(V)$ the first step in our proof is to show the existence of a formula $\psi \in \mathbf{P}(W)$ such that $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M}(\psi)$. As already discussed in the previous section, we cannot hope to obtain the existence of ψ without some condition on the set W. We conjectured the substitution rank of $\bar{\sigma} \circ \mathcal{M}(\phi)$ had to be smaller than $|W|$, i.e. $\text{rnk}(\,\bar{\sigma} \circ \mathcal{M}(\phi)\,) \leq |W|$. So assuming this condition holds, we are setting out to prove the existence of ψ which is the object of theorem (17) below. Until now, most of our results have been obtained by structural induction arguments. In this case, structural induction does not seem to work. It appears the notion of *substitution rank* does not lend itself easily to induction, and we shall need to find some other route. So let us go back to the simple case when $\phi = \forall y(x \in y)$ with $x \neq y$. Assuming $\sigma(x) = u$ we obtain $\bar{\sigma} \circ \mathcal{M}(\phi) = \forall\, 0(u \in 0) \in \mathbf{P}(\bar{W})$.

Our first objective will be to show the existence of some $\psi_1 \in \mathbf{P}(\bar{W})$ such that $\mathrm{Var}(\psi_1) \subseteq W$ and $\bar{\sigma} \circ \mathcal{M}(\phi) \sim \psi_1$ where $\sim$ denotes the substitution congruence on $\mathbf{P}(\bar{W})$. Hopefully the condition $\mathrm{rnk}(\,\bar{\sigma} \circ \mathcal{M}(\phi)\,) \leq |W|$ will allow us to do that using proposition (104). Following our example, the formula ψ_1 would look something like $\psi_1 = \forall v(u \in v) \in \mathbf{P}(\bar{W})$ for some $v \in W$ and $u \neq v$. Once we have the formula ψ_1 we can easily project it onto $\mathbf{P}(W)$ and define $\psi = q(\psi_1)$ where $q : \bar{W} \to W$ is an appropriate substitution. Having defined a formula $\psi \in \mathbf{P}(W)$ it will remain to show that:

$$\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M}(\psi) \tag{2.39}$$

We shall proceed as follows: we first consider the operator $\mathcal{N} : \mathbf{P}(\bar{W}) \to \mathbf{P}(\bar{W})$ defined by $\mathcal{N} = p \circ \bar{\mathcal{M}}$ where $p : \bar{\bar{W}} \to \bar{W}$ is an appropriate substitution and $\bar{\mathcal{M}} : \mathbf{P}(\bar{W}) \to \mathbf{P}(\bar{\bar{W}})$ is the minimal transform mapping. From the equivalence $\bar{\sigma} \circ \mathcal{M}(\phi) \sim \psi_1$ and theorem (14) of page 149 we obtain immediately:

$$\mathcal{N} \circ \bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{N}(\psi_1) \tag{2.40}$$

We then prove that $\mathcal{N} \circ \bar{\sigma} \circ \mathcal{M}(\phi) = \bar{\sigma} \circ \mathcal{M}(\phi)$ so as to obtain:

$$\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{N}(\psi_1) \tag{2.41}$$

Using the injection $i : W \to \bar{W}$ we finally prove that the minimal transform $\mathcal{M} : \mathbf{P}(W) \to \mathbf{P}(\bar{W})$ is in fact given by $\mathcal{M} = \mathcal{N} \circ i$, and we conclude by arguing that $\psi_1 = i \circ q(\psi_1) = i(\psi)$ which gives us equation (2.39) from (2.41).

Before we formally define the operator $\mathcal{N}$, we shall say a few words on the minimal extension $\bar{\bar{V}}$ of the set $\bar{V}$ which is itself the minimal extension of V. From definition (37) the minimal extension $\bar{V}$ is defined as:

$$\bar{V} = \{0\} \times V \cup \{1\} \times \mathbf{N}$$

Hence we have $\bar{\bar{V}} = \{0\} \times \bar{V} \cup \{1\} \times \mathbf{N}$. So the set $\bar{\bar{V}}$ contains three types of elements: those of the form $(0,(0,x))$ which we simply identify with $x \in V$, those of the form $(0,(1,n))$ which we identify with $n \in \mathbf{N}$, and those of the form $(1,n)$ which we denote $\bar{n}$ for all $n \in \mathbf{N}$. Thus, in the interest of lighter notations, we regard $\bar{\bar{V}}$ as the disjoint union $\bar{\bar{V}} = V \uplus \mathbf{N} \uplus \bar{\mathbf{N}}$ where $\bar{\mathbf{N}}$ is the image of $\mathbf{N}$ through the embedding $n \to \bar{n}$. So for example, if $\phi = \forall y(x \in y) \in \mathbf{P}(V)$, we shall continue to denote the minimal transform of ϕ as $\mathcal{M}(\phi) = \forall\, 0(x \in 0)$, while the minimal transform of $\mathcal{M}(\phi)$ is denoted $\bar{\mathcal{M}} \circ \mathcal{M}(\phi) = \forall\, \bar{0}(x \in \bar{0}) \in \mathbf{P}(\bar{\bar{V}})$. With these notational conventions in mind, we can now state:

Definition 44 *Let V be a set. We call* weak transform *on $\mathbf{P}(\bar{V})$ the map $\mathcal{N} : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{V})$ defined by $\mathcal{N} = p \circ \bar{\mathcal{M}}$ where $\bar{\mathcal{M}} : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{\bar{V}})$ is the minimal transform mapping and $p : \bar{\bar{V}} \to \bar{V}$ is defined by:*

$$\forall u \in \bar{\bar{V}}\ ,\ p\,(u) = \begin{cases} u & \text{if} \quad u \in \bar{V} \\ n & \text{if} \quad u = \bar{n} \in \bar{\mathbf{N}} \end{cases}$$

So for example, if $\phi = \forall 0(x \in 0) \in \mathbf{P}(\bar{V})$ we obtain $\bar{\mathcal{M}}(\phi) = \forall \bar{0}(x \in \bar{0})$ and consequently $\mathcal{N}(\phi) = \forall 0(x \in 0) = \phi$. However, if $\phi = \forall 1(0 \in 1)$ then $\bar{\mathcal{M}}(\phi) = \forall \bar{0}(0 \in \bar{0})$ and $\mathcal{N}(\phi) = \forall 0(0 \in 0)$. This last equality shows the limitations of the operator $\mathcal{N}$. It is not a very interesting operator, as the substitution equivalence $\mathcal{N}(\phi) \sim \phi$ is not necessarily preserved. On the positive side, the operator $\mathcal{N}$ has a simple definition which will make our forthcoming proofs a lot easier. It also has the useful properties allowing us to prove theorem (17):

Lemma 12 *Let V be a set and $\mathcal{N} : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{V})$ be the weak transform on $\mathbf{P}(\bar{V})$. Let $i : V \to \bar{V}$ be the inclusion map. Then we have:*

$$\mathcal{M} = \mathcal{N} \circ i$$

where $\mathcal{M} : \mathbf{P}(V) \to \mathbf{P}(\bar{V})$ is the minimal transform mapping.

Proof
Let $\bar{\mathcal{M}} : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{\bar{V}})$ be the minimal transform mapping and $p : \bar{\bar{V}} \to \bar{V}$ be the map of definition (43). Given $\phi \in \mathbf{P}(V)$, since $i : V \to \bar{V}$ is an injective map, in particular it is valid for ϕ. Hence we have:

$$\begin{aligned} \mathcal{N} \circ i(\phi) &= p \circ \bar{\mathcal{M}} \circ i(\phi) \\ \text{theorem (13)} \ \to \ &= p \circ \bar{i} \circ \mathcal{M}(\phi) \\ \text{A: to be proved} \ \to \ &= \mathcal{M}(\phi) \end{aligned}$$

So it remains to show that $p \circ \bar{i}(u) = u$ for all $u \in \bar{V}$, where $\bar{i} : \bar{V} \to \bar{\bar{V}}$ is the minimal extension of i. So let $u \in \bar{V}$. We shall distinguish two cases: first we assume that $u \in V$. Then $\bar{i}(u) = i(u) = u$ and consequently $p \circ \bar{i}(u) = p\,(u) = u$ as requested. Next we assume that $u \in \mathbf{N}$. Then $\bar{i}(u) = \bar{u}$ and it follows that $p \circ \bar{i}(u) = p\,(\bar{u}) = u$. So this appears to complete our proof. However, we feel this proof is not completely convincing, particularly with regards to the step $\bar{i}(u) = \bar{u}$. A blind reading of definition (39) for the minimal extension $\bar{i} : \bar{V} \to \bar{\bar{V}}$ seems to indicate that $\bar{i}(u) = u$ whenever $u \in \mathbf{N}$. But of course, the wording of definition (39) is the result of identifications, which are now possibly confusing us. So let $i_2 : \mathbf{N} \to \bar{V}$ and $j_2 : \mathbf{N} \to \bar{\bar{V}}$ be the inclusion maps. What is really meant by definition (39) is that $\bar{i} \circ i_2(u) = j_2(u)$ for all $u \in \mathbf{N}$. In our discussion prior to stating definition (43) we agreed to denote $j_2(u)$ as $\bar{u}$. Hence if we identify u and $i_2(u)$ we obtain $\bar{i}(u) = \bar{u}$ as claimed. So let us pursue this further and make all our identifications explicit. The wording of definition (43) is itself the result of identifications. Given $u \in \mathbf{N}$ the formula $p(\bar{u}) = u$ should be rigorously written as $p \circ j_2(u) = i_2(u)$. So given $u \in \mathbf{N}$, if we identify u and $i_2(u) \in \bar{V}$ we have the following equalities:

$$\begin{aligned} p \circ \bar{i}(u) &= p \circ \bar{i} \circ i_2(u) \\ \text{def. (39)} \ \to \ &= p \circ j_2(u) \\ \text{def. (43)} \ \to \ &= i_2(u) \\ \text{identification} \ \to \ &= u \end{aligned}$$

Likewise, if we denote $i_1 : V \to \bar{V}$ and $j_1 : \bar{V} \to \bar{\bar{V}}$ the inclusion mappings, and identify $i_1(u)$ and u for all $u \in V$, we obtain the following equalities:

$$\begin{aligned} p \circ \bar{i}(u) &= p \circ \bar{i} \circ i_1(u) \\ \text{def. (39)} \ \to &= p \circ j_1 \circ i(u) \\ \text{def. (43)} \ \to &= i(u) \\ i = i_1 \ \to &= i_1(u) \\ \text{identification} \ \to &= u \end{aligned}$$

.

Lemma 13 *Let V, W be sets and $\sigma : V \to W$ be a map. Then:*

$$\mathcal{N} \circ \bar{\sigma} \circ \mathcal{M} = \bar{\sigma} \circ \mathcal{M}$$

where $\mathcal{N} : \mathbf{P}(\bar{W}) \to \mathbf{P}(\bar{W})$ is the weak transform on $\mathbf{P}(\bar{W})$.

Proof
For once we shall be able to prove the formula without resorting to a structural induction argument. In the interest of lighter notations, we shall keep the same notations $\mathcal{M}, \bar{\mathcal{M}}, \mathcal{N}$ and p in relation to the sets V and W. So let $\phi \in \mathbf{P}(V)$:

$$\begin{aligned} \mathcal{N} \circ \bar{\sigma} \circ \mathcal{M}(\phi) &= p \circ \bar{\mathcal{M}} \circ \bar{\sigma} \circ \mathcal{M}(\phi) \\ \text{theorem (13) of p. 146} \ \to &= p \circ \bar{\bar{\sigma}} \circ \bar{\mathcal{M}} \circ \mathcal{M}(\phi) \\ \text{prop. (99)} \ \to &= p \circ \bar{\bar{\sigma}} \circ \bar{\mathcal{M}} \circ i(\phi) \\ \text{A: to be proved} \ \to &= \bar{\sigma} \circ p \circ \bar{\mathcal{M}} \circ i(\phi) \\ &= \bar{\sigma} \circ \mathcal{N} \circ i(\phi) \\ \text{lemma (12)} \ \to &= \bar{\sigma} \circ \mathcal{M}(\phi) \end{aligned}$$

So it remains to show that $p \circ \bar{\bar{\sigma}}(u) = \bar{\sigma} \circ p\,(u)$ for all $u \in \bar{\bar{V}}$. So let $u \in \bar{\bar{V}}$. Since $\bar{\bar{V}}$ is the disjoint union of $\bar{V}$ and $\bar{\mathbf{N}}$, we shall distinguish two cases: first we assume that $u \in \bar{V}$. Then $\bar{\bar{\sigma}}(u) = \bar{\sigma}(u) \in \bar{W}$ and consequently $p \circ \bar{\bar{\sigma}}(u) = \bar{\sigma}(u)$. So the equality $p \circ \bar{\bar{\sigma}}(u) = \bar{\sigma} \circ p\,(u)$ is satisfied since $p\,(u) = u$ for $u \in \bar{V}$. Next we assume that $u \in \bar{\mathbf{N}}$ i.e. that $u = \bar{n}$ for some $n \in \mathbf{N}$. Then $\bar{\bar{\sigma}}(u) = u = \bar{n}$ and consequently $p \circ \bar{\bar{\sigma}}(u) = n = \bar{\sigma} \circ p\,(u)$. .

Before we move on to theorem (17) which is our key result, we should pause a moment on an interesting consequence of lemma (13). In general given ϕ and $\psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$ where $\sim$ is the substitution congruence, we cannot conclude that $\phi = \psi$. Likewise if $\bar{\phi}, \bar{\psi} \in \mathbf{P}(\bar{V})$ are substitution equivalent, we cannot conclude that that $\bar{\phi} = \bar{\psi}$. However, if both $\bar{\phi}$ and $\bar{\psi}$ are minimal transforms then things are different: it is in fact possible to infer the equality $\mathcal{M}(\phi) = \mathcal{M}(\psi)$ simply from the substitution equivalence $\mathcal{M}(\phi) \sim \mathcal{M}(\psi)$:

Proposition 112 *Let V be a set and $\phi, \psi \in \mathbf{P}(V)$. Then we have:*

$$\mathcal{M}(\phi) \sim \mathcal{M}(\psi) \;\Rightarrow\; \mathcal{M}(\phi) = \mathcal{M}(\psi)$$

where the relation $\sim$ denotes the substitution congruence on $\mathbf{P}(\bar{V})$.

Proof
We assume that $\mathcal{M}(\phi) \sim \mathcal{M}(\psi)$. We need to show that $\mathcal{M}(\phi) = \mathcal{M}(\psi)$. However, from theorem (14) of page 149 we obtain $\bar{\mathcal{M}} \circ \mathcal{M}(\phi) = \bar{\mathcal{M}} \circ \mathcal{M}(\psi)$, where $\bar{\mathcal{M}} : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{\bar{V}})$ is the minimal transform mapping. Hence, from definition (43), we see that $\mathcal{N} \circ \mathcal{M}(\phi) = \mathcal{N} \circ \mathcal{M}(\psi)$. Applying lemma (13) to $W = V$ and the identity mapping $\sigma : V \to V$ we conclude that $\mathcal{M}(\phi) = \mathcal{M}(\psi)$. **.**

For future reference, we also quote the following lemma:

Lemma 14 *Let V be a set and $p : \bar{\bar{V}} \to \bar{V}$ be the map of* definition (43)*. Then for all $\phi \in \mathbf{P}(V)$, the substitution p is valid for the formula $\bar{\mathcal{M}} \circ \mathcal{M}(\phi)$.*

Proof
Using proposition (53) it is sufficient to show that p is injective on the set $\mathrm{Var}(\bar{\mathcal{M}} \circ \mathcal{M}(\phi))$. First we shall show that p is injective on $V \cup \bar{\mathbf{N}}$: so suppose $u, v \in V \cup \bar{\mathbf{N}}$ are such that $p\,(u) = p\,(v)$. We need to show that $u = v$. We shall distinguish four cases: first we assume that $u, v \in V \subseteq \bar{V}$. Then $u = v$ follows immediately from definition (43). Next we assume that $u, v \in \bar{\mathbf{N}}$. Then $u = \bar{n}$ and $v = \bar{m}$ for some $n, m \in \mathbf{N}$. From $p\,(u) = p\,(v)$ we obtain $n = m$ and consequently $u = v$. Next we assume that $u \in V$ and $v \in \bar{\mathbf{N}}$. Then $v = \bar{m}$ for some $m \in \mathbf{N}$ and from $p\,(u) = p\,(v)$ we obtain $u = n$ which contradicts the fact that $V \cap \mathbf{N} = \emptyset$. So this case is in fact impossible. The case $u \in \bar{\mathbf{N}}$ and $v \in V$ is likewise impossible and we have proved that p is injective on $V \cup \bar{\mathbf{N}}$. So it remains to show that $\mathrm{Var}(\bar{\mathcal{M}} \circ \mathcal{M}(\phi)) \subseteq V \cup \bar{\mathbf{N}}$. Let $u \in \mathrm{Var}(\bar{\mathcal{M}} \circ \mathcal{M}(\phi))$. We need to show that $u \in V \cup \bar{\mathbf{N}}$. Since $\bar{\bar{V}} = \bar{V} \uplus \bar{\mathbf{N}}$, we shall distinguish two cases: first we assume that $u \in \bar{V}$. Then using proposition (97) we obtain:

$$u \in \mathrm{Var}(\bar{\mathcal{M}} \circ \mathcal{M}(\phi)) \cap \bar{V} = \mathrm{Fr}(\mathcal{M}(\phi)) = \mathrm{Fr}(\phi) \subseteq V \subseteq V \cup \bar{\mathbf{N}}$$

Next we assume that $u \in \bar{\mathbf{N}}$. Then it is clear that $u \in V \cup \bar{\mathbf{N}}$. **.**

Theorem 17 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\phi \in \mathbf{P}(V)$ with:*

$$\mathrm{rnk}(\,\bar{\sigma} \circ \mathcal{M}(\phi)\,) \leq |W|$$

where $\bar{\sigma} : \bar{V} \to \bar{W}$ is the minimal extension of σ and $\mathcal{M}(\phi)$ is the minimal transform of ϕ. Then, there exists $\psi \in \mathbf{P}(W)$ such that $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M}(\psi)$.

Proof
Our first step is to find $\psi_1 \in \mathbf{P}(\bar{W})$ such that $\bar{\sigma} \circ \mathcal{M}(\phi) \sim \psi_1$ and $\mathrm{Var}(\psi_1) \subseteq W$, where $\sim$ denotes the substitution congruence on $\mathbf{P}(\bar{W})$. We shall do so using proposition (104) applied to the set $\bar{W}$ and the formula $\bar{\sigma} \circ \mathcal{M}(\phi) \in \mathbf{P}(\bar{W})$. Suppose for now that we have proved the inclusion $\mathrm{Fr}(\bar{\sigma} \circ \mathcal{M}(\phi)) \subseteq W$. Then from the assumption $\mathrm{rnk}(\,\bar{\sigma} \circ \mathcal{M}(\phi)\,) \leq |W|$ and proposition (104) we obtain

the existence of $\psi_1 \in \mathbf{P}(\bar{W})$ such that $\bar{\sigma} \circ \mathcal{M}(\phi) \sim \psi_1$ and $\mathrm{Var}(\psi_1) \subseteq W$. In fact, proposition (104) allows to assume that $|\mathrm{Var}(\psi_1)| = \mathrm{rnk}(\, \bar{\sigma} \circ \mathcal{M}(\phi)\,)$ but we shall not be using this property. So we need to prove that $\mathrm{Fr}(\bar{\sigma} \circ \mathcal{M}(\phi)) \subseteq W$:

$$\begin{array}{rcl}
\mathrm{Fr}(\bar{\sigma} \circ \mathcal{M}(\phi)) & = & \mathrm{Fr}(\, \bar{\sigma}(\mathcal{M}(\phi))\,) \\
\text{prop. (43)} \;\rightarrow & \subseteq & \bar{\sigma}(\, \mathrm{Fr}(\mathcal{M}(\phi))\,) \\
\text{prop. (97)} \;\rightarrow & = & \bar{\sigma}(\mathrm{Fr}(\phi)) \\
\phi \in \mathbf{P}(V) \;\rightarrow & \subseteq & \bar{\sigma}(V) \\
\text{def. (39)} \;\rightarrow & = & \sigma(V) \\
& \subseteq & W
\end{array}$$

So the existence of $\psi_1 \in \mathbf{P}(\bar{W})$ such that $\bar{\sigma} \circ \mathcal{M}(\phi) \sim \psi_1$ and $\mathrm{Var}(\psi_1) \subseteq W$ is now established. Next we want to project ψ_1 onto $\mathbf{P}(W)$ by defining $\psi = q(\psi_1)$ where $q : \bar{W} \rightarrow W$ is a substitution such that $q(u) = u$ for all $u \in W$. To be rigorous, we need to define $q(n)$ for $n \in \mathbf{N}$ which we cannot do when $W = \emptyset$. So in the case when $W \neq \emptyset$, let $u^* \in W$ and define $q : \bar{W} \rightarrow W$ as follows:

$$\forall u \in \bar{W}\ ,\ q(u) = \left\{ \begin{array}{ll} u & \text{if} \quad u \in W \\ u^* & \text{if} \quad u \in \mathbf{N} \end{array} \right.$$

and consider the associated substitution mapping $q : \mathbf{P}(\bar{W}) \rightarrow \mathbf{P}(W)$. In the case when $W = \emptyset$, there exists no substitution $q : \bar{W} \rightarrow W$ but we can define the operator $q : \mathbf{P}(\bar{W}) \rightarrow \mathbf{P}(W)$ with the following structural recursion:

$$q(\chi) = \left\{ \begin{array}{lll} \bot & \text{if} & \chi = (u \in v) \\ \bot & \text{if} & \chi = \bot \\ q(\chi_1) \rightarrow q(\chi_2) & \text{if} & \chi = \chi_1 \rightarrow \chi_2 \\ \bot & \text{if} & \chi = \forall u \chi_1 \end{array} \right. \tag{2.42}$$

In both cases we set $\psi = q(\psi_1) \in \mathbf{P}(W)$. We shall complete the proof of the theorem by proving the equality $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M}(\psi)$. Using lemma (13) :

$$\begin{array}{rcl}
\bar{\sigma} \circ \mathcal{M}(\phi) & = & \mathcal{N} \circ \bar{\sigma} \circ \mathcal{M}(\phi) \\
\text{def. (43)} \;\rightarrow & = & p \circ \bar{\mathcal{M}} \circ \bar{\sigma} \circ \mathcal{M}(\phi) \\
\text{theorem (14) and } \bar{\sigma} \circ \mathcal{M}(\phi) \sim \psi_1 \;\rightarrow & = & p \circ \bar{\mathcal{M}}(\psi_1) \\
& = & \mathcal{N}(\psi_1) \\
\text{A: to be proved} \;\rightarrow & = & \mathcal{N} \circ i \circ q(\psi_1) \\
\psi = q(\psi_1) \;\rightarrow & = & \mathcal{N} \circ i(\psi) \\
\text{lemma (12)} \;\rightarrow & = & \mathcal{M}(\psi)
\end{array}$$

So it remains to show that $i \circ q(\psi_1) = \psi_1$ where $i : W \rightarrow \bar{W}$ is the inclusion map. As before, we shall distinguish two cases: first we assume that $W \neq \emptyset$. Then q arises from the substitution $q : \bar{W} \rightarrow W$ and from proposition (36) it is sufficient to prove that $i \circ q(u) = u$ for all $u \in \mathrm{Var}(\psi_1)$. Since $\mathrm{Var}(\psi_1) \subseteq W$ the

equality is clear. Next we assume that $W = \emptyset$. From the inclusion $\mathrm{Var}(\psi_1) \subseteq W$ it follows that $\mathrm{Var}(\psi_1) = \emptyset$ and it is therefore sufficient to prove the property:

$$\mathrm{Var}(\chi) = \emptyset \;\Rightarrow\; i \circ q(\chi) = \chi$$

for all $\chi \in \mathbf{P}(\bar{W})$. We shall do so by structural induction. Note that when $W = \emptyset$, the inclusion map $i : W \to \bar{W}$ is simply the map with empty domain, namely the empty set. First we assume that $\chi = (u \in v)$ for some $u, v \in \bar{W}$. Then the above implication is vacuously true. Next we assume that $\chi = \bot$. Then $i \circ q(\chi) = \chi$ is clear. So we now assume that $\chi = \chi_1 \to \chi_2$ where χ_1, χ_2 satisfy the above implication. We need to show the same is true of χ. So we assume that $\mathrm{Var}(\chi) = \emptyset$. We need to show that $i \circ q(\chi) = \chi$. However, from $\mathrm{Var}(\chi) = \emptyset$ we obtain $\mathrm{Var}(\chi_1) = \emptyset$ and $\mathrm{Var}(\chi_2) = \emptyset$. Having assumed χ_1 and χ_2 satisfy the implication, we obtain the equalities $i \circ q(\chi_1) = \chi_1$ and $i \circ q(\chi_2) = \chi_2$ from which $i \circ q(\chi) = \chi$ follows immediately. So it remains to check the case when $\chi = \forall u \chi_1$ for which the above implication is also vacuously true. **.**

Theorem 18 *Let V, W be sets and $\sigma : V \to W$ be a map. Then, there exists an essential substitution mapping $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ associated with σ, if and only if $|W|$ is an infinite cardinal or the inequality $|V| \leq |W|$ holds.*

Proof
First we prove the 'if' part: so we assume that $|W|$ is an infinite cardinal, or that it is finite with $|V| \leq |W|$. We need to prove the existence of an essential substitution mapping $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ associated with σ. Let $c : \mathcal{P}(\mathbf{P}(W)) \backslash \{\emptyset\} \to \mathbf{P}(W)$ be a choice function whose existence follows from the axiom of choice. Let us accept for now that for all $\phi \in \mathbf{P}(V)$, there exists some $\psi \in \mathbf{P}(W)$ such that $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M}(\psi)$. Given $\psi \in \mathbf{P}(W)$, let $[\psi]$ denote the congruence class of ψ modulo the substitution congruence, which is a non-empty subset of $\mathbf{P}(W)$. Define $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ by setting $\sigma^*(\phi) = c([\psi])$, where ψ is an arbitrary formula of $\mathbf{P}(W)$ such that $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M}(\psi)$. We need to check that σ^* is well defined, namely that $\sigma^*(\phi)$ is independent of the particular choice of ψ. But if ψ' is such that $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M}(\psi')$ then $\mathcal{M}(\psi) = \mathcal{M}(\psi')$ and it follows from theorem (14) of page 149 that $[\psi] = [\psi']$. So it remains to show the existence of ψ such that $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M}(\psi)$ for all $\phi \in \mathbf{P}(V)$. So let $\phi \in \mathbf{P}(V)$. Using theorem (17) of page 172 it is sufficient to prove that $\mathrm{rnk}(\,\bar{\sigma} \circ \mathcal{M}(\phi)\,) \leq |W|$. The substitution rank of a formula being always finite, this is clearly true if $|W|$ is infinite. Otherwise, using proposition (110) :

$$\begin{array}{rcl} \mathrm{rnk}(\,\bar{\sigma} \circ \mathcal{M}(\phi)\,) & \leq & \mathrm{rnk}(\mathcal{M}(\phi)) \\ \text{prop. (106)} \;\to & = & \mathrm{rnk}(\phi) \\ & \leq & |\mathrm{Var}(\phi)| \\ & \leq & |V| \\ |V| \leq |W| \;\to & \leq & |W| \end{array}$$

We now prove the 'only if' part: So we assume there exists $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ essential substitution associated with σ. We need to show that $|W|$ is an infinite

cardinal, or that it is finite with $|V| \leq |W|$. So suppose $|W|$ is a finite cardinal. There exists $n \in \mathbf{N}$ such that $|W| = n$. We need to show that $|V| \leq n$ holds. So we assume to the contrary that $n+1 \leq |V|$ and we shall derive a contradiction. Using proposition (111) there exists a formula $\phi \in \mathbf{P}(V)$ such that $\mathrm{Fr}(\phi) = \emptyset$ and $\mathrm{rnk}(\phi) = n+1$. Hence we have the following:

$$\begin{array}{rcl} n+1 & = & \mathrm{rnk}(\phi) \\ \text{prop. (106)} \ \rightarrow & = & \mathrm{rnk}(\mathcal{M}(\phi)) \\ \text{A: to be proved} \ \rightarrow & = & \mathrm{rnk}(\bar{\sigma} \circ \mathcal{M}(\phi)) \\ \sigma^* \text{ associated with } \sigma \ \rightarrow & = & \mathrm{rnk}(\mathcal{M} \circ \sigma^*(\phi)) \\ \text{prop. (106)} \ \rightarrow & = & \mathrm{rnk}(\sigma^*(\phi)) \\ & \leq & |\mathrm{Var}(\sigma^*(\phi))| \\ \sigma^*(\phi) \in \mathbf{P}(W) \ \rightarrow & \leq & |W| \\ & = & n \end{array}$$

which is our desired contradiction. So it remains to show $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M}(\phi)$. From proposition (36) it is enough to prove that $\bar{\sigma}(u) = u$ for all $u \in \mathrm{Var}(\mathcal{M}(\phi))$. Using definition (39) of the minimal extension $\bar{\sigma}$ it is sufficient to show that $\mathrm{Var}(\mathcal{M}(\phi)) \subseteq \mathbf{N}$. Since $\bar{V} = V \uplus \mathbf{N}$, it is therefore sufficient to prove that $\mathrm{Var}(\mathcal{M}(\phi)) \cap V = \emptyset$. However from proposition (97) we have the equality $\mathrm{Var}(\mathcal{M}(\phi)) \cap V = \mathrm{Fr}(\phi)$. So the result follows from $\mathrm{Fr}(\phi) = \emptyset$. **.**

2.3.8 Properties of Essential Substitution

Until now we have always started from a map $\sigma : V \rightarrow W$ and investigated the existence of an associated essential substitution $\sigma^* : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$. Thanks to theorem (18) of page 174 we have a simple rule based on the cardinals $|V|$ and $|W|$ allowing us to determine when such existence occurs. In this section, we wish to investigate essential substitutions in their own right. We shall say that a map $\sigma^* : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$ is an *essential substitution* whenever there exists a map $\sigma : V \rightarrow W$ such that σ^* is an essential substitution associated with σ, as per definition (42). We believe essential substitutions should play an important role in mathematical logic. Our study of substitutions started with the (not essential) substitutions mappings $\sigma^* : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$ associated with a map $\sigma : V \rightarrow W$ as per definition (24). These substitution mappings allowed us to characterize the substitution congruence but are somewhat limited by the fact that σ is generally not a valid substitution for $\phi \in \mathbf{P}(V)$. The introduction of valid substitutions as per definition (30) allowed us to move forward somehow, but the issue with valid substitutions fundamentally remains: if a substitution $\sigma : V \rightarrow W$ is valid for $\phi \in \mathbf{P}(V)$, then the associated $\sigma^* : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$ behaves *properly* on ϕ. In other words, it is meaningful to speak of $\sigma^*(\phi)$. However, this validity of σ for ϕ is a *local* property so to speak, and we are still short of a map $\sigma^* : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$ with the right global property. This is what essential substitutions allow us to achieve: if $\sigma^* : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$ is an essential

substitution then $\sigma^*(\phi)$ is meaningful for all $\phi \in \mathbf{P}(V)$. It is as if the associated map $\sigma : V \to W$ had the global property of being valid for all $\phi \in \mathbf{P}(V)$.

Definition 45 *Let V, W be sets. We say that a map $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ is an* essential substitution *if and only if there exists $\sigma : V \to W$ such that:*

$$\mathcal{M} \circ \sigma^* = \bar{\sigma} \circ \mathcal{M}$$

where $\bar{\sigma} : \bar{V} \to \bar{W}$ is the minimal extension and $\mathcal{M}$ is the minimal transform.

The following proposition shows that any map $\sigma : V \to W$ associated with an essential substitution $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ is unique. This means an essential substitution σ^* can safely be regarded as a map $\sigma^* : V \to W$ without any risk of confusion. In fact, there is no need to have separate notations σ^* and σ. If $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is an essential substitution, it is meaningful to speak of $\sigma(x)$.

Proposition 113 *Let V, W be sets and $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ be an essential substitution. Then the map $\sigma : V \to W$ associated with σ^* is unique.*

Proof
Let $\sigma_0, \sigma_1 : V \to W$ such that $\mathcal{M} \circ \sigma^* = \bar{\sigma}_i \circ \mathcal{M}$ for all $i \in 2$. We need to show that $\sigma_0(x) = \sigma_1(x)$ for all $x \in V$. So let $x \in V$. Define $\phi = (x \in x)$. Then:

$$\begin{aligned}
(\sigma_0(x) \in \sigma_0(x)) &= (\bar{\sigma}_0(x) \in \bar{\sigma}_0(x)) \\
&= \bar{\sigma}_0(x \in x) \\
&= \bar{\sigma}_0 \circ \mathcal{M}(\phi) \\
&= \mathcal{M} \circ \sigma^*(\phi) \\
&= \bar{\sigma}_1 \circ \mathcal{M}(\phi) \\
&= (\sigma_1(x) \in \sigma_1(x))
\end{aligned}$$

From $(\sigma_0(x) \in \sigma_0(x)) = (\sigma_1(x) \in \sigma_1(x))$ we conclude that $\sigma_0(x) = \sigma_1(x)$. **.**

The notion of essential substitution is tailor made for the substitution congruence which is arguably the most important congruence in $\mathbf{P}(V)$. If an essential substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is redefined without changing the class of $\sigma(\phi)$ modulo substitution, we still obtain an essential substitution which is in fact identical to σ when viewed as a map $\sigma : V \to W$.

Proposition 114 *Let V, W be sets and $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ be an essential substitution. Let $\tau : \mathbf{P}(V) \to \mathbf{P}(W)$ be a map such that $\sigma(\phi) \sim \tau(\phi)$ for all $\phi \in \mathbf{P}(V)$ where $\sim$ is the substitution congruence on $\mathbf{P}(W)$. Then τ is itself an essential substitution with associated map $\tau : V \to W$ identical to σ.*

Proof
Since σ is essential we have $\mathcal{M} \circ \sigma(\phi) = \bar{\sigma} \circ \mathcal{M}(\phi)$ for all $\phi \in \mathbf{P}(V)$. Having assumed that $\sigma(\phi) \sim \tau(\phi)$ for all $\phi \in \mathbf{P}(V)$, from theorem (14) of page 149 we have $\mathcal{M} \circ \sigma(\phi) = \mathcal{M} \circ \tau(\phi)$. It follows that $\mathcal{M} \circ \tau(\phi) = \bar{\sigma} \circ \mathcal{M}(\phi)$ and we conclude that τ is itself essential with associated map $\sigma : V \to W$. **.**

Suppose $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is an essential substitution. We have an associated map $\sigma : V \to W$ which we have decided to call 'σ' to keep our notations light and natural. But to every map $\sigma : V \to W$ there is an associated variable substitution mapping $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ as per definition (24). It has been our practice so far to denote the variable substitution σ^* simply by 'σ'. Obviously we cannot keep calling everything 'σ' without creating great confusion. Whenever we are dealing with a map $\sigma : V \to W$ and another map $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$, the fact that these two maps have the same name is fine, as we can tell from the context which map is being referred to. We are now confronted with a situation where we have two maps $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ which cannot be distinguished from the data type of their argument, so to speak. Hence our notation $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ for the usual variable substitution as per definition (24). Now given $\phi \in \mathbf{P}(V)$, we may be wondering what relationship there is between $\sigma(\phi)$ and $\sigma^*(\phi)$. We cannot hope to have an equality in general since from proposition (114) we know that σ can be redefined modulo the substitution congruence without affecting its associated map $\sigma : V \to W$. However, if $\sim$ is the substitution congruence on $\mathbf{P}(W)$ we may be able to claim that $\sigma(\phi) \sim \sigma^*(\phi)$. Indeed, this is of course the case when σ is valid for ϕ:

Proposition 115 *Let V, W be sets and $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ be an essential substitution. Then if σ is valid for $\phi \in \mathbf{P}(V)$, we have the substitution equivalence:*

$$\sigma(\phi) \sim \sigma^*(\phi)$$

where $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ is the associated substitution as per definition (24).

Proof
We assume that σ is valid for ϕ. We need to show that $\sigma(\phi) \sim \sigma^*(\phi)$, that is $\mathcal{M} \circ \sigma(\phi) = \mathcal{M} \circ \sigma^*(\phi)$. However, having assumed σ is valid for ϕ, from theorem (13) of page 146 we have $\mathcal{M} \circ \sigma^*(\phi) = \bar{\sigma} \circ \mathcal{M}(\phi)$. Since σ is an essential substitution we also have $\mathcal{M} \circ \sigma(\phi) = \bar{\sigma} \circ \mathcal{M}(\phi)$. So the result follows. **.**

We have spent a lot of time proving the existence of essential substitutions without providing natural examples. The most obvious are the variable substitution mappings associated with injective maps $\sigma : V \to W$ as per definition (24). A more interesting and somewhat deeper result, is the fact that the minimal transform mapping $\mathcal{M} : \mathbf{P}(V) \to \mathbf{P}(\bar{V})$ is itself an essential substitution.

Proposition 116 *Let V, W be sets and $\sigma : V \to W$ be an injective map. Then the associated map $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is essential with associated map σ itself.*

Proof
Let $\sigma : V \to W$ be an injective map. Let $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ be the associated substitution mapping as per definition (24). The fact that both mappings are called 'σ' is standard practice at this stage for us. We need to prove that $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is an essential substitution mapping, with associated map $\sigma : V \to W$. In other words, we need to prove that $\mathcal{M} \circ \sigma(\phi) = \bar{\sigma} \circ \mathcal{M}(\phi)$ for all $\phi \in \mathbf{P}(V)$. Using theorem (13) of page 146 it is sufficient to show that σ is valid for ϕ which follows from proposition (53) and the injectivity of $\sigma : V \to W$. **.**

The minimal transform $\mathcal{M}$ is an essential substitution with associated map the inclusion $i : V \to \bar{V}$. In this case, we shall break with our own tradition and refrain from using the same notation for $\mathcal{M}$ and its associated map $i : V \to \bar{V}$.

Proposition 117 *Let V be a set. The minimal transform $\mathcal{M} : \mathbf{P}(V) \to \mathbf{P}(\bar{V})$ is an essential substitution with associated map the inclusion $i : V \to \bar{V}$.*

Proof
Let $\bar{\mathcal{M}} : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{\bar{V}})$ denote the minimal transform on $\mathbf{P}(\bar{V})$. We need to show that $\bar{\mathcal{M}} \circ \mathcal{M}(\phi) = \bar{i} \circ \mathcal{M}(\phi)$ for all $\phi \in \mathbf{P}(V)$. However, since i is injective, from proposition (53) it is valid for ϕ and it follows from theorem (13) of page 146 that $\bar{\mathcal{M}} \circ i(\phi) = \bar{i} \circ \mathcal{M}(\phi)$. Hence we need to show that $\bar{\mathcal{M}} \circ \mathcal{M}(\phi) = \bar{\mathcal{M}} \circ i(\phi)$. Using theorem (14) of page 149 we need to show $\mathcal{M}(\phi) \sim i(\phi)$ where $\sim$ is the substitution congruence on $\mathbf{P}(\bar{V})$, which we know is true from proposition (99). .

Given $\phi \in \mathbf{P}(V)$ and a map $\sigma : V \to V$ which is admissible for ϕ, we know from proposition (77) that $\sigma(\phi) \sim \phi$ where $\sim$ denotes the substitution congruence on $\mathbf{P}(V)$. In other words, if σ is valid for ϕ and $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\phi)$ then we have $\phi \sim \psi$ where $\psi = \sigma(\phi)$. The following proposition is an extension of this result for essential substitutions. In fact, the converse is now also true. If $\phi \sim \psi$ then we must have $\psi = \sigma(\phi)$ for some essential substitution σ such that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\phi)$. This is less deep than it looks:

Proposition 118 *Let V be a set and $\sim$ be the substitution congruence on $\mathbf{P}(V)$. Then for all $\phi, \psi \in \mathbf{P}(V)$ we have $\phi \sim \psi$ if and only if $\psi = \sigma(\phi)$ for some essential substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$ such that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\phi)$.*

Proof
First we show the 'if' part: so suppose $\psi = \sigma(\phi)$ for some essential substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$ such that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\phi)$. We need to show that $\phi \sim \psi$. From theorem (14) of page 149 it is sufficient to prove that $\mathcal{M}(\phi) = \mathcal{M}(\psi)$. Having assumed that $\psi = \sigma(\phi)$ we need to show that $\mathcal{M}(\phi) = \mathcal{M} \circ \sigma(\phi)$. However, since σ is essential we have $\mathcal{M} \circ \sigma(\phi) = \bar{\sigma} \circ \mathcal{M}(\phi)$. Hence we need to show that $\mathcal{M}(\phi) = \bar{\sigma} \circ \mathcal{M}(\phi)$. Using proposition (36) it is sufficient to prove that $\bar{\sigma}(u) = u$ for all $u \in \mathrm{Var}(\mathcal{M}(\phi))$. So let $u \in \mathrm{Var}(\mathcal{M}(\phi))$. Since $\bar{V} = V \uplus \mathbf{N}$ we shall distinguish two cases: first we assume that $u \in \mathbf{N}$. Then $\bar{\sigma}(u) = u$ is clear from definition (39). Next we assume that $u \in V$. Then from proposition (97) we obtain $u \in \mathrm{Fr}(\phi)$ and it follows that $\bar{\sigma}(u) = \sigma(u) = u$. We now prove the 'only if' part: so suppose $\phi \sim \psi$. We need to show that $\psi = \sigma(\phi)$ for some essential substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$ such that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\phi)$. Let $i : \mathbf{P}(V) \to \mathbf{P}(V)$ be the identity mapping. From proposition (116), i is an essential substitution associated with the identity $i : V \to V$. Let $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$ be defined by $\sigma(\chi) = i(\chi)$ whenever $\chi \neq \phi$ and $\sigma(\phi) = \psi$. Having assumed that $\phi \sim \psi$ we have $\sigma(\chi) \sim i(\chi)$ for all $\chi \in \mathbf{P}(V)$. It follows from proposition (114) that σ is an essential substitution whose associated map $\sigma : V \to V$ is the identity. In particular, we have $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\phi)$. .

The composition of two essential substitutions is itself essential, while the associated map is the obvious composition of the respective associated maps.

Proposition 119 *Let U, V and W be sets while the maps $\tau : \mathbf{P}(U) \to \mathbf{P}(V)$ and $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ are essential substitutions. Then $\sigma \circ \tau : \mathbf{P}(U) \to \mathbf{P}(W)$ is itself an essential substitution with associated map $\sigma \circ \tau : U \to W$.*

Proof
We need to show that $\mathcal{M} \circ (\sigma \circ \tau) = \overline{(\sigma \circ \tau)} \circ \mathcal{M}$. However from definition (39), it is clear that the minimal extension $\overline{(\sigma \circ \tau)} : \bar{U} \to \bar{W}$ is equal to the composition of the minimal extensions $\bar{\sigma} \circ \bar{\tau}$. Hence we have:

$$\begin{aligned} \mathcal{M} \circ (\sigma \circ \tau) &= \bar{\sigma} \circ \mathcal{M} \circ \tau \\ &= \bar{\sigma} \circ \bar{\tau} \circ \mathcal{M} \\ &= \overline{(\sigma \circ \tau)} \circ \mathcal{M} \end{aligned}$$

.

Suppose $\sigma : V \to W$ is a map which is valid for $\phi \in \mathbf{P}(V)$. From proposition (52) we know that $\mathrm{Fr}(\sigma(\phi)) = \sigma(\mathrm{Fr}(\phi))$. In fact this equality holds for every sub-formula $\psi \preceq \phi$. The following proposition shows that the equality $\mathrm{Fr}(\sigma(\phi)) = \sigma(\mathrm{Fr}(\phi))$ holds whenever $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is an essential substitution. As already pointed out, this is *as if* σ was valid for all $\phi \in \mathbf{P}(V)$. But of course, nothing about sub-formulas in this case. Consider the formula $\phi = \forall y(x \in y)$ where $V = \{x, y\}$ and $x \neq y$. Let $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$ be an essential substitution associated with $\sigma = [y/x]$. Then $\sigma : V \to V$ is clearly not valid for ϕ and the equality $\mathrm{Fr}(\sigma(\phi)) = \sigma(\mathrm{Fr}(\phi))$ may look very surprising. Indeed, we have $\mathrm{Fr}(\phi) = \{x\}$ and consequently $\sigma(\mathrm{Fr}(\phi)) = \{y\}$. It is very tempting to argue that $\sigma(\phi) = \forall y(y \in y)$ has no free variable and that the equality therefore cannot be true. But remember that $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$ does not refer to the substitution mapping associated with $\sigma : V \to V$. The context of our discussion makes it very clear that we are starting with $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$ as a given essential substitution. Hence $\sigma(\phi)$ is not equal to $\forall y(y \in y)$. In fact, we must have $\mathcal{M} \circ \sigma(\phi) = \forall\, 0(y \in 0)$ and since $V = \{x, y\}$ it is not difficult to prove that the only possible value is $\sigma(\phi) = \forall x(y \in x)$, and $\mathrm{Fr}(\sigma(\phi)) = \{y\}$.

Proposition 120 *Let V, W be sets and $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ be an essential substitution. Then for all $\phi \in \mathbf{P}(V)$ we have the equality:*

$$\mathrm{Fr}(\sigma(\phi)) = \sigma(\mathrm{Fr}(\phi))$$

Proof
Using proposition (97) we obtain the following:

$$\begin{aligned} \mathrm{Fr}(\sigma(\phi)) &= \mathrm{Fr}(\,\mathcal{M} \circ \sigma(\phi)\,) \\ &= \mathrm{Fr}(\,\bar{\sigma} \circ \mathcal{M}(\phi)\,) \\ \bar{\sigma} \text{ valid for } \mathcal{M}(\phi) \;\to\; &= \bar{\sigma}(\,\mathrm{Fr}(\mathcal{M}(\phi))\,) \\ \text{prop. (97)} \;\to\; &= \bar{\sigma}(\mathrm{Fr}(\phi)) \\ \mathrm{Fr}(\phi) \subseteq V \;\to\; &= \sigma(\mathrm{Fr}(\phi)) \end{aligned}$$

.

If $\sigma, \tau : V \to W$ are two maps and $\phi \in \mathbf{P}(V)$, we know from proposition (36) that $\sigma(\phi) = \tau(\phi)$ if and only if σ and τ coincide on $\mathrm{Var}(\phi)$. The following proposition provides the counterpart result for essential substitutions. So we start from $\sigma, \tau : \mathbf{P}(V) \to \mathbf{P}(W)$ two essential substitutions and we consider the equivalence $\sigma(\phi) \sim \tau(\phi)$ where $\sim$ is the substitution congruence. Note that there is not much point considering the equality $\sigma(\phi) = \tau(\phi)$ in the case of essential substitutions, since we know from proposition (114) that both σ and τ can be arbitrarily redefined modulo substitution, without affecting their associated maps $\sigma, \tau : V \to W$. So we can only focus on $\sigma(\phi) \sim \tau(\phi)$ which holds if and only if the associated maps $\sigma, \tau : V \to W$ coincide on $\mathrm{Fr}(\phi)$:

Proposition 121 *Let V, W be sets and $\sigma, \tau : \mathbf{P}(V) \to \mathbf{P}(W)$ be two essential substitutions. Then for all $\phi \in \mathbf{P}(V)$ we have the equivalence:*

$$\sigma_{|\mathrm{Fr}(\phi)} = \tau_{|\mathrm{Fr}(\phi)} \quad \Leftrightarrow \quad \sigma(\phi) \sim \tau(\phi)$$

where $\sim$ denotes the substitution congruence on the algebra $\mathbf{P}(W)$.

Proof
From theorem (14) of page 149, $\sigma(\phi) \sim \tau(\phi)$ is equivalent to the equality $\mathcal{M} \circ \sigma(\phi) = \mathcal{M} \circ \tau(\phi)$. Having assumed σ and τ are essential, this is in turn equivalent to $\bar{\sigma} \circ \mathcal{M}(\phi) = \bar{\tau} \circ \mathcal{M}(\phi)$. Using proposition (36), this last equality is equivalent to $\bar{\sigma}(u) = \bar{\tau}(u)$ for all $u \in \mathrm{Var}(\mathcal{M}(\phi))$. Hence we need to show that this last statement is equivalent to $\sigma(u) = \tau(u)$ for all $u \in \mathrm{Fr}(\phi)$. First we show $\Rightarrow$: so suppose $\bar{\sigma}(u) = \bar{\tau}(u)$ for all $u \in \mathrm{Var}(\mathcal{M}(\phi))$ and let $u \in \mathrm{Fr}(\phi)$. We need to show that $\sigma(u) = \tau(u)$. From proposition (97) we have $\mathrm{Var}(\mathcal{M}(\phi)) \cap V = \mathrm{Fr}(\phi)$. It follows that $u \in \mathrm{Var}(\mathcal{M}(\phi)) \cap V$ and consequently we have $\sigma(u) = \bar{\sigma}(u) = \bar{\tau}(u) = \tau(u)$ as requested. So we now prove $\Leftarrow$: So we assume that $\sigma(u) = \tau(u)$ for all $u \in \mathrm{Fr}(\phi)$ and consider $u \in \mathrm{Var}(\mathcal{M}(\phi))$. We need to show that $\bar{\sigma}(u) = \bar{\tau}(u)$. Since $\bar{V} = V \uplus \mathbf{N}$ we shall distinguish two cases: first we assume that $u \in \mathbf{N}$. Then $\bar{\sigma}(u) = u = \bar{\tau}(u)$. Next we assume that $u \in V$. Then $u \in \mathrm{Var}(\mathcal{M}(\phi)) \cap V = \mathrm{Fr}(\phi)$ and $\bar{\sigma}(u) = \sigma(u) = \tau(u) = \bar{\tau}(u)$. .

In theorem (15) of page 152 we proved that $\sigma(\phi) \sim \sigma(\psi)$ whenever $\phi \sim \psi$ and $\sigma : V \to W$ is a substitution which is valid for both ϕ and ψ. We now provide an extension of this result for an essential substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$. We should not confuse the following proposition with proposition (118) relative to essential substitutions $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$. If we want to claim that $\sigma(\phi) \sim \phi$ then proposition (118) requires that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\phi)$. This is not the same thing as claiming $\sigma(\phi) \sim \sigma(\psi)$ for which no special conditions on the set $\mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$ is attached (recall that $\mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$ whenever $\phi \sim \psi$). If you have $\phi \sim \psi$, then you can move the free variables around as much as you want with an essential substitution. It will not change the fact that $\sigma(\phi) \sim \sigma(\psi)$.

Proposition 122 *Let V, W be sets and $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ be an essential substitution. Then for all formulas $\phi, \psi \in \mathbf{P}(V)$ we have the implication:*

$$\phi \sim \psi \;\Rightarrow\; \sigma(\phi) \sim \sigma(\psi)$$

where $\sim$ *denotes the substitution congruence on* $\mathbf{P}(V)$ *and* $\mathbf{P}(W)$.

Proof
So we assume that $\phi \sim \psi$. We need to show that $\sigma(\phi) \sim \sigma(\psi)$. Using theorem (14) of page 149 it is sufficient to show that $\mathcal{M} \circ \sigma(\phi) = \mathcal{M} \circ \sigma(\psi)$. Having assumed that σ is essential, it is sufficient to show that $\bar{\sigma} \circ \mathcal{M}(\phi) = \bar{\sigma} \circ \mathcal{M}(\psi)$ which follows immediately from $\mathcal{M}(\phi) = \mathcal{M}(\psi)$, itself a consequence of $\phi \sim \psi$.
.

In proposition (107) we showed that a substitution $\sigma : V \to W$ which is valid for a formula $\phi \in \mathbf{P}(V)$ will preserve its substitution rank, provided $\sigma_{|\mathrm{Fr}(\phi)}$ is an injective map. The same is true of an essential substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$.

Proposition 123 *Let* V, W *be sets and* $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ *be an essential substitution. Let* $\phi \in \mathbf{P}(V)$ *such that* $\sigma_{|\mathrm{Fr}(\phi)}$ *is an injective map. Then:*

$$\mathrm{rnk}(\sigma(\phi)) = \mathrm{rnk}(\phi)$$

where rnk( ) *refers to the substitution rank as per* definition (41).

Proof
Using proposition (106) we obtain the following:

$$\begin{aligned} \mathrm{rnk}(\sigma(\phi)) &= \mathrm{rnk}(\mathcal{M} \circ \sigma(\phi)) \\ \sigma \text{ essential } \to &= \mathrm{rnk}(\bar{\sigma} \circ \mathcal{M}(\phi)) \\ \text{A: to be proved } \to &= \mathrm{rnk}(\mathcal{M}(\phi)) \\ \text{prop. (106) } \to &= \mathrm{rnk}(\phi) \end{aligned}$$

So it remains to show that $\mathrm{rnk}(\bar{\sigma} \circ \mathcal{M}(\phi)) = \mathrm{rnk}(\mathcal{M}(\phi))$. Using proposition (107) it is sufficient to show that $\bar{\sigma}$ is valid for $\mathcal{M}(\phi)$ and furthermore that it is injective on $\mathrm{Fr}(\mathcal{M}(\phi))$. We know that $\bar{\sigma}$ is valid for $\mathcal{M}(\phi)$ from proposition (100). We also know that $\mathrm{Fr}(\mathcal{M}(\phi)) = \mathrm{Fr}(\phi)$ from proposition (97). So it remains to show that $\bar{\sigma}$ is injective on $\mathrm{Fr}(\phi) \subseteq V$ which is clearly the case since $\bar{\sigma}$ coincide with σ on V and σ is by assumption injective on $\mathrm{Fr}(\phi)$. .

Without the injectivity of σ on $\mathrm{Fr}(\phi)$, the substitution rank is generally not preserved. However as can be seen below, it can never increase. The following proposition extends proposition (110) to essential substitutions.

Proposition 124 *Let* V, W *be sets and* $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ *be an essential substitution. Then for all formula* $\phi \in \mathbf{P}(V)$ *we have the inequality:*

$$\mathrm{rnk}(\sigma(\phi)) \leq \mathrm{rnk}(\phi)$$

where rnk( ) *refers to the substitution rank as per* definition (41).

Proof
Using proposition (106) we obtain the following:

$$\begin{aligned} \mathrm{rnk}(\sigma(\phi)) &= \mathrm{rnk}(\mathcal{M} \circ \sigma(\phi)) \\ \sigma \text{ essential } \to &= \mathrm{rnk}(\bar{\sigma} \circ \mathcal{M}(\phi)) \\ \text{prop. (110) } \to &\leq \mathrm{rnk}(\mathcal{M}(\phi)) \\ \text{prop. (106) } \to &= \mathrm{rnk}(\phi) \end{aligned}$$

.

Given an essential substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ and $\phi \in \mathbf{P}(V)$, there is only so much we can say about $\sigma(\phi)$, even if we know about the structure of ϕ. For example, if $\phi = \phi_1 \to \phi_2$ we cannot claim that $\sigma(\phi) = \sigma(\phi_1) \to \sigma(\phi_2)$. However, as the following proposition will show, we have $\sigma(\phi) \sim \sigma(\phi_1) \to \sigma(\phi_2)$ where $\sim$ is the substitution congruence on $\mathbf{P}(W)$. A more interesting example is the case when $\phi = \forall x \phi_1$. We would like to claim that $\sigma(\phi) \sim \forall \sigma(x) \sigma(\phi_1)$. However, there is little chance of this equivalence being true when $\sigma(x)$ happens to be a free variable of $\sigma(\phi)$. So the condition $\sigma(x) \notin \mathrm{Fr}(\sigma(\phi))$ should be a minimal requirement. Remember that the map $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is an *essential* substitution. It is not simply the substitution mapping associated with a map $\sigma : V \to W$ as per definition (24). If this was the case then the equality $\sigma(\phi) = \forall \sigma(x) \sigma(\phi_1)$ would hold, and the condition $\sigma(x) \notin \mathrm{Fr}(\sigma(\phi))$ would be automatically satisfied. When $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is an essential substitution, it is very well possible that $\sigma(x) \in \mathrm{Fr}(\sigma(\phi))$. Let $\phi = \forall x (x \in y)$ with $x \neq y$ and $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$ an essential substitution associated with $[y/x]$. Then $\sigma(x) = y$ while $\sigma(\phi) = \forall z (z \in y)$ for some $z \neq y$. So $\sigma(x) \in \mathrm{Fr}(\sigma(\phi))$. The following proposition will show that the condition $\sigma(x) \notin \mathrm{Fr}(\sigma(\phi))$ is in fact sufficient to obtain the equivalence $\sigma(\phi) \sim \forall \sigma(x) \sigma(\phi_1)$.

Proposition 125 *Let V, W be sets and $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ be an essential substitution. Let $\sim$ be the substitution congruence on $\mathbf{P}(W)$. Then we have:*

$$\forall \phi \in \mathbf{P}(V) \ , \ \sigma(\phi) : \begin{cases} = (\sigma(x) \in \sigma(y)) & \textit{if} \quad \phi = (x \in y) \\ = \bot & \textit{if} \quad \phi = \bot \\ \sim \sigma(\phi_1) \to \sigma(\phi_2) & \textit{if} \quad \phi = \phi_1 \to \phi_2 \\ \sim \forall \sigma(x) \sigma(\phi_1) & \textit{if} \quad \phi = \forall x \phi_1 \ , \ \sigma(x) \notin \mathrm{Fr}(\sigma(\phi)) \end{cases}$$

Proof
First we assume that $\phi = (x \in y)$ for some $x, y \in V$. We need to show that $\sigma(\phi) = \sigma(x) \in \sigma(y)$. However, any map $\sigma : V \to W$ is valid for ϕ. It follows from proposition (115) that $\sigma(\phi) \sim \sigma^*(\phi)$, where $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ is the associated substitution mapping as per definition (24). From $\sigma^*(\phi) = \sigma(x) \in \sigma(y)$ and the equivalence $\sigma(\phi) \sim \sigma^*(\phi)$, using theorem (12) of page 132 we conclude that $\sigma(\phi) = \sigma(x) \in \sigma(y)$ as requested. Next we assume that $\phi = \bot$. Then once again σ is valid for ϕ and we obtain $\sigma(\phi) \sim \sigma^*(\phi) = \bot$ and consequently from theorem (12) we have $\sigma(\phi) = \bot$. So we now assume that $\phi = \phi_1 \to \phi_2$ for some $\phi_1, \phi_2 \in \mathbf{P}(V)$. We need to show $\sigma(\phi) \sim \sigma(\phi_1) \to \sigma(\phi_2)$. Using theorem (14) of page 149, we simply compute the minimal transforms:

$$\begin{aligned} \mathcal{M} \circ \sigma(\phi) &= \bar{\sigma} \circ \mathcal{M}(\phi) \\ &= \bar{\sigma} \circ \mathcal{M}(\phi_1 \to \phi_2) \\ &= \bar{\sigma}(\mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2)) \\ &= \bar{\sigma} \circ \mathcal{M}(\phi_1) \to \bar{\sigma} \circ \mathcal{M}(\phi_2) \\ &= \mathcal{M} \circ \sigma(\phi_1) \to \mathcal{M} \circ \sigma(\phi_2) \\ &= \mathcal{M}(\sigma(\phi_1) \to \sigma(\phi_2)) \end{aligned}$$

So we now assume that $\phi = \forall x \phi_1$ and $\sigma(x) \notin \mathrm{Fr}(\sigma(\phi))$. We need to show that $\sigma(\phi) \sim \forall \sigma(x) \sigma(\phi_1)$. Likewise, we shall compute minimal transforms:

$$\begin{array}{rcl}
\mathcal{M} \circ \sigma(\phi) & = & \bar{\sigma} \circ \mathcal{M}(\phi) \\
 & = & \bar{\sigma} \circ \mathcal{M}(\forall x \phi_1) \\
n = \min\{k : [k/x] \text{ valid for } \mathcal{M}(\phi_1)\} \ \rightarrow & = & \bar{\sigma}(\forall n \mathcal{M}(\phi_1)[n/x]) \\
 & = & \forall \bar{\sigma}(n) \bar{\sigma}(\mathcal{M}(\phi_1)[n/x]) \\
 & = & \forall n \, \bar{\sigma} \circ [n/x] \circ \mathcal{M}(\phi_1) \\
\text{A: to be proved} \ \rightarrow & = & \forall n \, [n/\sigma(x)] \circ \bar{\sigma} \circ \mathcal{M}(\phi_1) \\
 & = & \forall n \, [n/\sigma(x)] \circ \mathcal{M} \circ \sigma(\phi_1) \\
 & = & \forall n \, \mathcal{M}[\sigma(\phi_1)][n/\sigma(x)] \\
\text{B: to be proved} \ \rightarrow & = & \forall m \, \mathcal{M}[\sigma(\phi_1)][m/\sigma(x)] \\
m = \min\{k : [k/\sigma(x)] \text{ valid for } \mathcal{M}[\sigma(\phi_1)]\} \ \rightarrow & = & \mathcal{M}(\forall \sigma(x) \sigma(\phi_1))
\end{array}$$

So it remains to justify point A and B. First we deal with point A: it is sufficient to prove the equality $\bar{\sigma} \circ [n/x] \circ \mathcal{M}(\phi_1) = [n/\sigma(x)] \circ \bar{\sigma} \circ \mathcal{M}(\phi_1)$, which follows from lemma (10) and $\sigma(x) \notin \sigma(\mathrm{Fr}(\phi))$, itself a consequence of $\sigma(x) \notin \mathrm{Fr}(\sigma(\phi))$ and proposition (120). We now deal with point B: it is sufficient to prove the equivalence $[k/x]$ valid for $\mathcal{M}(\phi_1) \ \Leftrightarrow \ [k/\sigma(x)]$ valid for $\bar{\sigma} \circ \mathcal{M}(\phi_1)$ which follows from lemma (11) and the fact that $\sigma(x) \notin \sigma(\mathrm{Fr}(\phi))$. **.**

This last proposition seems to indicate there is nothing we can say about $\sigma(\phi)$ if it happens to have $\sigma(x)$ as a free variable. Luckily this is not the case:

Proposition 126 *Let V, W be sets and $\sigma : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$ be an essential substitution. Let $\phi = \forall x \phi_1$ where $x \in V$, $\phi_1 \in \mathbf{P}(V)$. There exists an essential substitution $\tau : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$ such that $\tau = \sigma$ on $V \setminus \{x\}$ and $\tau(x) \notin \mathrm{Fr}(\sigma(\phi))$. Furthermore, for any such τ we have the substitution equivalence:*

$$\sigma(\phi) \sim \forall \tau(x) \tau(\phi_1)$$

Proof
We shall first prove the substitution equivalence. So let $\tau : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$ be an essential substitution which coincide with σ on $V \setminus \{x\}$ and such that $\tau(x) \notin \mathrm{Fr}(\sigma(\phi))$. We need to show that $\sigma(\phi) \sim \forall \tau(x) \tau(\phi_1)$ where $\sim$ denotes the substitution congruence on $\mathbf{P}(W)$. However, since $\mathrm{Fr}(\phi) \subseteq V \setminus \{x\}$ we see that σ and τ are essential substitutions which coincide on $\mathrm{Fr}(\phi)$. It follows from proposition (121) that $\sigma(\phi) \sim \tau(\phi)$. Hence it is sufficient to prove that $\tau(\phi) \sim \forall \tau(x) \tau(\phi_1)$. Applying proposition (125) it is sufficient to show that $\tau(x) \notin \mathrm{Fr}(\tau(\phi))$. However, by assumption we have $\tau(x) \notin \mathrm{Fr}(\sigma(\phi))$ and so:

$$\tau(x) \notin \mathrm{Fr}(\sigma(\phi)) = \sigma(\mathrm{Fr}(\phi)) = \tau(\mathrm{Fr}(\phi)) = \mathrm{Fr}(\tau(\phi))$$

where we have used proposition (120). It remains to show that such an essential substitution $\tau : \mathbf{P}(V) \to \mathbf{P}(W)$ exists. Suppose we have proved that $\mathrm{Fr}(\sigma(\phi))$ is a proper subset of W. Then there exists $y^* \in W$ such that $y^* \notin \mathrm{Fr}(\sigma(\phi))$. Consider the map $\tau : V \to W$ defined by:

$$\forall u \in V \ , \ \tau(u) = \begin{cases} \sigma(u) & \text{if} \quad u \in V \setminus \{x\} \\ y^* & \text{if} \quad u = x \end{cases}$$

Then it is clear that τ coincides with σ on $V \setminus \{x\}$ and $\tau(x) \notin \mathrm{Fr}(\sigma(\phi))$. In order to show the existence of $\tau : \mathbf{P}(V) \to \mathbf{P}(W)$ it is sufficient to show the existence of an essential substitution associated with $\tau : V \to W$. From theorem (18) of page 174 it is sufficient to show that $|W|$ is an infinite cardinal, or that it is finite with $|V| \leq |W|$. However, this follows immediately from the existence of the essential substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ and theorem (18). So it remains to show that $\mathrm{Fr}(\sigma(\phi))$ is a proper subset of W. This is clearly true if $|W|$ is an infinite cardinal. So we may assume that $|W|$ if finite, in which case we have $|V| \leq |W|$. In particular, $|V|$ is also a finite cardinal and since $x \notin \mathrm{Fr}(\phi)$ we have $|\mathrm{Fr}(\phi)| < |V|$. Hence we have the following inequalities:

$$|\mathrm{Fr}(\sigma(\phi))| = |\sigma(\mathrm{Fr}(\phi))| \leq |\mathrm{Fr}(\phi)| < |V| \leq |W|$$

So $\mathrm{Fr}(\sigma(\phi))$ is indeed a proper subset of W, as requested. **.**

2.4 The Permutation Congruence

2.4.1 The Permutation Congruence

We are still looking for the appropriate congruence which should be defined on $\mathbf{P}(V)$ so as to identify mathematical statements which are deemed *identical*. Until now, we have highlighted the *substitution congruence* defined in page 123 as a possible source of identity. Unfortunately whatever final congruence we go for, it will need to be larger (i.e. weaker) than the substitution congruence. As mathematicians, we are familiar with the fact that the *order of quantification* in a given mathematical statement is immaterial. For example, the formulas $\phi = \forall x \forall y (x \in y)$ and $\psi = \forall y \forall x (x \in y)$ should mean the same thing. Yet the equivalence of ϕ and ψ cannot be deduced from the substitution congruence alone when $x \neq y$. Indeed, let $\sim$ denote the substitution congruence on $\mathbf{P}(V)$ and suppose that $\phi \sim \psi$. Define $\phi_1 = \forall y (x \in y)$ and $\psi_1 = \forall x (x \in y)$. Then we have $\forall x \phi_1 \sim \forall y \psi_1$ with $x \neq y$. Using theorem (12) of page 132 it follows that $\psi_1 \sim \phi_1[y:x]$ which is $\forall x (x \in y) \sim \forall x (y \in x)$. Using theorem (12) once more we see that $(x \in y) \sim (y \in x)$ which contradicts theorem (12). Permuting the order of quantification cannot be achieved by substituting variables.

Definition 46 *Let V be a set. We call* permutation congruence on $\mathbf{P}(V)$ *the congruence on $\mathbf{P}(V)$ generated by the following set $R_0 \subseteq \mathbf{P}(V) \times \mathbf{P}(V)$:*

$$R_0 = \{ \, (\, \forall x \forall y \, \phi_1 \, , \, \forall y \forall x \, \phi_1 \,) : \phi_1 \in \mathbf{P}(V) \ , \ x, y \in V \, \}$$

We easily see that the permutation congruence preserves free variables :

Proposition 127 *Let $\sim$ denote the permutation congruence on $\mathbf{P}(V)$ where V is a set. Then for all $\phi, \psi \in \mathbf{P}(V)$ we have the implication:*

$$\phi \sim \psi \;\Rightarrow\; \mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$$

Proof
Let $\equiv$ denote the relation on $\mathbf{P}(V)$ defined by $\phi \equiv \psi$ if and only if we have $\mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$. Then we need to show that $\sim \subseteq \equiv$. However, we know from proposition (46) that $\equiv$ is a congruence on $\mathbf{P}(V)$. Since $\sim$ is defined as the smallest congruence on $\mathbf{P}(V)$ which contains the set R_0 of definition (45), we simply need to show that $R_0 \subseteq \equiv$. So let $\phi_1 \in \mathbf{P}(V)$ and $x, y \in V$. We need to show that $\forall x \forall y \phi_1 \equiv \forall y \forall x \phi_1$ which is $\mathrm{Fr}(\forall x \forall y \phi_1) = \mathrm{Fr}(\forall y \forall x \phi_1)$. This is clearly the case since both sets are equal to $\mathrm{Fr}(\phi_1) \setminus \{x, y\}$. .

Suppose $\phi_1 \in \mathbf{P}(V)$ and $x, y, z \in V$. If $\sim$ denotes the permutation congruence on $\mathbf{P}(V)$, then the following equivalence can easily be proved:

$$\forall x \forall y \forall z \phi_1 \sim \forall z \forall y \forall x \phi_1 \tag{2.43}$$

The most direct proof probably involves permuting pairs of adjacent variables until we reach the configuration $\forall z \forall y \forall x$ having started from $\forall x \forall y \forall z$. More generally, given $x \in V^n$ where $n \in \mathbf{N}$, given an arbitrary permutation $\sigma : n \to n$, we would expect the following equivalence to hold equally:

$$\forall x(n-1) \ldots \forall x(0)\, \phi_1 \sim \forall x(\sigma(n-1)) \ldots x(\sigma(0))\, \phi_1 \tag{2.44}$$

There are several issues to be addressed with equation (2.44). One of our concerns will be of course to establish its truth. There is also the use of the loose notation '...' which is arguably questionable in a document dealing with formal logic. More fundamentally, regardless of whether formula (2.44) is true or false, it is an ugly formula. Granted we could improve things slightly by writing:

$$\forall x_{n-1} \ldots \forall x_0\, \phi_1 \sim \forall x_{\sigma(n-1)} \ldots x_{\sigma(0)}\, \phi_1 \tag{2.45}$$

but this is hardly satisfactory. One of our objectives is therefore to design the appropriate formalism to remove the ugliness of (2.44). Now when it comes to establishing its proof, the key idea is the same as with $\forall x \forall y \forall z$ and involves permuting adjacent variables until we reach the appropriate configuration. So we shall need the fact that an arbitrary permutation can always be expressed as a composition of 'adjacent moves'. We provide a proof in the following section.

2.4.2 Integer Permutation

We start with a couple of definitions including that of *elementary permutation* which formalizes the idea of 'adjacent moves'.

Definition 47 *Let $n \in \mathbf{N}$ we call* permutation of order n *a bijection $\sigma : n \to n$.*

Definition 48 *Let $n \in \mathbf{N}$, $n \geq 2$. We call* elementary permutation of order n *any permutation $\sigma : n \to n$ of the form $\sigma = [i : i+1]$ for some $i \in n-1$.*

For the sake of brevity, we allowed ourselves to use the notational shortcut $\sigma = \tau_k \circ \ldots \circ \tau_1$ in the following proof. This is fair enough. In a way, we are still doing meta-mathematics with the established standards of usual mathematics. If we are one day to provide a formal proof of the following lemma, we shall either need to discard the '...', or create a high level language where its use is permitted, and corresponding formulas correctly compiled as low level formulas of first order logic with some form of recursive wording.

Lemma 15 *Let $n \in \mathbf{N}$, $n \geq 2$. Any permutation $\sigma : n \to n$ of order n is a composition of elementary permutations, i.e. there exist $k \in \mathbf{N}^*$ and elementary permutations $\tau_1, \ldots, \tau_k$ such that:*

$$\sigma = \tau_k \circ \ldots \circ \tau_1$$

Proof
We shall prove lemma (15), using an induction argument on $n \geq 2$. First we show that the lemma is true for $n = 2$. So suppose $\sigma : 2 \to 2$ is a permutation of order 2. We shall distinguish two cases. First we assume that $\sigma = [0:1]$. Then σ is an elementary permutation and there is nothing else to prove. We now assume that σ is the identity. Then σ can be expressed as $\sigma = [0:1] \circ [0:1]$. Having considered the only two possible cases, we conclude that lemma (15) is true when $n = 2$. We now assume that lemma (15) is true for $n \geq 2$. We need to show that it is true for $n+1$. So we assume that $\sigma : (n+1) \to (n+1)$ is a permutation of order $n+1$. We need to show that σ can be expressed as a composition of elementary permutations. We shall distinguish two cases. First we assume that $\sigma(n) = n$. Then the restriction $\sigma_{|n}$ is easily seen to be a permutation of order n. Indeed, it is clearly an injective map $\sigma_{|n} : n \to n$ which is also surjective. Using the induction hypothesis, there exist $k \in \mathbf{N}^*$ and elementary permutations $\tau_1, \ldots, \tau_k$ of order n such that:

$$\sigma_{|n} = \tau_k \circ \ldots \circ \tau_1$$

For all $j \in \{1, \ldots, k\}$ consider the extension τ_j^* of τ_j on $n+1$ defined by $(\tau_j^*)_{|n} = \tau_j$ and $\tau_j^*(n) = n$. Having assumed that $\sigma(n) = n$, we obtain:

$$\sigma = \tau_k^* \circ \ldots \circ \tau_1^*$$

It is therefore sufficient to show that each τ_j^* is an elementary permutation of order $n+1$. So let $j \in \{1, \ldots, k\}$. Since τ_j is an elementary permutation of order n, there exists $i \in n-1$ such that $\tau_j = [i : i+1]$ (of order n). It follows immediately that $\tau_j^* = [i : i+1]$ (or order $n+1$). So τ_j^* is indeed an elementary permutation of order $n+1$. This completes our proof of lemma (15) for $n+1$ in the case when $\sigma(n) = n$. We now assume that $\sigma(n) \neq n$. Then $\sigma(n) \in n$. In other words, there exists $j \in n$ such that $\sigma(n) = n-1-j$. We shall prove by induction on $j \in n$ that σ can be expressed as a composition of elementary

permutations of order $n+1$. Note that in order to do so, it is sufficient to prove the existence of $m \in \mathbf{N}^*$ and elementary permutations $\tau'_1, \ldots, \tau'_m$ such that:

$$\tau'_m \circ \ldots \circ \tau'_1 \circ \sigma(n) = n$$

Indeed if that is the case, having proved lemma (15) for $n+1$ in the case when $\sigma(n) = n$, we deduce the existence of $k \in \mathbf{N}^*$ and elementary permutations $\tau_1, \ldots, \tau_k$ of order $n+1$ such that:

$$\tau'_m \circ \ldots \circ \tau'_1 \circ \sigma = \tau_k \circ \ldots \circ \tau_1$$

and since $\tau^{-1} = \tau$ for every elementary permutation τ, we conclude that:

$$\sigma = \tau'_1 \circ \ldots \tau'_m \circ \tau_k \circ \ldots \circ \tau_1$$

So we need to show the existence of $m \in \mathbf{N}^*$ and elementary permutations $\tau'_1, \ldots, \tau'_m$ such that $\tau'_m \circ \ldots \circ \tau'_1 \circ \sigma(n) = n$, and we shall do so by induction on $j \in n$ such that $\sigma(n) = n-1-j$. First we assume that $j = 0$. Then $\sigma(n) = n-1$ and it is clear that $[\, n-1 : n \,] \circ \sigma(n) = n$. So the property is true for $j = 0$. We now assume that the property is true for $j \in (n-1)$ and we need to show that it is true for $j+1$. So we assume that $\sigma(n) = n-1-(j+1)$. Then we have:

$$[\, n-1-(j+1) \,:\, n-1-j \,] \circ \sigma(n) = n-1-j$$

Having assumed the property is true for j, there exist $m \in \mathbf{N}^*$ and elementary permutations $\tau'_1, \ldots, \tau'_m$ such that:

$$\tau'_m \circ \ldots \circ \tau'_1 \circ [\, n-1-(j+1) \,:\, n-1-j \,] \circ \sigma(n) = n$$

Hence we see that the property is also true for $j+1$. **.**

Having established that every permutation $\sigma : n \to n$ is a composition of elementary permutations for $n \geq 2$, our main objective is to design a proof of:

$$\forall x_{n-1} \ldots \forall x_0 \, \phi_1 \sim \forall x_{\sigma(n-1)} \ldots x_{\sigma(0)} \, \phi_1 \tag{2.46}$$

However, we would also like to do so while at the same time creating a more condensed formalism. In the next section, we shall define the notion of *iterated quantification*, allowing us to replace the expression $\forall x_{n-1} \ldots \forall x_0 \, \phi_1$ by a simple $\forall x \phi_1$ with $x \in V^n$. Before we do so we shall introduce a simple equivalence relation on V^n so as to identify $x \in V^n$ with $y = x \circ \sigma$. This will allow us to replace the statement of the equivalence (2.46) with the following implication:

$$x \sim y \;\Rightarrow\; \forall x \phi_1 \sim \forall y \phi_1$$

Definition 49 *Let V be a set, $n \in \mathbf{N}$ and $x, y \in V^n$. We say that x is* permutation equivalent to *y and we write $x \sim y$ if and only if there exists a permutation $\sigma : n \to n$ of order n such that $y = x \circ \sigma$.*

Proposition 128 *Let V be a set and $n \in \mathbf{N}$. Let $\sim$ denote the permutation equivalence on V^n. Then $\sim$ is an equivalence relation on V^n.*

Proof
We need to show that $\sim$ is a reflexive, symmetric and transitive relation on V^n. First we show that $\sim$ is reflexive. So suppose $x \in V^n$. We need to show that $x \sim x$. Let $\sigma : n \to n$ be the identity permutation. Then we have $x = x \circ \sigma$. Note that if $n = 0$, then $x = 0$ and $\sigma = 0$ and the equality $x = x \circ \sigma$ is still true. This shows that $x \sim x$. We now show that $\sim$ is symmetric. So suppose $x, y \in V^n$ and $x \sim y$. We need to show that $y \sim x$. By assumption, there exists a permutation $\sigma : n \to n$ such that $y = x \circ \sigma$. Composing to the right by the inverse permutation $\sigma^{-1} : n \to n$ we obtain $y \circ \sigma^{-1} = x$ and it follows that $y \sim x$. We now show that $\sim$ is transitive. So suppose $x, y, z \in V^n$ are such that $x \sim y$ and $y \sim z$. We need to show that $x \sim z$. However, there exist permutations $\sigma : n \to n$ and $\tau : n \to n$ such that $y = x \circ \sigma$ and $z = y \circ \tau$. It follows that $z = x \circ (\sigma \circ \tau)$ and finally $x \sim z$. **.**

2.4.3 Iterated Quantification

The following definition allows us to replace the formalism $\forall x(n-1) \ldots \forall x(0)\, \phi$ with a more condensed expression $\forall x \phi$. In doing so, we are overloading the symbol $\forall$ by creating a new unary operator $\forall x : \mathbf{P}(V) \to \mathbf{P}(V)$ for all $x \in V^n$ and $n \in \mathbf{N}$. This operator coincides with the standard operator $\forall x$ when $x \in V$. Note that when $n = 0$, the only possible element $x \in V^n$ is $x = 0$ and the operator $\forall\, 0 : \mathbf{P}(V) \to \mathbf{P}(V)$ is simply the identity. There is obviously a small risk of notational confusion when seeing $\forall\, 0$ especially in the context of minimal transforms. Overall, we do not think this risk is high enough to warrant the introduction of a different symbol for iterated quantification. Given $n \in \mathbf{N}$ and $x \in V^n$ we define $\forall x \phi$ in terms of the expression $\forall x(n-1) \ldots \forall x(0)\, \phi$. In case this is not clear, this is simply a notational shortcut for the more formal *definition by recursion* $\forall\, 0 \phi = \phi$ and if $x \in V^{n+1}$, $\forall x \phi = \forall x(n) \forall x_{|n} \phi$.

Definition 50 *Let V be a set, $n \in \mathbf{N}$ and $x \in V^n$. For all $\phi \in \mathbf{P}(V)$ we call* iterated quantification of ϕ by x *the element $\forall x \phi$ of $\mathbf{P}(V)$ defined by:*

$$\forall x \phi = \forall x(n-1) \ldots \forall x(0)\, \phi$$

where it is understood that if $n = 0$, we have $\forall\, 0\, \phi = \phi$.

Given any congruence relation $\sim$ on $\mathbf{P}(V)$, we have $\forall x \phi \sim \forall x \psi$ whenever $\phi \sim \psi$ and $x \in V$. Obviously this property should extend to iterated quantification:

Proposition 129 *Let V be a set, $n \in \mathbf{N}$ and $x \in V^n$. Let $\sim$ be an arbitrary congruent relation on $\mathbf{P}(V)$. Then for all $\phi, \psi \in \mathbf{P}(V)$ we have:*

$$\phi \sim \psi \;\Rightarrow\; \forall x \phi \sim \forall x \psi$$

Proof
We shall prove this result by induction on $n \in \mathbf{N}$. First we assume $n = 0$. Then $V^n = \{0\}$ and $x = 0$. By convention the corresponding iterated quantifications are defined as $\forall 0\phi = \phi$ and $\forall 0\psi = \psi$. So the property is clearly true. Next we assume that the property is true for $n \in \mathbf{N}$. We need to show that it is true for $n + 1$. So we assume that $\phi \sim \psi$ and $x \in V^{n+1}$. We need to show that $\forall x\phi \sim \forall x\psi$. However, we have $x_{|n} \in V^n$ and from the induction hypothesis we obtain $\forall x_{|n}\, \phi \sim \forall x_{|n}\, \psi$. Since $\sim$ is a congruent relation on $\mathbf{P}(V)$ we have:

$$\forall x\phi = \forall x(n)\forall x_{|n}\, \phi \sim \forall x(n)\forall x_{|n}\, \psi = \forall x\psi$$

So we conclude that the property is true for $n + 1$. **.**

We are now able to quote and prove what we set out from the beginning. If two iterated quantification operators are equivalent modulo some permutation, then the corresponding formulas are permutation equivalent. This all seems pretty obvious, but it has to be proved one way or another:

Proposition 130 *Let V be a set, $n \in \mathbf{N}$ and $x, y \in V^n$. Let $\sim$ denote the permutation congruence on $\mathbf{P}(V)$. Then for all $\phi \in \mathbf{P}(V)$ we have:*

$$x \sim y \;\Rightarrow\; \forall x\phi \sim \forall y\phi$$

where $x \sim y$ refers to the permutation equivalence on V^n.

Proof
We shall distinguish three cases. First we assume that $n = 0$. Then $x = y = 0$ and the result is clear. Next we assume that $n = 1$. Then $x \sim y$ implies that $x = y$ and the result is also clear. We now assume that $n \geq 2$ and $x \sim y$. We need to show that $\forall x\phi \sim \forall y\phi$. From $x \sim y$ there exists a permutation $\sigma : n \to n$ such that $y = x \circ \sigma$. We shall distinguish two cases. First we assume that σ is an elementary permutation, namely that there exists $i \in n - 1$ such that $\sigma = [i : i + 1]$ (of order n). We shall prove that $\forall x\phi \sim \forall y\phi$ using an induction argument on $n \geq 2$. First we assume that $n = 2$. Then we must have $i = 0$ and $\sigma = [0{:}1]$ (of order 2). Hence from $y = x \circ \sigma$ we obtain:

$$\forall y\phi = \forall y(1)\forall y(0)\, \phi = \forall x(0)\forall x(1)\, \phi$$

Comparing with $\forall x\phi = \forall x(1)\forall x(0)\phi$, it is clear that the ordered pair $(\forall x\phi, \forall y\phi)$ belongs to the generator R_0 of the permutation congruence as per definition (45). In particular we have $\forall x\phi \sim \forall y\phi$ which completes our proof in the case when σ is elementary and $n = 2$. We now assume that the property is true for σ elementary and $n \geq 2$. We need to show that it is also true for σ elementary and $n + 1$. So we assume the existence of $i \in n$ such that $\sigma = [i : i + 1]$ (of order $n + 1$). We need to show that $\forall x\phi \sim \forall y\phi$. We shall distinguish two cases. First we assume that $i = n - 1$ which is the highest possible value when $i \in n$. Then for all $j \in n - 1$ we have $j \neq i$ and $j \neq i + 1$ and consequently $y(j) = x \circ \sigma(j) = x \circ [i : i+1](j) = x(j)$. Hence we see that $x_{|n-1} = y_{|n-1}$, and:

$$\forall y\phi = \forall y(n)\, \forall y(n-1)\, \forall y_{|n-1}\, \phi = \forall x(n-1)\, \forall x(n)\, \forall x_{|n-1}\phi$$

while we have $\forall x\phi = \forall x(n)\,\forall x(n-1)\,\forall x_{|n-1}\phi$. Setting $u = x(n)$ and $v = x(n-1)$ with $\phi_1 = \forall x_{|n-1}\phi$, it follows that $\forall x\phi = \forall u\forall v\,\phi_1$ and $\forall y\phi = \forall v\forall u\,\phi_1$. Hence we see that the ordered pair $(\forall x\phi, \forall y\phi)$ belongs to the generator R_0 of the permutation congruence as per definition (45). In particular $\forall x\phi \sim \forall y\phi$. We now assume that $i \in n-1$. In particular we have $i+1 \neq n$ and $i \neq n$ and:

$$y(n) = x \circ \sigma(n) = x \circ [i : i+1](n) = x(n)$$

It follows that $\forall y\phi = \forall y(n)\forall y_{|n}\,\phi = \forall x(n)\forall y_{|n}\,\phi$ while $\forall x\phi = \forall x(n)\forall x_{|n}\,\phi$. Hence, we see that in order to show that $\forall x\phi \sim \forall y\phi$, the permutation congruence being a congruent relation on $\mathbf{P}(V)$, it is sufficient to prove that $\forall x_{|n}\,\phi \sim \forall y_{|n}\,\phi$. This follows immediately from our induction hypothesis and the fact that:

$$y_{|n} = x \circ \sigma_{|n} = x \circ [i : i+1]_{|n} = x_{|n} \circ [i : i+1]$$

where it is understood that the second occurrence of '$[i : i+1]$' in this equation refers to the elementary permutation of order n (rather than $n+1$) defined for $i \in n-1$. This completes our induction argument and we have proved that $\forall x\phi \sim \forall y\phi$ in the case when $y = x \circ \sigma$ with σ elementary. We now assume that $\sigma : n \to n$ is an arbitrary permutation of order n and we need to show that $\forall x\phi \sim \forall y\phi$. However since $n \geq 2$ it follows from lemma (15) that σ can be expressed as a composition of elementary permutations of order n. In other words, there exist $k \in \mathbf{N}^*$ and elementary permutations $\tau_1, \ldots, \tau_k$ such that:

$$\sigma = \tau_k \circ \ldots \circ \tau_1$$

We shall prove that $\forall x\phi \sim \forall y\phi$ by induction on the integer $k \in \mathbf{N}^*$. If $k = 1$ then σ is an elementary permutation and we have already proved that the result is true. We now assume that the result is true for $k \geq 1$ and we need to show it is also true for $k+1$. So we assume that:

$$\sigma = \tau_{k+1} \circ \tau_k \circ \ldots \circ \tau_1$$

Defining $\sigma^* = \tau_{k+1} \circ \ldots \circ \tau_2$ we obtain $\sigma = \sigma^* \circ \tau_1$. It follows that:

$$y = x \circ \sigma = x \circ \sigma^* \circ \tau_1 = y^* \circ \tau_1$$

where we have put $y^* = x \circ \sigma^*$. Now since τ_1 is an elementary permutation and $y = y^* \circ \tau_1$, we have already proved that $\forall y\phi \sim \forall y^*\phi$. Furthermore, since $y^* = x \circ \sigma^*$ and σ^* is a composition of k elementary permutations, it follows from our induction hypothesis that $\forall y^*\phi \sim \forall x\phi$. By transitivity of the permutation congruence, we conclude that $\forall x\phi \sim \forall y\phi$. **.**

2.4.4 Irreducible Formula

Having proved proposition (130) our next objective is to establish some characterization theorem for the permutation congruence, similar to theorem (12) of page 132 which was established for the substitution congruence. Suppose

$\phi = \forall u \forall v \forall w((u \in v) \to (v \in w))$. We know from theorem (2) of page 21 that the representation $\phi = \forall x \phi_1$ is unique: clearly $\phi_1 = \forall v \forall w((u \in v) \to (v \in w))$ and $x = u$. However, if we introduce iterated quantification as we have done, the representation $\phi = \forall x \phi_1$ with $x \in V^n$ and $n \in \mathbf{N}$ is not unique. However, such representation must be unique if we impose that ϕ_1 *does not start* as a quantification. For lack of a better word, we shall say that ϕ_1 is *irreducible* to indicate that no further quantification can be removed at the top level. Although we are not very happy with the chosen terminology (*irreducible* is a big word in algebra), this is simply a temporary notion soon to be forgotten. It will allow us to prove the uniqueness we require for our characterization theorem.

Definition 51 *Let V be a set and $\phi \in \mathbf{P}(V)$. We say that ϕ is* irreducible *if and only if one of the following is the case:*

$$\begin{array}{ll} (i) & \phi \in \mathbf{P}_0(V) \\ (ii) & \phi = \bot \\ (iii) & \phi = \phi_1 \to \phi_2 \ , \ \phi_1 \in \mathbf{P}(V) \ , \ \phi_2 \in \mathbf{P}(V) \end{array}$$

Proposition 131 *Let V be a set and $\phi \in \mathbf{P}(V)$. Then ϕ can be uniquely represented as $\phi = \forall x \phi_1$ where $x \in V^n$, $n \in \mathbf{N}$, $\phi_1 \in \mathbf{P}(V)$ and ϕ_1 is irreducible.*

Proof
Given $\phi \in \mathbf{P}(V)$ we need to show the existence of $n \in \mathbf{N}$, $x \in V^n$ and ϕ_1 irreducible such that $\phi = \forall x \phi_1$. Furthermore, we need to show that this representation is unique, namely that if $m \in \mathbf{N}$, $y \in V^m$, ψ_1 is irreducible and $\phi = \forall y \psi_1$, then we have $x = y$ and $\phi_1 = \psi_1$. Note that $x = y$ will automatically imply that $n = m$, as identical maps have identical domains. We shall carry out the proof by structural induction using theorem (3) of page 31. Since $\mathbf{P}_0(V)$ is a generator of $\mathbf{P}(V)$, we first check that the property is true for $\phi \in \mathbf{P}_0(V)$. So suppose $\phi \in \mathbf{P}_0(V)$. We take $n = 0$, $x = 0 \in V^n$ and $\phi_1 = \phi$. Then ϕ_1 is irreducible and we have $\phi = \forall x \phi_1$ which shows the existence of the representation. Suppose now that $\phi = \forall y \psi_1$ for some $y \in V^m$, $m \in \mathbf{N}$ and ψ_1 irreducible. Since $\phi \in \mathbf{P}_0(V)$, from theorem (2) of page 21, ϕ cannot be a quantification. It follows that $m = 0$, $y = 0$ and $\phi_1 = \phi = \forall 0 \psi_1 = \psi_1$. This proves the uniqueness of the representation, and the property is proved for $\phi \in \mathbf{P}_0(V)$. We now assume that $\phi = \bot$ or indeed that $\phi = \phi_1 \to \phi_2$. Then ϕ is irreducible and taking $n = 0$, $x = 0$ and $\phi_1 = \phi$ we obtain $\phi = \forall x \phi_1$. Once again from theorem (2), ϕ cannot be a quantification and it follows that this representation is unique. It remains to show that the property is true in the case when $\phi = \forall z \theta$ for some $z \in V$, and the property is true for θ. First we show the existence of the representation. Having assumed that the property is true for θ, there exists $n \in \mathbf{N}$, $x \in V^n$ and θ_1 irreducible such that $\theta = \forall x \theta_1$. Consider the map $x^* : (n+1) \to V$ defined by $x^*_{|n} = x$ and $x^*(n) = z$. Taking $\phi_1 = \theta_1$ we obtain:

$$\forall x^* \phi_1 = \forall x^*(n) \forall x^*_{|n} \, \phi_1 = \forall z \forall x \, \theta_1 = \forall z \theta = \phi$$

which shows the existence of the representation. We now prove the uniqueness. So suppose $m \in \mathbf{N}$, $y \in V^m$, ψ_1 is irreducible and $\phi = \forall y \psi_1$. We need to show

that $y = x^*$ and $\psi_1 = \phi_1$. From $\phi = \forall y \psi_1$ we obtain $\forall z \theta = \forall y \psi_1$. It follows that $\forall y \psi_1$ is a quantification and from theorem (2) it cannot be irreducible. This shows that $m \geq 1$, and consequently $m = p + 1$ for some $p \in \mathbf{N}$. Hence:

$$\forall z \theta = \phi = \forall y \psi_1 = \forall y(p) \forall y_{|p} \psi_1$$

Applying theorem (2) once more, we obtain $z = y(p)$ and $\theta = \forall y_{|p} \psi_1$. Having assumed the property is true for θ, its representation $\theta = \forall x \theta_1$ is unique. It follows that $y_{|p} = x$ and $\psi_1 = \theta_1$. So we have proved that $\psi_1 = \phi_1$. Furthermore from $y_{|p} = x$ it follows that $p = n$ and $m = n+1$. So y is a map $y : (n+1) \to V$ such that $y_{|n} = x$ and $y(n) = z$. We conclude that $y = x^*$. **.**

2.4.5 Characterization of the Permutation Congruence

We are now able to confront our next objective, that of establishing a characterization theorem for the permutation congruence, similar to theorem (12) of page 132. This type of theorem has proved very useful in the case of the substitution congruence. Whenever $\phi \sim \psi$ it is important to be able to say something about the common structure of ϕ and ψ. For example, if $\phi = \phi_1 \to \phi_2$, we want the ability to claim that ψ is also of the form $\psi = \psi_1 \to \psi_2$. An example of this is proposition (108) establishing the formula between substitution ranks $\mathrm{rnk}(\phi) = \max(\, |\mathrm{Fr}(\phi)| \,,\, \mathrm{rnk}(\phi_1) \,,\, \mathrm{rnk}(\phi_2) \,)$ when $\phi = \phi_1 \to \phi_2$. The strategy to prove our characterization theorem (19) below will follow very closely that of theorem (12). We shall not try to be clever: we define a new binary relation on $\mathbf{P}(V)$ which constitutes our best guess of what an appropriate characterization should look like. We then painstakingly prove that this new relation has all the desired properties: it contains the generator of the permutation congruence, it is reflexive, symmetric and transitive. It is a congruent relation, hence a congruence on $\mathbf{P}(V)$ which is in fact equivalent to the permutation congruence.

Definition 52 *Let $\sim$ be the permutation congruence on $\mathbf{P}(V)$ where V is a set. Let $\phi, \psi \in \mathbf{P}(V)$. We say that ϕ is* almost permutation equivalent to ψ *and we write $\phi \simeq \psi$, if and only if one of the following is the case:*

$$\begin{array}{ll} (i) & \phi \in \mathbf{P}_0(V) \ ,\ \psi \in \mathbf{P}_0(V) \ ,\ \textit{and}\ \phi = \psi \\ (ii) & \phi = \bot \ \textit{and}\ \psi = \bot \\ (iii) & \phi = \phi_1 \to \phi_2 \ ,\ \psi = \psi_1 \to \psi_2 \ ,\ \phi_1 \sim \psi_1 \ \textit{and}\ \phi_2 \sim \psi_2 \\ (iv) & \phi = \forall x \phi_1 \ ,\ \psi = \forall y \psi_1 \ ,\ \phi_1 \sim \psi_1 \ ,\ x \sim y \in V^n \ ,\ n \geq 1 \end{array}$$

where it is understood that ϕ_1 and ψ_1 are irreducible in (iv), and $x \sim y$ refers to the permutation equivalence on V^n as per definition (48)*.*

Proposition 132 *$(i), (ii), (iii), (iv)$ of* definition (51) *are mutually exclusive.*

Proof
This is an immediate consequence of theorem (2) of page 21 applied to the free universal algebra $\mathbf{P}(V)$ with free generator $\mathbf{P}_0(V)$, where a formula $\phi \in \mathbf{P}(V)$

is either an element of $\mathbf{P}_0(V)$, or the contradiction constant $\phi = \perp$, or an implication $\phi = \phi_1 \to \phi_2$, or a quantification $\phi = \forall x \phi_1$, but cannot be equal to any two of those things simultaneously. Note that we are requesting that $n \geq 1$ in (iv) of definition (51), so $\phi = \forall x \phi_1$ and $\psi = \forall y \psi_1$ are indeed quantifications when (iv) is the case. **.**

Proposition 133 *Let $\simeq$ be the almost permutation equivalence on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ contains the generator R_0 of* definition (45)*.*

Proof
Let $x, y \in V$ and $\phi_1 \in \mathbf{P}(V)$. Let $\phi = \forall x \forall y \phi_1$ and $\psi = \forall y \forall x \phi_1$. We need to show that $\phi \simeq \psi$. From proposition (131), there exist $n \in \mathbf{N}$, $z \in V^n$ and θ_1 irreducible such that $\phi_1 = \forall z \theta_1$. Consider the map $u : (n+2) \to V$ defined by $u_{|n} = z$, $u(n) = y$ and $u(n+1) = x$. Then we have:

$$\phi = \forall x \forall y \phi_1 = \forall u(n+1)\, \forall u(n)\, \forall u_{|n}\, \theta_1 = \forall u(n+1)\, \forall u_{|n+1}\, \theta_1 = \forall u \theta_1$$

Consider the map $v : (n+2) \to V$ defined by $v = u \circ [n : n+1]$. Then $v_{|n} = z$, $v(n) = x$ and $v(n+1) = y$ and it follows similarly that $\psi = \forall y \forall x \phi_1 = \forall v \theta_1$. Hence, we have found θ_1 irreducible, $u, v \in V^{n+2}$ with $u \sim v$ such that $\phi = \forall u \theta_1$ and $\psi = \forall v \theta_1$. From (iv) of definition (51) we conclude that $\phi \simeq \psi$. **.**

Proposition 134 *Let $\simeq$ be the almost permutation equivalence on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ is a reflexive relation on $\mathbf{P}(V)$.*

Proof
Let $\phi \in \mathbf{P}(V)$. We need to show that $\phi \simeq \phi$. From theorem (2) of page 21 we know that ϕ is either an element of $\mathbf{P}_0(V)$, or $\phi = \perp$ or $\phi = \phi_1 \to \phi_2$ or $\phi = \forall x \phi_1$ for some $\phi_1, \phi_2 \in \mathbf{P}(V)$ and $x \in V$. We shall consider these four mutually exclusive cases separately. Suppose first that $\phi \in \mathbf{P}_0(V)$: then from $\phi = \phi$ we obtain $\phi \simeq \phi$. Suppose next that $\phi = \perp$: then it is clear that $\phi \simeq \phi$. Suppose now that $\phi = \phi_1 \to \phi_2$. Since the permutation congruence $\sim$ is reflexive, we have $\phi_1 \sim \phi_1$ and $\phi_2 \sim \phi_2$. It follows from (iii) of definition (51) that $\phi \simeq \phi$. Suppose finally that $\phi = \forall x \phi_1$. From proposition (131), there exist $n \in \mathbf{N}$, $z \in V^n$ and θ_1 irreducible such that $\phi_1 = \forall z \theta_1$. Consider the map $u : (n+1) \to V$ defined by $u_{|n} = z$ and $u(n) = x$. Then we have:

$$\phi = \forall x \phi_1 = \forall x \forall z\, \theta_1 = \forall u(n)\, \forall u_{|n}\, \theta_1 = \forall u \theta_1$$

Since θ_1 is irreducible, $\theta_1 \sim \theta_1$ and $u \sim u$, we conclude from (iv) of definition (51) that $\phi \simeq \phi$. **.**

Proposition 135 *Let $\simeq$ be the almost permutation equivalence on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ is a symmetric relation on $\mathbf{P}(V)$.*

Proof
Let $\phi, \psi \in \mathbf{P}(V)$ be such that $\phi \simeq \psi$. We need to show that $\psi \simeq \phi$. We shall consider the four possible cases of definition (51): suppose first that $\phi \in \mathbf{P}_0(V)$,

$\psi \in \mathbf{P}_0(V)$ and $\phi = \psi$. Then it is clear that $\psi \simeq \phi$. Suppose next that $\phi = \bot$ and $\psi = \bot$. Then we also have $\psi \simeq \phi$. We now assume that $\phi = \phi_1 \to \phi_2$ and $\psi = \psi_1 \to \psi_2$ with $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$. Since the permutation congruence on $\mathbf{P}(V)$ is symmetric, we have $\psi_1 \sim \phi_1$ and $\psi_2 \sim \phi_2$. Hence we have $\psi \simeq \phi$. We now assume that $\phi = \forall x \phi_1$ and $\psi = \forall y \psi_1$ with $\phi_1 \sim \psi_1$ and ϕ_1, ψ_1 irreducible, $x \sim y \in V^n$ and $n \geq 1$. Then once again by symmetry of the permutation congruence we have $\psi_1 \sim \phi_1$ and furthermore $y \sim x$. It follows that $\psi \simeq \phi$. **.**

Proposition 136 *Let $\simeq$ be the almost permutation equivalence on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ is a transitive relation on $\mathbf{P}(V)$.*

Proof
Let ϕ, ψ and $\chi \in \mathbf{P}(V)$ be such that $\phi \simeq \psi$ and $\psi \simeq \chi$. We need to show that $\phi \simeq \chi$. We shall consider the four possible cases of definition (51) in relation to $\phi \simeq \psi$. Suppose first that $\phi, \psi \in \mathbf{P}_0(V)$ and $\phi = \psi$. Then from $\psi \simeq \chi$ we obtain $\psi, \chi \in \mathbf{P}_0(V)$ and $\psi = \chi$. It follows that $\phi, \chi \in \mathbf{P}_0(V)$ and $\phi = \chi$. Hence we see that $\phi \simeq \chi$. We now assume that $\phi = \psi = \bot$. Then from $\psi \simeq \chi$ we obtain $\psi = \chi = \bot$. It follows that $\phi = \chi = \bot$ and consequently $\phi \simeq \chi$. We now assume that $\phi = \phi_1 \to \phi_2$ and $\psi = \psi_1 \to \psi_2$ with $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$. From $\psi \simeq \chi$ we obtain $\chi = \chi_1 \to \chi_2$ with $\psi_1 \sim \chi_1$ and $\psi_2 \sim \chi_2$. The permutation congruence being transitive, it follows that $\phi_1 \sim \chi_1$ and $\phi_2 \sim \chi_2$. Hence we see that $\phi \simeq \chi$. We now assume that $\phi = \forall x \phi_1$ and $\psi = \forall y \psi_1$ with $\phi_1 \sim \psi_1$, and ϕ_1, ψ_1 irreducible, $x \sim y \in V^n$ and $n \geq 1$. Since $n \geq 1$, from $\psi \simeq \chi$ only the case (iv) of definition (51) is possible. Furthermore from proposition (131), the representation $\psi = \forall y \psi_1$ with ψ_1 irreducible is unique. It follows that $\chi = \forall z \chi_1$ with $\psi_1 \sim \chi_1$ irreducible and $y \sim z \in V^n$. The permutation congruence being transitive, we obtain $\phi_1 \sim \chi_1$. Furthermore, also by transitivity we obtain $x \sim z$ and we conclude that $\phi \simeq \chi$. **.**

Proposition 137 *Let $\simeq$ be the almost permutation equivalence and $\sim$ be the permutation congruence on $\mathbf{P}(V)$, where V is a set. For all $\phi, \psi \in \mathbf{P}(V)$:*

$$\phi \simeq \psi \;\Rightarrow\; \phi \sim \psi$$

Proof
Let $\phi, \psi \in \mathbf{P}(V)$ such that $\phi \simeq \psi$. We need to show that $\phi \sim \psi$. We shall consider the four possible cases of definition (51) in relation to $\phi \simeq \psi$. Suppose first that $\phi = \psi \in \mathbf{P}_0(V)$. From the reflexivity of the permutation congruence, it is clear that $\phi \sim \psi$. Suppose next that $\phi = \psi = \bot$. Then we also have $\phi \sim \psi$. We now assume that $\phi = \phi_1 \to \phi_2$ and $\psi = \psi_1 \to \psi_2$ where $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$. The permutation congruence being a congruent relation on $\mathbf{P}(V)$, we obtain $\phi \sim \psi$. Next we assume that $\phi = \forall x \phi_1$ and $\psi = \forall y \psi_1$ where $\phi_1 \sim \psi_1$ and ϕ_1, ψ_1 are irreducible, $x \sim y \in V^n$ and $n \geq 1$. The permutation congruence being a congruent relation on $\mathbf{P}(V)$, from proposition (129) and $\phi_1 \sim \psi_1$ we obtain $\forall y \phi_1 \sim \forall y \psi_1$. Hence by transitivity of the permutation congruence, it remains to show that $\forall x \phi_1 \sim \forall y \phi_1$ which follows immediately from $x \sim y$ and proposition (130). **.**

Proposition 138 *Let $\simeq$ be the almost permutation equivalence on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ is a congruent relation on $\mathbf{P}(V)$.*

Proof
From proposition (134), the almost permutation equivalence $\simeq$ is reflexive and so $\perp \simeq \perp$. We now assume that $\phi = \phi_1 \to \phi_2$ and $\psi = \psi_1 \to \psi_2$ where $\phi_1 \simeq \psi_1$ and $\phi_2 \simeq \psi_2$. We need to show that $\phi \simeq \psi$. However from proposition (137) we have $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$ and it follows from definition (51) that $\phi \simeq \psi$. We now assume that $\phi = \forall x \phi_1$ and $\psi = \forall x \psi_1$ where $\phi_1 \simeq \psi_1$ and $x \in V$. We need to show that $\phi \simeq \psi$. Once again from proposition (137) we have $\phi_1 \sim \psi_1$. We shall now distinguish two cases in relation to $\phi_1 \simeq \psi_1$. First we assume that (i) (ii) or (iii) of definition (51) is the case. Then both ϕ_1 and ψ_1 are irreducible. Defining $x^* : 1 \to V$ by setting $x^*(0) = x$ we obtain:

$$\phi = \forall x \phi_1 = \forall x^*(0)\, \phi_1 = \forall x^* \phi_1$$

and similarly $\psi = \forall x^* \psi_1$. From ϕ_1, ψ_1 irreducible and $\phi_1 \sim \psi_1$ we conclude that $\phi \simeq \psi$. We now assume that (iv) of definition (51) is the case. Then $\phi_1 = \forall u \phi_1^*$ and $\psi_1 = \forall v \psi_1^*$ where $\phi_1^* \sim \psi_1^*$ and ϕ_1^*, ψ_1^* are irreducible, $u \sim v \in V^n$ and $n \geq 1$. Defining $u^* : (n+1) \to V$ by setting $u^*_{|n} = u$ and $u^*(n) = x$ we obtain:

$$\phi = \forall x \phi_1 = \forall x \forall u \phi_1^* = \forall u^*(n) \forall u^*_{|n}\, \phi_1^* = \forall u^* \phi_1^*$$

and similarly $\psi = \forall v^* \psi_1^*$ where $v : (n+1) \to V$ is defined by $v^*_{|n} = v$ and $v^*(n) = x$. Since ϕ_1^*, ψ_1^* are irreducible and $\phi_1^* \sim \psi_1^*$, in order to show that $\phi \simeq \psi$ it is sufficient to prove that $u^* \sim v^*$. However since $u \sim v$, there exists a permutation $\sigma : n \to n$ of order n such that $v = u \circ \sigma$. Defining $\sigma^* : (n+1) \to (n+1)$ by $\sigma^*_{|n} = \sigma$ and $\sigma^*(n) = n$ we obtain a permutation of order $n+1$ such that $v^* = u^* \circ \sigma^*$. **.**

Proposition 139 *Let $\simeq$ be the almost permutation equivalence on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ is a congruence on $\mathbf{P}(V)$.*

Proof
We need to show that $\simeq$ is reflexive, symmetric, transitive and that it is a congruent relation on $\mathbf{P}(V)$. From proposition (134), the relation $\simeq$ is reflexive. From proposition (135) it is symmetric while from proposition (136) it is transitive. Finally from proposition (138) the relation $\simeq$ is a congruent relation. **.**

Proposition 140 *Let $\simeq$ be the almost permutation equivalence and $\sim$ be the permutation congruence on $\mathbf{P}(V)$, where V is a set. For all $\phi, \psi \in \mathbf{P}(V)$:*

$$\phi \simeq \psi \;\Leftrightarrow\; \phi \sim \psi$$

Proof
From proposition (137) it is sufficient to show the implication $\Leftarrow$ or equivalently the inclusion $\sim \subseteq \simeq$. Since $\sim$ is the permutation congruence on $\mathbf{P}(V)$, it is the

smallest congruence on $\mathbf{P}(V)$ which contains the set R_0 of definition (45). In order to show the inclusion $\sim \subseteq \simeq$ it is therefore sufficient to show that $\simeq$ is a congruence on $\mathbf{P}(V)$ such that $R_0 \subseteq \simeq$. The fact that it is a congruence stems from proposition (139). The fact that $R_0 \subseteq \simeq$ follows from proposition (133). .

Recall that *irreducible* formulas are defined in page 191. We can now forget about the *almost permutation equivalence* and simply remember the following characterization of the permutation congruence on $\mathbf{P}(V)$:

Theorem 19 *Let $\sim$ be the permutation congruence on $\mathbf{P}(V)$ where V is a set. For all $\phi, \psi \in \mathbf{P}(V)$, $\phi \sim \psi$ if and only if one of the following is the case:*

$$\begin{array}{ll} (i) & \phi \in \mathbf{P}_0(V)\ ,\ \psi \in \mathbf{P}_0(V)\ ,\ \textit{and}\ \phi = \psi \\ (ii) & \phi = \bot\ \textit{and}\ \psi = \bot \\ (iii) & \phi = \phi_1 \to \phi_2\ ,\ \psi = \psi_1 \to \psi_2\ ,\ \phi_1 \sim \psi_1\ \textit{and}\ \phi_2 \sim \psi_2 \\ (iv) & \phi = \forall x \phi_1\ ,\ \psi = \forall y \psi_1\ ,\ \phi_1 \sim \psi_1\ ,\ x \sim y \in V^n\ ,\ n \geq 1 \end{array}$$

where $x \sim y$ refers to the permutation equivalence on V^n as per definition (48). *Furthermore, we may assume that ϕ_1 and ψ_1 are irreducible in (iv).*

Proof
First we show the implication $\Rightarrow$. So we assume that $\phi \sim \psi$. We need to show that (i), (ii), (iii) or (iv) is the case. However from proposition (140) we have $\phi \simeq \psi$. It follows from definition (51) that (i), (ii), (iii) or (iv) is indeed the case with ϕ_1 and ψ_1 irreducible in the case of (iv). We now show the reverse implication $\Leftarrow$. So we assume that (i), (ii), (iii) or (iv) is the case. We need to show that $\phi \sim \psi$. We shall distinguish two cases. First we assume that (i), (ii) or (iii) is the case. Then from definition (51) we obtain $\phi \simeq \psi$ and consequently from proposition (140) we have $\phi \sim \psi$. We now assume that (iv) is the case. Then from proposition (129) and $\phi_1 \sim \psi_1$ we obtain $\forall x \phi_1 \sim \forall x \psi_1$. Furthermore, from proposition (130) and $x \sim y$ we obtain $\forall x \psi_1 \sim \forall y \psi_1$. By transitivity of the permutation congruence, we conclude that:

$$\phi = \forall x \phi_1 \sim \forall y \psi_1 = \psi$$

.

2.5 The Absorption Congruence

2.5.1 The Absorption Congruence

After the substitution and permutation congruence, following our pursuit of the *right* congruence on $\mathbf{P}(V)$ which should be defined to identify mathematical statements which have the same *meaning*, a third source of identity will be studied in this section. As mathematicians, it is not uncommon for us to regard a mathematical statement ϕ_1 as being exactly the same as $\forall x \phi_1$ whenever x is not a free variable of ϕ_1. We shall define the *absorption congruence* on $\mathbf{P}(V)$ as

being generated by the ordered pairs $(\phi_1, \forall x \phi_1)$ where $x \notin \mathrm{Fr}(\phi_1)$. Note that whichever final congruence we wish to adopt to define the *universal algebra of first order logic*, it is not completely obvious that such congruence should contain the absorption congruence: on the one hand it is appealing to say that $\bot$ and $\forall x \bot$ are the same mathematical statements. On the other hand, a consequence of doing so will be that $\top$ and $\exists x \top$ will also be identical statements, after we include some propositional equivalence, and define $\top$ and $\exists x$ in the obvious way. This state of affairs is somewhat unsatisfactory: The statement $\top$ does not say anything, contrary to the statement $\exists x \top$ which expresses the existence of something. If we are to use the *universal algebra of first order logic* to study axiomatic set theory at a later stage, we would rather have the existence of at least one set guaranteed by the axioms of **ZF**, rather than being embedded in the language being used. The universe being void is a logical possibility.

Definition 53 *Let V be a set. We call* absorption congruence *on $\mathbf{P}(V)$, the congruence on $\mathbf{P}(V)$ generated by the following set $R_0 \subseteq \mathbf{P}(V) \times \mathbf{P}(V)$:*

$$R_0 = \{ \, (\phi_1, \forall x \phi_1) \ : \ \ x \notin \mathrm{Fr}(\phi_1) \ , \ \phi_1 \in \mathbf{P}(V) \ , \ x \in V \ \}$$

Just like the substitution and the permutation congruence, the absorption congruence preserves free variables. The following proposition is similar to propositions (79) and (127) and simply involves checking the property on R_0 :

Proposition 141 *Let $\sim$ denote the absorption congruence on $\mathbf{P}(V)$ where V is a set. Then for all $\phi, \psi \in \mathbf{P}(V)$ we have the implication:*

$$\phi \sim \psi \ \Rightarrow \ \mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$$

Proof
Let $\equiv$ denote the relation on $\mathbf{P}(V)$ defined by $\phi \equiv \psi$ if and only if we have $\mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$. Then we need to show that $\sim \subseteq \equiv$. However, we know from proposition (46) that $\equiv$ is a congruence on $\mathbf{P}(V)$. Since $\sim$ is defined as the smallest congruence on $\mathbf{P}(V)$ which contains the set R_0 of definition (52), we simply need to show that $R_0 \subseteq \equiv$. So let $\phi_1 \in \mathbf{P}(V)$ and $x \in V$ such that $x \notin \mathrm{Fr}(\phi_1)$. We need to show that $\phi_1 \equiv \forall x \phi_1$ which is $\mathrm{Fr}(\phi_1) = \mathrm{Fr}(\forall x \phi_1)$. Since $\mathrm{Fr}(\forall x \phi_1) = \mathrm{Fr}(\phi_1) \setminus \{x\}$, the result follows from $x \notin \mathrm{Fr}(\phi_1)$. **.**

When $\sim$ is the substitution or permutation congruence and $\phi, \psi \in \mathbf{P}(V)$ are such that $\phi \sim \psi$, from the structural form of ϕ we are able to infer the structural form of ψ thanks to the characterizations of theorem (12) of page 132 and theorem (19) of page 196. For example, when $\phi = \phi_1 \to \phi_2$, we are able to tell that ψ must be of the form $\psi = \psi_1 \to \psi_2$ which can be very useful when dealing with structural induction arguments. So we would like to obtain a similar result for the absorption congruence, and we shall do so in theorem (20) of page 205. However, the case of the absorption congruence is more complicated than any other in this respect, as it does not preserve the structure of formulas. So for example if $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$ then the formula $\phi = \phi_1 \to \phi_2$ and $\psi = \psi_1 \to \psi_2$ must be equivalent simply because $\sim$ is a congruent relation.

But from the equivalence $\phi \sim \psi$ and the knowledge that $\phi = \phi_1 \to \phi_2$, it is impossible for us to conclude that $\psi = \psi_1 \to \psi_2$ with $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$. This is because we can always add quantifiers $\forall x$, $\forall y \forall x$ and $\forall z \forall y \forall x$ in front of the formula ψ with $x, y, z \notin \mathrm{Fr}(\psi)$, while preserving the equivalence class of ψ. So the situation appears hopeless, and one natural instinct is to give up attempting to provide a characterization theorem for the absorption congruence, in line with theorem (12) and theorem (19). However, it may be that the equivalence $\phi \sim \psi$ allows us to say something about ϕ and ψ nonetheless, something which may be a weaker statement than initially hoped for, but still better than nothing at all. Consider the formula $\phi \in \mathbf{P}(V)$: It may have a few *pointless quantifiers* coming at the front. In other words, it may be of the form $\phi = \forall z \forall y \forall x \phi^*$ with $x, y, z \notin \mathrm{Fr}(\phi^*)$. So let us assume that these *pointless* quantifications at the front have been removed and we are left with the formula ϕ^*. In particular, we assume that any quantifier coming at the front of ϕ^* is *meaningful*, in the sense that if $\phi^* = \forall x \phi_1$ then $x \in \mathrm{Fr}(\phi_1)$. Now consider the formula ψ: we can also remove the *first layer of meaningless* quantification and retain the *core* ψ^* of the formula ψ. It is clear that we have $\phi \sim \phi^*$ and $\psi \sim \psi^*$. So whenever the equivalence $\phi \sim \psi$ arises, we accept the inescapable fact that nothing can be said about the relative structures of ϕ and ψ as these are being obfuscated by the presence of *pointless quantifications* at the front. But it may be that something can be said about the relative structures of ϕ^* and ψ^*. In other words, after we remove the *first layer* of *meaningless quantifications*, the remaining *core formulas* may have a common structure. This is indeed the case, as will be seen from theorem (20) of page 205. For now, we shall concentrate on giving a precise definition of the *core formula* ϕ^* obtained from ϕ after removing the *first layer of pointless quantifications*. We shall prove in proposition (142) below that any formula ϕ can be uniquely expressed as $\phi = \forall u \phi^*$ with $u \in V^n$, $n \in \mathbf{N}$ and additional properties formalizing the idea that the iterated quantification $\forall u$ of definition (49) is *pointless* while any remaining quantifier at the front of ϕ^* is meaningful. This allows us to put forward the definition:

Definition 54 *Let V be a set and $\phi \in \mathbf{P}(V)$. We call $\phi = \forall u \phi^*$ of* proposition (142) the core decomposition *of ϕ, and we call ϕ^* the* core *of ϕ.*

Before we prove proposition (142) we shall establish the following lemma:

Lemma 16 *Let $n \in \mathbf{N}$, $u \in V^n$ and $\phi^* \in \mathbf{P}(V)$. The following are equivalent:*

$$(i) \qquad u(k) \notin \mathrm{Fr}(\phi^*) \text{ , for all } k \in n$$
$$(ii) \qquad u(k) \notin \mathrm{Fr}(\forall u_{|k} \phi^*) \text{ , for all } k \in n$$

Proof
In order to show the equivalence between (i) and (ii), it is sufficient to prove that if (i) or (ii) is satisfied, then the property $(k \in n) \Rightarrow \mathrm{Fr}(\phi^*) = \mathrm{Fr}(\forall u_{|k} \phi^*)$ is true. Recall that given $u \in V^n$, u is a map $u : n \to V$ and $u_{|k}$ is the restriction

of u to $k \subseteq n$. When $k = 0$, from definition (49) of the iterated quantification we have $\mathrm{Fr}(\,\forall u_{|k}\phi^*\,) = \mathrm{Fr}(\forall\, 0\phi^*) = \mathrm{Fr}(\phi^*)$ so the property is true, regardless of whether (i) or (ii) holds. So suppose the property is true for $k \in \mathbf{N}$. We need to show it is also true for $k+1$. So we assume that $(k+1) \in n$. We need to show the equality $\mathrm{Fr}(\phi^*) = \mathrm{Fr}(\,\forall u_{|(k+1)}\phi^*\,)$. Assuming (i) is true:

$$\begin{aligned} \mathrm{Fr}(\,\forall u_{|(k+1)}\phi^*\,) &= \mathrm{Fr}(\,\forall u(k)\forall u_{|k}\phi^*\,) \\ &= \mathrm{Fr}(\,\forall u_{|k}\phi^*\,) \setminus \{u(k)\} \\ \text{Induction hypothesis } \rightarrow &= \mathrm{Fr}(\phi^*) \setminus \{u(k)\} \\ (i) \ \rightarrow &= \mathrm{Fr}(\phi^*) \end{aligned}$$

If we assume that (ii) is true, then the argument goes as follows:

$$\begin{aligned} \mathrm{Fr}(\,\forall u_{|(k+1)}\phi^*\,) &= \mathrm{Fr}(\,\forall u(k)\forall u_{|k}\phi^*\,) \\ &= \mathrm{Fr}(\,\forall u_{|k}\phi^*\,) \setminus \{u(k)\} \\ (ii) \ \rightarrow &= \mathrm{Fr}(\,\forall u_{|k}\phi^*\,) \\ \text{Induction hypothesis } \rightarrow &= \mathrm{Fr}(\phi^*) \end{aligned}$$

.

In proposition (142) below, we chose to write $u(k) \notin \mathrm{Fr}(\,\forall u_{|k}\phi^*\,)$ in (i) rather than the simpler $u(k) \notin \mathrm{Fr}(\phi^*)$. This will make some of the formal proofs smoother. By virtue of lemma (16) the two are equivalent.

Proposition 142 *Let V be a set and $\phi \in \mathbf{P}(V)$. Then ϕ can be uniquely represented as $\phi = \forall u\phi^*$ where $u \in V^n$, $n \in \mathbf{N}$, $\phi^* \in \mathbf{P}(V)$ with the property:*

$$\begin{aligned} &(i) \qquad u(k) \notin \mathrm{Fr}(\,\forall u_{|k}\phi^*\,) \text{ , for all } k \in n \\ &(ii) \qquad \phi^* = \forall z\psi \ \Rightarrow \ z \in \mathrm{Fr}(\psi) \end{aligned}$$

where it is understood that (ii) holds for all $z \in V$ and $\psi \in \mathbf{P}(V)$.

Proof
We shall prove this property with a structural induction using theorem (3) of page 31. First we assume that $\phi = (x \in y)$ for some $x, y \in V$. Take $\phi^* = \phi$, $n = 0$ and $u = 0$. We claim that $\forall u\phi^*$ is a core decomposition of ϕ. From definition (49) of the iterated quantification, it is clear that $\phi = \forall u\phi^*$. Since $n = 0$, property (i) of proposition (142) is vacuously satisfied. Furthermore since $\phi^* = (x \in y)$, from theorem (2) of page 21 we see that ϕ^* cannot be expressed as $\phi^* = \forall z\psi$ where $z \in V$ and $\psi \in \mathbf{P}(V)$. It follows that (ii) is also vacuously satisfied. So we have proved the existence of the core decomposition $\phi = \forall u\phi^*$. We now show the uniqueness: so suppose $\phi = \forall u\phi^*$ for some $u \in V^n$, $n \in \mathbf{N}$ and $\phi^* \in \mathbf{P}(V)$. We need to show that $n = 0$, $u = 0$ and $\phi^* = \phi$. So suppose to the contrary that $n > 0$. Then we obtain the following equality:

$$(x \in y) = \phi = \forall u\phi^* = \forall u(n-1)\forall u_{|(n-1)}\phi^*$$

which contradict the uniqueness property of theorem (2). It follows that $n = 0$ and from $u \in V^n = \{0\}$ we obtain $u = 0$ and finally $\phi = \forall u \phi^* = \phi^*$. So we now assume that $\phi = \bot$. Once again, taking $\phi^* = \phi$, $n = 0$ and $u = 0$ we obtain a core decomposition $\forall u \phi^*$ of ϕ. Furthermore if we assume $\phi = \forall u \phi^*$ for some $u \in V^n$, $n \in \mathbf{N}$ and $\phi^* \in \mathbf{P}(V)$, then $n = 0$ follows immediately from theorem (2) and consequently $u = 0$ and $\phi^* = \phi$. So we now assume that $\phi = \phi_1 \to \phi_2$ for some $\phi_1, \phi_2 \in \mathbf{P}(V)$ which satisfy our property. We need to show the same is true of ϕ. Take $\phi^* = \phi$, $n = 0$ and $u = 0$. We obtain a core decomposition $\forall u \phi^*$ of ϕ which is unique by virtue of theorem (2). The fact that ϕ_1 and ϕ_2 are themselves uniquely decomposable is irrelevant here. So we now assume that $\phi = \forall x \phi_1$ for some $x \in V$ and $\phi_1 \in \mathbf{P}(V)$ satisfying our property. We need to show the same is true of ϕ. We shall distinguish two cases: first we assume that $x \in \mathrm{Fr}(\phi_1)$. Take $\phi^* = \phi$, $n = 0$ and $u = 0$. We claim that $\forall u \phi^*$ is a core decomposition of ϕ. Since $\phi = \forall u \phi^*$ and (i) is vacuously satisfied, we simply need to check that (ii) is true. So suppose $\phi^* = \forall z \psi$ for some $z \in V$ and $\psi \in \mathbf{P}(V)$. We need to show that $z \in \mathrm{Fr}(\psi)$. However the equality $\phi^* = \forall z \psi$ implies that $\forall x \phi_1 = \forall z \psi$ and consequently from theorem (2) we have $x = z$ and $\phi_1 = \psi$. It follows that $z \in \mathrm{Fr}(\psi)$ from the assumption $x \in \mathrm{Fr}(\phi_1)$. We now prove the uniqueness of the core decomposition in the case when $x \in \mathrm{Fr}(\phi_1)$. So suppose $\phi = \forall u \phi^*$ for some $u \in V^n$, $n \in \mathbf{N}$ and $\phi^* \in \mathbf{P}(V)$ satisfying (i) and (ii). We need to show that $n = 0$, $u = 0$ and $\phi^* = \phi$. Suppose to the contrary that $n > 0$. Then we obtain the following equality:

$$\forall x \phi_1 = \phi = \forall u \phi^* = \forall u(n-1) \forall u_{|(n-1)} \phi^*$$

Using theorem (2) we obtain $x = u(n-1)$ and $\phi_1 = \forall u_{|(n-1)} \phi^*$. Applying property (i) to $k = (n-1) \in n$ we obtain $x \notin \mathrm{Fr}(\phi_1)$ which contradicts our assumption. We now assume that $x \notin \mathrm{Fr}(\phi_1)$. First we show that a core decomposition exists: from our induction hypothesis there exists a core decomposition $\phi_1 = \forall u_1 \phi_1^*$ of ϕ_1, where $u_1 \in V^{n_1}$, $n_1 \in \mathbf{N}$ and $\phi_1^* \in \mathbf{P}(V)$ satisfying (i) and (ii). Take $\phi^* = \phi_1^*$, $n = n_1 + 1$ and $u \in V^n$ defined by $u_{|(n-1)} = u_1$ and $u(n-1) = x$. We claim $\forall u \phi^*$ is a core decomposition of ϕ:

$$\begin{aligned} \phi &= \forall x \phi_1 \\ &= \forall x \forall u_1 \phi_1^* \\ &= \forall u(n-1) \forall u_{|(n-1)} \phi^* \\ &= \forall u \phi^* \end{aligned}$$

So it remains to check that (i) and (ii) are satisfied. First we show (i). So let $k \in n$. We need to show that $u(k) \notin \mathrm{Fr}(\forall u_{|k} \phi^*)$. We shall distinguish two cases. First we assume that $k = n - 1$. Then we need to show that $x \notin \mathrm{Fr}(\forall u_1 \phi_1^*) = \mathrm{Fr}(\phi_1)$ which is true by assumption. Next we assume that $k \in (n-1)$. Then we need to show that $u_1(k) \notin \mathrm{Fr}(\forall (u_1)_{|k} \phi_1^*)$ which is true by virtue of property (i) applied to the core decomposition $\phi_1 = \forall u_1 \phi_1^*$. We now show property (ii). So we assume that $\phi^* = \forall z \psi$ for some $z \in V$ and $\psi \in \mathbf{P}(V)$. We need to show that $z \in \mathrm{Fr}(\psi)$. Since $\phi^* = \phi_1^*$, this follows from

property (ii) applied to the core decomposition $\phi_1 = \forall u_1 \phi_1^*$. So we have proved that $\forall u \phi^*$ is indeed a core decomposition of ϕ in the case when $x \notin \mathrm{Fr}(\phi_1)$. It remains to show the uniqueness. So we assume that $\phi = \forall u \phi^*$ for some $u \in V^n$, $n \in \mathbf{N}$ and $\phi^* \in \mathbf{P}(V)$ satisfying (i) and (ii). We need to show that $n = n_1 + 1$, $u(n-1) = x$, $u_{|(n-1)} = u_1$ and $\phi^* = \phi_1^*$. First we show that $n > 0$. Indeed if $n = 0$ then $u = 0$ and consequently we obtain $\phi^* = \forall u \phi^* = \phi = \forall x \phi_1$. It follows from property (ii) that $x \in \mathrm{Fr}(\phi_1)$ which contradicts our assumption. Having established that $n > 0$ we obtain the equality:

$$\forall u(n-1) \forall u_{|(n-1)} \phi^* = \forall u \phi^* = \phi = \forall x \phi_1 = \forall x \forall u_1 \phi_1^*$$

Using theorem (2) we see that $x = u(n-1)$ as requested and furthermore:

$$\forall u_{|(n-1)} \phi^* = \phi_1 = \forall u_1 \phi_1^*$$

From our induction hypothesis and the uniqueness of the core decomposition $\phi_1 = \forall u_1 \phi_1^*$, in order to show that $u_{|(n-1)} = u_1$ and $\phi^* = \phi_1^*$ it is sufficient to prove that $\forall u_{|(n-1)} \phi^*$ is a core decomposition of ϕ_1. So we simply need to check that (i) and (ii) are satisfied, which is clearly the case since (i) and (ii) are assumed to be true for the decomposition $\forall u \phi^*$. Having established the equality between the maps $u_{|(n-1)}$ and u_1, these must have identical domain and consequently $n = n_1 + 1$ as requested, which completes our induction. **.**

We shall now formally check that the core of ϕ is equivalent to ϕ modulo the absorption congruence, which is what we expect. Removing the *first layer of pointless quantification* does not affect the equivalence class of ϕ:

Proposition 143 *Let $\sim$ be the absorption congruence on $\mathbf{P}(V)$ where V is a set. Let $\phi \in \mathbf{P}(V)$ with core $\phi^* \in \mathbf{P}(V)$. Then we have the equivalence:*

$$\phi \sim \phi^*$$

Proof
We shall prove the equivalence with an induction argument over $n \in \mathbf{N}$, where n is the integer underlying the core decomposition $\phi = \forall u \phi^*$ where $u \in V^n$ and $\phi^* \in \mathbf{P}(V)$ satisfying (i) and (ii) of proposition (142). First we assume that $n = 0$. Then $u = 0$ and $\phi = \phi^*$ so the equivalence is clear. Next we assume that $n > 0$ and the equivalence is true for $n - 1$. We need to show that $\forall u \phi^* \sim \phi^*$. However, since $\forall u \phi^*$ satisfy (i) and (ii) of proposition (142), the same can be said of $\forall u_{|(n-1)} \phi^*$ which is therefore a core decomposition itself. From our induction hypothesis we obtain $\forall u_{|(n-1)} \phi^* \sim \phi^*$. It is therefore sufficient to prove that $\forall u(n-1) \forall u_{|(n-1)} \phi^* \sim \forall u_{|(n-1)} \phi^*$ which follows immediately from $u(n-1) \notin \mathrm{Fr}(\forall u_{|(n-1)} \phi^*)$ and definition (52). **.**

Lemma 17 *Let V be a set and $\phi \in \mathbf{P}(V)$ with core decomposition $\phi = \forall u \phi^*$ where $u \in V^n$. Let $x \in V$ with $x \notin \mathrm{Fr}(\phi)$. Then $\forall x \phi$ has core decomposition:*

$$\forall x \phi = \forall v \phi^*$$

where $v \in V^{n+1}$ is defined by the equalities $v(n) = x$ and $v_{|n} = u$.

Proof
We assume that $\forall u\phi^*$ is the core decomposition of ϕ where $u \in V^n$. Let $x \in V$ with $x \notin \mathrm{Fr}(\phi)$. Let $v \in V^{n+1}$ be defined by $v(n) = x$ and $v_{|n} = u$. We need to show that $\forall v\phi^*$ is the core decomposition of $\forall x\phi$. We have:

$$\begin{aligned} \forall v\phi^* &= \forall v(n)\forall v_{|n}\phi^* \\ &= \forall x\forall u\phi^* \\ &= \forall x\phi \end{aligned}$$

So it remains to show that (i) and (ii) of proposition (142) are satisfied. First we show (i). So let $k \in (n+1)$. We need to show that $v(k) \notin \mathrm{Fr}(\forall v_{|k}\phi^*)$. We shall distinguish two cases: first we assume that $k = n$. Then we need to show that $x \notin \mathrm{Fr}(\forall u\phi^*) = \mathrm{Fr}(\phi)$ which is true by assumption. Next we assume that $k \in n$. Then we need to show that $u(k) \notin \mathrm{Fr}(\forall u_{|k}\phi^*)$ which follows from (i) applied to the core decomposition $\forall u\phi^*$. We now prove (ii). So we assume that $\phi^* = \forall z\psi$ for some $z \in V$ and $\psi \in \mathbf{P}(V)$. We need to show that $z \in \mathrm{Fr}(\psi)$. This follows immediately from (ii) applied to the core decomposition $\forall u\phi^*$. **.**

2.5.2 Characterization of the Absorption Congruence

In this section, we shall provide a characterization theorem for the absorption congruence, in similar fashion to what was done for theorem (12) of page 132 and theorem (19) of page 196 of the substitution and permutation congruence respectively. As discussed in the previous section, if $\sim$ denotes the absorption congruence on $\mathbf{P}(V)$ then the equivalence $\phi \sim \psi$ does not allow us to say anything on the relative structures of ϕ and ψ. However, we are able to infer something about the core formulas ϕ^* and ψ^* of definition (53). Our strategy to prove theorem (20) below will mirror exactly that of theorem (12) and theorem (19). We start by defining a binary relation of *almost equivalence* on $\mathbf{P}(V)$ which is our best guess of what a proper characterization of the absorption congruence should look like. We then proceed to show that the *almost equivalence* is indeed an equivalence relation on $\mathbf{P}(V)$ which is in fact a congruent relation, and we conclude by showing that it coincides with the absorption congruence.

Definition 55 *Let $\sim$ be the absorption congruence on $\mathbf{P}(V)$ where V is a set. Let $\phi, \psi \in \mathbf{P}(V)$. We say that ϕ is* almost equivalent to *ψ and we write $\phi \simeq \psi$, if and only if one of the following is the case:*

$$\begin{array}{ll} (i) & \phi^* \in \mathbf{P}_0(V)\ ,\ \psi^* \in \mathbf{P}_0(V)\ ,\ \textit{and}\ \phi^* = \psi^* \\ (ii) & \phi^* = \bot\ \textit{and}\ \psi^* = \bot \\ (iii) & \phi^* = \phi_1 \to \phi_2\ ,\ \psi^* = \psi_1 \to \psi_2\ ,\ \phi_1 \sim \psi_1\ \textit{and}\ \phi_2 \sim \psi_2 \\ (iv) & \phi^* = \forall x\phi_1\ ,\ \psi^* = \forall x\psi_1\ ,\ x \in V\ \textit{and}\ \phi_1 \sim \psi_1 \end{array}$$

where ϕ^* and ψ^* are the core of ϕ and ψ respectively as per definition (53).

Proposition 144 *$(i), (ii), (iii), (iv)$ of* def. (54) *are mutually exclusive.*

Proof
This follows immediately from theorem (2) of page 21 applied to $\mathbf{P}(V)$. **.**

Proposition 145 *Let $\simeq$ be the almost equivalence relation on $\mathbf{P}(V)$ where V is a set. Then $\simeq$ contains the generator R_0 of* definition (52)*.*

Proof
Let $x \in V$ and $\phi_1 \in \mathbf{P}(V)$ such that $x \notin \mathrm{Fr}(\phi_1)$. We need to show that $\phi_1 \simeq \forall x \phi_1$. Let $\phi_1 = \forall u \phi^*$ where $u \in V^n$ be the core decomposition of ϕ_1. Since $x \notin \mathrm{Fr}(\phi_1)$, from lemma (17) we see that the core decomposition of $\forall x \phi_1$ is $\forall v \phi^*$ for some $v \in V^{n+1}$. In particular, ϕ_1 and $\forall x \phi_1$ have identical core ϕ^*. Using theorem (2) of page 21, we must have $\phi^* \in \mathbf{P}_0(V)$ or $\phi^* = \bot$ or $\phi^* = \phi_1 \to \phi_2$ for some $\phi_1, \phi_2 \in \mathbf{P}(V)$ or $\phi^* = \forall z \psi$ for some $z \in V$ and $\psi \in \mathbf{P}(V)$. So (i), (ii), (iii) or (iv) of definition (54) must be the case. **.**

Proposition 146 *The almost equivalence relation on $\mathbf{P}(V)$ is reflexive.*

Proof
Let $\phi \in \mathbf{P}(V)$. We need to show that $\phi \simeq \phi$. Let ϕ^* be the core of ϕ. From theorem (2) of page 21, one of the four following cases must occur: if $\phi^* = (x \in y)$ for some $x, y \in V$, then $\phi \simeq \phi$ follows from $\phi^* = \phi^*$. If $\phi^* = \bot$ then $\phi \simeq \phi$ follows again from $\phi^* = \phi^*$. If ϕ^* is of the form $\phi^* = \phi_1 \to \phi_2$ then $\phi \simeq \phi$ follows from the reflexivity of $\sim$. If ϕ^* is of the form $\phi^* = \forall x \phi_1$, then $\phi \simeq \phi$ follows again from the reflexivity of $\sim$, which completes our proof. **.**

Proposition 147 *The almost equivalence relation on $\mathbf{P}(V)$ is symmetric.*

Proof
Follows immediately from the symmetry of the absorption congruence $\sim$. **.**

Proposition 148 *The almost equivalence relation on $\mathbf{P}(V)$ is transitive.*

Proof
Let $\phi, \psi, \chi \in \mathbf{P}(V)$ such that $\phi \simeq \psi$ and $\psi \simeq \chi$. We need to show that $\phi \simeq \chi$. We shall consider the four possible cases (i), (ii), (iii) and (iv) of definition (54) in relation to $\phi \simeq \psi$. Let ϕ^*, ψ^* and χ^* denote the core of ϕ, ψ and χ respectively. First we assume that $\phi^* \in \mathbf{P}_0(V)$, $\psi^* \in \mathbf{P}_0(V)$ with $\phi^* = \psi^*$. Then from $\psi \simeq \chi$ we must have $\chi^* \in \mathbf{P}_0(V)$ and $\psi^* = \chi^*$. It follows that $\phi^* \in \mathbf{P}_0(V)$, $\chi^* \in \mathbf{P}_0(V)$ and $\phi^* = \chi^*$ and we see that $\phi \simeq \chi$. Next we assume that $\phi^* = \bot = \psi^*$. Then from $\psi \simeq \chi$ we must have $\psi^* = \bot = \chi^*$ and we conclude once again that $\phi \simeq \chi$. Next we assume that ϕ^* and ψ^* are of the form $\phi^* = \phi_1 \to \phi_2$ and $\psi^* = \psi_1 \to \psi_2$ with $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$. Then from $\psi \simeq \chi$ we see that χ^* must be of the form $\chi^* = \chi_1 \to \chi_2$ with $\psi_1 \sim \chi_1$ and $\psi_2 \sim \chi_2$. From the transitivity of the absorption congruence, it follows that $\phi_1 \sim \chi_1$ and $\phi_2 \sim \chi_2$ and consequently $\phi \simeq \chi$. Finally, we assume that ϕ^* and ψ^* are of the form $\phi^* = \forall x \phi_1$ and $\psi^* = \forall x \psi_1$ with $\phi_1 \sim \psi_1$. Then from $\psi \simeq \chi$ we see that χ^* must be of the form $\chi^* = \forall x \chi_1$ with $\psi_1 \sim \chi_1$. Once again by transitivity we obtain $\phi_1 \sim \chi_1$ and finally $\phi \simeq \chi$ as requested. **.**

Proposition 149 *Let $\simeq$ be the almost equivalence and $\sim$ be the absorption congruence on $\mathbf{P}(V)$, where V is a set. For all $\phi, \psi \in \mathbf{P}(V)$:*

$$\phi \simeq \psi \;\Rightarrow\; \phi \sim \psi$$

Proof
Let $\phi, \psi \in \mathbf{P}(V)$ such that $\phi \simeq \psi$. We need to show that $\phi \sim \psi$. We shall consider the four possible cases (i), (ii), (iii) and (iv) of definition (54) in relation to $\phi \simeq \psi$. Let ϕ^* and ψ^* denote the core of ϕ and ψ respectively. From proposition (143) we have $\phi \sim \phi^*$ and $\psi \sim \psi^*$. It is therefore sufficient to prove that $\phi^* \sim \psi^*$. This equivalence is clear in cases (i) and (ii) of definition (54). So we assume that ϕ^* and ψ^* are of the form $\phi^* = \phi_1 \to \phi_2$ and $\psi^* = \psi_1 \to \psi_2$ where $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$. The absorption congruence being a congruent relation we obtain $\phi^* \sim \psi^*$ as requested. Finally, we assume that ϕ^* and ψ^* are of the form $\phi^* = \forall x \phi_1$ and $\psi^* = \forall x \psi_1$ with $\phi_1 \sim \psi_1$. Once again, using the fact that the absorption congruence is a congruent relation we obtain $\phi^* \sim \psi^*$.
.

Proposition 150 *The almost equivalence relation on $\mathbf{P}(V)$ is congruent.*

Proof
By reflexivity, we already know that $\bot \simeq \bot$. So we assume that $\phi = \phi_1 \to \phi_2$ and $\psi = \psi_1 \to \psi_2$ where $\phi_1 \simeq \psi_1$ and $\phi_2 \simeq \psi_2$. We need to show that $\phi \simeq \psi$. However, using proposition (142), it is clear the core decomposition of ϕ and ψ are $\phi = \forall u \phi^*$ and $\psi = \forall v \psi^*$ with $u = v = 0$, $\phi^* = \phi$ and $\psi^* = \psi$. Furthermore, from proposition (149) we have $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$. It follows that ϕ^* and ψ^* are of the form $\phi^* = \phi_1 \to \phi_2$ and $\psi^* = \psi_1 \to \psi_2$ with $\phi_1 \sim \psi_1$ and $\phi_2 \sim \psi_2$. Hence we see that $\phi \simeq \psi$ as requested. We now assume that $\phi = \forall x \phi_1$ and $\psi = \forall x \psi_1$ where $x \in V$ and $\phi_1 \simeq \psi_1$. We need to show that $\phi \simeq \psi$. We shall distinguish two cases: first we assume that $x \in \mathrm{Fr}(\phi_1)$. From $\phi_1 \simeq \psi_1$ and proposition (149) we obtain $\phi_1 \sim \psi_1$. It follows from proposition (141) that $\mathrm{Fr}(\phi_1) = \mathrm{Fr}(\psi_1)$ and consequently $x \in \mathrm{Fr}(\psi_1)$. Using proposition (142) it is clear that the core decomposition of ϕ and ψ are $\phi = \forall u \phi^*$ and $\psi = \forall v \psi^*$ where $u = v = 0$, $\phi^* = \phi$ and $\psi^* = \psi$. Note that the conditions $x \in \mathrm{Fr}(\phi_1)$ and $x \in \mathrm{Fr}(\psi_1)$ are crucially required to ensure (ii) of proposition (142) is satisfied. So we have proved that ϕ^* and ψ^* are of the form $\phi^* = \forall x \phi_1$ and $\psi^* = \forall x \psi_1$ with $\phi_1 \sim \psi_1$ and we conclude that $\phi \simeq \psi$ as requested. We now assume that $x \notin \mathrm{Fr}(\phi_1)$. Then we also have $x \notin \mathrm{Fr}(\psi_1)$. Let $\phi_1 = \forall u_1 \phi^*$ and $\psi_1 = \forall v_1 \psi^*$ be the core decompositions of ϕ_1 and ψ_1 respectively. Then from lemma (17) the core decompositions of ϕ and ψ are of the form $\phi = \forall u \phi^*$ and $\psi = \forall v \psi^*$. In particular, ϕ and ϕ_1 have identical core ϕ^* while ψ and ψ_1 have identical core ψ^*. From $\phi_1 \simeq \psi_1$ and definition (54) we conclude that $\phi \simeq \psi$ as requested. .

Proposition 151 *The almost equivalence relation on $\mathbf{P}(V)$ is a congruence.*

Proof
From proposition (146), the relation $\simeq$ is reflexive. From proposition (147)

it is symmetric while from proposition (148) it is transitive. It is therefore an equivalence relation on $\mathbf{P}(V)$. Furthermore, from proposition (150), the relation $\simeq$ is congruent. We conclude that it is a congruence relation on $\mathbf{P}(V)$. .

Proposition 152 *Let $\simeq$ be the almost equivalence and $\sim$ be the absorption congruence on $\mathbf{P}(V)$, where V is a set. For all $\phi, \psi \in \mathbf{P}(V)$:*

$$\phi \simeq \psi \;\Leftrightarrow\; \phi \sim \psi$$

Proof
We need to show the equality $\simeq = \sim$. The inclusion $\subseteq$ follows from proposition (149). So it remains to show $\supseteq$. However, since $\sim$ is the smallest congruence on $\mathbf{P}(V)$ which contains the set R_0 of definition (52), it is sufficient to show that $\simeq$ is a congruence which contains R_0. The fact that $\simeq$ is a congruence follows from proposition (151). The fact that it contains R_0 follows from (145). .

We can now forget about the *almost equivalence* and conclude with:

Theorem 20 *Let $\sim$ be the absorption congruence on $\mathbf{P}(V)$ where V is a set. For all $\phi, \psi \in \mathbf{P}(V)$, $\phi \sim \psi$ if and only if one of the following is the case:*

$$\begin{array}{ll}
(i) & \phi^* \in \mathbf{P}_0(V)\ ,\ \psi^* \in \mathbf{P}_0(V)\ ,\ \textit{and}\ \phi^* = \psi^* \\
(ii) & \phi^* = \bot\ \textit{and}\ \psi^* = \bot \\
(iii) & \phi^* = \phi_1 \to \phi_2\ ,\ \psi^* = \psi_1 \to \psi_2\ ,\ \phi_1 \sim \psi_1\ \textit{and}\ \phi_2 \sim \psi_2 \\
(iv) & \phi^* = \forall x \phi_1\ ,\ \psi^* = \forall x \psi_1\ ,\ x \in V\ \textit{and}\ \phi_1 \sim \psi_1
\end{array}$$

where ϕ^* and ψ^* are the core of ϕ and ψ respectively as per definition (53).

Proof
This follows immediately from definition (54) and proposition (152). .

2.5.3 Absorption Mapping and Absorption Congruence

In definition (38) we introduced the minimal transform $\mathcal{M} : \mathbf{P}(V) \to \mathbf{P}(\bar{V})$ which allowed us to characterize an α-equivalence $\phi \sim \psi$ with a simple equality $\mathcal{M}(\phi) = \mathcal{M}(\psi)$, as follows from theorem (14) of page 149. We would like to achieve a similar result for the absorption congruence. As we shall see, things are a lot simpler in this case. We shall define a mapping $\mathcal{A} : \mathbf{P}(V) \to \mathbf{P}(V)$ which effectively removes *pointless quantifications* from a formula. We shall then prove that the absorption equivalence $\phi \sim \psi$ can be reduced to the equality $\mathcal{A}(\phi) = \mathcal{A}(\psi)$. This will be done in proposition (156) below. In general given a congruence $\sim$ on $\mathbf{P}(V)$, we believe there is enormous benefit in reducing the equivalence $\phi \sim \psi$ to an equality $f(\phi) = f(\psi)$ for some map $f : \mathbf{P}(V) \to A$ where A is an arbitrary set. This can always be done of course, as $\phi \sim \psi$ is equivalent to an equality $[\phi] = [\psi]$ between equivalence classes. However, if

we can find a map f which is *computable* in some sense with a codomain A in which the equality is *decidable*, this will ensure that the congruence $\sim$ is itself *decidable*. Granted we have no idea what *computable* and *decidable* mean at this stage, but at some point we shall want to know. This is for later.

Definition 56 *Let V be a set. We call* absorption mapping on $\mathbf{P}(V)$ *the map $\mathcal{A} : \mathbf{P}(V) \to \mathbf{P}(V)$ defined by the following recursive equation:*

$$\forall \phi \in \mathbf{P}(V)\ ,\ \mathcal{A}(\phi) = \begin{cases} (x \in y) & \text{if} \quad \phi = (x \in y) \\ \bot & \text{if} \quad \phi = \bot \\ \mathcal{A}(\phi_1) \to \mathcal{A}(\phi_2) & \text{if} \quad \phi = \phi_1 \to \phi_2 \\ \forall x \mathcal{A}(\phi_1) & \text{if} \quad \phi = \forall x \phi_1,\ x \in \mathrm{Fr}(\phi_1) \\ \mathcal{A}(\phi_1) & \text{if} \quad \phi = \forall x \phi_1,\ x \notin \mathrm{Fr}(\phi_1) \end{cases}$$

Proposition 153 *The structural recursion of* definition (55) *is legitimate.*

Proof
We have to be slightly careful in this case. As usual, we have a choice between theorem (4) of page 42 and theorem (5) of page 44. Given $\phi = \forall x \phi_1$, looking at definition (55) it seems that $\mathcal{A}(\phi)$ is not simply a function of $\mathcal{A}(\phi_1)$ but also involves a dependence in ϕ_1. So it would seem that theorem (5) has to be used in this case. Of course, it is not difficult to see that an equivalent definition could be obtained by replacing $\mathrm{Fr}(\phi_1)$ by $\mathrm{Fr}(\mathcal{A}(\phi_1))$, allowing us to use theorem (4) instead. However, we have no need to worry about that. So let us use theorem (5) with $X = \mathbf{P}(V)$, $X_0 = \mathbf{P}_0(V)$ and $A = \mathbf{P}(V)$. We define $g_0 : X_0 \to A$ by setting $g_0(x \in y) = (x \in y)$ which ensures the first condition of definition (55) is met. Next, we define $h(\bot) : A^0 \times X^0 \to A$ by setting $h(\bot)(0, 0) = \bot$ which gives us the second condition. Next, we define $h(\to) : A^2 \times X^2 \to A$ be setting $h(a, \phi) = a(0) \to a(1)$. Finally, we define $h(\forall x) : A^1 \times X^1 \to A$ be setting $h(\forall x)(a, \phi) = \forall x a(0)$ if $x \in \mathrm{Fr}(\phi(0))$ and $h(\forall x)(a, \phi) = a(0)$ otherwise. So let us check that conditions 3, 4 and 5 are met. If $\phi = \phi_1 \to \phi_2$ we have the following equalities:

$$\begin{array}{rcl} \mathcal{A}(\phi) & = & \mathcal{A}(\phi_1 \to \phi_2) \\ f = \to,\ \phi = (\phi_1, \phi_2) \ \to & = & \mathcal{A}(f(\phi)) \\ \mathcal{A} : X^2 \to A^2 \ \to & = & h(f)(\mathcal{A}(\phi), \phi) \\ & = & h(\to)(\mathcal{A}(\phi), \phi) \\ & = & \mathcal{A}(\phi)(0) \to \mathcal{A}(\phi)(1) \\ \mathcal{A} : X \to A \ \to & = & \mathcal{A}(\phi(0)) \to \mathcal{A}(\phi(1)) \\ & = & \mathcal{A}(\phi_1) \to \mathcal{A}(\phi_2) \end{array}$$

If $\phi = \forall x \phi_1$ with $x \in \mathrm{Fr}(\phi_1)$, then we have the following equalities:

$$\begin{array}{rcl} \mathcal{A}(\phi) & = & \mathcal{A}(\forall x \phi_1) \\ f = \forall x,\ \phi(0) = \phi_1 \ \to & = & \mathcal{A}(f(\phi)) \end{array}$$

$$\begin{array}{rcl}
\mathcal{A}:X^1\to A^1\ \to & = & h(f)(\mathcal{A}(\phi),\phi)\\
 & = & h(\forall x)(\mathcal{A}(\phi),\phi)\\
x\in \mathrm{Fr}(\phi(0))\ \to & = & \forall x\mathcal{A}(\phi)(0)\\
\mathcal{A}:X\to A\ \to & = & \forall x\mathcal{A}(\phi(0))\\
 & = & \forall x\mathcal{A}(\phi_1)
\end{array}$$

The case $x\notin \mathrm{Fr}(\phi_1)$ is dealt with in a similar way. **.**

In proposition (99) we showed that $\mathcal{M}(\phi)\sim i(\phi)$ where $\sim$ is the substitution congruence and $i:V\to\bar{V}$ is the inclusion map. In effect, this shows that the minimal transform preserves the equivalence class of ϕ. Of course, this is not quite true as the minimal transform takes values in $\mathbf{P}(\bar{V})$ and not $\mathbf{P}(V)$. So the equivalence class of ϕ is preserved only after we embed ϕ in $\mathbf{P}(\bar{V})$ as $i(\phi)$. In the case of the absorption congruence things are simpler: since the absorption mapping takes values in $\mathbf{P}(V)$ itself, we are able to write equivalence $\mathcal{A}(\phi)\sim\phi$.

Proposition 154 *Let V be a set and $\mathcal{A}:\mathbf{P}(V)\to\mathbf{P}(V)$ be the absorption mapping. Let $\sim$ be the absorption congruence on $\mathbf{P}(V)$. Then given $\phi\in\mathbf{P}(V)$:*

$$\mathcal{A}(\phi)\sim\phi$$

Proof
We shall prove this equivalence with a structural induction, using theorem (3) of page 31. The equivalence is clear in the case when $\phi=(x\in y)$ and $\phi=\bot$. So we assume that $\phi=\phi_1\to\phi_2$ where $\phi_1,\phi_2\in\mathbf{P}(V)$ satisfy our equivalence:

$$\begin{array}{rcl}
\mathcal{A}(\phi) & = & \mathcal{A}(\phi_1\to\phi_2)\\
 & = & \mathcal{A}(\phi_1)\to\mathcal{A}(\phi_2)\\
 & \sim & \phi_1\to\phi_2\\
 & = & \phi
\end{array}$$

Next we assume that $\phi=\forall x\phi_1$ for some $x\in V$ and $\phi_1\in\mathbf{P}(V)$ satisfying our equivalence. We shall distinguish two cases. First we assume that $x\in\mathrm{Fr}(\phi_1)$:

$$\begin{array}{rcl}
\mathcal{A}(\phi) & = & \mathcal{A}(\forall x\phi_1)\\
x\in\mathrm{Fr}(\phi_1)\ \to & = & \forall x\mathcal{A}(\phi_1)\\
 & \sim & \forall x\phi_1\\
 & = & \phi
\end{array}$$

Next we assume that $x\notin\mathrm{Fr}(\phi_1)$. Then we have:

$$\begin{array}{rcl}
\mathcal{A}(\phi) & = & \mathcal{A}(\forall x\phi_1)\\
x\notin\mathrm{Fr}(\phi_1)\ \to & = & \mathcal{A}(\phi_1)\\
 & \sim & \phi_1\\
x\notin\mathrm{Fr}(\phi_1)\ \to & \sim & \forall x\phi_1\\
 & = & \phi
\end{array}$$

.

Before we prove that the equivalence $\phi \sim \psi$ can be reduced to the quality $\mathcal{A}(\phi) = \mathcal{A}(\psi)$ we shall need to show that this equality defines a congruence:

Proposition 155 *Let V be a set and $\equiv$ be the relation on $\mathbf{P}(V)$ defined by:*

$$\phi \equiv \psi \;\Leftrightarrow\; \mathcal{A}(\phi) = \mathcal{A}(\psi)$$

where $\mathcal{A} : \mathbf{P}(V) \to \mathbf{P}(V)$ is the absorption mapping. Then $\equiv$ is a congruence.

Proof
The relation $\equiv$ is clearly an equivalence relation on $\mathbf{P}(V)$. So it remains to show that it is also a congruent relation. By reflexivity, we already know that $\bot \equiv \bot$. So let $\phi = \phi_1 \to \phi_2$ and $\psi = \psi_1 \to \psi_2$ be such that $\phi_1 \equiv \psi_1$ and $\phi_2 \equiv \psi_2$. We need to show that $\phi \equiv \psi$ or equivalently $\mathcal{A}(\phi) = \mathcal{A}(\psi)$ which goes as follows:

$$\begin{array}{rcl} \mathcal{A}(\phi) & = & \mathcal{A}(\phi_1 \to \phi_2) \\ & = & \mathcal{A}(\phi_1) \to \mathcal{A}(\phi_2) \\ \phi_i \equiv \psi_i \;\to & = & \mathcal{A}(\psi_1) \to \mathcal{A}(\psi_2) \\ & = & \mathcal{A}(\psi_1 \to \psi_2) \\ & = & \mathcal{A}(\psi) \end{array}$$

We now assume that $\phi = \forall x \phi_1$ and $\psi = \forall x \psi_1$ where $\phi_1 \equiv \psi_1$. We need to show that $\phi \equiv \psi$ or equivalently $\mathcal{A}(\phi) = \mathcal{A}(\psi)$. We shall distinguish two cases: first we assume that $x \in \mathrm{Fr}(\phi_1)$. Having assumed that $\phi_1 \equiv \psi_1$, we obtain $\mathcal{A}(\phi_1) = \mathcal{A}(\psi_1)$ and consequently from proposition (154) we have $\phi_1 \sim \psi_1$, where $\sim$ is the absorption congruence on $\mathbf{P}(V)$. It follows from proposition (141) that $\mathrm{Fr}(\phi_1) = \mathrm{Fr}(\psi_1)$ and thus $x \in \mathrm{Fr}(\psi_1)$. Hence we have:

$$\begin{array}{rcl} \mathcal{A}(\phi) & = & \mathcal{A}(\forall x \phi_1) \\ x \in \mathrm{Fr}(\phi_1) \;\to & = & \forall x \mathcal{A}(\phi_1) \\ \phi_1 \equiv \psi_1 \;\to & = & \forall x \mathcal{A}(\psi_1) \\ x \in \mathrm{Fr}(\psi_1) \;\to & = & \mathcal{A}(\forall x \psi_1) \\ & = & \mathcal{A}(\psi) \end{array}$$

We now assume that $x \notin \mathrm{Fr}(\phi_1)$. Then we also have $x \notin \mathrm{Fr}(\psi_1)$ and hence:

$$\begin{array}{rcl} \mathcal{A}(\phi) & = & \mathcal{A}(\forall x \phi_1) \\ x \notin \mathrm{Fr}(\phi_1) \;\to & = & \mathcal{A}(\phi_1) \\ \phi_1 \equiv \psi_1 \;\to & = & \mathcal{A}(\psi_1) \\ x \notin \mathrm{Fr}(\psi_1) \;\to & = & \mathcal{A}(\forall x \psi_1) \\ & = & \mathcal{A}(\psi) \end{array}$$

.

Proposition 156 *Let $\sim$ be the absorption congruence on $\mathbf{P}(V)$ where V is a set. Then for all $\phi, \psi \in \mathbf{P}(V)$ we have the following equivalence:*

$$\phi \sim \psi \;\Leftrightarrow\; \mathcal{A}(\phi) = \mathcal{A}(\psi)$$

where $\mathcal{A} : \mathbf{P}(V) \to \mathbf{P}(V)$ is the absorption mapping as per definition (55)*.*

Proof
First we show $\Rightarrow$: Let $\equiv$ be the relation on $\mathbf{P}(V)$ defined by $\phi \equiv \psi$ if and only if $\mathcal{A}(\phi) = \mathcal{A}(\psi)$. We need to show the inclusion $\sim \subseteq \equiv$. However, since $\sim$ is the smallest congruence on $\mathbf{P}(V)$ which contains the set R_0 of definition (52), it is sufficient to show that $\equiv$ is a congruence on $\mathbf{P}(V)$ which contains R_0. We already know from proposition (155) that $\equiv$ is a congruence on $\mathbf{P}(V)$. So it remains to show that $R_0 \subseteq \equiv$. So let $\phi_1 \in \mathbf{P}(V)$ and $x \in V$ such that $x \notin \mathrm{Fr}(\phi_1)$. We need to show that $\mathcal{A}(\phi_1) = \mathcal{A}(\forall x \phi_1)$ which follows immediately from definition (55). We now prove $\Leftarrow$: so we assume that $\mathcal{A}(\phi) = \mathcal{A}(\psi)$. We need to show that $\phi \sim \psi$, which follows immediately from proposition (154). **.**

2.6 The Propositional Congruence

2.6.1 The Propositional Congruence

Definition 57 *Let V be a set. We call* propositional valuation *on $\mathbf{P}(V)$ any map $v : \mathbf{P}(V) \to 2$ satisfying the following properties. Given $\phi_1, \phi_2 \in \mathbf{P}(V)$:*

$$\begin{array}{ll} (i) & v(\bot) = 0 \\ (ii) & v(\phi_1 \to \phi_2) = v(\phi_1) \to v(\phi_2) \end{array}$$

Definition 58 *Let V be a set. We call* propositional congruence *on $\mathbf{P}(V)$, the congruence on $\mathbf{P}(V)$ generated by the following set $R_0 \subseteq \mathbf{P}(V) \times \mathbf{P}(V)$:*

$$R_0 = \{\, (\phi, \psi) \;:\; v(\phi) = v(\psi) \text{ for all } v : \mathbf{P}(V) \to 2 \text{ propositional valuation} \,\}$$

To be continued...

Chapter 3

The Free Universal Algebra of Proofs

3.1 The Hilbert Deductive Congruence

3.1.1 Preliminaries

In this section we introduce yet another congruence on $\mathbf{P}(V)$ which we have chosen to call the *Hilbert deductive congruence*, hoping this will make it obvious to the familiar reader. Another possible name could have been the *Lindenbaum-Tarski congruence* since it is the congruence giving rise to the Lindenbaum-Tarski algebra, a seemingly well established term in mathematical logic. The Hilbert deductive congruence is probably not what we are looking for to define our *Universal Algebra of First Order Logic*. We are looking to identify mathematical statements which have the same meaning, and such identification should be decidable. We are not looking for theorems. However, the study of the Hilbert deductive congruence gives us a great opportunity to introduce fundamental notions of mathematical logic which we shall no doubt require at a later stage: these are the concept of proof and provability, the deduction theorem, the notion of semantics and model, and of course Gödel's completeness theorem. These are the bread and butter of any textbook on mathematical logic and it is about time we touch upon them. So our first objective will be to define the notion of proof and provability, which is the question of axiomatization of first order logic. Having reviewed some of the existing textbooks and references, it is astonishing to see how little consensus there is on the subject. It is impossible to find two references which will universally agree on which axioms should be used, or which rules of inference. So we had to make our own mind and decide for ourselves what constitutes a *good* axiomatization of first order logic, and here it is: firstly, a good axiomatization of first order logic should be *sound* and ensure Gödel's completeness theorem holds. This is rather uncontroversial so we shall not say more about it. Secondly, The deduction theorem should hold *without*

any form of restriction. Most references will depart from this principle and quote the deduction theorem imposing some form of restriction, typically that a formula should be closed (e.g. [18], [30], [32], [39], [43], [44], [45], [62]). The only exception known to us is [4] where the deduction theorem is restored to its full glory. This we believe should be the case. There is also a web page [46] on `http://planetmath.org` indicating the awareness by some living mathematicians that the deduction theorem need not fail in first order logic, provided the concept of proof is carefully defined. This brings us to our third requirement which a good axiomatization of first order logic ought to meet: the concept of proof *should not* be presented in terms of finite sequences of formulas. Instead, proofs should be defined as formal expressions in a free universal algebra generated by the formulas of the language itself (the set of possible hypothesis) and whose operators are the chosen rules of inference: to every formula ϕ corresponds a proof $\pi = \partial\phi$ arising from a constant operator, indicating that ϕ is invoked as an axiom; to every proof π corresponds another proof $\nabla x\pi$ arising from a unary operator indicating a *generalization* with respect to the variable x; to every pair of proof (π_1, π_2) corresponds another proof $\pi_1 \oplus \pi_2$ arising from a binary operator, that of *modus ponens* for example... On this algebra of proofs should be defined a key semantics associating every proof to its conclusion. By imposing this free algebraic structure on proofs, we are preserving their natural tree structure, giving us the full power of structural induction and structural recursion which we cannot enjoy with the linear structure of finite sequences. These should be abandoned. Some authors still want to define formulas as finite sequences of characters and will go as far as introducing a concatenation operator on their *strings*, explaining why the parenthesis (and) should be used. At best, they are just creating a free universal algebra of formulas which could have been defined in a generic way, up to isomorphism. At worse, by insisting on the details of their *string* implementation, they are making everything very awkward to prove. Finite sequences are not suited to mathematical logic.

3.1.2 Axioms of First Order Logic

We are now introducing the axioms which we intend to use as part of our deductive system. These axioms come in five different groups which we shall describe individually. The first three groups of axioms are often referred to as *propositional axioms* while the other two are specific to first order logic, dealing with quantification. We have no axiom relating to equality of course, having dismissed the equality predicate from our language. As already explained prior to definition (22) of page 67, we are hoping to define the notion of equality in terms of the primitive symbol '$\in$', and make equality axioms simple consequences of our specific coding. So no equality for now. In choosing these five groups of axioms, we have tried to keep it lean and simple, while reaching the greatest possible consensus between the references available to us. The axioms below are pretty much those of Donald W. Barnes and John M. Mack [4], Miklós Ferenczi and Miklós Szőts [18], P.T. Johnstone [32], Elliot Mendelson [43] and G. Takeuti and W.M. Zaring [61]. They are referred to as *traditional textbook axioms of*

predicate calculus by Norman Megill's Metamath web site [45] which we find reassuring. However, these references disagree on some minor details so we had to choose between them. For example, contrary to [18] we do not wish to speak of *formula scheme*, which we feel do not bring much mathematical value. We have also decided against [4] and avoided as much congruence as possible when defining axioms, to keep the material as down to earth as possible. Finally, we have ignored a few oddities in [32] which were seemingly motivated by P.T. Johnstone's desire to allow the *empty* model.

Our first group of axioms corresponds to 'Axiom ax-1' of Metamath [45]. We have decided to follow this reference in calling an axiom within this group a *simplification axiom*. It appears the terminology originates from the link between these axioms and the formula $\phi_1 \wedge \phi_2 \to \phi_1$. Some historical background can be found on the web page `http://us.metamath.org/mpegif/ax-1.html`.

Definition 59 *Let V be a set. We call* simplification axiom *on $\mathbf{P}(V)$ any formula $\phi \in \mathbf{P}(V)$ for which there exist $\phi_1, \phi_2 \in \mathbf{P}(V)$ such that:*

$$\phi = \phi_1 \to (\phi_2 \to \phi_1)$$

The set of simplification axioms on $\mathbf{P}(V)$ is denoted $\mathbf{A}_1(V)$.

Our second group of axioms corresponds to 'Axiom ax-2' of Metamath [45]. We have again decided to follow this reference in calling an axiom within this group a *Frege axiom*. Further details and historical background can be found on the web page `http://us.metamath.org/mpegif/ax-2.html`.

Definition 60 *Let V be a set. We call* Frege axiom *on $\mathbf{P}(V)$ any formula $\phi \in \mathbf{P}(V)$ for which there exist $\phi_1, \phi_2, \phi_3 \in \mathbf{P}(V)$ such that:*

$$\phi = [\phi_1 \to (\phi_2 \to \phi_3)] \to [(\phi_1 \to \phi_2) \to (\phi_1 \to \phi_3)]$$

The set of Frege axioms on $\mathbf{P}(V)$ is denoted $\mathbf{A}_2(V)$.

Our third group of axioms corresponds to 'Axiom ax-3' of Metamath [45] which can be found on `http://us.metamath.org/mpegif/ax-3.html`. However, we chose a different form for these axioms, namely $[(\phi_1 \to \bot) \to \bot] \to \phi_1$ following [4] and [32] rather than $(\neg\phi_1 \to \neg\phi_2) \to (\phi_2 \to \phi_1)$ which is also the form encountered in [18]. It is easy to believe that both choices lead to the same notion of provability. Our terminology is *transposition axiom* following [45].

Definition 61 *Let V be a set. We call* transposition axiom *on $\mathbf{P}(V)$ any formula $\phi \in \mathbf{P}(V)$ for which there exists $\phi_1 \in \mathbf{P}(V)$ such that:*

$$\phi = [(\phi_1 \to \bot) \to \bot] \to \phi_1$$

The set of transposition axioms on $\mathbf{P}(V)$ is denoted $\mathbf{A}_3(V)$.

Our fourth group of axioms is that of 'Theorem stdpc5' in Metamath [45] which can be found on `http://us.metamath.org/mpegif/stdpc5.html`. Norman Megill has this as a theorem rather than an axiom but it is still mentioned on `http://us.metamath.org/mpegif/mmset.html#traditional` as a

traditional textbook axiom. It is indeed a chosen axiom of [4], [18] and [32]. As we were not able to find an obvious name, we chose *quantification axiom*.

Definition 62 *Let V be a set. We call* quantification axiom *on $\mathbf{P}(V)$ any formula $\phi \in \mathbf{P}(V)$ for which there exist $\phi_1, \phi_2 \in \mathbf{P}(V)$ and $x \in V$ such that:*

$$x \notin \mathrm{Fr}(\phi_1)\ ,\ \phi = \forall x(\phi_1 \to \phi_2) \to (\phi_1 \to \forall x \phi_2)$$

The set of quantification axioms on $\mathbf{P}(V)$ is denoted $\mathbf{A}_4(V)$.

Our fifth and last group of axioms is 'Theorem stdpc4' of Metamath [45] which can be found on `http://us.metamath.org/mpegif/stdpc4.html`. Following this reference once again, we have decided to call axioms within this group a *specialization axiom*. It is a chosen group of axioms for [4], [18] and [32] with varying wordings in relation to the highly delicate problem of making sure variable substitutions are valid. Indeed, a specialization axiom is of the form:

$$\forall x \phi_1 \to \phi_1[y/x] \tag{3.1}$$

Strictly speaking, this formula will have a different meaning, and require different verbal qualifications, depending on the specifics of how the substitution $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ is defined. For example, most references in the literature will define $[y/x]$ with a recursive formula in which *bound occurrences of x* are not replaced by y. This is contrary to our own definition (24) of page 69 where all variables are systematically substituted regardless of whether they are free or bound occurrences. As it turns out, we did not rely on definition (24) to define specialization axioms, but defined them instead in terms of an *essential substitution* $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ as per definition (44). In other words, if $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ denotes an essential substitution associated with the map $[y/x] : V \to V$ of definition (26), then the formula (3.1) is a legitimate *specialization axiom*. In a more condensed form, $\forall x \phi_1 \to \phi_1[y/x]$ is an axiom whenever $[y/x]$ is an *essential substitution of y in place of x*. This is beautiful, this is short and does not require any further qualification such as '*provided y is free for x in ϕ_1*', i.e. provided $[y/x]$ is valid for ϕ_1 as per definition (30). There is however a huge disadvantage in using essential substitutions when defining specialization axioms: the level of mathematical sophistication required to follow the analysis is a lot higher and most people will stop reading. Surely we do not want that. Another drawback is that essential substitutions are intertwined with the notion of substitution congruence. If $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$ is an essential substitution and $\phi \in \mathbf{P}(V)$ then $\sigma(\phi)$ is of course a well defined formula of $\mathbf{P}(V)$ but the specifics of $\sigma(\phi)$ are usually unknown. We typically only know about the class of $\sigma(\phi)$ modulo the substitution congruence. Luckily this is often all we care about, but it does mean we are not able to provide an axiomatization of first order logic without dependencies to the substitution congruence. In the light of these considerations, our preferred option would have been to define the specialization axioms in line with the existing literature:

$$\forall x \phi_1 \to \phi_1[y/x]\ ,\ \text{where } [y/x] \text{ is valid for } \phi_1 \tag{3.2}$$

where the substitution $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ is now simply the substitution associated with $[y/x] : V \to V$ as per definition (24). This would have the advantage of being simple, consistent with the usual practice and devoid of any reference to the substitution congruence. The fact that our substitutions of definition (24) have an impact on bound occurrences of variables is contrary to standard practice, but of little significance. The notion of *valid substitution* of definition (30) is not commonly found in textbooks, but is a nice and simple generalization of the idea that *y is free for x in ϕ_1*. So why not simply use (3.2) to define specialization axioms? Why introduce the elaborate notion of *essential substitutions* and seemingly make everything more complicated with no visible benefit? The answer is this: we do not have a choice. This document is devoted to the study of the algebra $\mathbf{P}(V)$ where V is a set of arbitrary cardinality. In particular V can be a finite set. By contrast, the existing literature focusses on first order languages where the number of variables is typically countably infinite. This makes a big difference. We believe our insistence on allowing V to be finite will be rewarded. We cannot be sure at this stage, but we are quite certain the theory of vector spaces was not solely developed in the infinite dimensional case. There must be value in the study of first order languages which are *finite dimensional*. This is of course no more than a hunch, but we are not quite ready to give it up. So let us understand why allowing V to be finite changes everything: consider $V = \{x, y\}$ and $\phi = \forall x \phi_1 = \forall x \forall y (x \in y)$ where $x \neq y$. We know from theorem (18) of page 174 that there exists an essential substitution $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ associated with $[y/x] : V \to V$. It is not difficult to prove that the only possible value for $[y/x](\phi_1)$ is $\forall x (y \in x)$. So because we have chosen to define specialization axioms in terms of essential substitutions, from $\forall x \phi_1 \to \phi_1[x/x]$ and $\forall x \phi_1 \to \phi_1[y/x]$ we obtain:

$$\begin{array}{ll} (i) & \forall x \forall y (x \in y) \to \forall y (x \in y) \\ (ii) & \forall x \forall y (x \in y) \to \forall x (y \in x) \end{array}$$

as the two possible specialization axioms associated with $\phi = \forall x \phi_1$. However, suppose we had opted for (3.2) to define specialization axioms. Then the formula $\forall x \phi_1 \to \phi_1[y/x]$ would need to be excluded as an axiom because $[y/x]$ is clearly not a valid substitution for $\phi_1 = \forall y (x \in y)$. So the formula (ii) above would seemingly not be an axiom for us. Does it matter? Well in general no: for in general we have a spare variable z to work with. So suppose $\{x, y, z\} \subseteq V$ with x, y, z distinct. Then from $\forall x \forall y (x \in y)$ we can prove $(z \in x)$ by successive specialization. By successive generalization we obtain $\forall z \forall x (z \in x)$ and finally by specializing once more we conclude that $\forall x (y \in x)$. It follows that the formula (ii) above would fail to be an axiom, but it would still be a theorem of our deductive system, keeping the resulting notion of provability unchanged. However, in the case when $V = \{x, y\}$ we have a problem. There doesn't seem to be a way to turn the formula (ii) into a theorem. Does it matter? Yes it does. It is clear that $\forall x \forall y (x \in y) \to \forall x (y \in x)$ is going to be true in any model, under any variables assignment. Unless it is also a theorem, Gödel's completeness theorem will fail, which we do not want in a successful axiomatization of first

order logic. We are now in a position to state our chosen definition:

Definition 63 *Let V be a set. We call* specialization axiom *on $\mathbf{P}(V)$ any formula $\phi \in \mathbf{P}(V)$ for which there exist $\phi_1 \in \mathbf{P}(V)$ and $x, y \in V$ such that:*

$$\phi = \forall x \phi_1 \rightarrow \phi_1[y/x]$$

where $[y/x] : \mathbf{P}(V) \rightarrow \mathbf{P}(V)$ is an essential substitution of y in place of x. The set of specialization axioms on $\mathbf{P}(V)$ is denoted $\mathbf{A}_5(V)$.

We know from proposition (114) that an essential substitution $\sigma : \mathbf{P}(V) \rightarrow \mathbf{P}(V)$ can be redefined arbitrarily without changing its associated map $\sigma : V \rightarrow V$, as long as such re-definition preserves classes modulo the substitution congruence. It follows that if $[y/x] : \mathbf{P}(V) \rightarrow \mathbf{P}(V)$ is an essential substitution of y in place of x, it remains an essential substitution of y in place of x after re-definition modulo substitution. It follows that any formula $\forall x \phi_1 \rightarrow \phi_1^*$ is a specialization axiom, as long as $\phi_1^* \sim \phi_1[y/x]$, where $\sim$ denotes the substitution congruence:

Proposition 157 *Let V be a set. Let $\phi_1 \in \mathbf{P}(V)$ and $x, y \in V$. Let $\phi_1^* \in \mathbf{P}(V)$ such that $\phi_1^* \sim \phi_1[y/x]$ where $[y/x] : \mathbf{P}(V) \rightarrow \mathbf{P}(V)$ is an essential substitution of y in place of x. Then the formula $\phi = \forall x \phi_1 \rightarrow \phi_1^*$ is a specialization axiom.*

Proof
Suppose $\phi_1^* \sim \phi_1[y/x]$ where $[y/x] : \mathbf{P}(V) \rightarrow \mathbf{P}(V)$ is an essential substitution associated with the map $[y/x] : V \rightarrow V$. Define $\sigma : \mathbf{P}(V) \rightarrow \mathbf{P}(V)$ by setting $\sigma(\psi) = [y/x](\psi)$ if $\psi \neq \phi_1$ and $\sigma(\phi_1) = \phi_1^*$. Having assumed that $\phi_1^* \sim \phi_1[y/x]$ we see that $\sigma(\psi) \sim [y/x](\psi)$ for all $\psi \in \mathbf{P}(V)$. It follows from proposition (114) that σ is also an essential substitution associated with $[y/x] : V \rightarrow V$. In other words, σ is also an essential substitution of y in place of x. Using definition (62) it follows that $\phi = \forall x \phi_1 \rightarrow \sigma(\phi_1)$ is a specialization axiom. From $\sigma(\phi_1) = \phi_1^*$ we conclude that $\phi = \forall x \phi_1 \rightarrow \phi_1^*$ is a specialization axiom as requested. **.**

Definition 64 *Let V be a set. We call* axiom of first order logic *on $\mathbf{P}(V)$ any formula $\phi \in \mathbf{P}(V)$ which belongs to the set $\mathbf{A}(V)$ defined by:*

$$\mathbf{A}(V) = \mathbf{A}_1(V) \cup \mathbf{A}_2(V) \cup \mathbf{A}_3(V) \cup \mathbf{A}_4(V) \cup \mathbf{A}_5(V)$$

3.1.3 Proofs as Free Universal Algebra

Most textbook references we know about define proofs as finite sequences of formulas, and inference rules as ordered pairs (Φ, ϕ) where Φ is a finite sequence of formulas and ϕ is a formula. A good illustration of this is Definition 1.6 of page 12 in [18]. As far as we can tell, this approach does not work. Having proofs as finite sequences of formulas means that in order to establish any result, the only tool available to us is induction on the length of the proof. This makes it excruciatingly painful and messy to prove anything and is far inferior to the seamless flow of a proof by structural induction. Furthermore, denying the structure of a free algebra to the set of proofs means we cannot use structural recursion to

define anything. There are many interesting functionals which could be defined on the set of proofs. It is a shame to give that up. Granted, finite sequences of formulas are easily understood. Everyone likes them for this reason. Not everyone is familiar with the machinery of universal algebras which require some effort to acquire. But it is well worth it. Now when it comes to rules of inference, the structure (Φ, ϕ) is also inadequate. Indeed, it does not allow *generalization* to be expressed in a sensible way. In Definition 2.10 of page 22 in [18], the *generalization* is introduced as $((\phi_1), \forall x \phi_1)$. In other words, if the formula ϕ_1 has been proved, so has the formula $\forall x \phi_1$. Surely this cannot be right. And yet this is the accepted approach by many authors such as Marc Hoyois [30], J. Donald Monk [44] and George Tourlakis [62]. Our favorite web site [45] also has it, as can be seen on `http://us.metamath.org/mpegif/ax-gen.html`. Even if we are willing to disregard the uncomfortable paradox of claiming $\forall x \phi_1$ is proved whenever ϕ_1 is, we know this approach is failing because the deduction theorem is no longer true for non-closed formulas. Granted there are other logical systems we are told, where the deduction theorem does not work. Logicians are free to do what they want. In this document we care about classical first order logic, meta-mathematics, the language of **ZF** and we are looking for mathematical objects which offer a natural formalization of standard mathematical arguments. It is clear the deduction theorem has to hold. Suppose we need to prove a statement of the form $\forall x(p(x) \to q(x))$. A standard mathematician will proceed as follows: let x be arbitrary. Suppose $p(x)$ holds... Then a long proof follows... So we see that $q(x)$ is true. Hence we conclude that $p(x) \to q(x)$ and since x was arbitrary we obtain $\forall x(p(x) \to q(x))$. This is a standard mathematical argument, the essence of which is to construct a proof of $q(x)$ from the single hypothesis $p(x)$. So a standard mathematician will devote most of his energy establishing the sequent $\{p(x)\} \vdash q(x)$. He will then implicity use the deduction theorem to claim that $\vdash (p(x) \to q(x))$ and conclude $\vdash \forall x(p(x) \to q(x))$ from generalization, having rightly argued that x is arbitrary. So strictly speaking, a standard mathematician does not write a complete proof $\forall x(p(x) \to q(x))$. Instead, he resorts to some form of sequent calculus to argue that his conclusion must be true if the sequent $\{p(x)\} \vdash q(x)$ is itself true. This whole reasoning is what he regards as a valid proof. Now we are free to formalize the notion of proof in anyway we want. We are personally convinced that every theorem of Metamath [45] is correct. We are sure Don Monk is right. However, as far as we are concerned, it is unthinkable to design a concept of proof for which the arguments of the standard mathematician fail to be legitimate. We must be able to infer the sequent $\vdash (p(x) \to q(x))$ from $\{p(x)\} \vdash q(x)$. The deduction theorem should be true, regardless of whether a formula is closed or not.

In the light of these discussions, it should be clear by now that we wish to construct our set of proofs as a free universal algebra X of some type α generated by a set of formula $X_0 \subseteq \mathbf{P}(V)$. On this algebra should be defined two key semantics $\mathrm{Val} : X \to \mathbf{P}(V)$ and $\mathrm{Hyp} : X \to \mathcal{P}(\mathbf{P}(V))$ so that given a proof $\pi \in X$, the valuation $\mathrm{Val}(\pi)$ would represent the conclusion being proved by π, while $\mathrm{Hyp}(\pi)$ would be the set of hypothesis. With this in mind, we could

then define a consequence relation $\vdash \subseteq \mathcal{P}(\mathbf{P}(V)) \times \mathbf{P}(V)$ as follows:

$$\Gamma \vdash \phi \;\Leftrightarrow\; (\mathrm{Val}(\pi) = \phi) \wedge (\mathrm{Hyp}(\pi) \subseteq \Gamma) \text{ for some } \pi \in X$$

This is the outline of the plan. We now need to provide the specifics. Our first task is to determine the exact type α of the universal algebra X. In the case of classical first order logic it would seem natural to have a binary operator $\oplus$ for the rule of inference known as *modus ponens*, and a unary operator ∇x for the *generalization* with respect to the variable $x \in V$. This would work as follows: if π_1 was a proof of ϕ_1 and π_2 was a proof of $\phi_1 \to \phi_2$, then $\pi_1 \oplus \pi_2$ would be a proof of ϕ_2. This can be enforced by making sure the valuation $\mathrm{Val} : X \to \mathbf{P}(V)$ satisfies $\mathrm{Val}(\pi_1 \oplus \pi_2) = \phi_2$. Of course we need operators to be defined everywhere, so the proof $\pi_1 \oplus \pi_2$ has to be meaningful even in the case when the conclusion $\mathrm{Val}(\pi_2)$ cannot be expressed in the form of $\mathrm{Val}(\pi_1) \to \phi_2$ for some formula ϕ_2. But what is the conclusion of a proof $\pi_1 \oplus \pi_2$ which stems from a flawed application of the modus ponens rule of inference? We clearly haven't proved anything. So the conclusion of $\pi_1 \oplus \pi_2$ should be the weakest mathematical result of all. In other words, we should simply make sure the valuation $\mathrm{Val} : X \to \mathbf{P}(V)$ satisfies $\mathrm{Val}(\pi_1 \oplus \pi_2) = \bot \to \bot$. In the case of generalization, if π_1 was a proof of ϕ_1, then $\nabla x \pi_1$ would be a proof of $\forall x \phi_1$, provided the variable x is truly *arbitrary*. This last condition can be formalized by saying that x is not a free variable of any formula belonging to $\mathrm{Hyp}(\pi_1)$. We shall write this as $x \notin \mathrm{Sp}(\pi_1)$. So whenever this condition holds, we simply need to make sure the valuation $\mathrm{Val} : X \to \mathbf{P}(V)$ satisfies $\mathrm{Val}(\nabla x \pi_1) = \forall x \mathrm{Val}(\pi_1)$. In the case when $x \in \mathrm{Sp}(\pi_1)$, then $\nabla x \pi_1$ constitutes a flawed application of the generalization rule of inference, and we should simply set $\mathrm{Val}(\nabla x \pi_1) = \bot \to \bot$.

So we have decided to include a binary operator $\oplus$ and a unary operator ∇x for all $x \in V$, in defining the type α of our free universal algebra of proofs. But what about axioms? If $\phi \in \mathbf{A}(V)$ is an axiom of first order logic and $\pi \in X$ is a proof which relies on the axiom ϕ, how should this axiom be accounted for? One solution is not to treat axioms in any special way and regard ϕ simply as yet another hypothesis of the proof π. In that case we have $\phi \in \mathrm{Hyp}(\pi)$. However, this is not a good solution: for suppose we wish to design a proof of the formula $\forall x((x \in x) \to (x \in x))$. Conceivably, the only solution is to design a proof $\pi = \nabla x \pi_1$ as the generalization in x of another proof π_1 whose conclusion is $\mathrm{Val}(\pi_1) = (x \in x) \to (x \in x)$. We shall soon see that finding a proof π_1 is not difficult. However such a proof relies on axioms which have x as a free variable. Consequently, if we were to include axioms as part of the set of hypothesis $\mathrm{Hyp}(\pi_1)$ the condition $x \notin \mathrm{Sp}(\pi_1)$ would not hold and $\pi = \nabla x \pi_1$ would constitute a case of flawed generalization, whose conclusion is $\mathrm{Val}(\pi) = \bot \to \bot$, and not what we set out to prove. Of course it would be possible to have a set of axioms which have no free variables, by considering universal closures. However, this is not the solution we adopted. We chose a set of axioms which may potentially have free variables, and it is important that we exclude those axioms from the set of hypothesis of a given proof. Hence, for every axiom $\phi \in \mathbf{A}(V)$ we shall define a constant operator $\partial\phi : X^0 \to X$, so that $\pi = \partial\phi(0)$ is simply a proof with conclusion $\mathrm{Val}(\pi) = \phi$ and the crucial

property $\text{Hyp}(\pi) = \emptyset$. In fact, we shall introduce a unary operator $\partial\phi : X^0 \to X$ for every formula $\phi \in \mathbf{P}(V)$ and not simply for $\phi \in \mathbf{A}(V)$. If $\pi = \partial\phi(0)$ is a proof where ϕ is not a legitimate axiom, we shall simply regard the proof π as a case of *flawed invocation of axiom* and set $\text{Val}(\pi) = \bot \to \bot$.

The choice of creating an operator $\partial\phi : X^0 \to X$ even in the case when ϕ is not a legitimate axiom may seem odd at first glance. What is the point of doing this? This choice will effectively increase our free universal algebra of proofs by allowing *flawed* and seemingly pointless proofs of the form $\partial\phi$ where ϕ is not an axiom. Why? Well, firstly we should realize that this isn't the end of the world. We have already accepted the idea of having many proofs of the form $\pi_1 \oplus \pi_2$ or $\nabla x \pi_1$ which are flawed in some sense, as they are illegitimate use of inference rules and whose conclusion is $\bot \to \bot$. Allowing the possibility of wrongly invoking an axiom makes little difference to the existing status. More importantly, this flexibility brings considerable advantages as we shall discover in later part of this document. One advantage is to seamlessly define the notion of variable substitution in proofs. Given a map $\sigma : V \to W$ we shall define a corresponding substitution for proofs as per definition (74). Allowing $\partial\phi$ to be meaningful regardless of whether ϕ is a legitimate axiom allows us to set $\sigma(\partial\phi) = \partial\sigma(\phi)$ without having to worry whether or not the formula $\sigma(\phi)$ is indeed an axiom. This makes a lot of the formalism smoother and more elegant. Another advantage is the ability to study other deductive systems based on an alternative set of axioms without having to consider a different algebra of proofs. We can keep the same free universal algebra of proofs and simply change the semantics $\text{Val} : X \to \mathbf{P}(V)$ giving rise to an alternative notion of provability.

Definition 65 *Let V be a set. We call* Hilbert Deductive Proof Type *associated with V, the type of universal algebra α defined by:*

$$\alpha = \{\partial\phi \ : \ \phi \in \mathbf{P}(V)\} \cup \{\oplus\} \cup \{\nabla x \ : \ x \in V\}$$

where $\partial\phi = ((0,\phi),0)$, $\phi \in \mathbf{P}(V)$, $\oplus = ((1,0),2)$ and $\nabla x = ((2,x),1)$, $x \in V$.

The specifics of how $\partial\phi$, $\oplus$ and ∇x are defined are obviously not important. The coding is done in such a way that the Hilbert deductive proof type α is indeed a set of ordered pairs which is functional and with range in $\mathbf{N}$. So the set α is a map with range in $\mathbf{N}$, and is therefore a type of universal algebra as per definition (1). We have also set up the coding to ensure each operator has the expected arity, namely $\alpha(\partial\phi) = 0$, $\alpha(\oplus) = 2$ and $\alpha(\nabla x) = 1$. We are now ready to define our free universal algebra of proofs X of type α. We shall adopt the generator $X_0 = \mathbf{P}(V)$ and denote this algebra $\mathbf{\Pi}(V)$:

Definition 66 *Let V be a set with associated Hilbert deductive proof type α. We call* Free Universal Algebra of Proofs *associated with V, the free universal algebra $\mathbf{\Pi}(V)$ of type α with free generator $\mathbf{P}(V)$.*

Recall that the existence of $\mathbf{\Pi}(V)$ is guaranteed by theorem (1) of page 20. It follows that we have $\mathbf{P}(V) \subseteq \mathbf{\Pi}(V)$: any formula $\phi \in \mathbf{P}(V)$ is also a proof. It is

simply the proof which has itself as a premise, and itself as a conclusion. In other words, we shall have $\text{Hyp}(\phi) = \{\phi\}$ and $\text{Val}(\phi) = \phi$. Note that if $\phi \in \mathbf{P}(V)$ then both ϕ and $\partial\phi$ are proofs, where we casually use the notation '$\partial\phi$' as a shortcut for $\partial\phi(0)$. These proofs have the same conclusion ϕ, provided the formula ϕ is an axiom. The difference between them is that an axiom has no premise, namely $\text{Hyp}(\partial\phi) = \emptyset$. One other important point needs to be made: both $\mathbf{P}(V)$ and $\mathbf{\Pi}(V)$ are free universal algebras for which is defined a natural notion of *sub-formula* and *sub-proof* as per definition (19). So given $\phi, \psi \in \mathbf{P}(V)$ and $\pi, \rho \in \mathbf{\Pi}(V)$ it is meaningful to write $\phi \preceq \psi$ and $\pi \preceq \rho$ expressing the idea that ψ is a sub-formula of ϕ and π is a sub-proof of ρ. However, since $\mathbf{P}(V) \subseteq \mathbf{\Pi}(V)$ the statement $\phi \preceq \psi$ is ambiguous. It is not clear whether we are referring to the sub-formula partial order on $\mathbf{P}(V)$ or $\mathbf{\Pi}(V)$. The distinction is crucial: the only sub-proof of ϕ is ϕ itself, while ϕ may have many sub-formulas. So we have a problem for which a solution is to use two different symbols, one referring to sub-formulas and one referring to sub-proofs. In these notes, we have decided to keep the same symbol $\preceq$ for both notions, hoping the context will always make clear which of the two notions is being considered. In general, we shall want to avoid this sort of situation. Whenever extending one notion from formulas to proofs, we shall always make sure the meaning remains the same regardless of whether ϕ is viewed as an element of $\mathbf{P}(V)$ or $\mathbf{\Pi}(V)$. For example, the variables $\text{Var}(\pi)$, free variables $\text{Fr}(\pi)$ and bound variables $\text{Bnd}(\pi)$ of a proof π will be defined with this in mind. The same will apply to the notions of valid substitution, the image $\sigma(\pi)$ of a proof π and its minimal transform $\mathcal{M}(\pi)$. So the sub-formula partial order $\preceq$ is an exception, where a confusion is possible. Recall that another example of possibly confusing notation exists in this note namely '$\forall 0$' which may refer to the standard quantification $\forall x$ with $x = 0$, or to the iterated quantification as per definition (49). Before we formally define the set of hypothesis $\text{Hyp}(\pi)$ for a given proof $\pi \in \mathbf{\Pi}(V)$, we would like to stress:

Proposition 158 *Let V be a set and $\phi, \psi \in \mathbf{P}(V)$. Then we have:*

$$\partial\phi = \partial\psi \;\Rightarrow\; \phi = \psi$$

Proof
We are now familiar with the free universal algebra of first order logic $\mathbf{P}(V)$ and a common abuse of notation regarding the symbol '$\bot$'. This symbol is inherently ambiguous as it may refer to three different things: firstly, it refers to an operator symbol namely an element $\bot \in \alpha(V)$ of the first order logic type of definition (22). Secondly, it refers to the actual operator $\bot : \{0\} \to \mathbf{P}(V)$ of $\mathbf{P}(V)$ with arity $\alpha(\bot) = 0$. Thirdly, it refers to the actual formula $\bot(0)$ which we commonly denote '$\bot$' in order to keep our notations lighter. Given a formula $\phi \in \mathbf{P}(V)$, the same thing can be said of the notation '$\partial\phi$' which is equally ambiguous: it refers to the operator symbol of definition (64) or the actual operator $\partial\phi : \{0\} \to \mathbf{\Pi}(V)$ or the proof $\partial\phi(0)$ which we casually denote '$\partial\phi$'. So when it comes to proposition (158) which we are now attempting to prove, there is potentially a problem. Luckily the statement of this proposition is true regardless of how we wish to interpret the notations '$\partial\phi$' and '$\partial\psi$'. If

the two symbols are equal, then the two operators are equal and consequently the two proofs are equal. So it is sufficient to prove the following implication:

$$\partial\phi(0) = \partial\psi(0) \;\Rightarrow\; \phi = \psi$$

which is our initial statement where the abuse of notation has been removed. So suppose $\partial\phi(0) = \partial\psi(0)$. Using theorem (3) of page 31 we obtain the equality between symbols $\partial\phi = \partial\psi$. However, from definition (64) we have $\partial\phi = ((0,\phi),0)$ and $\partial\psi = ((0,\psi),0)$. So we conclude that $\phi = \psi$ as requested. **.**

Definition 67 *Let V be a set. The map* $\mathrm{Hyp} : \mathbf{\Pi}(V) \to \mathcal{P}(\mathbf{P}(V))$ *defined by the following structural recursion is called the* hypothesis mapping *on* $\mathbf{\Pi}(V)$*:*

$$\forall \pi \in \mathbf{\Pi}(V)\ ,\ \mathrm{Hyp}(\pi) = \begin{cases} \{\phi\} & \text{if} \quad \pi = \phi \in \mathbf{P}(V) \\ \emptyset & \text{if} \quad \pi = \partial\phi \\ \mathrm{Hyp}(\pi_1) \cup \mathrm{Hyp}(\pi_2) & \text{if} \quad \pi = \pi_1 \oplus \pi_2 \\ \mathrm{Hyp}(\pi_1) & \text{if} \quad \pi = \nabla x \pi_1 \end{cases} \tag{3.3}$$

We say that ϕ is a hypothesis *of the proof $\pi \in \mathbf{\Pi}(V)$ if and only if $\phi \in \mathrm{Hyp}(\pi)$.*

Note that given a proof $\pi \in \mathbf{\Pi}(V)$, if we regard π as some formal expression involving variables of $\mathbf{P}(V)$, then the set of hypothesis $\mathrm{Hyp}(\pi)$ is simply the set of variables occurring in π. We should also note that the recursive definition (3.3) is easily seen to be legitimate and furthermore that $\mathrm{Hyp}(\pi)$ is a finite set, as a straightforward structural induction will show. Our next step is to define the valuation mapping $\mathrm{Val} : \mathbf{\Pi}(V) \to \mathbf{P}(V)$ which returns the conclusion $\mathrm{Val}(\pi)$ of a proof $\pi \in \mathbf{\Pi}(V)$. Before we can do so we need to define the set $\mathrm{Sp}(\pi)$ representing the free variables occurring in the premises of the proof π. This set is important to formally decide whether a proof of the form $\nabla x \pi_1$ constitutes a legitimate application of the *generalization* rule of inference. Obviously, having proved the formula $\mathrm{Val}(\pi_1)$ using a proof π_1, we cannot claim to have proved $\forall x \mathrm{Val}(\pi_1)$ unless the variable x was truly arbitrary, that is $x \notin \mathrm{Sp}(\pi_1)$.

Definition 68 *Let V be a set. Given $\Gamma \subseteq \mathbf{P}(V)$, we say that $x \in V$ is a* free variable of Γ*, if and only if it belongs to the set* $\mathrm{Fr}(\Gamma)$ *defined by:*

$$\mathrm{Fr}(\Gamma) = \cup\{\, \mathrm{Fr}(\phi) \;:\; \phi \in \Gamma \,\}$$

Given $\pi \in \mathbf{\Pi}(V)$, we say that $x \in V$ is a specific variable of the proof π*, if and only if it belongs to the set* $\mathrm{Sp}(\pi)$ *defined by the equality:*

$$\mathrm{Sp}(\pi) = \mathrm{Fr}(\mathrm{Hyp}(\pi)) = \cup\{\, \mathrm{Fr}(\phi) \;:\; \phi \in \mathrm{Hyp}(\pi) \,\}$$

We also need to formally decide whether a proof of the form $\pi_1 \oplus \pi_2$ constitutes a legitimate application of the rule of inference known as *modus ponens*. This is the case when the conclusion $\mathrm{Val}(\pi_2)$ of the proof π_2 can be expressed as $\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \to \phi$ for some formula $\phi \in \mathbf{P}(V)$. When this is the case, the proof $\pi_1 \oplus \pi_2$ is a proof of ϕ. Otherwise, it simply becomes a proof of $\bot \to \bot$ which is a very weak result. This motivates the following:

Definition 69 *Let V be a set. We call* modus ponens mapping *on* $\mathbf{P}(V)$ *the map* $M : \mathbf{P}(V)^2 \to \mathbf{P}(V)$ *defined by:*

$$\forall \phi_1, \phi_2 \in \mathbf{P}(V) \ , \ M(\phi_1, \phi_2) = \begin{cases} \phi & \text{if} \quad \phi_2 = \phi_1 \to \phi \\ \bot \to \bot & \text{otherwise} \end{cases}$$

Note that the modus ponens mapping $M : \mathbf{P}(V)^2 \to \mathbf{P}(V)$ is well-defined by virtue of theorem (2) of page 21 which guarantees the uniqueness of any $\phi \in \mathbf{P}(V)$ such that $\phi_2 = \phi_1 \to \phi$, assuming such ϕ does exist.

Definition 70 *Let V be a set. We call* valuation mapping *on* $\mathbf{\Pi}(V)$ *the map* $\mathrm{Val} : \mathbf{\Pi}(V) \to \mathbf{P}(V)$ *defined by the following structural recursion:*

$$\forall \pi \in \mathbf{\Pi}(V) \ , \ \mathrm{Val}(\pi) = \begin{cases} \phi & \text{if} \quad \pi = \phi \in \mathbf{P}(V) \\ \phi & \text{if} \quad \pi = \partial\phi, \ \phi \in \mathbf{A}(V) \\ \bot \to \bot & \text{if} \quad \pi = \partial\phi, \ \phi \notin \mathbf{A}(V) \\ M(\mathrm{Val}(\pi_1), \mathrm{Val}(\pi_2)) & \text{if} \quad \pi = \pi_1 \oplus \pi_2 \\ \forall x \mathrm{Val}(\pi_1) & \text{if} \quad \pi = \nabla x \pi_1, \ x \notin \mathrm{Sp}(\pi_1) \\ \bot \to \bot & \text{if} \quad \pi = \nabla x \pi_1, \ x \in \mathrm{Sp}(\pi_1) \end{cases}$$

where $M : \mathbf{P}(V)^2 \to \mathbf{P}(V)$ refers to the modus ponens mapping on $\mathbf{P}(V)$.

Proposition 159 *The structural recursion of* definition (69) *is legitimate.*

Proof
We need to prove the existence and uniqueness of the map $\mathrm{Val} : \mathbf{\Pi}(V) \to \mathbf{P}(V)$. We have to be slightly more careful than usual, as we cannot apply theorem (4) of page 42 in this case. The reason for this is that we do not wish $\mathrm{Val}(\nabla x \pi_1)$ to be simply a function of $\mathrm{Val}(\pi_1)$. Indeed, the conclusion of the proof $\nabla x \pi_1$ depends on whether $x \in \mathrm{Sp}(\pi_1)$ or not. So we want $\mathrm{Val}(\nabla x \pi_1)$ to be a function of both $\mathrm{Val}(\pi_1)$ and π_1. So the main point is to define the mapping $h(\nabla x) : \mathbf{P}(V) \times \mathbf{\Pi}(V) \to \mathbf{P}(V)$ by $h(\nabla x)(\phi_1, \pi_1) = \forall x \phi_1$ if $x \notin \mathrm{Sp}(\pi_1)$ and $h(\nabla x)(\phi_1, \pi_1) = \bot \to \bot$ otherwise. We can then apply theorem (5) of page 44. Note that the mapping $h(\partial\phi) : \mathbf{P}(V)^0 \times \mathbf{\Pi}(V)^0 \to \mathbf{P}(V)$ should be defined differently, depending on whether ϕ is an axiom of first order logic or not. If $\phi \in \mathbf{A}(V)$ we set $h(\partial\phi)(0,0) = \phi$ and otherwise $h(\partial\phi)(0,0) = \bot \to \bot$.
.

3.1.4 Provability and Sequent Calculus

Having constructed the free universal algebra of proofs $\mathbf{\Pi}(V)$, we are now ready to define the notion of provability and syntactic entailment. We shall introduce a binary *consequence* relation $\vdash \subseteq \mathcal{P}(\mathbf{P}(V)) \times \mathbf{P}(V)$ as follows:

Definition 71 *Let V be a set. Let $\Gamma \subseteq \mathbf{P}(V)$ and $\phi \in \mathbf{P}(V)$. We say that $\pi \in \mathbf{\Pi}(V)$ is a* proof of the formula ϕ from Γ *if and only if we have:*

$$\mathrm{Val}(\pi) = \phi \text{ and } \mathrm{Hyp}(\pi) \subseteq \Gamma$$

Furthermore, we say that ϕ is provable from Γ *or that* Γ entails ϕ*, and we write:*

$$\Gamma \vdash \phi$$

if and only if there exists a proof $\pi \in \mathbf{\Pi}(V)$ of the formula ϕ from Γ. We say that ϕ is provable *and we write $\vdash \phi$ if and only if it is provable from $\Gamma = \emptyset$.*

The relation $\vdash$ satisfies a few properties which are highlighted in [50]: the *identity property* is satisfied as we clearly have $\{\phi\} \vdash \phi$ for all $\phi \in \mathbf{P}(V)$. Indeed, the proof $\pi = \phi$ is a proof of ϕ from the set $\{\phi\}$. The *monotonicity* property is also satisfied as we have the implication $(\Gamma \supseteq \Delta) \wedge (\Delta \vdash \phi) \Rightarrow \Gamma \vdash \phi$. Indeed, if $\pi \in \mathbf{\Pi}(V)$ is a proof with $\mathrm{Val}(\pi) = \phi$ and $\mathrm{Hyp}(\pi) \subseteq \Delta$ then in particular we have $\mathrm{Hyp}(\pi) \subseteq \Gamma$ and consequently π is also a proof of ϕ from Γ. Another property satisfied by $\vdash$ is the *finitary* property: if $\Gamma \vdash \phi$ then there exists a finite subset $\Gamma_0 \subseteq \Gamma$ such that $\Gamma_0 \vdash \phi$. Indeed, if π is a proof of ϕ from Γ, then it is also a proof of ϕ from $\Gamma_0 = \mathrm{Hyp}(\pi) \subseteq \Gamma$. Other properties such as *transitivity* and *structurality* are considered in Umberto Rivieccio [50]. We shall prove *transitivity* after we have established the deduction theorem (21) of page 226. The property of *structurality* is slightly more delicate in the case of first order logic with terms. We would like to be able to claim that $\sigma(\Gamma) \vdash \sigma(\phi)$ whenever we have $\Gamma \vdash \phi$ and $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$ is a map of a certain type. The existing literature on abstract algebraic logic e.g. W.J. Blok and D. Pigozzi [6] and the already mentioned [50] seem to consider logical systems without terms, where the algebra of formulas is similar to that of propositional logic. In our case, things are slightly more complicated as it is not immediately obvious which type of $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$ should be used to define the *structurality* property. However, with a little bit of thought, it seems that a pretty good candidate is to consider the class of essential substitutions $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$ as per definition (44). In fact, we hope to be able to prove a *substitution theorem*: $\Gamma \vdash \phi \Rightarrow \sigma(\Gamma) \vdash \sigma(\phi)$ in the more general case when $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is an essential substitution and W is a set of variables, which may not be equal to V. Such theorem is already stated in [4] as Theorem 4.3 page 33 using the notion of *semi-homomorphism*. For now, we shall complete this section by proving other properties of the consequence relation $\vdash$. The idea behind this is to develop a naive and heuristic form of sequent calculus allowing us to prove a sequent $\Gamma \vdash \phi$ as easily as possible. The claim that '$\Gamma \vdash \phi$' (i.e. 'Γ *entails* ϕ') is that there exists a proof π of ϕ from Γ. It is usually a painful exercise to exhibit an element $\pi \in \mathbf{\Pi}(V)$ such that $\mathrm{Val}(\pi) = \phi$ and $\mathrm{Hyp}(\pi) \subseteq \Gamma$. It is a lot easier to prove the existence of such a π without actually saying what it is. The following propositions will allow us to do that. Of course, this will not be very helpful if we are interested in proof searching algorithms at a later stage. However, it would be wrong to think that *proof searching* requires that we *find* a proof $\pi \in \mathbf{\Pi}(V)$. Another approach consists in attempting to formally prove or falsify the sequent $\Gamma \vdash \phi$, possibly along the lines of the Gentzen system described in Jean H. Gallier [24] or Gilles Dowek [16], using another algebra of proofs based on another language of sequents. The next proposition establishes that the sequent $\Gamma \vdash \phi$ is always true when ϕ is an axiom of first order logic:

Proposition 160 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. Let $\phi \in \mathbf{A}(V)$ be an axiom of first order logic. Then ϕ is provable from Γ, i.e. we have $\Gamma \vdash \phi$.*

Proof
Given an axiom of first order logic $\phi \in \mathbf{A}(V)$, consider the proof $\pi = \partial\phi$. Then $\mathrm{Val}(\pi) = \phi$ and $\mathrm{Hyp}(\pi) = \emptyset$. In particular, we have $\mathrm{Val}(\pi) = \phi$ and $\mathrm{Hyp}(\pi) \subseteq \Gamma$. It follows that $\pi \in \mathbf{\Pi}(V)$ is a proof of ϕ from Γ, so $\Gamma \vdash \phi$. **.**

One way to look at proposition (160) is to say that to every axiom ϕ of first order logic is associated a group of axioms $\Gamma \vdash \phi$ in the language of sequents. An axiom of the form $\Gamma \vdash \phi$ can be viewed as an inference rule of arity 0, that is a constant operator on a new algebra of proofs by sequents. We are not claiming to be doing anything here, but simply indicating an avenue for future development. In a similar fashion, the modus ponens rule of the algebra $\mathbf{\Pi}(V)$ gives rise to a binary rule of inference in the language of sequents:

Proposition 161 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. For all $\phi, \psi \in \mathbf{P}(V)$ we have:*

$$(\Gamma \vdash \phi) \wedge (\Gamma \vdash (\phi \to \psi)) \;\Rightarrow \Gamma \vdash \psi$$

Proof
Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. Let $\phi, \psi \in \mathbf{P}(V)$ be formulas such that $\Gamma \vdash \phi$ and $\Gamma \vdash (\phi \to \psi)$. From $\Gamma \vdash \phi$ we obtain the existence of a proof $\pi_1 \in \mathbf{\Pi}(V)$ such that $\mathrm{Val}(\pi_1) = \phi$ and $\mathrm{Hyp}(\pi_1) \subseteq \Gamma$. From $\Gamma \vdash (\phi \to \psi)$ we obtain the existence of a proof $\pi_2 \in \mathbf{\Pi}(V)$ such that $\mathrm{Val}(\pi_2) = \phi \to \psi$ and $\mathrm{Hyp}(\pi_2) \subseteq \Gamma$. Define the proof $\pi = \pi_1 \oplus \pi_2$. Then, from definition (69) we have:

$$\begin{aligned}
\mathrm{Val}(\pi) &= \mathrm{Val}(\pi_1 \oplus \pi_2) \\
&= M(\mathrm{Val}(\pi_1), \mathrm{Val}(\pi_2)) \\
&= M(\phi, \phi \to \psi) \\
&= \psi
\end{aligned}$$

where $M : \mathbf{P}(V)^2 \to \mathbf{P}(V)$ is the modus ponens mapping as per definition (68). Furthermore, using definition (66) we obtain:

$$\begin{aligned}
\mathrm{Hyp}(\pi) &= \mathrm{Hyp}(\pi_1 \oplus \pi_2) \\
&= \mathrm{Hyp}(\pi_1) \cup \mathrm{Hyp}(\pi_2) \\
&\subseteq \Gamma
\end{aligned}$$

It follows that $\pi \in \mathbf{\Pi}(V)$ is a proof of ψ from Γ and we have proved that $\Gamma \vdash \psi$.
.

Similarly, the generalization rule of the algebra $\mathbf{\Pi}(V)$ gives rise to a unary rule of inference in the language of sequents.

Proposition 162 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. For all $\phi \in \mathbf{P}(V)$ and $x \in V$:*

$$(\Gamma \vdash \phi) \wedge (x \notin \mathrm{Fr}(\Gamma)) \;\Rightarrow\; \Gamma \vdash \forall x \phi$$

Proof
Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. Let $\phi \in \mathbf{P}(V)$ and $x \in V$ be such that $\Gamma \vdash \phi$ and $x \notin \mathrm{Fr}(\Gamma)$. From $\Gamma \vdash \phi$ we obtain the existence of a proof $\pi_1 \in \mathbf{\Pi}(V)$ such that $\mathrm{Val}(\pi_1) = \phi$ and $\mathrm{Hyp}(\pi_1) \subseteq \Gamma$. From $x \notin \mathrm{Fr}(\Gamma)$ and $\mathrm{Hyp}(\pi_1) \subseteq \Gamma$ it follows in particular that $x \notin \mathrm{Sp}(\pi_1)$. Define the proof $\pi = \nabla x \pi_1 \in \mathbf{\Pi}(V)$. Then:

$$\begin{array}{rcl} \mathrm{Val}(\pi) & = & \mathrm{Val}(\nabla x \pi_1) \\ x \notin \mathrm{Sp}(\pi_1) \ \rightarrow & = & \forall x \mathrm{Val}(\pi_1) \\ & = & \forall x \phi \end{array}$$

Furthermore, we have $\mathrm{Hyp}(\pi) = \mathrm{Hyp}(\nabla x \pi_1) = \mathrm{Hyp}(\pi_1) \subseteq \Gamma$. It follows that $\pi \in \mathbf{\Pi}(V)$ is a proof of $\forall x \phi$ from Γ and we conclude that $\Gamma \vdash \forall x \phi$. **.**

Every axiom of first order logic is of the form $\phi = \phi_1 \rightarrow \phi_2$. Hence, given $\Gamma \subseteq \mathbf{P}(V)$ from proposition (160) we have $\Gamma \vdash \phi_1 \rightarrow \phi_2$. It follows that if the sequent $\Gamma \vdash \phi_1$ has been proved, we obtain $\Gamma \vdash \phi_2$ immediately by application of the modus ponens property of proposition (161). So every axiom of first order logic also gives rise to a unary rule of inference in the language of sequents. We shall now make these explicit by considering each of the five possible groups of axioms separately. Of course, these unary rules of inference can be deduced from other existing rules. So we may wish to regard them simply as *theorems* of the form '$\Gamma \vdash \phi_1 \ \Rightarrow \ \Gamma \vdash \phi_2$' in the language of sequents.

Proposition 163 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. For all $\phi_1, \phi_2 \in \mathbf{P}(V)$:*

$$\Gamma \vdash \phi_1 \ \Rightarrow \ \Gamma \vdash (\phi_2 \rightarrow \phi_1)$$

Proof
Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. Let $\phi_1, \phi_2 \in \mathbf{P}(V)$ such that $\Gamma \vdash \phi_1$. From definition (58) the formula $\phi_1 \rightarrow (\phi_2 \rightarrow \phi_1)$ is a simplification axiom and it follows from proposition (160) that $\Gamma \vdash \phi_1 \rightarrow (\phi_2 \rightarrow \phi_1)$. Hence, using $\Gamma \vdash \phi_1$ and the modus ponens property of proposition (161) we conclude that $\Gamma \vdash (\phi_2 \rightarrow \phi_1)$. **.**

Proposition 164 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. For all $\phi_1, \phi_2, \phi_3 \in \mathbf{P}(V)$:*

$$\Gamma \vdash \phi_1 \rightarrow (\phi_2 \rightarrow \phi_3) \ \Rightarrow \ \Gamma \vdash (\phi_1 \rightarrow \phi_2) \rightarrow (\phi_1 \rightarrow \phi_3)$$

Proof
Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. Let $\phi_1, \phi_2, \phi_3 \in \mathbf{P}(V)$ with $\Gamma \vdash \phi_1 \rightarrow (\phi_2 \rightarrow \phi_3)$. From definition (59), $[\phi_1 \rightarrow (\phi_2 \rightarrow \phi_3)] \rightarrow [(\phi_1 \rightarrow \phi_2) \rightarrow (\phi_1 \rightarrow \phi_3)]$ is a Frege axiom and it follows from proposition (160) that:

$$\Gamma \vdash [\phi_1 \rightarrow (\phi_2 \rightarrow \phi_3)] \rightarrow [(\phi_1 \rightarrow \phi_2) \rightarrow (\phi_1 \rightarrow \phi_3)]$$

Hence, using $\Gamma \vdash \phi_1 \rightarrow (\phi_2 \rightarrow \phi_3)$ and the modus ponens property of proposition (161) we conclude that $\Gamma \vdash (\phi_1 \rightarrow \phi_2) \rightarrow (\phi_1 \rightarrow \phi_3)$. **.**

Proposition 165 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. For all $\phi_1 \in \mathbf{P}(V)$ we have:*

$$\Gamma \vdash (\phi_1 \to \bot) \to \bot \;\Rightarrow\; \Gamma \vdash \phi_1$$

Proof
Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. Let $\phi_1 \in \mathbf{P}(V)$ such that $\Gamma \vdash (\phi_1 \to \bot) \to \bot$. From definition (60) the formula $[(\phi_1 \to \bot) \to \bot] \to \phi_1$ is a transposition axiom and it follows from proposition (160) that $\Gamma \vdash [(\phi_1 \to \bot) \to \bot] \to \phi_1$. Hence, using $\Gamma \vdash (\phi_1 \to \bot) \to \bot$ and the modus ponens property of proposition (161) we conclude that $\Gamma \vdash \phi_1$. **.**

Proposition 166 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. For all $\phi_1, \phi_2 \in \mathbf{P}(V)$, $x \in V$:*

$$(x \notin \mathrm{Fr}(\phi_1)) \wedge (\Gamma \vdash \forall x(\phi_1 \to \phi_2)) \;\Rightarrow\; \Gamma \vdash \phi_1 \to \forall x \phi_2$$

Proof
Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. Let $\phi_1, \phi_2 \in \mathbf{P}(V)$ and $x \in V$ such that $x \notin \mathrm{Fr}(\phi_1)$ and $\Gamma \vdash \forall x(\phi_1 \to \phi_2)$. From definition (61) and $x \notin \mathrm{Fr}(\phi_1)$ the formula $\forall x(\phi_1 \to \phi_2) \to (\phi_1 \to \forall x \phi_2)$ is a quantification axiom and it follows from proposition (160) that $\Gamma \vdash \forall x(\phi_1 \to \phi_2) \to (\phi_1 \to \forall x \phi_2)$. Hence, using $\Gamma \vdash \forall x(\phi_1 \to \phi_2)$ and the modus ponens property of proposition (161) we conclude that $\Gamma \vdash \phi_1 \to \forall x \phi_2$. **.**

Proposition 167 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. For all $\phi_1 \in \mathbf{P}(V)$, $x, y \in V$:*

$$\Gamma \vdash \forall x \phi_1 \;\Rightarrow\; \Gamma \vdash \phi_1[y/x]$$

where $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ is an essential substitution of y in place of x.

Proof
Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. Let $\phi_1 \in \mathbf{P}(V)$ and $x, y \in V$ such that $\Gamma \vdash \forall x \phi_1$. Let $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ be an essential substitution associated with $[y/x] : V \to V$ as per definition (42). From definition (62) the formula $\forall x \phi_1 \to \phi_1[y/x]$ is a specialization axiom and it follows from proposition (160) that $\Gamma \vdash \forall x \phi_1 \to \phi_1[y/x]$. Hence, using $\Gamma \vdash \forall x \phi_1$ and the modus ponens property of proposition (161) we conclude that $\Gamma \vdash \phi_1[y/x]$. **.**

The following proposition can also be viewed as an axiom in the language of sequents. We shall need it when proving the deduction theorem.

Proposition 168 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. For all $\phi_1 \in \mathbf{P}(V)$ we have:*

$$\Gamma \vdash (\phi_1 \to \phi_1)$$

Proof
Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. Let $\phi_1 \in \mathbf{P}(V)$. Since $\phi_1 \to (\phi_1 \to \phi_1)$ is a simplification axiom, from proposition (160) we have $\Gamma \vdash \phi_1 \to (\phi_1 \to \phi_1)$. So in order to show $\Gamma \vdash (\phi_1 \to \phi_1)$, by virtue of the modus ponens property of proposition (161) it is sufficient to prove that:

$$\Gamma \vdash [\phi_1 \to (\phi_1 \to \phi_1)] \to (\phi_1 \to \phi_1)$$

From proposition (164) it is therefore sufficient to prove that:

$$\Gamma \vdash \phi_1 \to [(\phi_1 \to \phi_1) \to \phi_1]$$

which follows immediately from the fact that $\phi_1 \to [(\phi_1 \to \phi_1) \to \phi_1]$ is also a simplification axiom. .

3.1.5 The Deduction Theorem

It is now time to deliver on our promise. Our chosen axiomatization of first order logic allows us to state the deduction theorem in its full generality. As already mentioned, a good number of references (e.g. [18], [30], [32], [39], [43], [44], [45], [62]) have chosen axiomatic systems in which the deduction theorem fails in general, and can only be stated for closed formulas. As far as we can tell, the most common source of failure is the acceptance of $(\phi_1, \forall x \phi_1)$ as a rule of inference. This is in contrast with the formalization presented in these notes, where the conclusion $\forall x \phi_1$ is only reached when ϕ_1 is the conclusion of a proof π_1 such that $x \notin \mathrm{Sp}(\pi_1)$, i.e. x is not a *specific variable* of π_1. This is in line with the common mathematical practice of not claiming $\forall x \phi_1$ from ϕ_1 unless the variable x is truly *arbitrary*. The deduction theorem also appears in full generality as Theorem 4.9 page 34 in Donald W. Barnes, John M. Mack [4]. Their proof relies on an induction argument based on the length of the proof underlying the sequent $\Gamma \cup \{\phi\} \vdash \psi$. Having chosen a free algebraic structure for our set $\mathbf{\Pi}(V)$, our own proof of the deduction theorem will benefit from the clarity and power of structural induction. Interestingly, the online course of Prof. Arindama Singh of IIT Madras [55] also offers a proof of the deduction theorem in full generality which implicitly makes use of structural induction, despite having proofs defined as finite sequences of formulas. This can be seen at the end of the lecture 39 available on YouTube via the link `http://nptel.iitm.ac.in/courses/111106052/39`.

Theorem 21 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. For all $\phi, \psi \in \mathbf{P}(V)$ we have:*

$$\Gamma \cup \{\phi\} \vdash \psi \;\Leftrightarrow\; \Gamma \vdash (\phi \to \psi)$$

Proof
We shall first prove the implication $\Leftarrow$: so suppose V is a set and $\Gamma \subseteq \mathbf{P}(V)$ is such that $\Gamma \vdash (\phi \to \psi)$ where $\phi, \psi \in \mathbf{P}(V)$. In particular, we have:

$$\Gamma \cup \{\phi\} \vdash (\phi \to \psi)$$

and it is clear that $\Gamma \cup \{\phi\} \vdash \phi$. From the modus ponens property of proposition (161) it follows that $\Gamma \cup \{\phi\} \vdash \psi$ as requested. We now prove the reverse implication $\Rightarrow$: let Π^* be the set of all proofs $\pi \in \mathbf{\Pi}(V)$ with the property that for all $\Gamma \subseteq \mathbf{P}(V)$ and $\phi, \psi \in \mathbf{P}(V)$ the following implication holds:

$$(\mathrm{Val}(\pi) = \psi) \wedge (\mathrm{Hyp}(\pi) \subseteq \Gamma \cup \{\phi\}) \;\Rightarrow\; \Gamma \vdash (\phi \to \psi)$$

First we shall prove that in order to complete the proof of this theorem it is sufficient to show that $\Pi^* = \mathbf{\Pi}(V)$. So we assume that $\Pi^* = \mathbf{\Pi}(V)$. Let $\Gamma \subseteq \mathbf{P}(V)$ and $\phi, \psi \in \mathbf{P}(V)$ be such that $\Gamma \cup \{\phi\} \vdash \psi$. We need to show that $\Gamma \vdash (\phi \to \psi)$. From the assumption $\Gamma \cup \{\phi\} \vdash \psi$ we obtain the existence of a proof $\pi \in \mathbf{\Pi}(V)$ such that $\mathrm{Val}(\pi) = \psi$ and $\mathrm{Hyp}(\pi) \subseteq \Gamma \cup \{\phi\}$. However, having assumed $\Pi^* = \mathbf{\Pi}(V)$ it follows that π is also an element of Π^*. From $\mathrm{Val}(\pi) = \psi$ and $\mathrm{Hyp}(\pi) \subseteq \Gamma \cup \{\phi\}$ we therefore conclude that $\Gamma \vdash (\phi \to \psi)$ as requested. We shall now complete the proof of this theorem by showing the equality $\Pi^* = \mathbf{\Pi}(V)$ using a structural induction argument as per theorem (3) of page 31. Since $\mathbf{P}(V)$ is a generator of the algebra $\mathbf{\Pi}(V)$ we first check that $\mathbf{P}(V) \subseteq \Pi^*$. So suppose π is a proof of the form $\pi = \phi_1$ for some $\phi_1 \in \mathbf{P}(V)$. We need to show that $\phi_1 \in \Pi^*$. So let $\Gamma \subseteq \mathbf{P}(V)$ and $\phi, \psi \in \mathbf{P}(V)$ be such that $\phi_1 = \mathrm{Val}(\pi) = \psi$ and $\{\phi_1\} = \mathrm{Hyp}(\pi) \subseteq \Gamma \cup \{\phi\}$. We need to show that $\Gamma \vdash (\phi \to \psi)$, that is to say $\Gamma \vdash (\phi \to \phi_1)$. We shall distinguish two cases: first we assume that $\phi_1 \in \Gamma$. In that case, $\mathrm{Hyp}(\pi) \subseteq \Gamma$ and π is in fact a proof of ϕ_1 from Γ. So $\Gamma \vdash \phi_1$ and our desired conclusion $\Gamma \vdash (\phi \to \phi_1)$ follows immediately from the simplification property of proposition (163). We now assume that $\phi_1 \notin \Gamma$. From the inclusion $\{\phi_1\} \subseteq \Gamma \cup \{\phi\}$ it follows that $\phi_1 = \phi$ and we therefore need to show that $\Gamma \vdash (\phi_1 \to \phi_1)$ which follows immediately from proposition (168). This completes our proof of $\mathbf{P}(V) \subseteq \Pi^*$. We shall now proceed with our induction argument by showing that every proof $\pi \in \mathbf{\Pi}(V)$ of the form $\pi = \partial\phi_1$ for some $\phi_1 \in \mathbf{P}(V)$ is an element of Π^*. So suppose $\pi = \partial\phi_1$ and let $\Gamma \subseteq \mathbf{P}(V)$ and $\phi, \psi \in \mathbf{P}(V)$ be such that $\mathrm{Val}(\pi) = \psi$ and $\emptyset = \mathrm{Hyp}(\pi) \subseteq \Gamma \cup \{\phi\}$ (This inclusion of course does not tell us anything). We need to show that $\Gamma \vdash (\phi \to \psi)$. We shall distinguish two cases: first we assume that $\phi_1 \in \mathbf{A}(V)$, i.e. that ϕ_1 is an axiom. Then we have $\phi_1 = \mathrm{Val}(\pi) = \psi$ and we need to show that $\Gamma \vdash (\phi \to \phi_1)$. However, having assumed $\phi_1 \in \mathbf{A}(V)$ is an axiom of first order logic, we have $\Gamma \vdash \phi_1$ and $\Gamma \vdash (\phi \to \phi_1)$ follows immediately from the simplification property of proposition (163). We now assume that $\phi_1 \notin \mathbf{A}(V)$. Then we have $(\bot \to \bot) = \mathrm{Val}(\pi) = \psi$ and we need to show that $\Gamma \vdash (\phi \to (\bot \to \bot))$. However, we know that $\Gamma \vdash (\bot \to \bot)$ is true by virtue of proposition (168) and $\Gamma \vdash (\phi \to (\bot \to \bot))$ therefore follows from the simplification property of proposition (163). We shall now proceed with our induction argument by assuming $\pi \in \mathbf{\Pi}(V)$ is of the form $\pi = \pi_1 \oplus \pi_2$ where both π_1 and π_2 are elements of Π^*. We need to show that π is also an element of Π^*. So let $\Gamma \subseteq \mathbf{P}(V)$ and $\phi, \psi \in \mathbf{P}(V)$ be such that $M(\mathrm{Val}(\pi_1), \mathrm{Val}(\pi_2)) = \mathrm{Val}(\pi) = \psi$ and $\mathrm{Hyp}(\pi_1) \cup \mathrm{Hyp}(\pi_2) = \mathrm{Hyp}(\pi) \subseteq \Gamma \cup \{\phi\}$, where $M : \mathbf{P}(V)^2 \to \mathbf{P}(V)$ is the modus ponens mapping of definition (68). We need to show that $\Gamma \vdash (\phi \to \psi)$. We shall distinguish two cases: first we assume that $\mathrm{Val}(\pi_2)$ is not of the form $\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \to \phi_1$ for any $\phi_1 \in \mathbf{P}(V)$. From definition (68) it follows that $M(\mathrm{Val}(\pi_1), \mathrm{Val}(\pi_2)) = \bot \to \bot$ and consequently $\psi = \bot \to \bot$. So we need to prove that $\Gamma \vdash \phi \to (\bot \to \bot)$ which follows from the simplification property of proposition (163) and the fact that $\Gamma \vdash (\bot \to \bot)$, itself an outcome of proposition (168). We now assume that $\mathrm{Val}(\pi_2)$ is of the form $\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \to \phi_1$ for some $\phi_1 \in \mathbf{P}(V)$. In this case we obtain $M(\mathrm{Val}(\pi_1), \mathrm{Val}(\pi_2)) = \phi_1 = \psi$ so we need to prove that $\Gamma \vdash (\phi \to \phi_1)$. From

the modus ponens property of proposition (161) it is therefore sufficient to show that $\Gamma \vdash (\phi \to \mathrm{Val}(\pi_1))$ and $\Gamma \vdash (\phi \to \mathrm{Val}(\pi_1)) \to (\phi \to \phi_1)$. In fact, from the Frege property of proposition (164), $\Gamma \vdash (\phi \to \mathrm{Val}(\pi_1)) \to (\phi \to \phi_1)$ is itself a consequence of $\Gamma \vdash \phi \to (\mathrm{Val}(\pi_1) \to \phi_1)$ so we can concentrate on proving this last entailment together with $\Gamma \vdash (\phi \to \mathrm{Val}(\pi_1))$. First we show that $\Gamma \vdash (\phi \to \mathrm{Val}(\pi_1))$. Recall our assumption that the proof π_1 is an element of Π^*, and from $\mathrm{Hyp}(\pi_1) \cup \mathrm{Hyp}(\pi_2) \subseteq \Gamma \cup \{\phi\}$ we obtain in particular $\mathrm{Hyp}(\pi_1) \subseteq \Gamma \cup \{\phi\}$. Hence from the equality $\mathrm{Val}(\pi_1) = \mathrm{Val}(\pi_1)$ we conclude immediately that $\Gamma \vdash (\phi \to \mathrm{Val}(\pi_1))$ as requested. We now show that $\Gamma \vdash \phi \to (\mathrm{Val}(\pi_1) \to \phi_1)$. Since $\mathrm{Val}(\pi_1) \to \phi_1 = \mathrm{Val}(\pi_2)$ this is in fact the same as showing $\Gamma \vdash (\phi \to \mathrm{Val}(\pi_2))$ which is also a simple consequence of the assumption $\pi_2 \in \Pi^*$ and $\mathrm{Hyp}(\pi_2) \subseteq \Gamma \cup \{\phi\}$. This completes our proof in the case when $\pi \in \mathbf{\Pi}(V)$ is of the form $\pi = \pi_1 \oplus \pi_2$. We now assume that π is of the form $\pi = \nabla x \pi_1$ where $x \in V$ and π_1 is an element of Π^*. We need to show that π is also an element of Π^*. So let $\Gamma \subseteq \mathbf{P}(V)$ and $\phi, \psi \in \mathbf{P}(V)$ be such that $\mathrm{Val}(\nabla x \pi_1) = \mathrm{Val}(\pi) = \psi$ and $\mathrm{Hyp}(\pi_1) = \mathrm{Hyp}(\pi) \subseteq \Gamma \cup \{\phi\}$. We need to show that $\Gamma \vdash (\phi \to \psi)$. We shall distinguish two cases: first we assume that $x \in \mathrm{Sp}(\pi_1)$. In this case we have $\mathrm{Val}(\nabla x \pi_1) = \bot \to \bot$ and therefore $\psi = \bot \to \bot$. So we need to prove that $\Gamma \vdash \phi \to (\bot \to \bot)$ which we already know is true as we have shown in this proof. We now assume that $x \notin \mathrm{Sp}(\pi_1)$. Once again, we need to show that $\Gamma \vdash (\phi \to \psi)$ and we shall distinguish two further cases: first we assume that $x \in \mathrm{Fr}(\phi)$. From $x \notin \mathrm{Sp}(\pi_1) = \mathrm{Fr}(\mathrm{Hyp}(\pi_1))$ it follows that $\phi \notin \mathrm{Hyp}(\pi_1)$. Hence, from $\mathrm{Hyp}(\pi) = \mathrm{Hyp}(\pi_1) \subseteq \Gamma \cup \{\phi\}$ we obtain $\mathrm{Hyp}(\pi) \subseteq \Gamma$, which together with $\mathrm{Val}(\pi) = \psi$ imply that $\Gamma \vdash \psi$. So $\Gamma \vdash (\phi \to \psi)$ follows immediately from the simplification property of proposition (163). We now assume that $x \notin \mathrm{Fr}(\phi)$. From $x \notin \mathrm{Sp}(\pi_1)$ it follows that $\mathrm{Val}(\nabla x \pi_1) = \forall x \mathrm{Val}(\pi_1)$ and consequently $\psi = \forall x \mathrm{Val}(\pi_1)$. Hence we need to show that $\Gamma \vdash (\phi \to \forall x \mathrm{Val}(\pi_1))$. However, since $x \notin \mathrm{Fr}(\phi)$, from the quantification property of proposition (166), it is sufficient to prove that $\Gamma \vdash \forall x(\phi \to \mathrm{Val}(\pi_1))$. From $\mathrm{Hyp}(\pi_1) \subseteq \Gamma \cup \{\phi\}$, defining $\Gamma^* = \mathrm{Hyp}(\pi_1) \setminus \{\phi\}$ we obtain $\Gamma^* \subseteq \Gamma$. It is therefore sufficient to prove that $\Gamma^* \vdash \forall x(\phi \to \mathrm{Val}(\pi_1))$. From $x \notin \mathrm{Sp}(\pi_1) = \mathrm{Fr}(\mathrm{Hyp}(\pi_1))$ it follows that $x \notin \mathrm{Fr}(\Gamma^*)$. Using the generalization property of proposition (162), it is therefore sufficient to prove that $\Gamma^* \vdash (\phi \to \mathrm{Val}(\pi_1))$. Now recall our assumption that the proof π_1 is an element of Π^*. From $\mathrm{Hyp}(\pi_1) \subseteq \Gamma^* \cup \{\phi\}$ and $\mathrm{Val}(\pi_1) = \mathrm{Val}(\pi_1)$ we obtain immediately $\Gamma^* \vdash (\phi \to \mathrm{Val}(\pi_1))$ as requested. This completes our induction argument. .

3.1.6 Transitivity of Consequence Relation

We are now in a position to provide a proof of the transitivity property of the consequence relation $\vdash$: if $\Gamma \vdash \psi$ for all $\psi \in \Delta$ and $\Delta \vdash \phi$, then we must have $\Gamma \vdash \phi$. In essence, we shall use the deduction theorem (21) to argue that:

$$\vdash (\psi_n \to (\psi_{n-1} \to \ldots (\psi_1 \to \phi)$$

where $\{\psi_1, \ldots, \psi_n\} \subseteq \Delta$ is the set of hypothesis of a proof underlying the sequent $\Delta \vdash \phi$. From $\Gamma \vdash \psi_k$ and a repeated use of modus ponens, we conclude

that $\Gamma \vdash \phi$. Note that if π is a proof of ϕ from Δ, it would be tempting to design a new proof of ϕ from Γ by replacing every assumption ψ_k of the proof π by a proof π_k of ψ_k from Γ. For those who care, this idea does not work: the proof π may contain cases of generalization with respect to a variable x which become invalidated by the presence of x as a free variable in some $\mathrm{Hyp}(\pi_k)$. Despite our best efforts, we have not been able to design a proof along those lines.

Proposition 169 *Let V be a set. Let $\Gamma, \Delta \subseteq \mathbf{P}(V)$ and $\phi \in \mathbf{P}(V)$. Then:*

$$(\Gamma \vdash \psi \text{ for all } \psi \in \Delta) \wedge (\Delta \vdash \phi) \;\Rightarrow\; \Gamma \vdash \phi \tag{3.4}$$

Proof
Without loss of generality we may assume that Δ is a finite set. Indeed, suppose the implication (3.4) has been proved in this case. We shall show that it is then true in general. So suppose $\Gamma \vdash \psi$ for all $\psi \in \Delta$ and $\Delta \vdash \phi$. We need to show that $\Gamma \vdash \phi$. However, there exists Δ_0 finite such that $\Delta_0 \subseteq \Delta$ and $\Delta_0 \vdash \phi$. Hence we have $\Gamma \vdash \psi$ for all $\psi \in \Delta_0$ and $\Delta_0 \vdash \phi$. Having assumed the implication (3.4) is true for Δ finite, it follows that $\Gamma \vdash \phi$ as requested. So we assume without loss of generality that Δ is a finite set. We shall show that (3.4) is true for all $\Gamma \subseteq \mathbf{P}(V)$ and $\phi \in \mathbf{P}(V)$, using an induction argument on the cardinal $|\Delta|$ of the set Δ. First we assume that $|\Delta| = 0$. Let $\Gamma \subseteq \mathbf{P}(V)$ and $\phi \in \mathbf{P}(V)$. From $\Delta = \emptyset$ and $\Delta \vdash \phi$ we obtain $\vdash \phi$ and in particular $\Gamma \vdash \phi$. Hence the implication (3.4) is necessarily true. We now assume that (3.4) is true for all $\Gamma \subseteq \mathbf{P}(V)$ and $\phi \in \mathbf{P}(V)$ whenever $|\Delta| = n$ for some $n \in \mathbf{N}$. We need to show the same is true when $|\Delta| = n+1$. So let $\Gamma \subseteq \mathbf{P}(V)$ and $\phi \in \mathbf{P}(V)$. We assume that $\Gamma \vdash \psi$ for all $\psi \in \Delta$ and $\Delta \vdash \phi$. We need to show that $\Gamma \vdash \phi$. Having assumed $|\Delta| = n + 1$, in particular $\Delta \neq \emptyset$. Let $\psi^* \in \Delta$ and define $\Delta^* = \Delta \setminus \{\psi^*\}$. Then $|\Delta^*| = n$. Furthermore we have $\Delta = \Delta^* \cup \{\psi^*\}$ and consequently $\Delta^* \cup \{\psi^*\} \vdash \phi$. Using the deduction theorem (21) we obtain $\Delta^* \vdash (\psi^* \to \phi)$. However, since $\Delta^* \subseteq \Delta$ we also have $\Gamma \vdash \psi$ for all $\psi \in \Delta^*$. Having assumed the implication (3.4) is true for all $\Gamma \subseteq \mathbf{P}(V)$, $\phi \in \mathbf{P}(V)$ and $|\Delta| = n$, in particular it is true for Γ, $(\psi^* \to \phi)$ and Δ^*. Hence we see that $\Gamma \vdash (\psi^* \to \phi)$ is true. Furthermore, since $\psi^* \in \Delta$ we have $\Gamma \vdash \psi^*$. Using the modus ponens property of proposition (161) we conclude that $\Gamma \vdash \phi$. **.**

There is an interesting corollary to proposition (169) which looks like the *cut rule* for sequent calculus. In case this turns out to be useful we quote:

Proposition 170 *Let V be a set. Let $\Gamma \subseteq \mathbf{P}(V)$ and $\phi, \psi \in \mathbf{P}(V)$. Then:*

$$(\,\Gamma \cup \{\psi\} \vdash \phi\,) \wedge (\,\Gamma \cup \{\psi \to \bot\} \vdash \phi\,) \;\Rightarrow\; \Gamma \vdash \phi$$

Proof
Using the deduction theorem (21) of page 226, by assumption we have the sequents $\Gamma \vdash (\psi \to \phi)$ and $\Gamma \vdash ((\psi \to \bot) \to \phi)$. Defining the set of formulas $\Delta = \{\psi \to \phi, (\psi \to \bot) \to \phi\}$ it follows that $\Gamma \vdash \chi$ for all $\chi \in \Delta$. In order to prove that $\Gamma \vdash \phi$, from the transitivity of proposition (169) it is therefore sufficient to prove that $\Delta \vdash \phi$. Using the transposition property of proposition (165), we

simply need to show that $\Delta \vdash (\phi \to \bot) \to \bot$. From the deduction theorem (21), this amounts to showing that $\Delta^* \vdash \bot$ where $\Delta^* = \Delta \cup \{\phi \to \bot\}$. Let us accept for now that $\Delta^* \vdash (\psi \to \bot)$ and $\Delta^* \vdash (\psi \to \bot) \to \bot$. Then from the modus ponens property of proposition (161) we obtain $\Delta^* \vdash \bot$ as requested. So it remains to show that $\Delta^* \vdash (\psi \to \bot)$ and $\Delta^* \vdash (\psi \to \bot) \to \bot$. First we show the sequent $\Delta^* \vdash (\psi \to \bot)$: from the deduction theorem (21), we need to show that $\Delta^* \cup \{\psi\} \vdash \bot$ which follows from proposition (161) and the fact that $\Delta^* \cup \{\psi\}$ contains the three formulas ψ, $\psi \to \phi$ and $\phi \to \bot$. So we now show the sequent $\Delta^* \vdash (\psi \to \bot) \to \bot$: from the deduction theorem (21), we need to show that $\Delta^* \cup \{\psi \to \bot\} \vdash \bot$ which follows from proposition (161) and the fact that $\Delta^* \cup \{\psi \to \bot\}$ contains the three formulas $\psi \to \bot$, $(\psi \to \bot) \to \phi$ and $\phi \to \bot$. **.**

3.1.7 The Hilbert Deductive Congruence

Having created a sensible consequence relation $\vdash \subseteq \mathcal{P}(\mathbf{P}(V)) \times \mathbf{P}(V)$ we can now formally define the Hilbert deductive congruence on $\mathbf{P}(V)$. Given $\phi, \psi \in \mathbf{P}(V)$, we shall say that ϕ and ψ are equivalent if and only if both formulas $\phi \to \psi$ and $\psi \to \phi$ are provable. So we naturally start with a study of the relation $\leq$ defined by $\phi \leq \psi \Leftrightarrow \vdash (\phi \to \psi)$ which shall be seen to be a preorder:

Definition 72 *Let V be a set. We call* Hilbert deductive preorder *on $\mathbf{P}(V)$ the relation $\leq$ defined by $\phi \leq \psi$ if and only if $\vdash (\phi \to \psi)$, for all $\phi, \psi \in \mathbf{P}(V)$.*

Recall that a preorder is a binary relation which is reflexive and transitive. The proof that $\leq$ is indeed a preorder follows. Note that by virtue the deduction theorem (21) of page 226, the statement $\vdash (\phi \to \psi)$ is equivalent to $\{\phi\} \vdash \psi$.

Proposition 171 *Let V be a set. Then, the Hilbert deductive preorder $\leq$ on $\mathbf{P}(V)$ is a reflexive and transitive relation on $\mathbf{P}(V)$.*

Proof
First we show that $\leq$ is reflexive, namely that $\phi \leq \phi$ for all $\phi \in \mathbf{P}(V)$. We have to show that $\vdash (\phi \to \phi)$, which follows from proposition (168). Next we show that $\leq$ is transitive. So let $\phi, \psi, \chi \in \mathbf{P}(V)$ such that $\phi \leq \psi$ and $\psi \leq \chi$. We need to show that $\phi \leq \chi$, that is $\vdash (\phi \to \chi)$. Using the deduction theorem (21), it is sufficient to prove that $\{\phi\} \vdash \chi$. However, from the assumption $\phi \leq \psi$ we have $\vdash (\phi \to \psi)$ and consequently $\{\phi\} \vdash \psi$. From the assumption $\psi \leq \chi$ we obtain $\vdash (\psi \to \chi)$ and in particular $\{\phi\} \vdash (\psi \to \chi)$. Using the modus ponens property of proposition (161) we conclude that $\{\phi\} \vdash \chi$ as requested. **.**

The Hilbert deductive preorder is not a congruent relation. If $\phi_1 \leq \psi_1$ and $\phi_2 \leq \psi_2$, we cannot argue that $\phi_1 \to \phi_2 \leq \psi_1 \to \psi_2$. Although it would be easy to provide a counterexample, we shall refrain from doing so at this stage, as we are not able to prove anything: we do have some tools allowing us to establish a given sequent $\vdash (\phi \to \psi)$, but we are not yet equipped to refute such a sequent. Proving that a formula is not provable is difficult. We shall need some model theory to do this. For now, we shall focus on the positive result:

Proposition 172 *Let V be a set and $\leq$ be the Hilbert deductive preorder on $\mathbf{P}(V)$. Let ϕ_1, ϕ_2 and $\psi_1, \psi_2 \in \mathbf{P}(V)$ such that $\psi_1 \leq \phi_1$ and $\phi_2 \leq \psi_2$. Then:*

$$\phi_1 \to \phi_2 \leq \psi_1 \to \psi_2$$

Proof
We assume that $\psi_1 \leq \phi_1$ and $\phi_2 \leq \psi_2$, i.e. $\vdash (\psi_1 \to \phi_1)$ and $\vdash (\phi_2 \to \psi_2)$. We need to show that $\phi_1 \to \phi_2 \leq \psi_1 \to \psi_2$ i.e. $\vdash (\phi_1 \to \phi_2) \to (\psi_1 \to \psi_2)$. Using the deduction theorem (21) of page 226 it is sufficient to prove that $\{\phi_1 \to \phi_2\} \vdash (\psi_1 \to \psi_2)$. In fact, using theorem (21) once more, it is sufficient to prove that $\Gamma \vdash \psi_2$ where $\Gamma = \{\, \phi_1 \to \phi_2 \,,\, \psi_1 \,\}$. From the assumption $\vdash (\psi_1 \to \phi_1)$ we obtain $\{\psi_1\} \vdash \phi_1$ and consequently $\Gamma \vdash \phi_1$. Furthermore, it is clear that $\Gamma \vdash (\phi_1 \to \phi_2)$. Using the modus ponens property of proposition (161) we obtain $\Gamma \vdash \phi_2$. However, from the assumption $\vdash (\phi_2 \to \psi_2)$ we have in particular $\Gamma \vdash (\phi_2 \to \psi_2)$. Using the modus ponens property of proposition (161) once more we obtain $\Gamma \vdash \psi_2$ as requested. **.**

As we have just seen, the implication operator $\to$ formally behaves like a *difference* $\phi_2 - \phi_1$ when it comes to the Hilbert deductive preorder. By contrast, the quantification operator $\forall x$ respects the order:

Proposition 173 *Let V be a set and $\leq$ be the Hilbert deductive preorder on $\mathbf{P}(V)$. Let $\phi_1, \psi_1 \in \mathbf{P}(V)$ such that $\phi_1 \leq \psi_1$. Then for all $x \in V$ we have:*

$$\forall x \phi_1 \leq \forall x \psi_1$$

Proof
Suppose $\phi_1 \leq \psi_1$ and let $x \in V$. we need to show that $\forall x \phi_1 \leq \forall x \psi_1$ which is $\vdash (\forall x \phi_1 \to \forall x \psi_1)$. Using the deduction theorem (21) of page 226 it is sufficient to prove that $\Gamma \vdash \forall x \psi_1$ with $\Gamma = \{\forall x \phi_1\}$. It is clear that $\Gamma \vdash \forall x \phi_1$. From proposition (116) the identity mapping $i : \mathbf{P}(V) \to \mathbf{P}(V)$ is an essential substitution associated with the identity $i : V \to V$. In particular, it is an *essential substitution of y in place of x* in the case when $y = x$. Using the specialization property of proposition (167) it follows that $\Gamma \vdash \phi_1$. However, the assumption $\phi_1 \leq \psi_1$ leads to $\vdash (\phi_1 \to \psi_1)$ and in particular $\Gamma \vdash (\phi_1 \to \psi_1)$. Using the modus ponens property of proposition (161) we obtain $\Gamma \vdash \psi_1$. Since $x \notin \mathrm{Fr}(\Gamma)$ we conclude $\Gamma \vdash \forall x \psi_1$ from the generalization property of proposition (162). **.**

We shall now define the Hilbert deductive congruence in terms of the Hilbert deductive preorder, and prove it is indeed a congruence on $\mathbf{P}(V)$.

Definition 73 *Let V be a set and $\leq$ be the Hilbert deductive preorder on $\mathbf{P}(V)$. We call* Hilbert deductive congruence *on $\mathbf{P}(V)$ the relation $\equiv$ defined by:*

$$\phi \equiv \psi \quad \Leftrightarrow \quad (\phi \leq \psi) \wedge (\psi \leq \phi)$$

Proposition 174 *The Hilbert deductive congruence on $\mathbf{P}(V)$ is a congruence.*

Proof
Let $\equiv$ denote the Hilbert deductive congruence on $\mathbf{P}(V)$. We need to prove that

$\equiv$ is an equivalence relation which is also a congruent relation. First we show that it is indeed an equivalence relation. Let $\leq$ denote the Hilbert deductive preorder on $\mathbf{P}(V)$. From proposition (171), $\leq$ is reflexive. So it is clear that $\equiv$ is also reflexive. It is also obvious that $\equiv$ is symmetric. So it remains to show that $\equiv$ is transitive. So suppose $\phi, \psi, \chi \in \mathbf{P}(V)$ are such that $\phi \equiv \psi$ and $\psi \equiv \chi$. In particular we have $\phi \leq \psi$ and $\psi \leq \chi$ and it follows from the transitivity of $\leq$ that $\phi \leq \chi$. We show similarly that $\chi \leq \phi$ and we conclude that $\phi \equiv \chi$. So it remains to show that $\equiv$ is a congruent relation on $\mathbf{P}(V)$. We have already proved that $\bot \equiv \bot$ from reflexivity. Suppose $\phi_1 \equiv \psi_1$ and $\phi_2 \equiv \psi_2$. We need to show that $\phi_1 \to \phi_2 \equiv \psi_1 \to \psi_2$. First we show that $\phi_1 \to \phi_2 \leq \psi_1 \to \psi_2$. This follows from proposition (172) and the fact that $\psi_1 \leq \phi_1$ and $\phi_2 \leq \psi_2$. Using $\phi_1 \leq \psi_1$ and $\psi_2 \leq \phi_2$ we prove similarly that $\psi_1 \to \psi_2 \leq \phi_1 \to \phi_2$. Suppose now that $\phi_1 \equiv \psi_1$ and $x \in V$. We need to show that $\forall x\phi_1 \equiv \forall x\psi_1$. However, from $\phi_1 \leq \psi_1$ and proposition (173) we obtain $\forall x\phi_1 \leq \forall x\psi_1$. Likewise from $\psi_1 \leq \phi_1$ we have $\forall x\psi_1 \leq \forall x\phi_1$. The equivalence $\forall x\phi_1 \equiv \forall x\psi_1$ follows. **.**

The Hilbert deductive congruence expresses the idea of *logical equivalence* between formulas. We are already familiar with other congruences which formalize the idea of *identical meaning*. Obviously we should expect formulas which have *identical meaning* to be *logically equivalent*. We shall now check this is indeed the case, starting with the substitution congruence on $\mathbf{P}(V)$:

Proposition 175 *Let V be a set. Let $\sim$ and $\equiv$ denote the substitution and Hilbert deductive congruence on $\mathbf{P}(V)$ respectively. Then for all $\phi, \psi \in \mathbf{P}(V)$:*

$$\phi \sim \psi \;\Rightarrow\; \phi \equiv \psi$$

The substitution congruence is stronger than the Hilbert deductive congruence.

Proof

We need to show the inclusion $\sim \subseteq \equiv$, for which it is sufficient to show $R_0 \subseteq \equiv$ where R_0 is a generator of the substitution congruence. Using definition (35) it is therefore sufficient to prove that $\phi \equiv \psi$ where $\phi = \forall x\phi_1$ for some $x \in V$ and $\phi_1 \in \mathbf{P}(V)$, and $\psi = \forall y\phi_1[y:x]$ with $x \neq y$ and $y \notin \mathrm{Fr}(\phi_1)$. First we show that $\phi \leq \psi$ where $\leq$ is the Hilbert preorder on $\mathbf{P}(V)$. So we need to show that $\vdash (\phi \to \psi)$. Using the deduction theorem (21) of page 226 it is sufficient to prove that $\{\phi\} \vdash \psi$, which is $\Gamma \vdash \forall y\phi_1[y:x]$ where $\Gamma = \{\forall x\phi_1\}$. However, having assumed that $y \notin \mathrm{Fr}(\phi_1)$, in particular we have $y \notin \mathrm{Fr}(\Gamma)$. Using the generalization property of proposition (162) it is therefore sufficient to prove that $\Gamma \vdash \phi_1[y:x]$. Let us accept for now that the formula $\chi = \forall x\phi_1 \to \phi_1[y:x]$ is a specialization axiom. Then from proposition (160) we have $\vdash \chi$ and using the deduction theorem once more we obtain $\Gamma \vdash \phi_1[y:x]$ as requested. So it remains to show that χ is indeed a specialization axiom. From proposition (157) it is sufficient to show that $\phi_1[y:x] \sim \phi_1[y/x]$ where $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ is an essential substitution of y in place of x. Since the permutation $[y:x] : V \to V$ is injective, from proposition (116) its associated map $[y:x] : \mathbf{P}(V) \to \mathbf{P}(V)$ is also an essential substitution. Hence, in order to show the equivalence $\phi_1[y:x] \sim \phi_1[y/x]$, from proposition (121) it is sufficient to show that $[y/x]$ and $[y:x]$

coincide on $\mathrm{Fr}(\phi_1)$. This is clearly the case since $y \notin \mathrm{Fr}(\phi_1)$. So we have proved that $\phi \leq \psi$ and it remains to show that $\psi \leq \phi$. However, define $\phi_1^* = \phi_1[y:x]$. Then it is clear that $\phi_1 = \phi_1^*[x:y]$ and we need to show that $\forall y \phi_1^* \leq \forall x \phi_1^*[x:y]$, for which we can use an identical proof as previously, provided we show that $x \notin \mathrm{Fr}(\phi_1^*)$. So suppose to the contrary that $x \in \mathrm{Fr}(\phi_1^*)$. Using proposition (44), since $[y:x]$ is injective we have $\mathrm{Fr}(\phi_1^*) = [x:y](\mathrm{Fr}(\phi_1))$. It follows that there exists $u \in \mathrm{Fr}(\phi_1)$ such that $x = [x:y](u)$. Hence $u = y$ which contradicts $y \notin \mathrm{Fr}(\phi_1)$. **.**

Two formulas which are permutation equivalent are also logically equivalent:

Proposition 176 *Let V be a set. Let $\sim$ and $\equiv$ denote the permutation and Hilbert deductive congruence on $\mathbf{P}(V)$ respectively. Then for all $\phi, \psi \in \mathbf{P}(V)$:*

$$\phi \sim \psi \;\Rightarrow\; \phi \equiv \psi$$

The permutation congruence is stronger than the Hilbert deductive congruence.

Proof
We need to show the inclusion $\sim \subseteq \equiv$, for which it is sufficient to show $R_0 \subseteq \equiv$ where R_0 is a generator of the permutation congruence. Using definition (45) it is therefore sufficient to prove that $\phi \equiv \psi$ where $\phi = \forall x \forall y \phi_1$ and $\psi = \forall y \forall x \phi_1$ where $\phi_1 \in \mathbf{P}(V)$ and $x, y \in V$. By symmetry, it is sufficient to show that $\phi \leq \psi$ i.e. $\vdash (\phi \to \psi)$. Using the deduction theorem (21) of page 226 it is therefore sufficient to prove that $\{\phi\} \vdash \psi$ which is $\Gamma \vdash \forall y \forall x \phi_1$ where $\Gamma = \{\forall x \forall y \phi_1\}$. It is clear that $\Gamma \vdash \forall x \forall y \phi_1$. Using the specialization property of proposition (167) we obtain $\Gamma \vdash \forall y \phi_1$. Hence, using specialization once more we obtain $\Gamma \vdash \phi_1$. However, it is clear that $x \notin \mathrm{Fr}(\Gamma)$. So we can use the generalization property of proposition (162) to obtain $\Gamma \vdash \forall x \phi_1$. With one additional use of generalization, since $y \notin \mathrm{Fr}(\Gamma)$, we conclude that $\Gamma \vdash \forall y \forall x \phi_1$ as requested. **.**

Two formulas which are absorption equivalent are also logically equivalent:

Proposition 177 *Let V be a set. Let $\sim$ and $\equiv$ denote the absorption and Hilbert deductive congruence on $\mathbf{P}(V)$ respectively. Then for all $\phi, \psi \in \mathbf{P}(V)$:*

$$\phi \sim \psi \;\Rightarrow\; \phi \equiv \psi$$

The absorption congruence is stronger than the Hilbert deductive congruence.

Proof
We need to show the inclusion $\sim \subseteq \equiv$, for which it is sufficient to show $R_0 \subseteq \equiv$ where R_0 is a generator of the absorption congruence. Using definition (52) it is therefore sufficient to prove that $\phi_1 \equiv \forall x \phi_1$ where $\phi_1 \in \mathbf{P}(V)$ and $x \notin \mathrm{Fr}(\phi_1)$. First we show that $\phi_1 \leq \forall x \phi_1$. We need to show that $\vdash (\phi_1 \to \forall x \phi_1)$ which is $\{\phi_1\} \vdash \forall x \phi_1$ after application of the deduction theorem (21) of page 226. However, since $x \notin \mathrm{Fr}(\phi_1)$, from $\{\phi_1\} \vdash \phi_1$ and the generalization property of proposition (162) we obtain $\{\phi_1\} \vdash \forall x \phi_1$ as requested. So it remains to show that $\forall x \phi_1 \leq \phi_1$, which is $\vdash (\forall x \phi_1 \to \phi_1)$, which follows immediately from proposition (160) and the fact that $\forall x \phi_1 \to \phi_1$ is a specialization axiom. **.**

Propositional equivalence is also stronger than logical equivalence:

Proposition 178 *Let V be a set. Let $\sim$ and $\equiv$ denote the propositional and Hilbert deductive congruence on $\mathbf{P}(V)$ respectively. Then for all $\phi, \psi \in \mathbf{P}(V)$:*

$$\phi \sim \psi \;\Rightarrow\; \phi \equiv \psi$$

The propositional congruence is stronger than the Hilbert deductive congruence.

Proof
To be determined. **.**

So the substitution, permutation, absorption and propositional congruences are all stronger than the Hilbert deductive congruence. The following proposition is an easy consequence of this, and can be added to our set of rules for sequent calculus: if a formula ϕ is provable while having the same *meaning* as a formula ψ, then ψ is also provable. In fact, if a formula ϕ is provable while being logically equivalent to a formula ψ, then ψ is also provable.

Proposition 179 *Let V be a set and $\sim$ be a congruence which is stronger than the Hilbert deductive congruence. Then for all $\phi, \psi \in \mathbf{P}(V)$ and $\Gamma \subseteq \mathbf{P}(V)$:*

$$(\Gamma \vdash \phi) \wedge (\phi \sim \psi) \;\Rightarrow\; \Gamma \vdash \psi$$

Proof
We assume that $\Gamma \vdash \phi$ and $\phi \sim \psi$. We need to show that $\Gamma \vdash \psi$. However the congruence $\sim$ on $\mathbf{P}(V)$ is stronger than the Hilbert deductive congruence $\equiv$. Hence from $\phi \sim \psi$ we obtain $\phi \equiv \psi$. It follows in particular that $\phi \leq \psi$, i.e. $\vdash (\phi \to \psi)$ and consequently we have $\Gamma \vdash (\phi \to \psi)$. From $\Gamma \vdash \phi$ and the modus ponens property of proposition (161) we conclude that $\Gamma \vdash \psi$ as requested. **.**

3.2 The Free Universal Algebra of Proofs

3.2.1 Totally Clean Proof

The universal algebra of proofs $\mathbf{\Pi}(V)$ of definition (65) is not as natural as it looks: a universal algebra has operators which must be defined everywhere. However, the modus ponens operator $\oplus$ should not be defined in most cases. It makes little sense to infer anything from two conclusions ϕ_1 and ϕ_2 using modus ponens, unless the conclusion ϕ_2 is of the form $\phi_2 = \phi_1 \to \phi$ in which case we can derive the new conclusion ϕ. In other words, the proof $\pi_1 \oplus \pi_2$ is not a valid application of the modus ponens rule, unless $\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \to \phi$ for some $\phi \in \mathbf{P}(V)$. In a similar way, the proof $\nabla x \pi_1$ is not a valid application of the generalization rule, unless the condition $x \notin \mathrm{Sp}(\pi_1)$ is met, i.e. the variable x is truly general and not specific. So in some sense, it may be argued that the structure of universal algebra is not suited to represent a set of proofs. These proofs have operators which are naturally partial functions, while universal algebras require operators which are total functions. There is a prominent example for which this issue arises: the algebraic structure of field has an inverse operator which is not defined on 0. So there is a problem: our solution to it is to regard

proofs simply as formal expressions where the operators $\oplus$ and ∇x are defined everywhere, and to introduce $\mathrm{Val} : \mathbf{\Pi}(V) \to \mathbf{P}(V)$ as a semantics representing the conclusion being proved by a given formal expression. So defying common sense, we assign meaning to all proofs $\pi = \pi_1 \oplus \pi_2$, $\pi = \nabla x \pi_1$ and even $\pi = \partial\phi$ when ϕ is not an axiom of first order logic, while attempting to redeem ourselves by setting $\mathrm{Val}(\pi) = \bot \to \bot$ whenever a proof arises from a flawed application of a rule of inference or flawed invocation of axiom.

In this section, we introduce the notion of *totally clean* proof to emphasize the case when no such flawed inference occurs. We shall use the phrase '*totally clean*' rather than simply '*clean*' so as to reserve the latter for a weaker notion of *flawlessness* which we shall introduce in definition (86) when dealing with proofs modulo. In this section, we shall also establish proposition (185) below showing that any true sequent $\Gamma \vdash \phi$ can always be proved in a *totally clean* way. This gives us some degree of reassurance: although our universal algebra of proofs $\mathbf{\Pi}(V)$ is arguably too large and contains proofs which may be deemed to be flawed, every conclusion reached by such a flawed proof is in fact provable in the orthodox way. So it would be possible to reject $\mathbf{\Pi}(V)$ and only consider its subset of *totally clean* proofs, but this would not change the notion of provability as introduced in definition (70). However, beyond our peace of mind there is another good reason to introduce the notion of *totally clean* proof: given a map $\sigma : V \to W$ and a proof $\pi \in \mathbf{\Pi}(V)$, we shall soon want to substitute the variables of π as specified by the map σ, thereby defining a map $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ which we shall do in definition (74). This map may give us a tool to create new proofs from old proofs, allowing us to show some provability statements which would otherwise be out of reach. For example, suppose we want to prove $\vdash \sigma(\phi)$ knowing that $\vdash \phi$ is true. One possible line of attack is to consider a proof $\pi \in \mathbf{\Pi}(V)$ underlying the sequent $\vdash \phi$ and hope that $\sigma(\pi)$ is in fact a proof with conclusion $\sigma(\phi)$. So we need the following equation to hold:

$$\mathrm{Val} \circ \sigma(\pi) = \sigma \circ \mathrm{Val}(\pi) \tag{3.5}$$

This equation is bound to play an important role. More generally, a transformation $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ is interesting if we control the conclusion of $\sigma(\pi)$ in some way, given the conclusion of π. Now consider the following proof:

$$\pi = (x \in x) \oplus ((y \in y) \to (z \in z))$$

Whenever $x \neq y$, this proof is not totally clean as it contains a flawed application of modus ponens. However, if $\sigma(x) = \sigma(y) = u$ while $\sigma(z) = v$ we obtain:

$$\sigma(\pi) = (u \in u) \oplus ((u \in u) \to (v \in v))$$

This is a totally clean proof with conclusion $v \in v$. It should be clear from this example that we cannot hope to prove properties such as (3.5) in full generality, and must restrict our attention to the case of totally clean proofs. Too many bizarre things may happen otherwise. It is very hard to carry out a sensible analysis of proofs which are not totally clean. Hence the following:

Definition 74 *Let V be a set. The map $s : \mathbf{\Pi}(V) \to 2 = \{0,1\}$ defined by the following structural recursion is called the* strength mapping *on $\mathbf{\Pi}(V)$:*

$$\forall \pi \in \mathbf{\Pi}(V)\ ,\ s(\pi) = \begin{cases} 1 & \textit{if} \quad \pi = \phi \in \mathbf{P}(V) \\ 1 & \textit{if} \quad \pi = \partial\phi,\ \phi \in \mathbf{A}(V) \\ 0 & \textit{if} \quad \pi = \partial\phi,\ \phi \notin \mathbf{A}(V) \\ s(\pi_1) \wedge s(\pi_2) \wedge \epsilon & \textit{if} \quad \pi = \pi_1 \oplus \pi_2 \\ s(\pi_1) \wedge \eta & \textit{if} \quad \pi = \nabla x \pi_1 \end{cases} \tag{3.6}$$

where $\epsilon \in 2 = \{0,1\}$ is defined by $\epsilon = 1$ if and only if we have the equality:

$$\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \to \mathrm{Val}(\pi)$$

and $\eta \in 2 = \{0,1\}$ is defined by $\eta = 1$ if and only if $x \notin \mathrm{Sp}(\pi_1)$. We say that a proof $\pi \in \mathbf{\Pi}(V)$ is totally clean *if and only if it has full strength, i.e. $s(\pi) = 1$.*

Proposition 180 *The structural recursion of* definition (73) *is legitimate.*

Proof
We need to show the existence and uniqueness of $s : \mathbf{\Pi}(V) \to 2$ satisfying the five conditions of equation (3.6). We shall do so using theorem (5) of page 44 with $X = \mathbf{\Pi}(V)$, $X_0 = \mathbf{P}(V)$ and $A = 2$. Choosing the map $g_0 : X_0 \to A$ defined by $g_0(\phi) = 1$ we ensure the first condition is met. Next for every formula $\phi \in \mathbf{P}(V)$ we define $h(\partial\phi) : A^0 \times X^0 \to A$ by setting $h(\partial\phi)(0,0) = 1$ if $\phi \in \mathbf{A}(V)$ and $h(\partial\phi)(0,0) = 0$ otherwise. This ensures the second and third conditions are met. Next we define $h(\oplus) : A^2 \times X^2 \to A$ with the following formula:

$$h(\oplus)(\epsilon_1, \epsilon_2, \pi_1, \pi_2) = \begin{cases} \epsilon_1 \wedge \epsilon_2 & \text{if} \quad \mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \to \mathrm{Val}(\pi_1 \oplus \pi_2) \\ 0 & \text{if} \quad \mathrm{Val}(\pi_2) \neq \mathrm{Val}(\pi_1) \to \mathrm{Val}(\pi_1 \oplus \pi_2) \end{cases}$$

This takes care of the fourth condition. Finally we define $h(\nabla x) : A^1 \times X^1 \to A$:

$$h(\nabla x)(\epsilon_1, \pi_1) = \begin{cases} \epsilon_1 & \text{if} \quad x \notin \mathrm{Sp}(\pi_1) \\ 0 & \text{if} \quad x \in \mathrm{Sp}(\pi_1) \end{cases}$$

which ensures the fifth condition is met and completes our proof. **.**

A proof which relies on a flawed sub-proof is itself flawed. Hence a proof cannot be totally clean unless every one of its sub-proofs is totally clean.

Proposition 181 *Let V be a set and $s : \mathbf{\Pi}(V) \to 2$ be the strength mapping. Then the strength of a sub-proof is higher than the strength of a proof, i.e.*

$$\rho \preceq \pi \ \Rightarrow\ s(\pi) \leq s(\rho)$$

A proof $\pi \in \mathbf{\Pi}(V)$ is totally clean if and only if every $\rho \preceq \pi$ is totally clean.

Proof
The implication is a simple application of proposition (25) to $s : X \to A$ where $X = \mathbf{\Pi}(V)$ and $A = 2$ where the chosen preorder on A is the usual order

$\geq$ (reversed) on $\{0,1\}$. We simply need to check that given $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ and $x \in V$ we have the inequalities $s(\pi_1) \geq s(\pi_1 \oplus \pi_2)$, $s(\pi_2) \geq s(\pi_1 \oplus \pi_2)$ and $s(\pi_1) \geq s(\nabla x \pi_1)$ which follow immediately from the recursive definition (73). It remains to check that $\pi \in \mathbf{\Pi}(V)$ is totally clean if and only if every one of its sub-proofs is totally clean. Since π is a sub-proof of itself, the 'if' part is clear. Conversely, let $\rho \preceq \pi$ be a sub-proof of π where π is totally clean. Then $s(\pi) = 1$ and since $s(\pi) \leq s(\rho)$ we see that $s(\rho) = 1$. So the proof ρ is also totally clean. .

A proof arising from modus ponens is of the form $\pi = \pi_1 \oplus \pi_2$. Such a proof cannot be totally clean unless the use of modus ponens is legitimate, i.e. the conclusion of π_2 is of the form $\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \to \mathrm{Val}(\pi)$. Of course we also need both π_1 and π_2 to be totally clean. These conditions are in turn sufficient. The following proposition is useful to carry out structural induction arguments.

Proposition 182 *Let V be a set and π be a proof of the form $\pi = \pi_1 \oplus \pi_2$. Then π is totally clean if and only if both π_1, π_2 are totally clean and:*

$$\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \to \mathrm{Val}(\pi)$$

Proof
First we show the 'only if' part: so we assume that $\pi = \pi_1 \oplus \pi_2$ is totally clean. Then $s(\pi) = 1$ and from definition (73) we obtain $s(\pi_1) \wedge s(\pi_2) \wedge \epsilon = 1$. It follows that $s(\pi_1) = s(\pi_2) = \epsilon = 1$. So π_1 and π_2 are totally clean and from $\epsilon = 1$ and definition (73) we conclude that $\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \to \mathrm{Val}(\pi)$. We now prove the 'if' part: so we assume that $\pi = \pi_1 \oplus \pi_2$ where π_1, π_2 are totally clean and $\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \to \mathrm{Val}(\pi)$. Then from definition (73):

$$s(\pi) = s(\pi_1) \wedge s(\pi_2) \wedge \epsilon = 1 \wedge 1 \wedge 1 = 1$$

It follows that π is itself a totally clean proof, as requested. .

A proof arising from generalization is of the form $\pi = \nabla x \pi_1$. Such a proof cannot be totally clean unless the use of generalization is legitimate, that is $x \notin \mathrm{Sp}(\pi_1)$. We also need π_1 to be totally clean, and these conditions are in turn sufficient. The following proposition is also useful for structural induction.

Proposition 183 *Let V be a set and π be a proof of the form $\pi = \nabla x \pi_1$. Then π is totally clean if and only if π_1 is totally clean and $x \notin \mathrm{Sp}(\pi_1)$.*

Proof
First we show the 'only if' part: so we assume that $\pi = \nabla x \pi_1$ is totally clean. Then $s(\pi) = 1$ and from definition (73) we obtain $s(\pi_1) \wedge \eta = 1$. It follows that $s(\pi_1) = \eta = 1$. So π_1 is totally clean and furthermore from $\eta = 1$ and definition (73) we conclude that $x \notin \mathrm{Sp}(\pi_1)$. We now prove the 'if' part: so we assume that $\pi = \nabla x \pi_1$, where π_1 is totally clean and $x \notin \mathrm{Sp}(\pi_1)$. Then from definition (73) $s(\pi) = s(\pi_1) \wedge \eta = 1 \wedge 1 = 1$. So π is itself totally clean. .

We decided to define a *totally clean* proof in terms of strength $s : \mathbf{\Pi}(V) \to 2$ as per definition (73). This was not the only way to go about it. A *totally clean*

proof is one which is not *flawed*. This means that every axiom invocation or use of modus ponens or generalization is legitimate. The following proposition confirms that a *totally clean* proof can be defined as one without flawed steps:

Proposition 184 *Let V be a set. Then $\pi \in \mathbf{\Pi}(V)$ is totally clean if and only if for all $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$, $\phi \in \mathbf{P}(V)$ and $x \in V$, we have the following:*

$$
\begin{array}{ll}
(i) & \partial\phi \preceq \pi \;\Rightarrow\; \phi \in \mathbf{A}(V) \\
(ii) & \pi_1 \oplus \pi_2 \preceq \pi \;\Rightarrow\; \mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \rightarrow \mathrm{Val}(\pi_1 \oplus \pi_2) \\
(iii) & \nabla x \pi_1 \preceq \pi \;\Rightarrow\; x \notin \mathrm{Sp}(\pi_1)
\end{array}
$$

Proof
First we show the 'only if' part: so we assume that $\pi \in \mathbf{\Pi}(V)$ is totally clean. We need to show that (i), (ii) and (iii) hold. First we show (i): so we assume that $\rho \preceq \pi$ is a sub-proof of π of the form $\rho = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. We need to show that $\phi \in \mathbf{A}(V)$, i.e. that ϕ is an axiom. Having assumed that π is totally clean, from proposition (181) the proof $\rho = \partial\phi$ is also totally clean. So $\phi \in \mathbf{A}(V)$ follows immediately from definition (73). Next we show (ii): so we assume that $\rho \preceq \pi$ is a sub-proof of π of the form $\rho = \pi_1 \oplus \pi_2$. We need to show that $\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \rightarrow \mathrm{Val}(\rho)$. Having assumed that π is totally clean, from proposition (181) the proof ρ is also totally clean. However, ρ is of the form $\rho = \pi_1 \oplus \pi_2$ and it follows from proposition (182) that we have $\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \rightarrow \mathrm{Val}(\rho)$ as requested. We now show (iii): so we assume that $\rho \preceq \pi$ is a sub-proof of π of the form $\rho = \nabla x \pi_1$. We need to show that $x \notin \mathrm{Sp}(\pi_1)$. Having assumed that π is totally clean, from proposition (181) the proof ρ is also totally clean. However, ρ is of the form $\rho = \nabla x \pi_1$ and it follows from proposition (183) that $x \notin \mathrm{Sp}(\pi_1)$ as requested. We now show this 'if' part: we need to prove that every $\pi \in \mathbf{\Pi}(V)$ satisfies the property $(i) + (ii) + (iii) \;\Rightarrow\; (\,\pi$ is totally clean$\,)$. We shall do so with a structural induction argument, using theorem (3) of page 31. So first we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. From definition (73) we obtain $s(\pi) = 1$. So π is always totally clean and the property is satisfied. Next we assume that $\pi = \partial\phi$ where $\phi \in \mathbf{P}(V)$. We need to show π satisfies our property. So we assume that (i), (ii) and (iii) hold. We need to show that π is totally clean. However, since π is a sub-proof of itself we have $\partial\phi \preceq \pi$ and using (i) we obtain $\phi \in \mathbf{A}(V)$. It follows from definition (73) that $s(\pi) = s(\partial\phi) = 1$ and we conclude that π is totally clean as requested. Next we assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ satisfy our induction property. We need to show the same is true of π. So we assume that (i), (ii) and (iii) hold for π. We need to show that π is totally clean. Using proposition (182), it is sufficient to prove that both π_1 and π_2 are totally clean and furthermore that $\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \rightarrow \mathrm{Val}(\pi)$. This last equality is an immediate consequence of condition (ii) and the fact that π is a sub-proof of itself i.e. $\pi = \pi_1 \oplus \pi_2 \preceq \pi$. So it remains to show that π_1 and π_2 are totally clean. Having assumed that π_1 and π_2 satisfy our induction property, it is therefore sufficient to prove that (i), (ii) and (iii) are satisfied by π_1 and π_2. First we show that (i) is satisfied by π_1: so we assume that $\rho \preceq \pi_1$

is a sub-proof of π_1 of the form $\rho = \partial\phi$. We need to show that $\phi \in \mathbf{A}(V)$. However, having assumed that (i) holds for $\pi = \pi_1 \oplus \pi_2$, it is sufficient to prove that $\rho \preceq \pi$ which follows immediately from $\rho \preceq \pi_1$ and $\pi_1 \preceq \pi$. We prove similarly that (i) holds for π_2. Next we show that (ii) is satisfied by π_1 : so we assume that $\rho \preceq \pi_1$ is a sub-proof of π_1 of the form $\rho = \rho_1 \oplus \rho_2$. We need to show that $\mathrm{Val}(\rho_2) = \mathrm{Val}(\rho_1) \to \mathrm{Val}(\rho)$. However, having assumed that (ii) holds for $\pi = \pi_1 \oplus \pi_2$, it is sufficient to prove that $\rho \preceq \pi$ which follows immediately from $\rho \preceq \pi_1$ and $\pi_1 \preceq \pi$. We prove similarly that (ii) holds for π_2 and we now show that (iii) holds for π_1 : so we assume that $\rho \preceq \pi_1$ is a sub-proof of π_1 of the form $\rho = \nabla x \rho_1$. We need to show that $x \notin \mathrm{Sp}(\rho_1)$. However, having assumed that (iii) holds for $\pi = \pi_1 \oplus \pi_2$, it is sufficient to prove that $\rho \preceq \pi$ which again follows from $\rho \preceq \pi_1$ and $\pi_1 \preceq \pi$. We prove similarly that (iii) holds for π_2 which completes our induction argument in the case when $\pi = \pi_1 \oplus \pi_2$. So we finally assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ satisfies our induction property. We need to show the same is true of π. So we assume that (i), (ii) and (iii) hold for π. We need to show that π is totally clean. Using proposition (183), it is sufficient to prove that π_1 is totally clean and furthermore that $x \notin \mathrm{Sp}(\pi_1)$. This last property is an immediate consequence of condition (iii) and the fact that π is a sub-proof of itself i.e. $\pi = \nabla x \pi_1 \preceq \pi$. So it remains to show that π_1 is totally clean. Having assumed that π_1 satisfies our induction property, it is therefore sufficient to prove that (i), (ii) and (iii) hold for π_1. First we show that (i) is true: so we assume that $\rho \preceq \pi_1$ is a sub-proof of π_1 of the form $\rho = \partial\phi$. We need to show that $\phi \in \mathbf{A}(V)$. However, having assumed that (i) holds for $\pi = \nabla x \pi_1$, it is sufficient to prove that $\rho \preceq \pi$ which follows immediately from $\rho \preceq \pi_1$ and $\pi_1 \preceq \pi$. Next we show that (ii) is true: so we assume that $\rho \preceq \pi_1$ is a sub-proof of π_1 of the form $\rho = \rho_1 \oplus \rho_2$. We need to show that $\mathrm{Val}(\rho_2) = \mathrm{Val}(\rho_1) \to \mathrm{Val}(\rho)$. However, having assumed that (ii) holds for $\pi = \nabla x \pi_1$, it is sufficient to prove that $\rho \preceq \pi$ which follows immediately from $\rho \preceq \pi_1$ and $\pi_1 \preceq \pi$. We now show that (iii) is satisfied: so we assume that $\rho \preceq \pi_1$ is a sub-proof of π_1 of the form $\rho = \nabla u \rho_1$. We need to show that $u \notin \mathrm{Sp}(\rho_1)$. However, having assumed that (iii) holds for $\pi = \nabla x \pi_1$, it is sufficient to prove that $\rho \preceq \pi$ which again follows from $\rho \preceq \pi_1$ and $\pi_1 \preceq \pi$.
.

As we shall see in proposition (185) below, any true sequent $\Gamma \vdash \phi$ can be established with a totally clean proof. The key to the argument is that any flawed step $\rho \preceq \pi$ of a proof with conclusion $\mathrm{Val}(\rho) = \bot \to \bot$ can be discarded and replaced by a totally clean fragment as the following lemma shows:

Lemma 18 *Let V be a set. There exists a totally clean proof $\pi \in \mathbf{\Pi}(V)$ with:*

$$(\,\mathrm{Hyp}(\pi) = \emptyset\,) \wedge (\,\mathrm{Val}(\pi) = \bot \to \bot\,)$$

Proof
Consider the formulas $\phi_1 = ((\bot \to \bot) \to \bot) \to \bot$ and $\phi_2 = \phi_1 \to (\bot \to \bot)$. Let us accept for now that both ϕ_1 and ϕ_2 are axioms and define $\pi = \partial\phi_1 \oplus \partial\phi_2$. It is clear that $\mathrm{Hyp}(\pi) = \emptyset$ and furthermore we have the equality:

$$\mathrm{Val}(\pi) \quad = \quad \mathrm{Val}(\partial\phi_1 \oplus \partial\phi_2)$$

$$\begin{array}{rcl} \text{def. (69)} \ \rightarrow & = & M(\,\mathrm{Val}(\partial\phi_1), \mathrm{Val}(\partial\phi_2)\,) \\ \phi_1, \phi_2 \in \mathbf{A}(V) \ \rightarrow & = & M(\phi_1, \phi_2) \\ & = & M(\,\phi_1\,,\, \phi_1 \rightarrow (\bot \rightarrow \bot)\,) \\ & = & \bot \rightarrow \bot \end{array}$$

So it remains to show that π is totally clean. However, from definition (73) both $\partial\phi_1$ and $\partial\phi_2$ are totally clean and it follows from proposition (182) and:

$$\mathrm{Val}(\partial\phi_2) = \mathrm{Val}(\partial\phi_1) \rightarrow \mathrm{Val}(\pi)$$

that π is also totally clean. It remains to check that both ϕ_1 and ϕ_2 are indeed axioms of first order logic. However, we have $\phi_1 = ((\psi_1 \rightarrow \bot) \rightarrow \bot) \rightarrow \psi_1$ where $\psi_1 = \bot$. So ϕ_1 is a transposition axiom as per definition (60). Likewise, we have $\phi_2 = ((\psi_2 \rightarrow \bot) \rightarrow \bot) \rightarrow \psi_2$ where $\psi_2 = \bot \rightarrow \bot$ and ϕ_2 is an axiom. **.**

We can now prove the main result of this section: there is no loss of generality in assuming that a true sequent $\Gamma \vdash \phi$ has an underlying proof which is totally clean. This shows that defining our syntactic entailment solely in terms of totally clean proofs would have made no difference to the final notion of provability. However, not working on the free universal algebra of proofs $\mathbf{\Pi}(V)$ would have made formal developments considerably more cumbersome.

Proposition 185 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. Let $\phi \in \mathbf{P}(V)$ be such that the sequent $\Gamma \vdash \phi$ is true. Then there exists a totally clean proof of ϕ from Γ.*

Proof
In order to establish this proposition, we shall first prove it is sufficient to show that every proof $\pi \in \mathbf{\Pi}(V)$ has a 'totally clean counterpart', namely that:

$$\exists \pi^* \in \mathbf{\Pi}(V)\ ,\ (\pi^* \text{ totally clean}) \wedge (\,\mathrm{Val}(\pi^*) = \mathrm{Val}(\pi)\,) \wedge (\,\mathrm{Hyp}(\pi^*) \subseteq \mathrm{Hyp}(\pi)\,)$$

In other words, for every proof $\pi \in \mathbf{\Pi}(V)$, there exists a totally clean proof π^* with the same conclusion as π, and fewer hypothesis. So let us assume this is the case for now. We need to show the proposition is true. So let $\Gamma \subseteq \mathbf{P}(V)$ and $\phi \in \mathbf{P}(V)$ such that $\Gamma \vdash \phi$. Then there exists a proof π of ϕ from Γ, i.e. $\pi \in \mathbf{\Pi}(V)$ such that $\mathrm{Val}(\pi) = \phi$ and $\mathrm{Hyp}(\pi) \subseteq \Gamma$. Taking a totally clean counterpart of π, we obtain a totally clean proof $\pi^* \in \mathbf{\Pi}(V)$ such that $\mathrm{Val}(\pi^*) = \mathrm{Val}(\pi)$ and $\mathrm{Hyp}(\pi^*) \subseteq \mathrm{Hyp}(\pi)$. It follows that π^* is a totally clean proof of ϕ from Γ as requested. So we need to show that every proof $\pi \in \mathbf{\Pi}(V)$ has a totally clean counterpart. We shall do so by structural induction, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then π is totally clean and there is nothing else to prove. So we now assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. We shall distinguish two cases: first we assume that $\phi \in \mathbf{A}(V)$. Then π is totally clean and we are done. We now assume that $\phi \notin \mathbf{A}(V)$. Then $\mathrm{Val}(\pi) = \bot \rightarrow \bot$. Using lemma (18) there exists a totally clean proof $\pi^* \in \mathbf{\Pi}(V)$ such that $\mathrm{Hyp}(\pi^*) = \emptyset$ and $\mathrm{Val}(\pi^*) = \bot \rightarrow \bot$. It follows that $\mathrm{Hyp}(\pi^*) \subseteq \mathrm{Hyp}(\pi)$ and $\mathrm{Val}(\pi^*) = \mathrm{Val}(\pi)$ and we have found a totally clean counterpart of π. Next we assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are

proofs with totally clean counterparts. We need to show that π also has a totally clean counterpart. So let π_1^* and π_2^* be totally clean counterparts of π_1 and π_2 respectively. We shall distinguish two cases. First we assume that:

$$\mathrm{Val}(\pi_2^*) = \mathrm{Val}(\pi_1^*) \to \mathrm{Val}(\pi_1^* \oplus \pi_2^*) \tag{3.7}$$

Then defining $\pi^* = \pi_1^* \oplus \pi_2^*$, since π_1^* and π_2^* are totally clean it follows from proposition (182) that π^* is totally clean. Furthermore, we have:

$$\begin{aligned}
\mathrm{Hyp}(\pi^*) &= \mathrm{Hyp}(\pi_1^* \oplus \pi_2^*) \\
&= \mathrm{Hyp}(\pi_1^*) \cup \mathrm{Hyp}(\pi_2^*) \\
&\subseteq \mathrm{Hyp}(\pi_1) \cup \mathrm{Hyp}(\pi_2) \\
&= \mathrm{Hyp}(\pi_1 \oplus \pi_2) \\
&= \mathrm{Hyp}(\pi)
\end{aligned}$$

and:

$$\begin{aligned}
\mathrm{Val}(\pi^*) &= \mathrm{Val}(\pi_1^* \oplus \pi_2^*) \\
\text{def. (69)} \ \to &= M(\,\mathrm{Val}(\pi_1^*), \mathrm{Val}(\pi_2^*)\,) \\
\mathrm{Val}(\pi_i^*) = \mathrm{Val}(\pi_i) \ \to &= M(\,\mathrm{Val}(\pi_1), \mathrm{Val}(\pi_2)\,) \\
&= \mathrm{Val}(\pi_1 \oplus \pi_2) \\
&= \mathrm{Val}(\pi)
\end{aligned}$$

So we have found a totally clean counterpart π^* of π as requested. Next we assume that equation (3.7) does not hold. Then $\mathrm{Val}(\pi_2^*) = \mathrm{Val}(\pi_1^*) \to \phi$ is false for all $\phi \in \mathbf{P}(V)$. It follows that $\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \to \phi$ is also false for all ϕ and consequently from definition (69) $\mathrm{Val}(\pi) = \bot \to \bot$. Using lemma (18) there exists a totally clean proof $\pi^* \in \mathbf{\Pi}(V)$ such that $\mathrm{Hyp}(\pi^*) = \emptyset$ and $\mathrm{Val}(\pi^*) = \bot \to \bot$. It follows that $\mathrm{Hyp}(\pi^*) \subseteq \mathrm{Hyp}(\pi)$ and furthermore $\mathrm{Val}(\pi^*) = \mathrm{Val}(\pi)$. So we have found a totally clean counterpart of π. Finally, we assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof which has a totally clean counterpart. We need to show that π also has a totally clean counterpart. So let π_1^* be a totally clean counterpart of π_1. We shall distinguish two cases: first we assume that $x \notin \mathrm{Sp}(\pi_1)$. Since $\mathrm{Hyp}(\pi_1^*) \subseteq \mathrm{Hyp}(\pi_1)$ we have $\mathrm{Sp}(\pi_1^*) \subseteq \mathrm{Sp}(\pi_1)$ and consequently $x \notin \mathrm{Sp}(\pi_1^*)$. Hence, defining $\pi^* = \nabla x \pi_1^*$, since π_1^* is totally clean it follows from proposition (183) that π^* is itself totally clean. Furthermore we have the following inclusion:

$$\mathrm{Hyp}(\pi^*) = \mathrm{Hyp}(\pi_1^*) \subseteq \mathrm{Hyp}(\pi_1) = \mathrm{Hyp}(\pi)$$

and the equalities:

$$\begin{aligned}
\mathrm{Val}(\pi^*) &= \mathrm{Val}(\nabla x \pi_1^*) \\
x \notin \mathrm{Sp}(\pi_1^*) \ \to &= \forall x \mathrm{Val}(\pi_1^*) \\
&= \forall x \mathrm{Val}(\pi_1) \\
x \notin \mathrm{Sp}(\pi_1) \ \to &= \mathrm{Val}(\nabla x \pi_1) \\
&= \mathrm{Val}(\pi)
\end{aligned}$$

So we have found a totally clean counterpart π^* of π as requested. Next we assume that $x \in \mathrm{Sp}(\pi_1)$. Then from definition (69) we have $\mathrm{Val}(\pi) = \bot \to \bot$, and using lemma (18) we see once again that π has a totally clean counterpart. .

3.2.2 Variable Substitution in Proof

In definition (24) we introduced the substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ associated with a map $\sigma : V \to W$. This substitution is crude in the sense that it is generally not capture-avoiding. In other words, given a formula $\phi \in \mathbf{P}(V)$, the substitution σ is generally not valid for ϕ, as per definition (30). However, the introduction of the minimal transform of definition (38) allowed us to build on this elementary substitution and derive a new type of variable substitution mapping $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$, the so-called essential substitutions of definition (44). Essential substitutions are capture-avoiding and their existence is guaranteed by theorem (18) with a mere cardinality assumption on V and W. A notable application of essential substitutions is our ability to put forward an axiomatization of first order logic where the specialization axioms of definition (62), i.e. $\forall x \phi_1 \to \phi_1[y/x]$ are stated without the usual caveat of *y being free for x in ϕ_1*.

What was done for formulas can be done for proofs. Given a map $\sigma : V \to W$ and a proof $\pi \in \mathbf{\Pi}(V)$, it is meaningful to ask which proof $\sigma(\pi) \in \mathbf{\Pi}(W)$ can be derived by systematically substituting variables in π according to the map σ. As in the case of formulas, we cannot expect miracles from this as the transformation will most likely be too crude in general. However, this may be a good starting point which is certainly worth investigating. There are many reasons for us to attempt building substitutions on proofs which are associated in some way with a map $\sigma : V \to W$. Any $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ can be viewed as a tool to create new proofs. This tool may prove invaluable when attempting to show that a *proof exists*. Gödel's completeness theorem is a case when the existence of a proof has to be established. Many common arguments in mathematical logic involve *language extensions* which can be viewed as embeddings. It is usually implicit in the argument that what is provable (or inconsistent) in one space, remains provable in the other. As we do not wish to take anything for granted, this is one reason for us to look into substitution of variables in proofs. Another reason is to establish some form of *structurality condition* for our consequence relation $\vdash$. This condition is stated in [6] and [50] as $\Gamma \vdash \phi \;\Rightarrow\; \sigma(\Gamma) \vdash \sigma(\phi)$. However, at this point of the document it is not clear to us what type of substitution σ would allow the structurality condition to hold in the context of first order logic with terms. Our hope is that essential substitutions will work, and indeed they will as theorem (30) of page 388 will show. The work leading up to this important theorem requires a new tool, namely the ability to consider variable substitutions in proofs. With this in mind, we define:

Definition 75 *Let V, W be sets and $\sigma : V \to W$ be a map. We call* proof

substitution associated with σ, *the map* $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ *defined by:*

$$\forall \pi \in \mathbf{\Pi}(V)\ ,\ \sigma^*(\pi) = \begin{cases} \sigma(\phi) & \textit{if} \quad \pi = \phi \in \mathbf{P}(V) \\ \partial\sigma(\phi) & \textit{if} \quad \pi = \partial\phi \\ \sigma^*(\pi_1) \oplus \sigma^*(\pi_2) & \textit{if} \quad \pi = \pi_1 \oplus \pi_2 \\ \nabla\sigma(x)\sigma^*(\pi_1) & \textit{if} \quad \pi = \nabla x \pi_1 \end{cases} \tag{3.8}$$

where $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ *also denotes the associated substitution mapping.*

Given a map $\sigma : V \to W$ and $\phi \in \mathbf{P}(V)$ the notation $\sigma(\phi)$ is potentially ambiguous. Since $\mathbf{P}(V) \subseteq \mathbf{\Pi}(V)$, it may refer to the proof of definition (74) or to the formula of definition (24). Luckily, the two notions coincide.

Proposition 186 *The structural recursion of* definition (74) *is legitimate.*

Proof
We need to prove the existence and uniqueness of the map $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ satisfying the four conditions of equation (3.8). We shall do so using theorem (4) of page 42 applied to the free universal algebra $X = \mathbf{\Pi}(V)$ with $X_0 = \mathbf{P}(V)$ and $A = \mathbf{\Pi}(W)$. First we define $g_0 : X_0 \to A$ by $g_0(\phi) = \sigma(\phi)$ which ensures the first condition is met. Next, given a formula $\phi \in \mathbf{P}(V)$ we define $h(\partial\phi) : A^0 \to A$ by setting $h(\partial\phi)(0) = \partial\sigma(\phi)$ which ensures the second condition is met. Next we define $h(\oplus) : A^2 \to A$ by setting $h(\oplus)(\pi_1, \pi_2) = \pi_1 \oplus \pi_2$ which ensures the third condition is met. Finally, given $x \in V$ we define $h(\nabla x) : A^1 \to A$ by setting $h(\nabla x)(\pi_1) = \nabla\sigma(x)\pi_1$. This guarantees our fourth condition is met. **.**

Given $\sigma : V \to W$, the associated proof substitution $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ is denoted σ^* and not σ. The following proposition will allow us to change that and revert to the simple notation $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ just as we have done with $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$. This proposition should be compared with proposition (28). Once we know that $(\sigma \circ \tau)^* = \sigma^* \circ \tau^*$ we can safely get rid of the star '$*$'.

Proposition 187 *Let* U, V, W *be sets. Let* $\tau : U \to V$ *and* $\sigma : V \to W$ *be maps. Let* $\tau^* : \mathbf{\Pi}(U) \to \mathbf{\Pi}(V)$ *and* $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ *be the proof substitutions associated with* τ *and* σ *respectively. Then we have the equality:*

$$(\sigma \circ \tau)^* = \sigma^* \circ \tau^*$$

where $(\sigma \circ \tau)^* : \mathbf{\Pi}(U) \to \mathbf{\Pi}(W)$ *is the proof substitution associated with* $\sigma \circ \tau$.

Proof
We need to show that $(\sigma \circ \tau)^*(\pi) = \sigma^* \circ \tau^*(\pi)$ for all $\pi \in \mathbf{\Pi}(U)$. We shall do so with a structural induction argument, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(U)$. Then we have the equalities:

$$\begin{aligned} (\sigma \circ \tau)^*(\pi) &= (\sigma \circ \tau)^*(\phi) \\ &= \sigma \circ \tau(\phi) \\ &= \sigma^*(\tau(\phi)) \\ &= \sigma^* \circ \tau^*(\phi) \end{aligned}$$

Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(U)$. Then we have:

$$\begin{aligned}(\sigma \circ \tau)^*(\pi) &= (\sigma \circ \tau)^*(\partial\phi) \\ &= \partial(\sigma \circ \tau(\phi)) \\ &= \sigma^*(\partial\tau(\phi)) \\ &= \sigma^* \circ \tau^*(\partial\phi) \\ &= \sigma^* \circ \tau^*(\pi)\end{aligned}$$

Next we assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(U)$ satisfy our property:

$$\begin{aligned}(\sigma \circ \tau)^*(\pi) &= (\sigma \circ \tau)^*(\pi_1 \oplus \pi_2) \\ &= (\sigma \circ \tau)^*(\pi_1) \oplus (\sigma \circ \tau)^*(\pi_2) \\ &= \sigma^* \circ \tau^*(\pi_1) \oplus \sigma^* \circ \tau^*(\pi_2) \\ &= \sigma^*(\, \tau^*(\pi_1) \oplus \tau^*(\pi_2)\,) \\ &= \sigma^* \circ \tau^*(\pi_1 \oplus \pi_2) \\ &= \sigma^* \circ \tau^*(\pi)\end{aligned}$$

Finally, we assume that $\pi = \nabla x \pi_1$ where $x \in U$ and π_1 satisfies our property:

$$\begin{aligned}(\sigma \circ \tau)^*(\pi) &= (\sigma \circ \tau)^*(\nabla x \pi_1) \\ &= \nabla\sigma \circ \tau(x)\,(\sigma \circ \tau)^*(\pi_1) \\ &= \nabla\sigma \circ \tau(x)\,\sigma^* \circ \tau^*(\pi_1) \\ &= \sigma^*(\, \nabla\tau(x)\,\tau^*(\pi_1)\,) \\ &= \sigma^* \circ \tau^*(\nabla x \pi_1) \\ &= \sigma^* \circ \tau^*(\pi)\end{aligned}$$

.

As in the case of proposition (29), the following spells out the obvious:

Proposition 188 *Let V be a set and $i : V \to V$ be the identity mapping. Then, the associated proof substitution mapping $i : \mathbf{\Pi}(V) \to \mathbf{\Pi}(V)$ is also the identity.*

Proof
We need to show that $i(\pi) = \pi$ for all $\pi \in \mathbf{\Pi}(V)$. We shall do so with a structural induction argument using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then $i(\pi) = i(\phi)$ and using proposition (29) it follows that $i(\pi) = \phi = \pi$. Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then we have $i(\pi) = \partial i(\phi) = \partial\phi = \pi$. Next we assume that $\pi = \pi_1 \oplus \pi_2$ in which case we obtain $i(\pi) = i(\pi_1) \oplus i(\pi_2) = \pi_1 \oplus \pi_2 = \pi$. Finally we assume that $\pi = \nabla x \pi_1$ which yields $i(\pi) = \nabla i(x) i(\pi_1) = \nabla x \pi_1 = \pi$. **.**

The map $\sigma : \mathbf{\Pi}(V) \rightarrow \mathbf{\Pi}(W)$ is a structural substitution as per definition (21). This allows us to claim that $\text{Sub}(\sigma(\pi)) = \sigma(\text{Sub}(\pi))$. Hence:

$$\rho \preceq \pi \;\Rightarrow\; \sigma(\rho) \preceq \sigma(\pi)$$

In other words, if ρ is a sub-proof of π then $\sigma(\rho)$ is a sub-proof of $\sigma(\pi)$. We also have the converse: any sub-proof of $\sigma(\pi)$ is of the form $\sigma(\rho)$ where ρ is a sub-proof of π. The following proposition is the analogue of proposition (30).

Proposition 189 *Let V, W be sets and $\sigma : V \rightarrow W$ be a map. The associated proof substitution $\sigma : \mathbf{\Pi}(V) \rightarrow \mathbf{\Pi}(W)$ is structural and for all $\pi \in \mathbf{\Pi}(V)$:*

$$\text{Sub}(\sigma(\pi)) = \sigma(\text{Sub}(\pi))$$

Proof
By virtue of proposition (26) it is sufficient to prove that $\sigma : \mathbf{\Pi}(V) \rightarrow \mathbf{\Pi}(W)$ is a structural substitution as per definition (21). Let $\alpha(V)$ and $\alpha(W)$ denote the Hilbert deductive proof types associated with V and W respectively as per definition (64). Let $q : \alpha(V) \rightarrow \alpha(W)$ be the map defined by:

$$\forall f \in \alpha(V)\ ,\ q(f) = \begin{cases} \partial\sigma(\phi) & \text{if} \quad f = \partial\phi \\ \oplus & \text{if} \quad f = \oplus \\ \nabla\sigma(x) & \text{if} \quad f = \nabla x \end{cases}$$

Then q is clearly arity preserving. In order to show that σ is a structural substitution, we simply need to check that properties (i) and (ii) of definition (21) are met. First we start with property (i): so let $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. We need to show that $\sigma(\pi) \in \mathbf{P}(W)$ which follows immediately from $\sigma(\pi) = \sigma(\phi)$. So we now show property (ii): given $f \in \alpha(V)$, given $\pi \in \mathbf{\Pi}(V)^{\alpha(f)}$ we need to show that $\sigma(f(\pi)) = q(f)(\sigma(\pi))$. First we assume that $f = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then $\alpha(f) = 0$, $\pi = 0$ and consequently we have:

$$\begin{aligned} \sigma(f(\pi)) &= \sigma(\partial\phi(0)) \\ \partial\phi(0) \text{ denoted } '\partial\phi' \;\rightarrow\; &= \sigma(\partial\phi) \\ \text{def. (74)} \;\rightarrow\; &= \partial\sigma(\phi) \\ \partial\sigma(\phi)(0) \text{ denoted } '\partial\sigma(\phi)' \;\rightarrow\; &= \partial\sigma(\phi)(0) \\ \sigma : \{0\} \rightarrow \{0\} \;\rightarrow\; &= q(\partial\phi)(\sigma(0)) \\ &= q(f)(\sigma(\pi)) \end{aligned}$$

Next we assume that $f = \oplus$. Then $\alpha(f) = 2$ and given $\pi = (\pi_0, \pi_1)$:

$$\begin{aligned} \sigma(f(\pi)) &= \sigma(\pi_0 \oplus \pi_1) \\ \text{def. (74)} \;\rightarrow\; &= \sigma(\pi_0) \oplus \sigma(\pi_1) \\ \sigma : \mathbf{\Pi}(V)^2 \rightarrow \mathbf{\Pi}(W)^2 \;\rightarrow\; &= q(\oplus)(\sigma(\pi_0, \pi_1)) \\ &= q(f)(\sigma(\pi)) \end{aligned}$$

Finally we assume that $f = \nabla x$, $x \in V$. Then $\alpha(f) = 1$ and given $\pi = (\pi_0)$:

$$\begin{array}{rcl} \sigma(f(\pi)) & = & \sigma(\nabla x \pi_0) \\ \text{def. (74)} \ \rightarrow & = & \nabla \sigma(x) \sigma(\pi_0) \\ \sigma : \mathbf{\Pi}(V)^1 \rightarrow \mathbf{\Pi}(W)^1 \ \rightarrow & = & q(\nabla x)(\sigma(\pi_0)) \\ & = & q(f)(\sigma(\pi)) \end{array}$$

.

When dealing with congruences on $\mathbf{\Pi}(V)$ we shall need the following:

Proposition 190 *Let V and W be sets and $\sigma : V \rightarrow W$ be a map. Let $\simeq$ be an arbitrary congruence on $\mathbf{\Pi}(W)$ and let $\equiv$ be the relation on $\mathbf{\Pi}(V)$ defined by:*

$$\pi \equiv \rho \ \Leftrightarrow \ \sigma(\pi) \simeq \sigma(\rho)$$

for all $\pi, \rho \in \mathbf{\Pi}(V)$. Then $\equiv$ is a congruence on $\mathbf{\Pi}(V)$.

Proof
Since the congruence $\simeq$ on $\mathbf{\Pi}(W)$ is an equivalence relation, $\equiv$ is clearly reflexive, symmetric and transitive on $\mathbf{\Pi}(V)$. So we simply need to show that $\equiv$ is a congruent relation on $\mathbf{\Pi}(V)$. Since $\simeq$ is reflexive, we have $\sigma(\partial\phi) \simeq \sigma(\partial\phi)$ for all $\phi \in \mathbf{P}(V)$, and so $\partial\phi \equiv \partial\phi$. Suppose π_1, π_2, ρ_1 and $\rho_2 \in \mathbf{\Pi}(V)$ are such that $\pi_1 \equiv \rho_1$ and $\pi_2 \equiv \rho_2$. Define $\pi = \pi_1 \oplus \pi_2$ and $\rho = \rho_1 \oplus \rho_2$. We need to show that $\pi \equiv \rho$, or equivalently that $\sigma(\pi) \simeq \sigma(\rho)$. This follows from the fact that $\sigma(\pi_1) \simeq \sigma(\rho_1)$, $\sigma(\pi_2) \simeq \sigma(\rho_2)$ and furthermore:

$$\begin{array}{rcl} \sigma(\pi) & = & \sigma(\pi_1 \oplus \pi_2) \\ & = & \sigma(\pi_1) \oplus \sigma(\pi_2) \\ & \simeq & \sigma(\rho_1) \oplus \sigma(\rho_2) \\ & = & \sigma(\rho_1 \oplus \rho_2) \\ & = & \sigma(\rho) \end{array}$$

where the intermediate $\simeq$ crucially depends on $\simeq$ being a congruent relation on $\mathbf{\Pi}(W)$. We now suppose that $\pi_1, \rho_1 \in \mathbf{\Pi}(V)$ are such that $\pi_1 \equiv \rho_1$. Let $x \in V$ and define $\pi = \nabla x \pi_1$ and $\rho = \nabla x \rho_1$. We need to show that $\pi \equiv \rho$, or equivalently that $\sigma(\pi) \simeq \sigma(\rho)$. This follows from $\sigma(\pi_1) \simeq \sigma(\rho_1)$ and:

$$\begin{array}{rcl} \sigma(\pi) & = & \sigma(\nabla x \pi_1) \\ & = & \nabla \sigma(x) \, \sigma(\pi_1) \\ & \simeq & \nabla \sigma(x) \sigma(\rho_1) \\ & = & \sigma(\nabla x \rho_1) \\ & = & \sigma(\rho) \end{array}$$

where the intermediate $\simeq$ crucially depends on $\simeq$ being a congruent relation. .

3.2.3 Hypothesis of a Proof

Given a proof $\pi \in \mathbf{\Pi}(V)$, the set of hypothesis $\mathrm{Hyp}(\pi)$ was defined in an earlier section as per definition (66). At the time, a simple definition was enough so we could define the set of specific variables $\mathrm{Sp}(\pi)$ which in turn allowed us to speak of the valuation mapping $\mathrm{Val} : \mathbf{\Pi}(V) \to \mathbf{P}(V)$ and correspondingly establish the notion of provability and sequent $\Gamma \vdash \phi$, as per definition (70). It is now time to be a little bit more thorough and state some of the elementary properties satisfied by the set of hypothesis $\mathrm{Hyp}(\pi)$. We start with the fact that $\mathrm{Hyp}(\pi)$ is simply the set of formulas $\phi \in \mathbf{P}(V)$ which are sub-proofs of π:

Proposition 191 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$. Then for all $\phi \in \mathbf{P}(V)$:*

$$\phi \in \mathrm{Hyp}(\pi) \;\Leftrightarrow\; \phi \preceq \pi$$

In other words, ϕ is a hypothesis of π if and only if ϕ is a sub-proof of π.

Proof
We need to show the equality $\mathrm{Hyp}(\pi) = \mathrm{Sub}(\pi) \cap \mathbf{P}(V)$. We shall do so with a structural induction argument using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then we have $\mathrm{Hyp}(\pi) = \{\phi\}$ and from definition (19) $\mathrm{Sub}(\pi) = \{\phi\}$. So the equality is clear. Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then $\mathrm{Hyp}(\pi) = \emptyset$ while $\mathrm{Sub}(\pi) = \{\partial\phi\}$. Using theorem (2) of page 21 we obtain $\mathrm{Sub}(\pi) \cap \mathbf{P}(V) = \emptyset$. So the equality is true. Next we assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ satisfy the equality. Then:

$$\begin{array}{rcl}
\mathrm{Hyp}(\pi) & = & \mathrm{Hyp}(\pi_1 \oplus \pi_2) \\
& = & \mathrm{Hyp}(\pi_1) \cup \mathrm{Hyp}(\pi_2) \\
& = & (\mathrm{Sub}(\pi_1) \cap \mathbf{P}(V)) \cup (\mathrm{Sub}(\pi_2) \cap \mathbf{P}(V)) \\
& = & (\,\mathrm{Sub}(\pi_1) \cup \mathrm{Sub}(\pi_2)\,) \cap \mathbf{P}(V) \\
\text{theorem (2) of p. 21} \;\to & = & (\,\{\pi_1 \oplus \pi_2\} \cup \mathrm{Sub}(\pi_1) \cup \mathrm{Sub}(\pi_2)\,) \cap \mathbf{P}(V) \\
& = & \mathrm{Sub}(\pi_1 \oplus \pi_2) \cap \mathbf{P}(V) \\
& = & \mathrm{Sub}(\pi) \cap \mathbf{P}(V)
\end{array}$$

Finally we assume that $\pi = \nabla x \pi_1$ where $x \in V$ and π_1 satisfies the equality:

$$\begin{array}{rcl}
\mathrm{Hyp}(\pi) & = & \mathrm{Hyp}(\nabla x \pi_1) \\
& = & \mathrm{Hyp}(\pi_1) \\
& = & \mathrm{Sub}(\pi_1) \cap \mathbf{P}(V) \\
\text{theorem (2) of p. 21} \;\to & = & (\,\{\nabla x \pi_1\} \cup \mathrm{Sub}(\pi_1)\,) \cap \mathbf{P}(V) \\
& = & \mathrm{Sub}(\nabla x \pi_1) \cap \mathbf{P}(V) \\
& = & \mathrm{Sub}(\pi) \cap \mathbf{P}(V)
\end{array}$$

.

The map $\mathrm{Hyp} : \mathbf{\Pi}(V) \to \mathcal{P}(\mathbf{P}(V))$ defined on the free universal algebra $\mathbf{\Pi}(V)$ is increasing with respect to the inclusion partial order on $\mathcal{P}(\mathbf{P}(V))$.

Proposition 192 *Let V be a set and $\rho, \pi \in \mathbf{\Pi}(V)$. Then we have:*

$$\rho \preceq \pi \;\Rightarrow\; \mathrm{Hyp}(\rho) \subseteq \mathrm{Hyp}(\pi)$$

Proof
This follows from an application of proposition (25) to $\mathrm{Hyp} : X \to A$ where $X = \mathbf{\Pi}(V)$ and $A = \mathcal{P}(\mathbf{P}(V))$ where the preorder $\leq$ on A is the usual inclusion $\subseteq$. We simply need to check that given $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ and $x \in V$ we have the inclusions $\mathrm{Hyp}(\pi_1) \subseteq \mathrm{Hyp}(\pi_1 \oplus \pi_2)$, $\mathrm{Hyp}(\pi_2) \subseteq \mathrm{Hyp}(\pi_1 \oplus \pi_2)$ and $\mathrm{Hyp}(\pi_1) \subseteq \mathrm{Hyp}(\nabla x \pi_1)$ which follow from the recursive definition (66). **.**

Given a map $\sigma : V \to W$ and a proof $\pi \in \mathbf{\Pi}(V)$, the hypothesis of the proof $\sigma(\pi)$ are the images by $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ of the hypothesis of π. Note that the symbol 'σ' is overloaded and refers to three possible maps: apart from $\sigma : V \to W$, there is $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ when referring to $\sigma(\pi)$. There is also $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ whose restriction to $\mathrm{Hyp}(\pi)$ has a range denoted $\sigma(\mathrm{Hyp}(\pi))$.

Proposition 193 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\pi \in \mathbf{\Pi}(V)$:*

$$\mathrm{Hyp}(\sigma(\pi)) = \sigma(\mathrm{Hyp}(\pi))$$

where $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ also denotes the proof substitution mapping.

Proof
We shall proof this equality with an induction argument, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then we have:

$$\begin{array}{rcl} \mathrm{Hyp}(\sigma(\pi)) & = & \mathrm{Hyp}(\sigma(\phi)) \\ \text{def. (66)} \;\to & = & \{\sigma(\phi)\} \\ & = & \sigma(\{\phi\}) \\ & = & \sigma(\mathrm{Hyp}(\pi)) \end{array}$$

So we now assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then $\mathrm{Hyp}(\pi) = \emptyset$. However from definition (74), $\sigma(\pi) = \partial\sigma(\phi)$ and we have $\mathrm{Hyp}(\sigma(\pi)) = \emptyset$. So the equality $\mathrm{Hyp}(\sigma(\pi)) = \sigma(\mathrm{Hyp}(\pi))$ holds. So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs for which the equality is true. Then:

$$\begin{array}{rcl} \mathrm{Hyp}(\sigma(\pi)) & = & \mathrm{Hyp}(\sigma(\pi_1 \oplus \pi_2)) \\ & = & \mathrm{Hyp}(\,\sigma(\pi_1) \oplus \sigma(\pi_2)\,) \\ & = & \mathrm{Hyp}(\sigma(\pi_1)) \cup \mathrm{Hyp}(\sigma(\pi_2)) \\ & = & \sigma(\mathrm{Hyp}(\pi_1)) \cup \sigma(\mathrm{Hyp}(\pi_2)) \\ & = & \sigma(\,\mathrm{Hyp}(\pi_1) \cup \mathrm{Hyp}(\pi_2)\,) \\ & = & \sigma(\mathrm{Hyp}(\pi_1 \oplus \pi_2)) \\ & = & \sigma(\mathrm{Hyp}(\pi)) \end{array}$$

Finally, we assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof for which the equality is true. We need to show the same is true of π:

$$\begin{aligned} \mathrm{Hyp}(\sigma(\pi)) &= \mathrm{Hyp}(\sigma(\nabla x \pi_1)) \\ &= \mathrm{Hyp}(\, \nabla \sigma(x) \sigma(\pi_1)\,) \\ &= \mathrm{Hyp}(\sigma(\pi_1)) \\ &= \sigma(\mathrm{Hyp}(\pi_1)) \\ &= \sigma(\mathrm{Hyp}(\nabla x \pi_1)) \\ &= \sigma(\mathrm{Hyp}(\pi)) \end{aligned}$$

.

3.2.4 Axiom of a Proof

In this section, we define and establish elementary properties of the set $\mathrm{Ax}(\pi)$ representing the set of all axioms being invoked in a proof $\pi \in \mathbf{\Pi}(V)$. The set $\mathrm{Ax}(\pi)$ is casually called the *set of axioms of* π just like $\mathrm{Hyp}(\pi)$ is the set of hypothesis of π. An element of $\mathrm{Ax}(\pi)$ is casually called an *axiom of* π. This terminology is slightly unfortunate since an *axiom of* π may not be an axiom at all. For convenience, we allowed $\partial\phi$ to be meaningful for all $\phi \in \mathbf{P}(V)$. So the inclusion $\mathrm{Ax}(\pi) \subseteq \mathbf{A}(V)$ does not hold in general, unless π is totally clean.

Definition 76 *Let V be a set. The map $\mathrm{Ax} : \mathbf{\Pi}(V) \to \mathcal{P}(\mathbf{P}(V))$ defined by the following structural recursion is called the* axiom set mapping *on $\mathbf{\Pi}(V)$:*

$$\forall \pi \in \mathbf{\Pi}(V)\ ,\ \mathrm{Ax}(\pi) = \begin{cases} \emptyset & \text{if} \quad \pi = \phi \in \mathbf{P}(V) \\ \{\phi\} & \text{if} \quad \pi = \partial\phi \\ \mathrm{Ax}(\pi_1) \cup \mathrm{Ax}(\pi_2) & \text{if} \quad \pi = \pi_1 \oplus \pi_2 \\ \mathrm{Ax}(\pi_1) & \text{if} \quad \pi = \nabla x \pi_1 \end{cases} \tag{3.9}$$

We say that $\phi \in \mathbf{P}(V)$ is an axiom of $\pi \in \mathbf{\Pi}(V)$ if and only if $\phi \in \mathrm{Ax}(\pi)$.

The recursive definition (75) is easily seen to be legitimate and furthermore $\mathrm{Ax}(\pi)$ is a finite set, as a straightforward structural induction will show.

Proposition 194 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$. Then for all $\phi \in \mathbf{P}(V)$:*

$$\phi \in \mathrm{Ax}(\pi) \ \Leftrightarrow\ \partial\phi \preceq \pi$$

In other words, ϕ is an axiom π if and only if $\partial\phi$ is a sub-proof of π.

Proof
Consider the map $\partial : \mathbf{P}(V) \to \mathbf{\Pi}(V)$ defined by $\partial(\phi) = \partial\phi$. We need to show:

$$\mathrm{Ax}(\pi) = \partial^{-1}(\mathrm{Sub}(\pi)) = \{\phi \in \mathbf{P}(V)\ :\ \partial(\phi) \in \mathrm{Sub}(\pi)\}$$

We shall do so with an induction argument using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then $\mathrm{Ax}(\pi) = \emptyset$ while $\mathrm{Sub}(\pi) = \{\phi\}$.

Using theorem (2) of page 21 we obtain $\partial^{-1}(\mathrm{Sub}(\pi)) = \emptyset$. So the equality is true. Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then we have $\mathrm{Ax}(\pi) = \{\phi\}$ and from definition (19) $\mathrm{Sub}(\pi) = \{\partial\phi\}$. Since from proposition (158) ∂ is an injective map, we have $\partial^{-1}(\mathrm{Sub}(\pi)) = \{\phi\}$ and the equality is true. Next we assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ satisfy the equality:

$$\begin{aligned}
\mathrm{Ax}(\pi) &= \mathrm{Ax}(\pi_1 \oplus \pi_2) \\
&= \mathrm{Ax}(\pi_1) \cup \mathrm{Ax}(\pi_2) \\
&= \partial^{-1}(\mathrm{Sub}(\pi_1)) \cup \partial^{-1}(\mathrm{Sub}(\pi_2)) \\
&= \partial^{-1}(\,\mathrm{Sub}(\pi_1) \cup \mathrm{Sub}(\pi_2)\,) \\
\text{theorem (2) of p. 21} \;\rightarrow\; &= \partial^{-1}(\,\{\pi_1 \oplus \pi_2\} \cup \mathrm{Sub}(\pi_1) \cup \mathrm{Sub}(\pi_2)\,) \\
&= \partial^{-1}(\mathrm{Sub}(\pi_1 \oplus \pi_2)) \\
&= \partial^{-1}(\mathrm{Sub}(\pi))
\end{aligned}$$

Finally we assume that $\pi = \nabla x \pi_1$ where $x \in V$ and π_1 satisfies the equality:

$$\begin{aligned}
\mathrm{Ax}(\pi) &= \mathrm{Ax}(\nabla x \pi_1) \\
&= \mathrm{Ax}(\pi_1) \\
&= \partial^{-1}(\mathrm{Sub}(\pi_1)) \\
\text{theorem (2) of p. 21} \;\rightarrow\; &= \partial^{-1}(\,\{\nabla x \pi_1\} \cup \mathrm{Sub}(\pi_1)\,) \\
&= \partial^{-1}(\mathrm{Sub}(\nabla x \pi_1)) \\
&= \partial^{-1}(\mathrm{Sub}(\pi))
\end{aligned}$$

.

The axioms of a totally clean proof are indeed axioms of first order logic.

Proposition 195 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$. Then we have the implication:*

$$(\pi \textit{ totally clean}) \;\Rightarrow\; \mathrm{Ax}(\pi) \subseteq \mathbf{A}(V)$$

Proof
Let $\pi \in \mathbf{\Pi}(V)$ be totally clean. We need to show that $\mathrm{Ax}(\pi) \subseteq \mathbf{A}(V)$. So let $\phi \in \mathrm{Ax}(\pi)$. We need to show that $\phi \in \mathbf{A}(V)$. However from proposition (194) we obtain $\partial\phi \preceq \pi$. Since π is totally clean, it follows from proposition (181) that $\partial\phi$ is also totally clean. From definition (73) we see that $\phi \in \mathbf{A}(V)$. **.**

The map $\mathrm{Ax} : \mathbf{\Pi}(V) \rightarrow \mathcal{P}(\mathbf{P}(V))$ defined on the free universal algebra $\mathbf{\Pi}(V)$ is increasing with respect to the inclusion partial order on $\mathcal{P}(\mathbf{P}(V))$.

Proposition 196 *Let V be a set and $\rho, \pi \in \mathbf{\Pi}(V)$. Then we have:*

$$\rho \preceq \pi \;\Rightarrow\; \mathrm{Ax}(\rho) \subseteq \mathrm{Ax}(\pi)$$

Proof
This follows from an application of proposition (25) to $\mathrm{Ax} : X \rightarrow A$ where $X = \mathbf{\Pi}(V)$ and $A = \mathcal{P}(\mathbf{P}(V))$ where the preorder $\leq$ on A is the usual inclusion

$\subseteq$. We simply need to check that given $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ and $x \in V$ we have the inclusions $\mathrm{Ax}(\pi_1) \subseteq \mathrm{Ax}(\pi_1 \oplus \pi_2)$, $\mathrm{Ax}(\pi_2) \subseteq \mathrm{Ax}(\pi_1 \oplus \pi_2)$ and $\mathrm{Ax}(\pi_1) \subseteq \mathrm{Ax}(\nabla x \pi_1)$ which follow from the recursive definition (75). .

Given a map $\sigma : V \to W$ and a proof $\pi \in \mathbf{\Pi}(V)$, the axioms of the proof $\sigma(\pi)$ are the images by $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ of the axioms of π. Note that the symbol 'σ' is overloaded and refers to three possible maps: apart from $\sigma : V \to W$, there is $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ when referring to $\sigma(\pi)$. There is also $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ whose restriction to $\mathrm{Ax}(\pi)$ has a range denoted $\sigma(\mathrm{Ax}(\pi))$. Hence we have:

Proposition 197 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\pi \in \mathbf{\Pi}(V)$:*

$$\mathrm{Ax}(\sigma(\pi)) = \sigma(\mathrm{Ax}(\pi))$$

where $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ also denotes the proof substitution mapping.

Proof
We shall prove this equality with an induction argument, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then $\sigma(\pi) = \sigma(\phi)$ and consequently $\mathrm{Ax}(\sigma(\pi)) = \emptyset$. So the equality is clear. Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then we have the equalities:

$$\begin{aligned}
\mathrm{Ax}(\sigma(\pi)) &= \mathrm{Ax}(\sigma(\partial\phi)) \\
&= \mathrm{Ax}(\partial\sigma(\phi)) \\
&= \{\sigma(\phi)\} \\
&= \sigma(\{\phi\}) \\
&= \sigma(\mathrm{Ax}(\partial\phi)) \\
&= \sigma(\mathrm{Ax}(\pi))
\end{aligned}$$

Next we assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs for which the equality is true. We need to show the same is true of π:

$$\begin{aligned}
\mathrm{Ax}(\sigma(\pi)) &= \mathrm{Ax}(\sigma(\pi_1 \oplus \pi_2)) \\
&= \mathrm{Ax}(\, \sigma(\pi_1) \oplus \sigma(\pi_2)\,) \\
&= \mathrm{Ax}(\sigma(\pi_1)) \cup \mathrm{Ax}(\sigma(\pi_2)) \\
&= \sigma(\mathrm{Ax}(\pi_1)) \cup \sigma(\mathrm{Ax}(\pi_2)) \\
&= \sigma(\, \mathrm{Ax}(\pi_1) \cup \mathrm{Ax}(\pi_2)\,) \\
&= \sigma(\mathrm{Ax}(\pi_1 \oplus \pi_2)) \\
&= \sigma(\mathrm{Ax}(\pi))
\end{aligned}$$

Finally, we assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof for which the equality is true. We need to show the same is true of π:

$$\begin{aligned}
\mathrm{Ax}(\sigma(\pi)) &= \mathrm{Ax}(\sigma(\nabla x \pi_1)) \\
&= \mathrm{Ax}(\, \nabla\sigma(x)\sigma(\pi_1)\,)
\end{aligned}$$

$$
\begin{aligned}
&= \mathrm{Ax}(\sigma(\pi_1)) \\
&= \sigma(\mathrm{Ax}(\pi_1)) \\
&= \sigma(\mathrm{Ax}(\nabla x \pi_1)) \\
&= \sigma(\mathrm{Ax}(\pi))
\end{aligned}
$$

.

3.2.5 Variable of a Proof

It feels somewhat artificial to define the set of variables $\mathrm{Var}(\pi)$ of a proof π. All variables involved are very different in nature and it seems very little benefit can be derived from aggregating them in one big set. Among these, there are the free or bound variables coming from the set of hypothesis $\mathrm{Hyp}(\pi)$, and those coming from the set of axioms $\mathrm{Ax}(\pi)$. There are also the variables involved in the use of generalization. These five groups of variables are not mutually exclusive, unless when a proof is totally clean and no specific variable of $\mathrm{Sp}(\pi)$ can be used for generalization. So why define the set $\mathrm{Var}(\pi)$? Experience has shown us that given a formula $\phi \in \mathbf{P}(V)$, the set $\mathrm{Var}(\phi)$ was very useful in allowing us to strengthen a few results on substitutions. If $\sigma : V \to W$ is an injective map, then many things can be said about $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ or the formula $\sigma(\phi)$. However, we usually do not need to know that σ is injective to derive our conclusion. It is usually sufficient to assume the injectivity of the restriction $\sigma_{|\mathrm{Var}(\phi)}$. This distinction is in fact crucial: given an injective map $\tau : V \to W$, we often need to consider a left-inverse of τ, namely a map $\sigma : W \to V$ such that $\sigma \circ \tau(x) = x$ for all $x \in V$. Such a left-inverse is rarely injective, but the restriction $\sigma_{|\tau(V)}$ is an injective map. The set $\mathrm{Var}(\phi)$ together with $\mathrm{Fr}(\phi)$ and $\mathrm{Bnd}(\phi)$ were also crucial notions when dealing with valid substitutions and minimal transforms. As we shall soon discover, the same sort of analysis can be carried out for proofs, leading up to essential substitutions and their existence in theorem (29) of page 375. So $\mathrm{Var}(\phi)$ is a useful notion and so is $\mathrm{Var}(\pi)$.

Definition 77 *Let V be a set. The map* $\mathrm{Var} : \mathbf{\Pi}(V) \to \mathcal{P}(V)$ *defined by the following structural recursion is called* variable mapping on $\mathbf{\Pi}(V)$*:*

$$
\forall \pi \in \mathbf{\Pi}(V)\ ,\ \mathrm{Var}(\pi) = \begin{cases} \mathrm{Var}(\phi) & \text{if} \quad \pi = \phi \in \mathbf{P}(V) \\ \mathrm{Var}(\phi) & \text{if} \quad \pi = \partial\phi \\ \mathrm{Var}(\pi_1) \cup \mathrm{Var}(\pi_2) & \text{if} \quad \pi = \pi_1 \oplus \pi_2 \\ \{x\} \cup \mathrm{Var}(\pi_1) & \text{if} \quad \pi = \nabla x \pi_1 \end{cases} \tag{3.10}
$$

We say that $x \in V$ is a variable *of $\pi \in \mathbf{\Pi}(V)$ if and only if $x \in \mathrm{Var}(\pi)$.*

Given a formula $\phi \in \mathbf{P}(V)$ the notation $\mathrm{Var}(\phi)$ is potentially ambiguous. Since $\mathbf{P}(V) \subseteq \mathbf{\Pi}(V)$, it may refer to the usual $\mathrm{Var}(\phi)$ of definition (25), or to the set $\mathrm{Var}(\pi)$ where $\pi = \phi$ of definition (76). Luckily, the two notions coincide.

Proposition 198 *The structural recursion of* definition (76) *is legitimate.*

Proof
We need to show the existence and uniqueness of the map $\mathrm{Var} : \mathbf{\Pi}(V) \to \mathcal{P}(V)$ satisfying the four conditions of equation (3.10). This follows from an application of theorem (4) of page 42 with $X = \mathbf{\Pi}(V)$, $X_0 = \mathbf{P}(V)$ and $A = \mathcal{P}(V)$ where $g_0 : X_0 \to A$ is defined as $g_0(\phi) = \mathrm{Var}(\phi)$. Furthermore, given $\phi \in \mathbf{P}(V)$ we take $h(\partial\phi) : A^0 \to A$ defined $h(\partial\phi)(0) = \mathrm{Var}(\phi)$. We take $h(\oplus) : A^2 \to A$ defined by $h(\oplus)(A_0, A_1) = A_0 \cup A_1$ and $h(\nabla x) : A^1 \to A$ defined by $h(\nabla x)(A_0) = \{x\} \cup A_0$. .

Many elementary properties of $\mathrm{Var}(\pi)$ resemble those of $\mathrm{Var}(\phi)$. We have not attempted to design the right level of abstraction to avoid what may appear as tedious repetition. The following is the counterpart of proposition (33) :

Proposition 199 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$. Then $\mathrm{Var}(\pi)$ is finite.*

Proof
This follows from a structural induction argument using theorem (3) of page 31. If $\pi = \phi \in \mathbf{P}(V)$ then $\mathrm{Var}(\pi) = \mathrm{Var}(\phi)$ is finite by virtue of proposition (33). If $\pi = \partial\phi$ then $\mathrm{Var}(\pi) = \mathrm{Var}(\phi)$ is also finite. If $\pi = \pi_1 \oplus \pi_2$ then we have $\mathrm{Var}(\pi) = \mathrm{Var}(\pi_1) \cup \mathrm{Var}(\pi_2)$ which is finite. Finally if $\pi = \nabla x \pi_1$ then we have $\mathrm{Var}(\pi) = \{x\} \cup \mathrm{Var}(\pi_1)$ which is also finite if $\mathrm{Var}(\pi_1)$ is itself finite. .

The map $\mathrm{Var} : \mathbf{\Pi}(V) \to \mathcal{P}(V)$ is increasing with respect to the standard inclusion on $\mathcal{P}(V)$. In other words, the variables of a sub-proof are also variables of the proof itself. The following is the counterpart of proposition (34) :

Proposition 200 *Let V be a set and $\rho, \pi \in \mathbf{\Pi}(V)$. Then we have:*

$$\rho \preceq \pi \;\Rightarrow\; \mathrm{Var}(\rho) \subseteq \mathrm{Var}(\pi)$$

Proof
This is a simple application of proposition (25) to $\mathrm{Var} : X \to A$ where $X = \mathbf{\Pi}(V)$ and $A = \mathcal{P}(V)$ where the preorder $\leq$ on A is the usual inclusion $\subseteq$. We simply need to check that given $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ and $x \in V$ we have the inclusions $\mathrm{Var}(\pi_1) \subseteq \mathrm{Var}(\pi_1 \oplus \pi_2)$, $\mathrm{Var}(\pi_2) \subseteq \mathrm{Var}(\pi_1 \oplus \pi_2)$ and $\mathrm{Var}(\pi_1) \subseteq \mathrm{Var}(\nabla x \pi_1)$ which follow immediately from the recursive definition (76). .

Given a map $\sigma : V \to W$ and $\pi \in \mathbf{\Pi}(V)$, the variables of the proof $\sigma(\pi)$ are the images by σ of the variables of π. This is the counterpart of proposition (35) :

Proposition 201 *Let V and W be sets and $\sigma : V \to W$ be a map. Then:*

$$\forall \pi \in \mathbf{\Pi}(V)\ ,\ \mathrm{Var}(\sigma(\pi)) = \sigma(\mathrm{Var}(\pi))$$

where $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ also denotes the associated proof substitution mapping.

Proof
Given $\pi \in \mathbf{\Pi}(V)$, we need to show that $\mathrm{Var}(\sigma(\pi)) = \sigma(\mathrm{Var}(\pi))$. We shall do so by structural induction using theorem (3) of page 31. First we assume that

$\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then we have the equalities:

$$\begin{array}{rcl} \mathrm{Var}(\sigma(\pi)) & = & \mathrm{Var}(\sigma(\phi)) \\ \text{prop. (35)} \ \rightarrow & = & \sigma(\mathrm{Var}(\phi)) \\ & = & \sigma(\mathrm{Var}(\pi)) \end{array}$$

Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then we have:

$$\begin{array}{rcl} \mathrm{Var}(\sigma(\pi)) & = & \mathrm{Var}(\sigma(\partial\phi)) \\ & = & \mathrm{Var}(\partial\sigma(\phi)) \\ & = & \mathrm{Var}(\sigma(\phi)) \\ \text{prop. (35)} \ \rightarrow & = & \sigma(\mathrm{Var}(\phi)) \\ & = & \sigma(\mathrm{Var}(\partial\phi)) \\ & = & \sigma(\mathrm{Var}(\pi)) \end{array}$$

Next we check that the property is true for $\pi = \pi_1 \oplus \pi_2$ if it is true for π_1, π_2:

$$\begin{array}{rcl} \mathrm{Var}(\sigma(\pi)) & = & \mathrm{Var}(\sigma(\pi_1 \oplus \pi_2)) \\ & = & \mathrm{Var}(\sigma(\pi_1) \oplus \sigma(\pi_2)) \\ & = & \mathrm{Var}(\sigma(\pi_1)) \cup \mathrm{Var}(\sigma(\pi_2)) \\ & = & \sigma(\mathrm{Var}(\pi_1)) \cup \sigma(\mathrm{Var}(\pi_2)) \\ & = & \sigma(\, \mathrm{Var}(\pi_1) \cup \mathrm{Var}(\pi_2)\,) \\ & = & \sigma(\mathrm{Var}(\pi_1 \oplus \pi_2)) \\ & = & \sigma(\mathrm{Var}(\pi)) \end{array}$$

Finally we check that the property is true for $\pi = \nabla x \pi_1$ if it is true for π_1:

$$\begin{array}{rcl} \mathrm{Var}(\sigma(\pi)) & = & \mathrm{Var}(\sigma(\nabla x \pi_1)) \\ & = & \mathrm{Var}(\, \nabla \sigma(x) \sigma(\pi_1)\,) \\ & = & \{\sigma(x)\} \cup \mathrm{Var}(\sigma(\pi_1)) \\ & = & \{\sigma(x)\} \cup \sigma(\mathrm{Var}(\pi_1)) \\ & = & \sigma(\, \{x\} \cup \mathrm{Var}(\pi_1)\,) \\ & = & \sigma(\mathrm{Var}(\nabla x \pi_1)) \\ & = & \sigma(\mathrm{Var}(\pi)) \end{array}$$

.

In order to have the equality $\sigma(\pi) = \tau(\pi)$ is it sufficient that $\sigma, \tau : V \to W$ coincide on $\mathrm{Var}(\pi)$, which is pretty natural. What is less obvious is the fact that the converse is also true. The following is the counterpart of proposition (36) :

Proposition 202 *Let V and W be sets and $\sigma, \tau : V \to W$ be two maps. Then:*

$$\sigma_{|\mathrm{Var}(\pi)} = \tau_{|\mathrm{Var}(\pi)} \quad \Leftrightarrow \quad \sigma(\pi) = \tau(\pi)$$

for all $\pi \in \mathbf{\Pi}(V)$, where $\sigma, \tau : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ are also the proof substitutions.

Proof
First we prove $\Rightarrow$: We shall do so with an induction argument, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then we have $\mathrm{Var}(\pi) = \mathrm{Var}(\phi)$ so we assume that σ and τ coincide on $\mathrm{Var}(\phi)$. Using proposition (36) we obtain $\sigma(\phi) = \tau(\phi)$ which is $\sigma(\pi) = \tau(\pi)$. Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then again we have $\mathrm{Var}(\pi) = \mathrm{Var}(\phi)$ so we assume that σ and τ coincide on $\mathrm{Var}(\phi)$. Using proposition (36) once more we obtain $\sigma(\phi) = \tau(\phi)$. It follows that $\sigma(\pi) = \partial\sigma(\phi) = \partial\tau(\phi) = \tau(\pi)$. So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ satisfy our property. We need to show the same is true of π. So we assume that σ and τ coincide on $\mathrm{Var}(\pi)$. We need to show that $\sigma(\pi) = \tau(\pi)$. However since $\mathrm{Var}(\pi) = \mathrm{Var}(\pi_1) \cup \mathrm{Var}(\pi_2)$ we see that σ and τ coincide on $\mathrm{Var}(\pi_1)$ and $\mathrm{Var}(\pi_2)$, and it follows from our induction hypothesis that $\sigma(\pi_1) = \tau(\pi_1)$ and $\sigma(\pi_2) = \tau(\pi_2)$. Hence:

$$\begin{aligned}
\sigma(\pi) &= \sigma(\pi_1 \oplus \pi_2) \\
&= \sigma(\pi_1) \oplus \sigma(\pi_2) \\
&= \tau(\pi_1) \oplus \tau(\pi_2) \\
&= \tau(\pi_1 \oplus \pi_2) \\
&= \tau(\pi)
\end{aligned}$$

Finally, we assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ satisfies our property. We need to show the same is true of π. So we assume that σ and τ coincide on $\mathrm{Var}(\pi)$. We need to show that $\sigma(\pi) = \tau(\pi)$. However since $\mathrm{Var}(\pi) = \{x\} \cup \mathrm{Var}(\pi_1)$ we see that σ and τ coincide on $\mathrm{Var}(\pi_1)$, and it follows from our induction hypothesis that $\sigma(\pi_1) = \tau(\pi_1)$. Hence:

$$\begin{aligned}
\sigma(\pi) &= \sigma(\nabla x \pi_1) \\
&= \nabla\sigma(x)\sigma(\pi_1) \\
&= \nabla\sigma(x)\tau(\pi_1) \\
x \in \mathrm{Var}(\pi) \ \rightarrow \ &= \nabla\tau(x)\tau(\pi_1) \\
&= \tau(\nabla x \pi_1) \\
&= \tau(\pi)
\end{aligned}$$

We now show $\Leftarrow$: we shall do so with a structural induction argument, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then from $\sigma(\pi) = \tau(\pi)$ we obtain $\sigma(\phi) = \tau(\phi)$ and from proposition (36) it follows that σ and τ coincide on $\mathrm{Var}(\phi) = \mathrm{Var}(\pi)$. Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Suppose $\sigma(\pi) = \tau(\pi)$. Then $\partial\sigma(\phi) = \partial\tau(\phi)$ and consequently from proposition (158) we have $\sigma(\phi) = \tau(\phi)$. Using proposition (36) once more

it follows that σ and τ coincide on $\mathrm{Var}(\phi) = \mathrm{Var}(\pi)$. We now assume that $\pi = \pi_1 \oplus \pi_2$ where π_1, π_2 are proofs which satisfy our implication. We need to show the same is true of π. So we assume that $\sigma(\pi) = \tau(\pi)$. We need to show that σ and τ coincide on $\mathrm{Var}(\pi) = \mathrm{Var}(\pi_1) \cup \mathrm{Var}(\pi_2)$. However, from $\sigma(\pi) = \tau(\pi)$ we obtain $\sigma(\pi_1) \oplus \sigma(\pi_2) = \tau(\pi_1) \oplus \tau(\pi_2)$ and consequently using theorem (2) of page 21 we have $\sigma(\pi_1) = \tau(\pi_1)$ and $\sigma(\pi_2) = \tau(\pi_2)$. Having assumed that π_1 and π_2 satisfy our implication, it follows that σ and τ coincide on $\mathrm{Var}(\pi_1)$ and also on $\mathrm{Var}(\pi_2)$. So they coincide on $\mathrm{Var}(\pi)$ as requested. So we now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof which satisfies our implication. We need to show the same is true of π. So we assume that $\sigma(\pi) = \tau(\pi)$. We need to show that σ and τ coincide on $\mathrm{Var}(\pi) = \{x\} \cup \mathrm{Var}(\pi_1)$. However, from $\sigma(\pi) = \tau(\pi)$ we obtain $\nabla\sigma(x)\sigma(\pi_1) = \nabla\tau(x)\tau(\pi_1)$ and consequently using theorem (2) of page 21 we have $\sigma(\pi_1) = \tau(\pi_1)$ and $\sigma(x) = \tau(x)$. Having assumed that π_1 satisfies our implication, it follows that σ and τ coincide on $\mathrm{Var}(\pi_1)$. Since $\sigma(x) = \tau(x)$, they also coincide on $\mathrm{Var}(\pi) = \{x\} \cup \mathrm{Var}(\pi_1)$ as requested. **.**

Given a proof $\pi \in \mathbf{\Pi}(V)$, any variable which belongs to the conclusion $\mathrm{Val}(\rho)$ of a sub-proof $\rho \preceq \pi$ is of course a variable of π. Note that the converse is not true in general, unless π is totally clean: if $\pi = \partial\phi$ and $\phi \notin \mathbf{A}(V)$ then we have $\mathrm{Val}(\pi) = \bot \to \bot$ and any sub-proof of π is π itself. Hence we have $\cup\{\, \mathrm{Var}(\mathrm{Val}(\rho)) \;:\; \rho \preceq \pi \,\} = \emptyset$, while $\mathrm{Var}(\pi) = \mathrm{Var}(\phi)$ may not be empty. We shall deal with the case when π is totally clean later in proposition (243).

Proposition 203 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$. Then we have:*

$$\cup\{\, \mathrm{Var}(\mathrm{Val}(\rho)) \;:\; \rho \preceq \pi \,\} \subseteq \mathrm{Var}(\pi) \tag{3.11}$$

i.e. the variables of conclusions of sub-proofs of π are variables of π.

Proof
Using proposition (200) we have $\mathrm{Var}(\rho) \subseteq \mathrm{Var}(\pi)$ for all $\rho \preceq \pi$. It is therefore sufficient prove the inclusion $\mathrm{Var}(\mathrm{Val}(\pi)) \subseteq \mathrm{Var}(\pi)$ for all $\pi \in \mathbf{\Pi}(V)$ which we shall do with a structural induction argument, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then the inclusion follows immediately from $\mathrm{Val}(\phi) = \phi$. Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. The inclusion is clear in the case when $\mathrm{Val}(\pi) = \bot \to \bot$. So we may assume that $\mathrm{Val}(\pi) \neq \bot \to \bot$ in which case ϕ must be an axiom of first order logic, i.e. $\phi \in \mathbf{A}(V)$ and $\mathrm{Val}(\pi) = \phi$. The inclusion follows from $\mathrm{Var}(\pi) = \mathrm{Var}(\phi)$. So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs satisfying our inclusion. We need to show the same is true of π. This is clearly the case if $\mathrm{Val}(\pi) = \bot \to \bot$. So we may assume $\mathrm{Val}(\pi) \neq \bot \to \bot$ in which case we must have $\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \to \mathrm{Val}(\pi)$. Hence we see that:

$$\begin{aligned}
\mathrm{Var}(\mathrm{Val}(\pi)) &\subseteq \mathrm{Var}(\mathrm{Val}(\pi_1)) \cup \mathrm{Var}(\mathrm{Val}(\pi)) \\
&= \mathrm{Var}(\,\mathrm{Val}(\pi_1) \to \mathrm{Val}(\pi)\,) \\
&= \mathrm{Var}(\mathrm{Val}(\pi_2)) \\
&\subseteq \mathrm{Var}(\pi_2)
\end{aligned}$$

$$\begin{aligned} &\subseteq \quad \mathrm{Var}(\pi_1) \cup \mathrm{Var}(\pi_2) \\ &= \quad \mathrm{Var}(\pi_1 \oplus \pi_2) \\ &= \quad \mathrm{Var}(\pi) \end{aligned}$$

So we now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ satisfies our inclusion. We need to show the same is true of π. This is clearly the case if $\mathrm{Val}(\pi) = \bot \to \bot$. So we may assume that $\mathrm{Val}(\pi) \neq \bot \to \bot$ in which case we must have $x \notin \mathrm{Sp}(\pi_1)$ and $\mathrm{Val}(\pi) = \forall x \mathrm{Val}(\pi_1)$. Hence we see that:

$$\begin{aligned} \mathrm{Var}(\mathrm{Val}(\pi)) &= \mathrm{Var}(\, \forall x \mathrm{Val}(\pi_1)\,) \\ &= \{x\} \cup \mathrm{Var}(\mathrm{Val}(\pi_1)) \\ &\subseteq \{x\} \cup \mathrm{Var}(\pi_1) \\ &= \mathrm{Var}(\nabla x \pi_1) \\ &= \mathrm{Var}(\pi) \end{aligned}$$

.

3.2.6 Specific Variable of a Proof

The notion of *specific variable* of a proof should now be natural to us . To every proof π is associated a set of hypothesis $\mathrm{Hyp}(\pi)$ and a set of axioms $\mathrm{Ax}(\pi)$. Every formula $\phi \in \mathrm{Hyp}(\pi)$ has a set of free variables $\mathrm{Fr}(\phi)$, and so has every formula $\phi \in \mathrm{Ax}(\pi)$. In definition (67) we decided to call a *specific variable of* π only those variables which are free variables of some $\phi \in \mathrm{Hyp}(\pi)$. The *specific* variables are those which are not *general*. This allowed us to conveniently express the idea of *legitimate use of generalization* in $\nabla x \pi_1$, with the simple formalism $x \notin \mathrm{Sp}(\pi_1)$. In this section, we provide a few elementary properties of the set $\mathrm{Sp}(\pi)$. We start with a structural definition of $\mathrm{Sp}(\pi)$:

Proposition 204 *Let V be a set. The specific variable map* $\mathrm{Sp} : \mathbf{\Pi}(V) \to \mathcal{P}(V)$ *of* definition (67) *satisfies the following structural recursion equation:*

$$\forall \pi \in \mathbf{\Pi}(V)\ ,\ \mathrm{Sp}(\pi) = \begin{cases} \mathrm{Fr}(\phi) & \text{if} \quad \pi = \phi \in \mathbf{P}(V) \\ \emptyset & \text{if} \quad \pi = \partial\phi \\ \mathrm{Sp}(\pi_1) \cup \mathrm{Sp}(\pi_2) & \text{if} \quad \pi = \pi_1 \oplus \pi_2 \\ \mathrm{Sp}(\pi_1) & \text{if} \quad \pi = \nabla x \pi_1 \end{cases}$$

Proof
Using definition (67) we have $\mathrm{Sp}(\pi) = \cup\{\mathrm{Fr}(\phi)\ :\ \phi \in \mathrm{Hyp}(\pi)\}$. In the case when $\pi = \phi$ for $\phi \in \mathbf{P}(V)$, since $\mathrm{Hyp}(\pi) = \{\phi\}$ we obtain immediately $\mathrm{Sp}(\pi) = \mathrm{Fr}(\phi)$. In the case when $\pi = \partial\phi$ for $\phi \in \mathbf{P}(V)$, since $\mathrm{Hyp}(\pi) = \emptyset$ we obtain $\mathrm{Sp}(\pi) = \emptyset$. When $\pi = \pi_1 \oplus \pi_2$ for some $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ we have:

$$\mathrm{Sp}(\pi) \quad = \quad \mathrm{Sp}(\pi_1 \oplus \pi_2)$$

$$
\begin{array}{rcl}
 & = & \cup\{\,\mathrm{Fr}(\phi)\ :\ \phi \in \mathrm{Hyp}(\pi_1 \oplus \pi_2)\,\} \\
 & = & \cup\{\,\mathrm{Fr}(\phi)\ :\ \phi \in \mathrm{Hyp}(\pi_1) \cup \mathrm{Hyp}(\pi_2)\,\} \\
 & = & \cup(\,\{\mathrm{Fr}(\phi) : \phi \in \mathrm{Hyp}(\pi_1)\} \cup \{\mathrm{Fr}(\phi) : \phi \in \mathrm{Hyp}(\pi_2)\}\,) \\
 & = & (\cup\{\mathrm{Fr}(\phi) : \phi \in \mathrm{Hyp}(\pi_1)\}) \ \cup\ (\cup\{\mathrm{Fr}(\phi) : \phi \in \mathrm{Hyp}(\pi_2)\}) \\
 & = & \mathrm{Sp}(\pi_1) \cup \mathrm{Sp}(\pi_2)
\end{array}
$$

Finally if $\pi = \nabla x \pi_1$ for some $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ we obtain:

$$
\begin{array}{rcl}
\mathrm{Sp}(\pi) & = & \mathrm{Sp}(\nabla x \pi_1) \\
 & = & \cup\{\,\mathrm{Fr}(\phi)\ :\ \phi \in \mathrm{Hyp}(\nabla x \pi_1)\,\} \\
 & = & \cup\{\,\mathrm{Fr}(\phi)\ :\ \phi \in \mathrm{Hyp}(\pi_1)\,\} \\
 & = & \mathrm{Sp}(\pi_1)
\end{array}
$$

.

The map $\mathrm{Sp} : \mathbf{\Pi}(V) \to \mathcal{P}(V)$ is increasing with respect to the inclusion on $\mathcal{P}(V)$. So the specific variables of a sub-proof are specific variables of the proof.

Proposition 205 *Let V be a set and $\rho, \pi \in \mathbf{\Pi}(V)$. Then we have:*

$$\rho \preceq \pi \ \Rightarrow\ \mathrm{Sp}(\rho) \subseteq \mathrm{Sp}(\pi)$$

Proof
Suppose $\rho \preceq \pi$ is a sub-proof of $\pi \in \mathbf{\Pi}(V)$. Then we have:

$$
\begin{array}{rcl}
\mathrm{Sp}(\rho) & = & \mathrm{Fr}(\mathrm{Hyp}(\rho)) \\
 & = & \cup\{\mathrm{Fr}(\phi)\ :\ \phi \in \mathrm{Hyp}(\rho)\} \\
\text{prop. (192)}\ \rightarrow & \subseteq & \cup\{\mathrm{Fr}(\phi)\ :\ \phi \in \mathrm{Hyp}(\pi)\} \\
 & = & \mathrm{Fr}(\mathrm{Hyp}(\pi)) \\
 & = & \mathrm{Sp}(\pi)
\end{array}
$$

.

Let $\sigma : V \to W$ be a map and $\pi \in \mathbf{\Pi}(V)$ be a proof. Then $\sigma(\pi)$ is a proof whose specific variables are always images of specific variables of π by σ.

Proposition 206 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\pi \in \mathbf{\Pi}(V)$:*

$$\mathrm{Sp}(\sigma(\pi)) \subseteq \sigma(\mathrm{Sp}(\pi))$$

where $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ also denotes the proof substitution mapping.

Proof
There is no induction required in this case. Using definition (67) we have:

$$
\begin{array}{rcl}
\mathrm{Sp}(\sigma(\pi)) & = & \mathrm{Fr}(\,\mathrm{Hyp}(\sigma(\pi))\,) \\
\text{prop. (193)}\ \rightarrow & = & \mathrm{Fr}(\,\sigma(\mathrm{Hyp}(\pi))\,)
\end{array}
$$

$$
\begin{array}{rcl}
 & = & \cup\{\, \mathrm{Fr}(\psi) \;:\; \psi \in \sigma(\mathrm{Hyp}(\pi))\,\} \\
 & = & \cup\{\, \mathrm{Fr}(\sigma(\phi)) \;:\; \phi \in \mathrm{Hyp}(\pi)\,\} \\
\text{prop. (43)} \;\rightarrow & \subseteq & \cup\{\, \sigma(\mathrm{Fr}(\phi)) \;:\; \phi \in \mathrm{Hyp}(\pi)\,\} \\
 & = & \sigma(\,\cup\{\, \mathrm{Fr}(\phi) \;:\; \phi \in \mathrm{Hyp}(\pi)\,\}\,) \\
 & = & \sigma(\,\mathrm{Fr}(\mathrm{Hyp}(\pi))\,) \\
 & = & \sigma(\mathrm{Sp}(\pi))
\end{array}
$$

.

A specific variable of π is a variable of π. It had to be said once:

Proposition 207 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$. Then we have:*

$$\mathrm{Sp}(\pi) \subseteq \mathrm{Var}(\pi)$$

Proof
There is no induction required in this case. The proof goes as follows:

$$
\begin{array}{rcl}
\mathrm{Sp}(\pi) & = & \cup\{\, \mathrm{Fr}(\phi) \;:\; \phi \in \mathrm{Hyp}(\pi)\,\} \\
\text{prop. (48)} \;\rightarrow & \subseteq & \cup\{\, \mathrm{Var}(\phi) \;:\; \phi \in \mathrm{Hyp}(\pi)\,\} \\
\mathrm{Val}(\phi) = \phi \;\rightarrow & = & \cup\{\, \mathrm{Var}(\mathrm{Val}(\phi)) \;:\; \phi \in \mathrm{Hyp}(\pi)\,\} \\
\text{prop. (191)} \;\rightarrow & \subseteq & \cup\{\, \mathrm{Var}(\mathrm{Val}(\rho)) \;:\; \rho \preceq \pi\,\} \\
\text{prop. (203)} \;\rightarrow & \subseteq & \mathrm{Var}(\pi)
\end{array}
$$

.

3.2.7 Free Variable of a Proof

In this section we define and study the set of free variables $\mathrm{Fr}(\pi)$ of a proof $\pi \in \mathbf{\Pi}(V)$. The notion of free variables is crucial when attempting to formalize the idea of variable substitutions which avoid capture. Free variables also play a key role when considering minimal transforms which are in turn a key step in constructing essential substitutions. Essential substitutions for proofs will be shown to exist in theorem (29) of page 375. Given a proof $\pi \in \mathbf{\Pi}(V)$, the free variables of π are simply the free variables of the hypothesis and axioms of π, with the exception of generalization variables which are removed from $\mathrm{Fr}(\pi)$:

Definition 78 *Let V be a set. The map* $\mathrm{Fr} : \mathbf{\Pi}(V) \rightarrow \mathcal{P}(V)$ *defined by the following structural recursion is called* free variable mapping on $\mathbf{\Pi}(V)$*:*

$$
\forall \pi \in \mathbf{\Pi}(V)\ ,\ \mathrm{Fr}(\pi) = \left\{ \begin{array}{lll}
\mathrm{Fr}(\phi) & \textit{if} & \pi = \phi \in \mathbf{P}(V) \\
\mathrm{Fr}(\phi) & \textit{if} & \pi = \partial\phi \\
\mathrm{Fr}(\pi_1) \cup \mathrm{Fr}(\pi_2) & \textit{if} & \pi = \pi_1 \oplus \pi_2 \\
\mathrm{Fr}(\pi_1) \setminus \{x\} & \textit{if} & \pi = \nabla x \pi_1
\end{array} \right. \tag{3.12}
$$

We say that $x \in V$ is a free variable *of $\pi \in \mathbf{\Pi}(V)$ if and only if $x \in \mathrm{Fr}(\pi)$.*

Given a formula $\phi \in \mathbf{P}(V)$ the notation $\mathrm{Fr}(\phi)$ is potentially ambiguous. Since $\mathbf{P}(V) \subseteq \mathbf{\Pi}(V)$, it may refer to the usual $\mathrm{Fr}(\phi)$ of definition (28), or to the set $\mathrm{Fr}(\pi)$ where $\pi = \phi$ of definition (77). Luckily, the two notions coincide.

Proposition 208 *The structural recursion of* definition (77) *is legitimate.*

Proof
We need to show the existence and uniqueness of the map $\mathrm{Fr} : \mathbf{\Pi}(V) \to \mathcal{P}(V)$ satisfying the four conditions of equation (3.12). This follows from an application of theorem (4) of page 42 with $X = \mathbf{\Pi}(V)$, $X_0 = \mathbf{P}(V)$ and $A = \mathcal{P}(V)$ where $g_0 : X_0 \to A$ is defined as $g_0(\phi) = \mathrm{Fr}(\phi)$. Furthermore, given $\phi \in \mathbf{P}(V)$ we take $h(\partial\phi) : A^0 \to A$ defined $h(\partial\phi)(0) = \mathrm{Fr}(\phi)$. We take $h(\oplus) : A^2 \to A$ defined by $h(\oplus)(A_0, A_1) = A_0 \cup A_1$ and $h(\nabla x) : A^1 \to A$ defined by $h(\nabla x)(A_0) = A_0 \setminus \{x\}$.
.

Given a map $\sigma : V \to W$ with associated $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$, given a proof $\pi \in \mathbf{\Pi}(V)$ the free variables of the proof $\sigma(\pi)$ must be images of free variables of π by σ. The following proposition is the counterpart of proposition (43) :

Proposition 209 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\pi \in \mathbf{\Pi}(V)$:*

$$\mathrm{Fr}(\sigma(\pi)) \subseteq \sigma(\mathrm{Fr}(\pi))$$

where $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ also denotes the associated proof substitution mapping.

Proof
We shall prove the inclusion with a structural induction, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then we need to show that $\mathrm{Fr}(\sigma(\phi)) \subseteq \sigma(\mathrm{Fr}(\phi))$ which follows immediately from proposition (43). We now assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then we have:

$$\begin{array}{rcl} \mathrm{Fr}(\sigma(\pi)) & = & \mathrm{Fr}(\sigma(\partial\phi)) \\ & = & \mathrm{Fr}(\partial\sigma(\phi)) \\ & = & \mathrm{Fr}(\sigma(\phi)) \\ \text{prop. (43)} \ \to & \subseteq & \sigma(\mathrm{Fr}(\phi)) \\ & = & \sigma(\mathrm{Fr}(\partial\phi)) \\ & = & \sigma(\mathrm{Fr}(\pi)) \end{array}$$

We now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs which satisfy our inclusion. We need to show the same is true of π which goes as follows:

$$\begin{array}{rcl} \mathrm{Fr}(\sigma(\pi)) & = & \mathrm{Fr}(\sigma(\pi_1 \oplus \pi_2)) \\ & = & \mathrm{Fr}(\sigma(\pi_1) \oplus \sigma(\pi_2)) \\ & = & \mathrm{Fr}(\sigma(\pi_1)) \cup \mathrm{Fr}(\sigma(\pi_2)) \\ & \subseteq & \sigma(\mathrm{Fr}(\pi_1)) \cup \sigma(\mathrm{Fr}(\pi_2)) \end{array}$$

$$\begin{aligned} &= \sigma(\,\mathrm{Fr}(\pi_1) \cup \mathrm{Fr}(\pi_2)\,) \\ &= \sigma(\mathrm{Fr}(\pi_1 \oplus \pi_2)) \\ &= \sigma(\mathrm{Fr}(\pi)) \end{aligned}$$

Finally, we assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof satisfying our inclusion. We need to show the same is true of π:

$$\begin{aligned} \mathrm{Fr}(\sigma(\pi)) &= \mathrm{Fr}(\sigma(\nabla x \pi_1)) \\ &= \mathrm{Fr}(\,\nabla \sigma(x) \sigma(\pi_1)\,) \\ &= \mathrm{Fr}(\sigma(\pi_1)) \setminus \{\sigma(x)\} \\ &\subseteq \sigma(\mathrm{Fr}(\pi_1)) \setminus \{\sigma(x)\} \\ &= \sigma(\,\mathrm{Fr}(\pi_1) \setminus \{x\}\,) \setminus \{\sigma(x)\} \\ &\subseteq \sigma(\,\mathrm{Fr}(\pi_1) \setminus \{x\}\,) \\ &= \sigma(\mathrm{Fr}(\nabla x \pi_1)) \\ &= \sigma(\mathrm{Fr}(\pi)) \end{aligned}$$

.

The *specific variables* of a proof $\pi \in \mathbf{\Pi}(V)$ are those with respect to which generalization is not permitted. So if a proof is totally clean, it contains no flawed attempt at generalization and the specific variables remain free variables:

Proposition 210 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$ be totally clean. Then we have:*

$$\mathrm{Sp}(\pi) \subseteq \mathrm{Fr}(\pi)$$

In other words, the specific variables of π are also free variables of π.

Proof
For every proof $\pi \in \mathbf{\Pi}(V)$ we need to show the following implication:

$$(\pi \text{ totally clean}) \;\Rightarrow\; \mathrm{Sp}(\pi) \subseteq \mathrm{Fr}(\pi)$$

We shall do so with a structural induction, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then π is always totally clean in this case and we have $\mathrm{Sp}(\phi) = \mathrm{Fr}(\mathrm{Hyp}(\phi)) = \mathrm{Fr}(\{\phi\}) = \mathrm{Fr}(\phi)$. We now assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then $\mathrm{Sp}(\pi) = \emptyset$ and the implication is clearly true. So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs satisfying our implication. We need to show the same is true of π. So we assume that π is totally clean. We need to show the inclusion $\mathrm{Sp}(\pi) \subseteq \mathrm{Fr}(\pi)$. However, from proposition (182) both π_1 and π_2 are totally clean. Hence:

$$\begin{aligned} \mathrm{Sp}(\pi) &= \mathrm{Sp}(\pi_1 \oplus \pi_2) \\ \text{prop. (204)} \;\rightarrow\; &= \mathrm{Sp}(\pi_1) \cup \mathrm{Sp}(\pi_2) \end{aligned}$$

$$\begin{array}{rcl} \pi_1, \pi_2 \text{ totally clean } \rightarrow & \subseteq & \mathrm{Fr}(\pi_1) \cup \mathrm{Fr}(\pi_2) \\ & = & \mathrm{Fr}(\pi_1 \oplus \pi_2) \\ & = & \mathrm{Fr}(\pi) \end{array}$$

Note that the equality $\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \rightarrow \mathrm{Val}(\pi)$ which follows from π being totally clean, has not been used in the argument. We now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof satisfying our implication. We need to show the same is true for π. So we assume that π is totally clean. We need to show the inclusion $\mathrm{Sp}(\pi) \subseteq \mathrm{Fr}(\pi)$. However, from proposition (183) we see that π_1 is totally clean and $x \notin \mathrm{Sp}(\pi_1)$. Hence, we have:

$$\begin{array}{rcl} \mathrm{Sp}(\pi) & = & \mathrm{Sp}(\nabla x \pi_1) \\ \text{prop. (204)} \ \rightarrow & = & \mathrm{Sp}(\pi_1) \\ x \notin \mathrm{Sp}(\pi_1) \ \rightarrow & = & \mathrm{Sp}(\pi_1) \setminus \{x\} \\ \pi_1 \text{ totally clean} \ \rightarrow & \subseteq & \mathrm{Fr}(\pi_1) \setminus \{x\} \\ & = & \mathrm{Fr}(\nabla x \pi_1) \\ & = & \mathrm{Fr}(\pi) \end{array}$$

.

Just as we did for formulas, we shall need to consider congruences on $\mathbf{\Pi}(V)$. In particular, we shall introduce the *substitution congruence* on $\mathbf{\Pi}(V)$ as per definition (88). Whenever $\sim$ is a congruence on $\mathbf{\Pi}(V)$ we may wish to prove the implication $\pi \sim \rho \ \Rightarrow \ \mathrm{Fr}(\pi) = \mathrm{Fr}(\rho)$. One of the key steps in the proof is to argue that equality between sets of free variables is itself a congruence:

Proposition 211 *Let V be a set and $\equiv$ be the relation on $\mathbf{\Pi}(V)$ defined by:*

$$\pi \equiv \rho \ \Leftrightarrow \ \mathrm{Fr}(\pi) = \mathrm{Fr}(\rho)$$

for all $\pi, \rho \in \mathbf{\Pi}(V)$. Then $\equiv$ is a congruence on $\mathbf{\Pi}(V)$.

Proof
The relation $\equiv$ is clearly reflexive, symmetric and transitive on $\mathbf{\Pi}(V)$. So we simply need to show that $\equiv$ is a congruent relation on $\mathbf{\Pi}(V)$. By reflexivity, we already have $\partial\phi \equiv \partial\phi$ for all $\phi \in \mathbf{P}(V)$. So suppose π_1, π_2, ρ_1 and $\rho_2 \in \mathbf{\Pi}(V)$ are such that $\pi_1 \equiv \rho_1$ and $\pi_2 \equiv \rho_2$. Define $\pi = \pi_1 \oplus \pi_2$ and $\rho = \rho_1 \oplus \rho_2$. We need to show that $\pi \equiv \rho$, or equivalently that $\mathrm{Fr}(\pi) = \mathrm{Fr}(\rho)$. This follows from the fact that $\mathrm{Fr}(\pi_1) = \mathrm{Fr}(\rho_1)$, $\mathrm{Fr}(\pi_2) = \mathrm{Fr}(\rho_2)$ and furthermore:

$$\begin{array}{rcl} \mathrm{Fr}(\pi) & = & \mathrm{Fr}(\pi_1 \oplus \pi_2) \\ & = & \mathrm{Fr}(\pi_1) \cup \mathrm{Fr}(\pi_2) \\ & = & \mathrm{Fr}(\rho_1) \cup \mathrm{Fr}(\rho_2) \\ & = & \mathrm{Fr}(\rho_1 \oplus \rho_2) \\ & = & \mathrm{Fr}(\rho) \end{array}$$

We now assume that $\pi_1, \rho_1 \in \mathbf{\Pi}(V)$ are such that $\pi_1 \equiv \rho_1$. Let $x \in V$ and define $\pi = \nabla x \pi_1$ and $\rho = \nabla x \rho_1$. We need to show that $\pi \equiv \rho$, or equivalently that $\mathrm{Fr}(\pi) = \mathrm{Fr}(\rho)$. This follows from the fact that $\mathrm{Fr}(\pi_1) = \mathrm{Fr}(\rho_1)$ and:

$$\mathrm{Fr}(\pi) = \mathrm{Fr}(\nabla x \pi_1) = \mathrm{Fr}(\pi_1) \setminus \{x\} = \mathrm{Fr}(\rho_1) \setminus \{x\} = \mathrm{Fr}(\nabla x \rho_1) = \mathrm{Fr}(\rho)$$

.

3.2.8 Bound Variable of a Proof

In this section we define and study the set $\mathrm{Bnd}(\pi)$ of bound variables of a proof $\pi \in \mathbf{\Pi}(V)$. The notion of bound variables has proved particularly useful when dealing with the local inversion theorem (10) of page 105 for formulas. A counterpart of this theorem for proofs will be established as theorem (25) of page 345. The set of bound variables is also important in giving us a useful test for valid substitutions in the form of proposition (60) for which a counterpart shall be established for proofs as proposition (228). The bound variables of a proof π are simply the bound variables of the hypothesis and axioms of π, to which is added every variable occurring in the use of generalization.

Definition 79 *Let V be a set. The map* $\mathrm{Bnd} : \mathbf{\Pi}(V) \to \mathcal{P}(V)$ *defined by the following structural recursion is called* bound variable mapping on $\mathbf{\Pi}(V)$*:*

$$\forall \pi \in \mathbf{\Pi}(V) \ , \ \mathrm{Bnd}(\pi) = \begin{cases} \mathrm{Bnd}(\phi) & \text{if} \quad \pi = \phi \in \mathbf{P}(V) \\ \mathrm{Bnd}(\phi) & \text{if} \quad \pi = \partial \phi \\ \mathrm{Bnd}(\pi_1) \cup \mathrm{Bnd}(\pi_2) & \text{if} \quad \pi = \pi_1 \oplus \pi_2 \\ \{x\} \cup \mathrm{Bnd}(\pi_1) & \text{if} \quad \pi = \nabla x \pi_1 \end{cases} \tag{3.13}$$

We say that $x \in V$ is a bound variable *of $\pi \in \mathbf{\Pi}(V)$ if and only if $x \in \mathrm{Bnd}(\pi)$.*

Given a formula $\phi \in \mathbf{P}(V)$ the notation $\mathrm{Bnd}(\phi)$ is potentially ambiguous. Since $\mathbf{P}(V) \subseteq \mathbf{\Pi}(V)$, it may refer to the usual $\mathrm{Bnd}(\phi)$ of definition (29), or to the set $\mathrm{Bnd}(\pi)$ where $\pi = \phi$ of definition (78). Luckily, the two notions coincide.

Proposition 212 *The structural recursion of* definition (78) *is legitimate.*

Proof
We need to show the existence and uniqueness of the map $\mathrm{Bnd} : \mathbf{\Pi}(V) \to \mathcal{P}(V)$ satisfying the four conditions of equation (3.13). This follows from an application of theorem (4) of page 42 with $X = \mathbf{\Pi}(V)$, $X_0 = \mathbf{P}(V)$ and $A = \mathcal{P}(V)$ where $g_0 : X_0 \to A$ is defined as $g_0(\phi) = \mathrm{Bnd}(\phi)$. Furthermore, given $\phi \in \mathbf{P}(V)$ we take $h(\partial\phi) : A^0 \to A$ defined $h(\partial\phi)(0) = \mathrm{Bnd}(\phi)$. We take $h(\oplus) : A^2 \to A$ defined by $h(\oplus)(A_0, A_1) = A_0 \cup A_1$ and $h(\nabla x) : A^1 \to A$ defined by $h(\nabla x)(A_0) = \{x\} \cup A_0$. ■

The free and bound variables of a proof $\pi \in \mathbf{\Pi}(V)$ are variables of π, as we would expect. In fact, every variable of π is either free or bound, or both free and bound. The following proposition is the counterpart of proposition (48) :

Proposition 213 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$. Then we have:*

$$\mathrm{Var}(\pi) = \mathrm{Fr}(\pi) \cup \mathrm{Bnd}(\pi) \tag{3.14}$$

Proof
We shall prove the equality with a structural induction, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then the equality follows immediately from proposition (48). We now assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then using proposition (48) once more, we have:

$$\begin{array}{rcl} \mathrm{Var}(\pi) & = & \mathrm{Var}(\partial\phi) \\ & = & \mathrm{Var}(\phi) \\ \text{prop. (48)} \ \rightarrow & = & \mathrm{Fr}(\phi) \cup \mathrm{Bnd}(\phi) \\ & = & \mathrm{Fr}(\partial\phi) \cup \mathrm{Bnd}(\partial\phi) \\ & = & \mathrm{Fr}(\pi) \cup \mathrm{Bnd}(\pi) \end{array}$$

So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs satisfying the equality. We need to show that same is true of π which goes as follows:

$$\begin{array}{rcl} \mathrm{Var}(\pi) & = & \mathrm{Var}(\pi_1 \oplus \pi_2) \\ & = & \mathrm{Var}(\pi_1) \cup \mathrm{Var}(\pi_2) \\ & = & \mathrm{Fr}(\pi_1) \cup \mathrm{Bnd}(\pi_1) \cup \mathrm{Fr}(\pi_2) \cup \mathrm{Bnd}(\pi_2) \\ & = & \mathrm{Fr}(\pi_1 \oplus \pi_2) \cup \mathrm{Bnd}(\pi_1 \oplus \pi_2) \\ & = & \mathrm{Fr}(\pi) \cup \mathrm{Bnd}(\pi) \end{array}$$

We now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof satisfying our equality. We need to show the same is true of π which goes as follows:

$$\begin{array}{rcl} \mathrm{Var}(\pi) & = & \mathrm{Var}(\nabla x \pi_1) \\ & = & \{x\} \cup \mathrm{Var}(\pi_1) \\ & = & \{x\} \cup \mathrm{Fr}(\pi_1) \cup \mathrm{Bnd}(\pi_1) \\ & = & (\mathrm{Fr}(\pi_1) \setminus \{x\}) \cup \{x\} \cup \mathrm{Bnd}(\pi_1) \\ & = & \mathrm{Fr}(\nabla x \pi_1) \cup \mathrm{Bnd}(\nabla x \pi_1) \\ & = & \mathrm{Fr}(\pi) \cup \mathrm{Bnd}(\pi) \end{array}$$

.

The map $\mathrm{Bnd} : \mathbf{\Pi}(V) \rightarrow \mathcal{P}(V)$ is increasing with respect to the standard inclusion on $\mathcal{P}(V)$. In other words, the bound variables of a sub-proof are also bound variables of the proof itself, a property which does not hold for free variables. The following is the counterpart of proposition (49) :

Proposition 214 *Let V be a set and $\pi, \rho \in \mathbf{\Pi}(V)$. Then we have:*

$$\rho \preceq \pi \ \Rightarrow \ \mathrm{Bnd}(\rho) \subseteq \mathrm{Bnd}(\pi)$$

Proof
This follows from an application of proposition (25) to $\mathrm{Bnd} : X \to A$ where $X = \mathbf{\Pi}(V)$ and $A = \mathcal{P}(V)$ where the preorder $\leq$ on A is the usual inclusion $\subseteq$. We simply need to check that given $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ and $x \in V$ we have the inclusions $\mathrm{Bnd}(\pi_1) \subseteq \mathrm{Bnd}(\pi_1 \oplus \pi_2)$, $\mathrm{Bnd}(\pi_2) \subseteq \mathrm{Bnd}(\pi_1 \oplus \pi_2)$ and $\mathrm{Bnd}(\pi_1) \subseteq \mathrm{Bnd}(\nabla x \pi_1)$ which follow from the recursive definition (78). **.**

Given a map $\sigma : V \to W$ and $\pi \in \mathbf{\Pi}(V)$, the bound variables of the proof $\sigma(\pi)$ are the images by σ of the bound variables of π. A similar result for free variables cannot be stated, unless the substitution σ is valid for π, as will be seen from proposition (223). In general, only the inclusion $\mathrm{Fr}(\sigma(\pi)) \subseteq \sigma(\mathrm{Fr}(\pi))$ is true. The following is the counterpart of proposition (50) :

Proposition 215 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\pi \in \mathbf{\Pi}(V)$:*

$$\mathrm{Bnd}(\sigma(\pi)) = \sigma(\mathrm{Bnd}(\pi))$$

where $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ also denotes the associated proof substitution mapping.

Proof
We shall prove this equality with a structural induction, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then we need to show that $\mathrm{Bnd}(\sigma(\phi)) = \sigma(\mathrm{Bnd}(\phi))$ which follows from proposition (50). Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then we have:

$$\begin{array}{rcl}
\mathrm{Bnd}(\sigma(\pi)) & = & \mathrm{Bnd}(\sigma(\partial\phi)) \\
& = & \mathrm{Bnd}(\partial\sigma(\phi)) \\
& = & \mathrm{Bnd}(\sigma(\phi)) \\
\text{prop. (50)} \ \to & = & \sigma(\mathrm{Bnd}(\phi)) \\
& = & \sigma(\mathrm{Bnd}(\partial\phi)) \\
& = & \sigma(\mathrm{Bnd}(\pi))
\end{array}$$

We now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs satisfying our equality. We need to show the same is true of π which goes as follows:

$$\begin{array}{rcl}
\mathrm{Bnd}(\sigma(\pi)) & = & \mathrm{Bnd}(\sigma(\pi_1 \oplus \pi_2)) \\
& = & \mathrm{Bnd}(\sigma(\pi_1) \oplus \sigma(\pi_2)) \\
& = & \mathrm{Bnd}(\sigma(\pi_1)) \cup \mathrm{Bnd}(\sigma(\pi_2)) \\
& = & \sigma(\mathrm{Bnd}(\pi_1)) \cup \sigma(\mathrm{Bnd}(\pi_2)) \\
& = & \sigma(\,\mathrm{Bnd}(\pi_1) \cup \mathrm{Bnd}(\pi_2)\,) \\
& = & \sigma(\mathrm{Bnd}(\pi_1 \oplus \pi_2)) \\
& = & \sigma(\mathrm{Bnd}(\pi))
\end{array}$$

Finally, we assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof satisfying our equality. We need to show the same is true of π:

$$\begin{aligned}
\mathrm{Bnd}(\sigma(\pi)) &= \mathrm{Bnd}(\sigma(\nabla x \pi_1)) \\
&= \mathrm{Bnd}(\, \nabla \sigma(x) \sigma(\pi_1)\,) \\
&= \{\sigma(x)\} \cup \mathrm{Bnd}(\sigma(\pi_1)) \\
&= \{\sigma(x)\} \cup \sigma(\mathrm{Bnd}(\pi_1)) \\
&= \sigma(\,\{x\} \cup \mathrm{Bnd}(\pi_1)\,) \\
&= \sigma(\mathrm{Bnd}(\nabla x \pi_1)) \\
&= \sigma(\mathrm{Bnd}(\pi))
\end{aligned}$$

.

3.2.9 Valid Substitution of Variable in Proof

In definition (30) we defined what it meant for a substitution $\sigma : V \to W$ to be valid for a formula $\phi \in \mathbf{P}(V)$. We needed to introduce the notion that σ would not randomly distort the *logical structure* of ϕ, a property which is commonly known as *avoiding capture*. The purpose was obvious: we wanted to *carry over* properties of $\phi \in \mathbf{P}(V)$ into corresponding properties of $\sigma(\phi) \in \mathbf{P}(W)$. For example, theorem (15) of page 152 tells us that a substitution equivalence $\phi \sim \psi$ is preserved by σ provided it is valid for both ϕ and ψ. Another example will be seen as the *substitution lemma* in the context of model theory, where proposition (323) will show that if σ is valid for ϕ, then the truth of $\sigma(\phi)$ in a model M under an assignment $a : W \to M$ is equivalent to the truth of ϕ under the assignment $a \circ \sigma$. The notion of σ being valid for ϕ is crucially important.

One of the most interesting properties of formulas which we may wish to *carry over* is that of provability. If a sequent $\Gamma \vdash \phi$ is true, we all want to know under what conditions the corresponding sequent $\sigma(\Gamma) \vdash \sigma(\phi)$ is also true. It is very tempting to conjecture that provided σ is valid for ϕ and is also valid for every hypothesis $\psi \in \Gamma$, then the result will hold. Of course, an obvious issue is the fact that a sequent $\Gamma \vdash \phi$ does not tell us anything about the axioms being used in a proof underlying the sequent. So we cannot hope to simply *carry over* every step of the proof with σ, as our assumption does not guarantee σ is valid for every axiom involved in the proof. It only guarantees σ is valid for the conclusion, and for every hypothesis. In fairness, this issue only arises because we stubbornly insist on working with actual maps $\sigma : V \to W$, rather than essential substitutions $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ of definition (44). We know essential substitutions are the right concept. We somehow suspect our scheme to *carry over* proofs with the substitution $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ of definition (74) is most likely a waste of time. We should *carry over* proofs using essential substitutions only. There is however one thing to remember: from theorem (18) of page 174 an essential substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ can only exist if W is an infinite set, or V is a smaller set than W. So if we restrict our analysis to essential

substitutions, we cannot hope to *carry over* the sequent $\Gamma \vdash \phi$ into $\sigma(\Gamma) \vdash \sigma(\phi)$ in the case when W is a finite set of smaller cardinality than V.

We are certainly interested in saying something about $\sigma(\Gamma) \vdash \sigma(\phi)$ in the case when W is a smaller finite set. For example, suppose we have an embedding $j : W \to V$ between two finite sets, and Δ is a consistent subset of $\mathbf{P}(W)$. We certainly hope that $\Gamma = j(\Delta)$ is a consistent subset of $\mathbf{P}(V)$. If Γ is not consistent, as we shall see from definition (99) the sequent $\Gamma \vdash \bot$ is true. Assuming $W \neq \emptyset$ and j has a left inverse $\sigma : V \to W$, here is a case when we want to *carry over* the sequent $\Gamma \vdash \bot$ into a smaller finite set W: we want to argue that $\sigma(\Gamma) \vdash \bot$ is true so as to obtain $\Delta \vdash \bot$, contradicting the consistency of Δ. Most proofs of Gödel completeness theorem involve successive embeddings where constants are continually added to the language, and it is usually taken for granted that consistency is preserved as the language is extended. This is not completely obvious for us. We do not have constants, but only variables. As the set of variables is increased, the range of possible proofs becomes larger and it is conceivable that a contradiction may appear. In general, it is not clear that a sequent $j(\Delta) \vdash j(\phi)$ can be transported back into the smaller finite set, as the variables involved in the axioms may have no obvious counterpart in W.

In any case, although we strongly suspect essential substitutions will play an important role in allowing us to *carry over* sequents, we should not attempt to run before we can walk: when attempting to establish the sequent $\sigma(\Gamma) \vdash \sigma(\phi)$ we should start with the obvious, and the obvious consists in following every step of the proof underlying $\Gamma \vdash \phi$, and replacing all variables in line with the substitution σ. This is the purpose of definition (74), creating $\sigma(\pi) \in \mathbf{\Pi}(W)$ from $\pi \in \mathbf{\Pi}(V)$, in the hope that $\sigma(\pi)$ will become a proof of $\sigma(\phi)$, from the set of hypothesis $\sigma(\Gamma)$. Of course, this is not going to work in all cases. The proof $\sigma(\pi)$ is pretty worthless, unless we control its valuation $\mathrm{Val}(\sigma(\pi))$, that is:

$$\mathrm{Val} \circ \sigma(\pi) = \sigma \circ \mathrm{Val}(\pi) \tag{3.15}$$

It is clear equation (3.15) will fail unless $\sigma : V \to W$ has the right properties in relation to π. For example, if $\pi = \partial\phi$ where $\phi \in \mathbf{A}(V)$ is an axiom of first order logic, then $\sigma(\pi) = \partial\sigma(\phi)$ and if $\sigma(\phi)$ fails to be an axiom, then from definition (69) we obtain $\mathrm{Val} \circ \sigma(\pi) = \bot \to \bot$. So equation (3.15) will fail unless $\sigma(\phi)$ is itself an axiom. We shall see later in lemma (19) that $\sigma(\phi)$ is indeed an axiom, provided σ is valid for ϕ. It is not difficult to design a counterexample otherwise. So here is a case when the condition *σ is valid for ϕ* is a key condition to ensure that equation (3.15) is met by $\pi = \partial\phi$, at least in the case when π is totaly clean, that is when ϕ is an axiom. In our discussion preceding definition (73) we explained the importance of π being totally clean.

In this section, we want to define what it is for σ to be *valid for* π. Our purpose to the design the right conditions so as to ensure equation (3.15) will hold, whenever π is totally clean and σ is *valid for* π. The result will be proved in proposition (229). Choosing the right conditions which should be met by a substitution σ which is valid for a proof π is not completely obvious. We have seen that equation (3.15) plays a key role and we want σ to be valid

for ϕ whenever ϕ is an axiom of π. This will be imposed by condition (ii) of definition (79) below. Now given $\phi \in \mathrm{Hyp}(\pi)$, should we impose that σ be valid for ϕ? Yes, we should! Although it is possible to obtain a proof $\sigma(\pi)$ which satisfies equation (3.15) without requesting that σ be valid for every hypothesis of π, another consideration comes to mind: since $\mathbf{P}(V) \subseteq \mathbf{\Pi}(V)$ the mathematical statement 'σ is valid for ϕ' will become ambiguous after we define the notion of validity for proofs. What we certainly want to avoid, is designing a concept of *validity* for proof whereby 'σ is valid for ϕ' has a different meaning depending on whether ϕ is viewed as a formula or as a proof. So σ has to be valid for every $\phi \in \mathrm{Hyp}(\pi)$. This will be imposed by condition (i) of definition (79) below. Now the real essence of *validity* is the idea that a substitution should be *capture-avoiding*. This idea is somehow very general and relevant to every formal language with variable binding. We have formalized this idea for first order logic within the restricted language $\mathbf{P}(V)$, using definition (30). We now want to express the same idea in the formal language of Hilbert style proofs $\mathbf{\Pi}(V)$. We could equally do so for untyped λ-calculus and many other cases. Somehow, we know the analysis should be carried out in a general setting and with the right degree of abstraction. We have failed to provide this so far, leading to all sorts of tedious repetitions whereby simple results established for formulas are extended to proofs. For our defense, the situation is not as clear cut as it may appear: although there is an obvious syntactic parallel between $\mathbf{P}(V)$ and $\mathbf{\Pi}(V)$ with the constant operator $\bot$ versus $\partial\phi$, the binary operator $\to$ versus $\oplus$ and unary quantifications $\forall x$ versus ∇x, the generator of the free universal algebra $\mathbf{\Pi}(V)$ is the algebra $\mathbf{P}(V)$ itself, on which a lot of structure has already been defined. So when it comes to defining the notion of *validity* for proofs, we cannot simply re-use the idea of definition (30). We need to impose further conditions which are (i) and (ii) of definition (79) below. However, the idea of definition (30) is certainly fundamental and should be retained for the purpose of definition (79): if a substitution $\sigma : V \to W$ is *capture-avoiding* with respect to a proof $\pi \in \mathbf{\Pi}(V)$, any free variable of any sub-proof should remain free after substitution. This will be imposed by condition (iii) below:

Definition 80 *Let V and W be sets and $\sigma : V \to W$ be a map. Then σ is said to be* valid for $\pi \in \mathbf{\Pi}(V)$*, if and only if for all $\phi \in \mathbf{P}(V)$ and $\rho \in \mathbf{\Pi}(V)$:*

$$\begin{array}{ll} (i) & \phi \in \mathrm{Hyp}(\pi) \;\Rightarrow\; \sigma \textit{ valid for } \phi \\ (ii) & \phi \in \mathrm{Ax}(\pi) \;\Rightarrow\; \sigma \textit{ valid for } \phi \\ (iii) & \rho \preceq \pi \;\Rightarrow\; \forall u \,[\, u \in \mathrm{Fr}(\rho) \;\Rightarrow\; \sigma(u) \in \mathrm{Fr}(\sigma(\rho)) \,] \end{array}$$

Let $\sigma : V \to W$ be a map and $\phi \in \mathbf{P}(V)$. Since $\mathbf{P}(V) \subseteq \mathbf{\Pi}(V)$, the mathematical statement 'σ *is valid for* ϕ' has become ambiguous, as it may refer to this new definition (79) or to the usual definition (30). Luckily, as the next proposition shows, the two definitions lead to equivalent statements. The next proposition states that σ is valid for π if and only if it is valid for ϕ, whenever $\pi = \phi$. This seems rather tautological but of course it is not, as the two sides of the equivalence refer to definition (79) and definition (30) :

Proposition 216 *Let V, W be sets and $\sigma : V \to W$ be a map. Let π be of the form $\pi = \phi \in \mathbf{P}(V)$. Then σ is valid for π if and only if it is valid for ϕ.*

Proof
Suppose σ is valid for $\pi = \phi$. Since $\phi \in \mathrm{Hyp}(\pi)$ we see that σ is valid for ϕ. Conversely, suppose σ is valid for ϕ. We need to show that σ is valid for π. So suppose $\psi \in \mathrm{Hyp}(\pi)$. We need to show that σ is valid for ψ. However, $\mathrm{Hyp}(\pi) = \{\phi\}$ and consequently $\psi = \phi$. So σ is indeed valid for ψ. Furthermore since $\mathrm{Ax}(\pi) = \emptyset$, property (ii) of definition (79) is vacuously true. So we now check property (iii): so let $\rho \preceq \pi$ and $u \in \mathrm{Fr}(\rho)$. We need to show that $\sigma(u) \in \mathrm{Fr}(\sigma(\rho))$. However since $\pi = \phi \in \mathbf{P}(V)$, from definition (19) we have $\mathrm{Sub}(\pi) = \{\pi\}$. In other words, the only sub-proof of π is π itself. It follows that $\rho = \phi$ and we need to check that $\sigma(u) \in \mathrm{Fr}(\sigma(\phi))$ knowing that $u \in \mathrm{Fr}(\phi)$. This follows from definition (30) and the assumption that σ is valid for ϕ. **.**

A map $\sigma : V \to W$ is valid for π if and only if it is valid for every sub-proof of π. This property is similar to that encountered with formulas, as described in proposition (51). However as already pointed out, sub-formulas and sub-proofs are two different things. If $\phi \in \mathbf{P}(V)$, then it may have many sub-formulas but only one sub-proof, namely itself. The notion of sub-formula or sub-proof in a free universal algebra is formally introduced in definition (19) of page 57.

Proposition 217 *Let V, W be sets and $\sigma : V \to W$ be a map. Then σ is valid for $\pi \in \mathbf{\Pi}(V)$ if and only if it is valid for any sub-proof $\rho \preceq \pi$ of the proof π.*

Proof
If σ is valid for any sub-proof of π, then in particular it is valid for π. So we assume that σ is valid for π and consider a sub-proof $\rho \preceq \pi$. We need to show that σ is also valid for ρ. So suppose $\phi \in \mathrm{Hyp}(\rho) \cup \mathrm{Ax}(\rho)$. We need to show that σ is valid for ϕ. However, from proposition (192) and (196) we have the inclusions $\mathrm{Hyp}(\rho) \subseteq \mathrm{Hyp}(\pi)$ and $\mathrm{Ax}(\rho) \subseteq \mathrm{Ax}(\pi)$. It follows that $\phi \in \mathrm{Hyp}(\pi) \cup \mathrm{Ax}(\pi)$. Since σ is valid for π we see that σ is valid for ϕ. We now assume that $\kappa \preceq \rho$. Given $u \in \mathrm{Fr}(\kappa)$, we need to show that $\sigma(u) \in \mathrm{Fr}(\sigma(\kappa))$. However, this follows immediately from the validity of σ for π and the fact, by transitivity, that $\kappa \preceq \pi$.
.

Whenever $\pi = \partial\phi$ the validity of σ for π is equivalent to that of σ for ϕ. This property is of course natural but also crucial to guarantee the equality $\mathrm{Val} \circ \sigma(\pi) = \sigma \circ \mathrm{Val}(\pi)$ whenever ϕ is an axiom of first order logic and σ is valid for $\pi = \partial\phi$. Fundamentally, the image $\sigma(\phi)$ of an axiom by a valid substitution remains an axiom of first order logic, as will be seen from lemma (19).

Proposition 218 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\pi = \partial\phi$, where $\phi \in \mathbf{P}(V)$. Then σ is valid for π if and only if it is valid for ϕ.*

Proof
Suppose σ is valid for $\pi = \partial\phi$. Since $\phi \in \mathrm{Ax}(\pi)$ we see that σ is valid for ϕ. Conversely, suppose σ is valid for ϕ. We need to show that σ is valid for π. Since $\mathrm{Hyp}(\pi) = \emptyset$, property (i) of definition (79) is vacuously true. So we

now check property (ii): suppose $\psi \in \mathrm{Ax}(\pi)$. We need to show that σ is valid for ψ. However, $\mathrm{Ax}(\pi) = \{\phi\}$ and consequently $\psi = \phi$. So σ is indeed valid for ψ. We now check property (iii): Let $\rho \preceq \pi$ and $u \in \mathrm{Fr}(\rho)$. We need to show that $\sigma(u) \in \mathrm{Fr}(\sigma(\rho))$. However, from definition (19) we have $\mathrm{Sub}(\pi) = \mathrm{Sub}(\partial\phi(0)) = \{\partial\phi(0)\} = \{\pi\}$. In other words, the only sub-proof of π is π itself. It follows that $\rho = \pi = \partial\phi$. So we need to show that $\sigma(u) \in \mathrm{Fr}(\sigma(\phi))$ knowing that $u \in \mathrm{Fr}(\phi)$. This follows from the validity of σ for ϕ. .

Just as in the case of formulas with proposition (54) and proposition (55) which established a link between the validity of σ for $\phi = \phi_1 \to \phi_2$ or $\phi = \forall x\phi_1$ with the validity of σ for ϕ_1 and ϕ_2, we need to have a similar link between the validity of σ for $\pi = \pi_1 \oplus \pi_2$ or $\pi = \nabla x\pi_1$, with the validity of σ for π_1 and π_2. These results are very useful to carry out structural induction arguments.

Proposition 219 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$. Then σ valid for π if and only if it is valid for π_1 and π_2.*

Proof
First we show the 'only if' part: so we assume that σ is valid for $\pi = \pi_1 \oplus \pi_2$. From proposition (217) it is therefore valid for every sub-proof of π. Since $\pi_1 \preceq \pi$ and $\pi_2 \preceq \pi$ we conclude that σ is valid for both π_1 and π_2. We now show the 'if' part: so we assume that σ is valid for π_1 and π_2. We need to show that σ is valid for $\pi = \pi_1 \oplus \pi_2$. So let $\phi \in \mathrm{Hyp}(\pi)$. We need to show that σ is valid for ϕ. However $\mathrm{Hyp}(\pi) = \mathrm{Hyp}(\pi_1) \cup \mathrm{Hyp}(\pi_2)$. So ϕ is an element of $\mathrm{Hyp}(\pi_1)$ or $\mathrm{Hyp}(\pi_2)$ and in both cases we see that σ is valid for ϕ. So we now assume that $\phi \in \mathrm{Ax}(\pi)$. We need to show that σ is valid for ϕ. Once again, since $\mathrm{Ax}(\pi) = \mathrm{Ax}(\pi_1) \cup \mathrm{Ax}(\pi_2)$ the formula ϕ must be an element of $\mathrm{Ax}(\pi_1)$ or $\mathrm{Ax}(\pi_2)$. Either way, we see that σ is valid for ϕ. In order to show that σ is valid for π, it remains to show that (iii) of definition (79) is satisfied. So let $\rho \preceq \pi$ and $u \in \mathrm{Fr}(\rho)$. We need to show that $\sigma(u) \in \mathrm{Fr}(\sigma(\rho))$. If $\rho \preceq \pi_1$ or $\rho \preceq \pi_2$, then this follows immediately from the validity of σ for π_1 or π_2. So we assume that $\rho = \pi_1 \oplus \pi_2$. Then $\mathrm{Fr}(\rho) = \mathrm{Fr}(\pi_1) \cup \mathrm{Fr}(\pi_2)$ and we shall distinguish two cases: first we assume that $u \in \mathrm{Fr}(\pi_1)$. Then from the validity of σ for π_1 :

$$\begin{aligned}
\sigma(u) &\in \mathrm{Fr}(\sigma(\pi_1)) \\
&\subseteq \mathrm{Fr}(\sigma(\pi_1)) \cup \mathrm{Fr}(\sigma(\pi_2)) \\
&= \mathrm{Fr}(\,\sigma(\pi_1) \oplus \sigma(\pi_2)\,) \\
&= \mathrm{Fr}(\sigma(\pi_1 \oplus \pi_2)) \\
&= \mathrm{Fr}(\sigma(\rho))
\end{aligned}$$

Next we assume $u \in \mathrm{Fr}(\pi_2)$ and in identical fashion we obtain $\sigma(u) \in \mathrm{Fr}(\sigma(\rho))$. .

Proposition 220 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\pi = \nabla x\pi_1$. Then σ is valid for π if and only if it is valid for π_1 and for all $u \in V$:*

$$u \in \mathrm{Fr}(\nabla x\pi_1) \;\Rightarrow\; \sigma(u) \neq \sigma(x) \tag{3.16}$$

Proof
First we show the 'only if' part: so we assume that σ is valid for the proof $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$. From proposition (217), σ is valid for $\pi_1 \preceq \pi$. So it remains to show that the implication (3.16) holds. So suppose $u \in \mathrm{Fr}(\nabla x \pi_1)$. We need to show that $\sigma(u) \neq \sigma(x)$. However since π is a sub-proof of itself, having assumed that σ is valid for π we obtain:

$$\begin{aligned} \sigma(u) &\in \mathrm{Fr}(\sigma(\pi)) \\ &= \mathrm{Fr}(\, \sigma(\nabla x \pi_1)\,) \\ &= \mathrm{Fr}(\, \nabla \sigma(x) \sigma(\pi_1)\,) \\ &= \mathrm{Fr}(\sigma(\pi_1)) \setminus \{\sigma(x)\} \end{aligned}$$

In particular we have $\sigma(u) \neq \sigma(x)$. We now show the 'if' part: so we assume that σ is valid for π_1 and furthermore that (3.16) holds. We need to show that σ is valid for π. So let $\phi \in \mathrm{Hyp}(\pi) \cup \mathrm{Ax}(\pi)$. We need to show that σ is valid for ϕ. However, we have $\mathrm{Hyp}(\pi) = \mathrm{Hyp}(\pi_1)$ and $\mathrm{Ax}(\pi) = \mathrm{Ax}(\pi_1)$ and consequently $\phi \in \mathrm{Hyp}(\pi_1) \cup \mathrm{Ax}(\pi_1)$. Having assumed that σ is valid for π_1, it follows that σ is valid for ϕ as requested. In order to show that σ is valid for π, it remains to prove that (iii) of definition (79) holds. So let $\rho \preceq \pi$ and $u \in \mathrm{Fr}(\rho)$. We need to show that $\sigma(u) \in \mathrm{Fr}(\sigma(\rho))$. If $\rho \preceq \pi_1$ then this follows immediately from the validity of σ for π_1. So we assume that $\rho = \nabla x \pi_1$ in which case $u \in \mathrm{Fr}(\nabla x \pi_1)$. We need to show that $\sigma(u) \in \mathrm{Fr}(\sigma(\nabla x \pi_1)) = \mathrm{Fr}(\sigma(\pi_1)) \setminus \{\sigma(x)\}$. Having assumed that (3.16) holds, we already know that $\sigma(u) \neq \sigma(x)$. So it remains to show that $\sigma(u) \in \mathrm{Fr}(\sigma(\pi_1))$ which follows from the validity of σ for π_1. .

The following proposition is the counterpart of proposition (56) which was established for formulas. It offers a simpler criterion to establish validity. When attempting to prove (iii) of definition (79), it is no longer necessary to consider every sub-proof $\rho \preceq \pi$ and we can instead restrict our attention to sub-proofs of the form $\rho = \nabla x \pi_1$. Furthermore, rather than prove $\sigma(u) \in \mathrm{Fr}(\sigma(\rho))$ whenever $u \in \mathrm{Fr}(\rho)$, it is sufficient to prove the simpler property $\sigma(u) \neq \sigma(x)$.

Proposition 221 *Let V and W be sets and $\sigma : V \to W$ be a map. Then σ is* valid for $\pi \in \mathbf{\Pi}(V)$ *if and only if for all $\phi \in \mathbf{P}(V)$, $\pi_1 \in \mathbf{\Pi}(V)$ and $x \in V$:*

$$\begin{aligned} &(i) && \phi \in \mathrm{Hyp}(\pi) \;\Rightarrow\; \sigma \textit{ valid for } \phi \\ &(ii) && \phi \in \mathrm{Ax}(\pi) \;\Rightarrow\; \sigma \textit{ valid for } \phi \\ &(iii) && \nabla x \pi_1 \preceq \pi \;\Rightarrow\; \forall u \,[\; u \in \mathrm{Fr}(\nabla x \pi_1) \;\Rightarrow\; \sigma(u) \neq \sigma(x) \;] \end{aligned}$$

Proof
First we show the 'only if' part. So we assume that σ is valid for π. Then (i) and (ii) are satisfied by definition and we simply need to prove (iii). So we assume that $\nabla x \pi_1 \preceq \pi$ and $u \in \mathrm{Fr}(\nabla x \pi_1)$. We need to show $\sigma(u) \neq \sigma(x)$. However, from proposition (217) we see that σ is valid for $\nabla x \pi_1$. Having assumed that

$u \in \mathrm{Fr}(\nabla x \pi_1)$ we must have $\sigma(u) \in \mathrm{Fr}(\sigma(\nabla x \pi_1)) = \mathrm{Fr}(\sigma(\pi_1)) \setminus \{\sigma(x)\}$. It follows in particular that $\sigma(u) \neq \sigma(x)$ as requested. We now show the 'if' part: for every proof $\pi \in \mathbf{\Pi}(V)$ we need to show the following implication:

$$(i) + (ii) + (iii) \;\Rightarrow\; \sigma \text{ valid for } \pi$$

We shall do so with a structural induction, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. We need to show our implication is true for π. So we assume that (i), (ii) and (iii) hold. We need to show that σ is valid for ϕ. This follows immediately from (i) and the fact that $\phi \in \mathrm{Hyp}(\pi) = \{\phi\}$. So we now assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. We need to show our implication is true for π. So we assume that (i), (ii) and (iii) hold. We need to show that σ is valid for π. From proposition (218), we simply need to show that σ is valid for ϕ, which follows from (ii) and the fact that $\phi \in \mathrm{Ax}(\pi) = \{\phi\}$. We now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs satisfying our implication. We need to show the same is true of π. So we assume that (i), (ii) and (iii) hold for π. We need to show that σ is valid for π. Using proposition (219) it is sufficient to show that σ is valid for π_1 and π_2. Having assumed our implication is true for π_1 and π_2, we simply need to prove that (i), (ii) and (iii) hold for π_1 and π_2. First we deal with π_1 : the fact that (i) holds for π_1 follows from $\mathrm{Hyp}(\pi_1) \subseteq \mathrm{Hyp}(\pi)$ and the fact that (i) is true for π. Note that $\mathrm{Hyp}(\pi_1) \subseteq \mathrm{Hyp}(\pi)$ is a consequence of $\pi_1 \preceq \pi$ and proposition (192). The fact that (ii) holds for π_1 follows from $\mathrm{Ax}(\pi_1) \subseteq \mathrm{Ax}(\pi)$ and the fact that (ii) is true for π. Note that $\mathrm{Ax}(\pi_1) \subseteq \mathrm{Ax}(\pi)$ is a consequence of $\pi_1 \preceq \pi$ and proposition (196). The fact that (iii) holds for π_1 follows from $\pi_1 \preceq \pi$ and the transitivity of the sub-proof partial order $\preceq$ on $\mathbf{\Pi}(V)$, as well as the fact that (iii) is true for π. The case of π_2 is dealt with similarly. This completes our induction argument in the case when $\pi = \pi_1 \oplus \pi_2$. So we now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof satisfying our implication. We need to show the same is true for π. So we assume that (i), (ii) and (iii) hold for π. We need to show that σ is valid for π. Using proposition (220) it is sufficient to show that σ is valid for π_1 and furthermore, given $u \in V$:

$$u \in \mathrm{Fr}(\nabla x \pi_1) \;\Rightarrow\; \sigma(u) \neq \sigma(x)$$

This last implication follows immediately from (iii). So it remains to show that σ is valid for π_1. Having assumed our implication is true for π_1, we simply need to prove that (i), (ii) and (iii) hold for π_1. Again, this follows from $\pi_1 \preceq \pi$. .

In proposition (206) we established the inclusion $\mathrm{Sp}(\sigma(\pi)) \subseteq \sigma(\mathrm{Sp}(\pi))$ which holds for every map $\sigma : V \to W$ and $\pi \in \mathbf{\Pi}(V)$. This inclusion states that the specific variables of the proof $\sigma(\pi)$ must be images by σ of specific variables of the proof π. The following proposition offers a stronger result with the equality $\mathrm{Sp}(\sigma(\pi)) = \sigma(\mathrm{Sp}(\pi))$, provided σ is valid for π. If σ is not valid for π then the equality may fail, as the counterexample $\pi = \forall x(x \in y)$ with $x \neq y$ and $\sigma = [y/x]$ shows. In this case we obtain $\mathrm{Sp}(\sigma(\pi)) = \emptyset$ and $\sigma(\mathrm{Sp}(\pi)) = \{y\}$.

Proposition 222 *Let V, W be sets and $\sigma : V \to W$ be a map. Then for every proof $\pi \in \mathbf{\Pi}(V)$, if the substitution σ is valid for π we have:*

$$\mathrm{Sp}(\sigma(\pi)) = \sigma(\mathrm{Sp}(\pi))$$

where $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ also denotes the proof substitution mapping.

Proof
We assume that σ is valid for π. Then σ is valid for every $\phi \in \mathrm{Hyp}(\pi)$. Hence from proposition (52), $\mathrm{Fr}(\sigma(\phi)) = \sigma(\mathrm{Fr}(\phi))$ for all $\phi \in \mathrm{Hyp}(\pi)$ and:

$$\begin{array}{rcl}
\mathrm{Sp}(\sigma(\pi)) & = & \mathrm{Fr}(\,\mathrm{Hyp}(\sigma(\pi))\,) \\
\text{prop. (193)} \ \to & = & \mathrm{Fr}(\,\sigma(\mathrm{Hyp}(\pi))\,) \\
& = & \cup\{\,\mathrm{Fr}(\psi) \ : \ \psi \in \sigma(\mathrm{Hyp}(\pi))\,\} \\
& = & \cup\{\,\mathrm{Fr}(\sigma(\phi)) \ : \ \phi \in \mathrm{Hyp}(\pi)\,\} \\
\sigma \text{ valid for } \phi \in \mathrm{Hyp}(\pi) \ \to & = & \cup\{\,\sigma(\mathrm{Fr}(\phi)) \ : \ \phi \in \mathrm{Hyp}(\pi)\,\} \\
& = & \sigma(\,\cup\{\,\mathrm{Fr}(\phi) \ : \ \phi \in \mathrm{Hyp}(\pi)\,\}\,) \\
& = & \sigma(\,\mathrm{Fr}(\mathrm{Hyp}(\pi))\,) \\
& = & \sigma(\mathrm{Sp}(\pi))
\end{array}$$

.

The following proposition is the counterpart of proposition (52) which was established for formulas. The inclusion $\mathrm{Fr}(\sigma(\pi)) \subseteq \sigma(\mathrm{Fr}(\pi))$ is already known in general from proposition (209). The free variables of the proof $\sigma(\pi)$ must be images by σ of free variables of the proof π. We are now offering a stronger conclusion with the equality $\mathrm{Fr}(\sigma(\pi)) = \sigma(\mathrm{Fr}(\pi))$ provided σ is valid for π. Note that if σ is valid for π then it is valid for every sub-proof $\rho \preceq \pi$ and consequently the equality $\mathrm{Fr}(\sigma(\rho)) = \sigma(\mathrm{Fr}(\rho))$ is also true for every $\rho \preceq \pi$.

Proposition 223 *Let V, W be sets and $\sigma : V \to W$ be a map. Then for every proof $\pi \in \mathbf{\Pi}(V)$, if the substitution σ is valid for π we have:*

$$\mathrm{Fr}(\sigma(\pi)) = \sigma(\mathrm{Fr}(\pi))$$

where $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ also denotes the proof substitution mapping.

Proof
The inclusion $\subseteq$ follows from proposition (209). So it remains to show $\supseteq$. So let $u \in \mathrm{Fr}(\pi)$. We need to show that $\sigma(u) \in \mathrm{Fr}(\sigma(\pi))$. However, this follows immediately from the validity of σ for π and the fact that $\pi \preceq \pi$. .

The most obvious example of valid substitutions are those which are injective. In fact given $\sigma : V \to W$ and $\pi \in \mathbf{\Pi}(V)$, we only only need σ to be injective on $\mathrm{Var}(\pi)$. This simple proposition is one of the good reasons for us to define the set $\mathrm{Var}(\pi)$ in the first place. It is the counterpart of proposition (53).

Proposition 224 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\pi \in \mathbf{\Pi}(V)$. We assume that $\sigma_{|\mathrm{Var}(\pi)}$ is an injective map. Then σ is valid for π.*

Proof
We assume that $\sigma : V \to W$ is injective on $\mathrm{Var}(\pi)$. We need to show that σ is valid for π. So let $\phi \in \mathrm{Hyp}(\pi)$. We need to show that σ is valid for ϕ. Using proposition (53) it is sufficient to prove that σ is injective on $\mathrm{Var}(\phi)$. It is therefore sufficient to show that $\mathrm{Var}(\phi) \subseteq \mathrm{Var}(\pi)$, which follows from proposition (200) and $\phi \preceq \pi$, this last inequality being itself a consequence of proposition (191) and $\phi \in \mathrm{Hyp}(\pi)$. So we now assume that $\phi \in \mathrm{Ax}(\pi)$. We need to show that σ is valid for ϕ. Using proposition (53) it is sufficient to prove that σ is injective on $\mathrm{Var}(\phi)$. It is therefore sufficient to show that $\mathrm{Var}(\phi) \subseteq \mathrm{Var}(\pi)$ or equivalently $\mathrm{Var}(\partial\phi) \subseteq \mathrm{Var}(\pi)$. This follows from proposition (200) and $\partial\phi \preceq \pi$, this last inequality being itself a consequence of proposition (194) and $\phi \in \mathrm{Ax}(\pi)$. In order to show that σ is valid for π, we finally consider $\nabla x\pi_1 \preceq \pi$ and $u \in \mathrm{Fr}(\nabla x\pi_1)$. Using proposition (221) it is sufficient to prove that $\sigma(u) \neq \sigma(x)$. From $u \in \mathrm{Fr}(\nabla x\pi_1)$ in particular $u \neq x$ and having assumed σ is injective on $\mathrm{Var}(\pi)$, it is sufficient to prove that $\{u, x\} \subseteq \mathrm{Var}(\pi)$. From $\nabla x\pi_1 \preceq \pi$ and proposition (200) we obtain $x \in \mathrm{Var}(\nabla x\pi_1) \subseteq \mathrm{Var}(\pi)$. So it remains to show that $u \in \mathrm{Var}(\pi)$. Using propositions (213) and (200) :

$$u \in \mathrm{Fr}(\nabla x\pi_1) \subseteq \mathrm{Var}(\nabla x\pi_1) \subseteq \mathrm{Var}(\pi)$$

.

When replacing a variable x by a variable y in a formula ϕ, a standard textbook in mathematical logic will often assume that $y \notin \mathrm{Var}(\phi)$ to avoid capture. For us, *avoiding capture* means that a substitution of variable is valid for a given formula. So $[y/x]$ is valid for ϕ whenever $y \notin \mathrm{Var}(\phi)$, as can be seen from proposition (57). A similar property can now be established for proofs:

Proposition 225 *Let V be a set and $x, y \in V$. Let $\pi \in \mathbf{\Pi}(V)$. Then we have:*

$$y \notin \mathrm{Var}(\pi) \;\Rightarrow\; ([y/x] \textit{ valid for } \pi)$$

Proof
We assume that $y \notin \mathrm{Var}(\pi)$. We need to show that $[y/x]$ is valid for π. Using proposition (224), it is sufficient to prove that $[y/x]_{|\mathrm{Var}(\pi)}$ is an injective map. This follows immediately from $y \notin \mathrm{Var}(\pi)$ and proposition (38). **.**

Suppose $\tau : U \to V$ and $\sigma : V \to W$ are maps while $\pi \in \mathbf{\Pi}(U)$. If the substitution τ is capture-avoiding when acting on π and σ is capture-avoiding when acting on $\tau(\pi)$, then $\sigma \circ \tau$ avoids variable capture when acting on π. Conversely, if the substitution $\sigma \circ \tau$ is valid for π then both τ and σ are capture-avoiding when acting on π and $\tau(\pi)$ respectively. The following proposition is the counterpart of proposition (58) which was established for formulas:

Proposition 226 *Let U, V, W be sets and $\tau : U \to V$ and $\sigma : V \to W$ be maps. Then for all $\pi \in \mathbf{\Pi}(U)$ we have the equivalence:*

$$(\tau \textit{ valid for } \pi) \wedge (\sigma \textit{ valid for } \tau(\pi)) \;\Leftrightarrow\; (\sigma \circ \tau \textit{ valid for } \pi)$$

where $\tau : \mathbf{\Pi}(U) \to \mathbf{\Pi}(V)$ also denotes the associated proof substitution mapping.

Proof
First we show $\Rightarrow$: so we assume that τ is valid for π and σ is valid for $\tau(\pi)$. We need to show that $\sigma \circ \tau$ is valid for π. So let $\phi \in \mathrm{Hyp}(\pi) \cup \mathrm{Ax}(\pi)$. We need to show that $\sigma \circ \tau$ is valid for ϕ. Using proposition (58), it is sufficient to prove that τ is valid for ϕ and that σ is valid for $\tau(\phi)$. The fact that τ is valid for ϕ follows immediately from the validity of τ for π. So it remains to show that σ is valid for $\tau(\phi)$. However, from proposition (193) we have $\tau(\mathrm{Hyp}(\pi)) = \mathrm{Hyp}(\tau(\pi))$ and from proposition (197) we have $\tau(\mathrm{Ax}(\pi)) = \mathrm{Ax}(\tau(\pi))$. Hence we see that $\tau(\phi) \in \mathrm{Hyp}(\tau(\pi)) \cup \mathrm{Ax}(\tau(\pi))$, and having assumed that σ is valid for $\tau(\pi)$ we conclude that σ is valid for $\tau(\phi)$ as requested. We now consider $\nabla x \pi_1 \preceq \pi$. From proposition (221), in order to show that $\sigma \circ \tau$ is valid for π, we need:

$$u \in \mathrm{Fr}(\nabla x \pi_1) \;\Rightarrow\; \sigma \circ \tau(u) \neq \sigma \circ \tau(x) \tag{3.17}$$

However, since τ is valid for π, we know the following implication is true:

$$u \in \mathrm{Fr}(\nabla x \pi_1) \;\Rightarrow\; \tau(u) \neq \tau(x) \tag{3.18}$$

So we assume that $u \in \mathrm{Fr}(\nabla x \pi_1)$. We need to show that $\sigma \circ \tau(u) \neq \sigma \circ \tau(x)$. Defining $v = \tau(u) \in V$ and $y = \tau(x) \in V$, we need to show that $\sigma(v) \neq \sigma(y)$. However, from $\nabla x \pi_1 \preceq \pi$ and proposition (189) we obtain $\nabla y \tau(\pi_1) \preceq \tau(\pi)$. Having assumed that σ is valid for $\tau(\pi)$, the following implication holds:

$$v \in \mathrm{Fr}(\nabla y \tau(\pi_1)) \;\Rightarrow\; \sigma(v) \neq \sigma(y) \tag{3.19}$$

Thus, in order to show $\sigma(v) \neq \sigma(y)$ it is sufficient to prove $v \in \mathrm{Fr}(\nabla y \tau(\pi_1))$. We already know from the implication (3.18) that $v \neq y$. So it remains to show that $v \in \mathrm{Fr}(\tau(\pi_1))$. However we have $v = \tau(u) \in \tau(\mathrm{Fr}(\pi_1))$. It is therefore sufficient to prove that $\tau(\mathrm{Fr}(\pi_1)) = \mathrm{Fr}(\tau(\pi_1))$. Using proposition (223) we simply need to show that τ is valid for π_1 which follows from proposition (217) and the fact that $\pi_1 \preceq \nabla x \pi_1 \preceq \pi$, i.e. that π_1 is a sub-proof of π. We now show $\Leftarrow$: so we assume that $\sigma \circ \tau$ is valid for π. We need to show that τ is valid for π and σ is valid for $\tau(\pi)$. First we show that τ is valid for π: so let $\phi \in \mathrm{Hyp}(\pi) \cup \mathrm{Ax}(\pi)$. We need to show that τ is valid for ϕ. However we know by assumption that $\sigma \circ \tau$ is valid for ϕ. Using proposition (58) it follows that τ is valid for ϕ as requested. We now consider $\nabla x \pi_1 \preceq \pi$. In order to show that τ is valid for π we need to show the implication $u \in \mathrm{Fr}(\nabla x \pi_1) \;\Rightarrow\; \tau(u) \neq \tau(x)$. So let $u \in \mathrm{Fr}(\nabla x \pi_1)$. We need to show that $\tau(u) \neq \tau(x)$. However, we know by assumption that $\sigma \circ \tau(u) \neq \sigma \circ \tau(x)$. So $\tau(u) \neq \tau(x)$ must follow. We now show that σ is valid for $\tau(\pi)$. So let $\psi \in \mathrm{Hyp}(\tau(\pi)) \cup \mathrm{Ax}(\tau(\pi))$. We need to show that σ is valid for ψ. From proposition (193), $\mathrm{Hyp}(\tau(\pi)) = \tau(\mathrm{Hyp}(\pi))$ and from proposition (197) $\mathrm{Ax}(\tau(\pi)) = \tau(\mathrm{Ax}(\pi))$. It follows that $\psi = \tau(\phi)$ for some $\phi \in \mathrm{Hyp}(\pi) \cup \mathrm{Ax}(\pi)$. Having assumed that $\sigma \circ \tau$ is valid for π, it follows that $\sigma \circ \tau$ is valid for ϕ. Using proposition (58) we see that σ is valid for $\tau(\phi)$. In other words, σ is valid for ψ as requested. We now consider $\nabla y \rho_1 \preceq \tau(\pi)$. In order to show that σ is valid for $\tau(\pi)$ we need to prove the implication:

$$v \in \mathrm{Fr}(\nabla y \rho_1) \;\Rightarrow\; \sigma(v) \neq \sigma(y) \tag{3.20}$$

However since $\nabla y \rho_1$ is a sub-proof of $\tau(\pi)$, from proposition (189) we have $\nabla y \rho_1 = \tau(\rho)$ for some $\rho \preceq \pi$. Furthermore, from theorem (2) of page 21 the proof $\rho \in \mathbf{\Pi}(U)$ can only be of four types, namely $\rho = \phi$ for some $\phi \in \mathbf{P}(U)$ or $\rho = \partial\phi$ for some $\phi \in \mathbf{P}(U)$ or $\rho = \pi_1 \oplus \pi_2$ or $\rho = \nabla x \pi_1$. From the equation $\nabla y \rho_1 = \tau(\rho)$ and the uniqueness of representation stated in theorem (2) it is clear the only possibility is $\rho = \nabla x \pi_1$ for some $x \in U$ and $\pi_1 \in \mathbf{\Pi}(U)$. Hence, we have found x and π_1 such that $\nabla x \pi_1 \preceq \pi$ and $\nabla y \rho_1 = \tau(\nabla x \pi_1) = \nabla \tau(x) \tau(\pi_1)$, i.e. $y = \tau(x)$ and $\rho_1 = \tau(\pi_1)$. So the implication (3.20) can be stated as:

$$v \in \mathrm{Fr}(\, \nabla \tau(x) \tau(\pi_1)\,) \;\Rightarrow\; \sigma(v) \neq \sigma \circ \tau(x) \tag{3.21}$$

So let $v \in \mathrm{Fr}(\, \nabla \tau(x) \tau(\pi_1)\,)$. We need to show that $\sigma(v) \neq \sigma \circ \tau(x)$. However, from proposition (209) we have $\mathrm{Fr}(\tau(\pi_1)) \subseteq \tau(\mathrm{Fr}(\pi_1))$. It follows that we have $v = \tau(u)$ for some $u \in \mathrm{Fr}(\pi_1)$. Furthermore, since $v \neq \tau(x)$ we have $u \neq x$ and consequently $u \in \mathrm{Fr}(\nabla x \pi_1)$. Furthermore, recall that $\nabla x \pi_1 \preceq \pi$. Having assumed that $\sigma \circ \tau$ is valid for π the following implication holds:

$$u \in \mathrm{Fr}(\nabla x \pi_1) \;\Rightarrow\; \sigma \circ \tau(u) \neq \sigma \circ \tau(x) \tag{3.22}$$

Hence, we conclude that $\sigma \circ \tau(u) \neq \sigma \circ \tau(x)$ which is $\sigma(v) \neq \sigma \circ \tau(x)$ as requested.
.

Let $\sigma : V \to W$ be a map and $\pi \in \mathbf{\Pi}(V)$. When attempting to prove the validity of σ for π, a very useful shortcut is to argue that $\sigma(\pi)$ is in fact the same proof as $\tau(\pi)$ where $\tau : V \to W$ is a map which is known to be valid for π. The following proposition is the counterpart of proposition (59).

Proposition 227 *Let V, W be sets and $\sigma, \tau : V \to W$ be maps. Let $\pi \in \mathbf{\Pi}(V)$ such that the equality $\sigma(\pi) = \tau(\pi)$ holds. Then we have the equivalence:*

$$(\sigma \textit{ valid for } \pi) \;\Leftrightarrow\; (\tau \textit{ valid for } \pi)$$

Proof
It is sufficient to prove $\Rightarrow$: so we assume that $\sigma(\pi) = \tau(\pi)$ and that σ is valid for π. We need to show that τ is valid for π. Using proposition (202) we see that σ and τ coincide on $\mathrm{Var}(\pi)$. So let $\phi \in \mathrm{Hyp}(\pi) \cup \mathrm{Ax}(\pi)$. We need to show that τ is valid for ϕ. However since σ is valid for π, we know that σ is itself valid for ϕ. Using proposition (59), in order to show that τ is also valid for ϕ it is sufficient to prove that $\sigma(\phi) = \tau(\phi)$. From proposition (36) it is therefore sufficient to show that σ and τ coincide on $\mathrm{Var}(\phi)$. Having established that σ and τ coincide on $\mathrm{Var}(\pi)$, we simply need to prove that $\mathrm{Var}(\phi) \subseteq \mathrm{Var}(\pi)$. We shall distinguish two cases: first we assume that $\phi \in \mathrm{Hyp}(\pi)$. Then from proposition (191) we have $\phi \preceq \pi$ and using proposition (200) it follows that $\mathrm{Var}(\phi) \subseteq \mathrm{Var}(\pi)$ as requested. Next we assume that $\phi \in \mathrm{Ax}(\pi)$. Then from proposition (194) we see that $\partial\phi \preceq \pi$ and again from proposition (200) we have $\mathrm{Var}(\phi) = \mathrm{Var}(\partial\phi) \subseteq \mathrm{Var}(\pi)$. So we now consider $\nabla x \pi_1 \preceq \pi$. From proposition (221), in order to show that τ is valid for π, for all $u \in V$ we need to show the implication:

$$u \in \mathrm{Fr}(\nabla x \pi_1) \;\Rightarrow\; \tau(u) \neq \tau(x) \tag{3.23}$$

However, from the validity of σ for π we know the following is true:

$$u \in \mathrm{Fr}(\nabla x \pi_1) \;\Rightarrow\; \sigma(u) \neq \sigma(x) \tag{3.24}$$

In order to establish (3.23), since σ and τ coincide on $\mathrm{Var}(\pi)$ it is therefore sufficient to prove that $\{u, x\} \subseteq \mathrm{Var}(\pi)$. From $\nabla x \pi_1 \preceq \pi$ and proposition (200) :

$$x \in \mathrm{Var}(\nabla x \pi_1) \subseteq \mathrm{Var}(\pi)$$

So it remains to show that $u \in \mathrm{Var}(\pi)$. Using propositions (213) and (200) :

$$u \in \mathrm{Fr}(\nabla x \pi_1) \subseteq \mathrm{Var}(\nabla x \pi_1) \subseteq \mathrm{Var}(\pi)$$

.

Just as we did for formulas in definition (38), we shall define the notion of minimal transform for proofs in definition (87). The prime motivation of minimal transforms is to replace all bound variables of a formula or proof, with elements of a copy of $\mathbf{N}$ which is disjoint from V. In doing so, we ensure that any map $\sigma : V \to W$ is always capture-avoiding when acting on the minimal transform of a formula or proof. More precisely the map $\bar{\sigma} : \bar{V} \to \bar{W}$ which is the minimal extension of σ as per definition (39), is always valid for minimal transforms. The following proposition will allow us to easily prove this validity and is the counterpart of proposition (60) which was established for formulas.

Proposition 228 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\pi \in \mathbf{\Pi}(V)$. We assume that there exists a subset $V_0 \subseteq V$ with the following properties:*

$$\begin{array}{rl} (i) & \mathrm{Bnd}(\pi) \subseteq V_0 \\ (ii) & \sigma_{|V_0} \text{ is injective} \\ (iii) & \sigma(V_0) \cap \sigma(\mathrm{Var}(\pi) \setminus V_0) = \emptyset \end{array}$$

Then the map $\sigma : V \to W$ is valid for the proof $\pi \in \mathbf{\Pi}(V)$.

Proof
It is sufficient to show that properties (i), (ii) and (iii) of proposition (221) are satisfied. First we show property (i) and (ii) : so let $\phi \in \mathrm{Hyp}(\pi) \cup \mathrm{Ax}(\pi)$. We need to show that σ is valid for ϕ. Applying proposition (60) it is sufficient to show that $\mathrm{Bnd}(\phi) \subseteq V_0$ and $\sigma(V_0) \cap \sigma(\mathrm{Var}(\phi) \setminus V_0) = \emptyset$. Using (i) and (iii) it is therefore sufficient to prove that $\mathrm{Var}(\phi) \subseteq \mathrm{Var}(\pi)$. We shall distinguish two cases: first we assume that $\phi \in \mathrm{Hyp}(\pi)$. Then from proposition (191) we have $\phi \preceq \pi$ and $\mathrm{Var}(\phi) \subseteq \mathrm{Var}(\pi)$ follows from proposition (200). Next we assume that $\phi \in \mathrm{Ax}(\pi)$. Then from proposition (194) we have $\partial\phi \preceq \pi$ and consequently $\mathrm{Var}(\phi) = \mathrm{Var}(\partial\phi) \subseteq \mathrm{Var}(\pi)$ as requested. We now show property (iii) : Let $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ be such that $\nabla x \pi_1 \preceq \pi$. Given $u \in \mathrm{Fr}(\nabla x \pi_1)$ we need to show that $\sigma(u) \neq \sigma(x)$. However, from proposition (214) we have $\mathrm{Bnd}(\nabla x \pi_1) \subseteq \mathrm{Bnd}(\pi)$ and consequently $x \in \mathrm{Bnd}(\pi)$. From the assumption (i) it follows that $x \in V_0$. We shall now distinguish two cases: first we assume

that $u \in V_0$. Then from assumption (ii), in order to show $\sigma(u) \neq \sigma(x)$ it is sufficient to prove that $u \neq x$ which follows from $u \in \mathrm{Fr}(\nabla x \pi_1)$. We now assume that $u \notin V_0$. From proposition (200) we have $\mathrm{Var}(\nabla x \pi_1) \subseteq \mathrm{Var}(\pi)$ while from proposition (213), $\mathrm{Fr}(\nabla x \pi_1) \subseteq \mathrm{Var}(\nabla x \pi_1)$. Hence, $u \in \mathrm{Var}(\pi)$. It follows that $u \in \mathrm{Var}(\pi) \setminus V_0$ and $\sigma(u) \neq \sigma(x)$ is a consequence of (iii) and $x \in V_0$. .

3.2.10 Valid Substitution of Axiom

Given a map $\sigma : V \to W$ our plan is to carry over the sequent $\Gamma \vdash \phi$ into another sequent $\sigma(\Gamma) \vdash \sigma(\phi)$. Our strategy is based around the study of variable substitutions in proofs. So from $\sigma : V \to W$ we define $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ as per definition (74). We know that some of these substitutions will not be capture-avoiding, and we extended the notion of *valid substitution* for proofs in definition (79) to formalize the idea of capture-avoidance. The hope is that a valid substitution will satisfy the equality $\mathrm{Val} \circ \sigma(\pi) = \sigma \circ \mathrm{Val}(\pi)$ provided the proof π is totally clean, as per definition (73). From proposition (185), we know that a sequent $\Gamma \vdash \phi$ always has an underlying proof π which is totally clean. So if σ happens to be valid for π and satisfies our equality, then we see that $\sigma(\pi)$ is a proof of $\sigma(\phi)$. We also know from proposition (193) that $\mathrm{Hyp}(\sigma(\pi)) = \sigma(\mathrm{Hyp}(\pi)) \subseteq \sigma(\Gamma)$ and we conclude that $\sigma(\pi)$ is a proof underlying the sequent $\sigma(\Gamma) \vdash \sigma(\phi)$. There is of course a big outstanding problem: in general, we have no way to tell whether a substitution σ is valid for the proof underlying the sequent $\Gamma \vdash \phi$. The data which defines the sequent namely the set $\Gamma \subseteq \mathbf{P}(V)$ and the formula $\phi \in \mathbf{P}(V)$ do not tell us anything about the axioms being used in the proof. So we shall need to have another idea. In the meantime, if we assume that σ is valid for π and π is totally clean, we want the conclusion of $\sigma(\pi)$ to be the image by σ of the conclusion of π. Fundamentally, this cannot happen unless the axioms of π remain axioms of first order logic after substitution by σ. So let us look as the simple example $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Saying that π is totally clean amounts to saying that the axiom invocation $\partial\phi$ is legitimate. In other words, the formula ϕ is indeed an axiom of first order logic, i.e. we have $\phi \in \mathbf{A}(V)$ and consequently $\mathrm{Val}(\pi) = \phi$. In order to have $\mathrm{Val}(\sigma(\pi)) = \sigma(\phi)$, since $\sigma(\pi) = \partial\sigma(\phi)$ we need $\sigma(\phi)$ to be itself an axiom of first order logic. This will not be the case in general, but having assumed that σ is valid for π, it is valid for the formula ϕ. If the substitution σ is capture-avoiding and ϕ is an axiom of first order logic, we should hope that $\sigma(\phi)$ is itself an axiom. Proving this fact is the purpose of lemma (19) below. Note that the validity of σ for ϕ is crucially important when dealing with quantification axioms and specialization axioms, as per definition (61) and (62). It is not difficult to see that $\sigma(\phi)$ is always an axiom without the validity assumption, whenever ϕ is a simplification, Frege or transposition axiom. But consider the case when $\phi = \forall x[\,(y \in y) \to (x \in x)\,] \to [\,(y \in y) \to \forall x(x \in x)\,]$ with $x \neq y$ and $\sigma = [y/x]$. Then ϕ is a quantification axiom while σ is not valid for ϕ. It is clear that $\sigma(\phi) = \forall y[\,(y \in y) \to (y \in y)\,] \to [\,(y \in y) \to \forall y(y \in y)\,]$ is not an axiom of first order logic. In fact, for those already familiar with model theory and the soundness theorem (37) of page 426, it is clear that $\sigma(\phi)$ is not provable, i.e.

the sequent $\vdash \sigma(\phi)$ is false. Now consider $\phi = \forall y(x \in y) \to (x \in z)$ where x, y, z are distinct. Then ϕ is a specialization axiom while $\sigma = [y/x]$ is not valid for ϕ. We have $\sigma(\phi) = \forall y(y \in y) \to (y \in z)$ which is not an axiom of first order logic and is easily seen to be false for some model and assignment.

Lemma 19 *Let V, W be sets and $\sigma : V \to W$ be a map. Given $\phi \in \mathbf{A}(V)$:*

$$(\sigma \text{ valid for } \phi) \;\Rightarrow\; \sigma(\phi) \in \mathbf{A}(W)$$

In other words, the image of an axiom by a valid substitution is an axiom.

Proof
Let $\phi \in \mathbf{A}(V)$ and $\sigma : V \to W$ be valid for ϕ. We need to show that $\sigma(\phi)$ is an axiom of first order logic. Following definition (63) we shall consider the five possible types of axioms separately: first we assume that ϕ is a simplification axiom. Using definition (58) we have $\phi = \phi_1 \to (\phi_2 \to \phi_1)$ for $\phi_1, \phi_2 \in \mathbf{P}(V)$. It follows that $\sigma(\phi) = \psi_1 \to (\psi_2 \to \psi_1)$ where $\psi_1 = \sigma(\phi_1)$ and $\psi_2 = \sigma(\phi_2)$. So $\sigma(\phi)$ is also a simplification axiom. Next we assume that ϕ is a Frege axiom. Using definition (59), $\phi = [\phi_1 \to (\phi_2 \to \phi_3)] \to [(\phi_1 \to \phi_2) \to (\phi_1 \to \phi_3)]$ for $\phi_1, \phi_2, \phi_3 \in \mathbf{P}(V)$. Setting $\psi_1 = \sigma(\phi_1)$, $\psi_2 = \sigma(\phi_2)$ and $\psi_3 = \sigma(\phi_3)$ we have:

$$\sigma(\phi) = [\psi_1 \to (\psi_2 \to \psi_3)] \to [(\psi_1 \to \psi_2) \to (\psi_1 \to \psi_3)]$$

So $\sigma(\phi)$ is also a Frege axiom. Next we assume that ϕ is a transposition axiom. Using definition (60) we have $\phi = [(\phi_1 \to \bot) \to \bot] \to \phi_1$ for some $\phi_1 \in \mathbf{P}(V)$. It follows that $\sigma(\phi) = [(\psi_1 \to \bot) \to \bot] \to \psi_1$ where $\psi_1 = \sigma(\phi_1)$ and $\sigma(\phi)$ is also a transposition axiom. Next we assume that ϕ is a quantification axiom. Using definition (61) we have $\phi = \forall x(\phi_1 \to \phi_2) \to (\phi_1 \to \forall x \phi_2)$ where $\phi_1, \phi_2 \in \mathbf{P}(V)$ and $x \notin \mathrm{Fr}(\phi_1)$. Setting $\psi_1 = \sigma(\phi_1)$ and $\psi_2 = \sigma(\phi_2)$ we obtain:

$$\sigma(\phi) = \forall y(\psi_1 \to \psi_2) \to (\psi_1 \to \forall y \psi_2)$$

where $y = \sigma(x)$. However, we cannot argue that $\sigma(\phi)$ is a quantification axiom until we prove that $y \notin \mathrm{Fr}(\psi_1)$. So suppose to the contrary that $y \in \mathrm{Fr}(\psi_1)$. From proposition (43) we have $\mathrm{Fr}(\sigma(\phi_1)) \subseteq \sigma(\mathrm{Fr}(\phi_1))$ and it follows that $y \in \sigma(\mathrm{Fr}(\phi_1))$. Hence, there exists $u \in \mathrm{Fr}(\phi_1)$ such that $\sigma(x) = y = \sigma(u)$. However, we know that $x \notin \mathrm{Fr}(\phi_1)$ and consequently $u \neq x$. Thus, we see that $u \in \mathrm{Fr}(\phi_1) \setminus \{x\} = \mathrm{Fr}(\forall x \phi_1)$ and furthermore $\sigma(x) = \sigma(u)$. By virtue of proposition (55), this means σ is not a valid substitution for $\forall x \phi_1$. We shall obtain our desired contradiction by showing that σ is in fact valid for $\forall x \phi_1$. Indeed, by assumption we know that σ is valid for ϕ. Using proposition (54) it follows that σ is valid for $\forall x(\phi_1 \to \phi_2)$. Hence, from proposition (55) we see that σ is valid for $\phi_1 \to \phi_2$ and furthermore, given $v \in V$ we have the implication:

$$v \in \mathrm{Fr}(\forall x(\phi_1 \to \phi_2)) \;\Rightarrow\; \sigma(v) \neq \sigma(x)$$

Using proposition (54) once more, it follows that σ is valid for ϕ_1 and:

$$v \in \mathrm{Fr}(\forall x \phi_1) \;\Rightarrow\; \sigma(v) \neq \sigma(x)$$

this last implication being a consequence of $\mathrm{Fr}(\forall x\phi_1) \subseteq \mathrm{Fr}(\forall x(\phi_1 \to \phi_2))$. So we conclude from proposition (55) that σ is valid for $\forall x\phi_1$, which completes our proof that $\sigma(\phi)$ is indeed a quantification axiom. Note that the quantification axiom is the first case where we needed to use the assumption of validity of σ for ϕ. Finally, we assume that ϕ is a specialization axiom. Using definition (62) we have $\phi = \forall x\phi_1 \to \phi_1[y/x]$ where $\phi_1 \in V$, $x, y \in V$ and $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ refers to an essential substitution of y in place of x, i.e. an essential substitution associated with $[y/x] : V \to V$. Defining $\psi_1 = \sigma(\phi_1)$ and $\psi_1^* = \sigma \circ [y/x](\phi_1)$:

$$\sigma(\phi) = \forall z\psi_1 \to \psi_1^*$$

where $z = \sigma(x)$. In order to show that $\sigma(\phi)$ is itself a specialization axiom, from proposition (157) it is sufficient to show that $\psi_1^* \sim \psi_1[\sigma(y)/z]$ where the map $[\sigma(y)/z] : \mathbf{P}(W) \to \mathbf{P}(W)$ refers to an essential substitution of $\sigma(y)$ in place of $z = \sigma(x)$, and $\sim$ is the substitution congruence on $\mathbf{P}(W)$. In order to prove such equivalence, using theorem (14) of page 149 it is sufficient to prove the equality between the corresponding minimal transforms, which goes as follows:

$$\begin{aligned}
\mathcal{M}(\psi_1^*) &= \mathcal{M} \circ \sigma \circ [y/x](\phi_1) \\
\text{A: to be proved } \to &= \bar{\sigma} \circ \mathcal{M} \circ [y/x](\phi_1) \\
[y/x] \text{ essential } \to &= \bar{\sigma} \circ [y/x] \circ \mathcal{M}(\phi_1) \\
\text{B: to be proved } \to &= [\sigma(y)/\sigma(x)] \circ \bar{\sigma} \circ \mathcal{M}(\phi_1) \\
\text{C: to be proved } \to &= [\sigma(y)/\sigma(x)] \circ \mathcal{M} \circ \sigma(\phi_1) \\
&= [\sigma(y)/z] \circ \mathcal{M} \circ \sigma(\phi_1) \\
[\sigma(y)/z] \text{ essential } \to &= \mathcal{M} \circ [\sigma(y)/z] \circ \sigma(\phi_1) \\
&= \mathcal{M}(\, \psi_1[\sigma(y)/z]\,)
\end{aligned}$$

So it remains to prove points A, B and C. First we start with point A: using theorem (13) of page 146 we simply need to show that σ is valid for $[y/x](\phi_1)$, which follows from our assumption that σ is valid for $\phi = \forall x\phi_1 \to [y/x](\phi_1)$ and proposition (54). So we now prove point B: let $u \in \mathrm{Var}(\mathcal{M}(\phi_1))$. Using proposition (36) we need to show that $\bar{\sigma} \circ [y/x](u) = [\sigma(y)/\sigma(x)] \circ \bar{\sigma}(u)$. Since $\bar{V}$ is the disjoint union of V and $\mathbf{N}$, we shall distinguish two cases: first we assume that $u \in \mathbf{N}$. Then $u \neq x$ and $\bar{\sigma}(u) = u$. It follows that $\bar{\sigma}(u) \neq \sigma(x)$ and the equality is true. Next we assume that $u \in V$. Using proposition (97) it follows that $u \in \mathrm{Var}(\mathcal{M}(\phi_1)) \cap V = \mathrm{Fr}(\phi_1)$. We shall distinguish two further cases: first we assume that $u = x$. Then $\bar{\sigma}(u) = \sigma(x)$ and the equality is true. Finally we assume that $u \neq x$. Then $u \in \mathrm{Fr}(\phi_1) \setminus \{x\} = \mathrm{Fr}(\forall x\phi_1)$. Having assumed that σ is valid for $\phi = \forall x\phi_1 \to [y/x](\phi_1)$, in particular from proposition (54) it is valid for $\forall x\phi_1$. Hence from $u \in \mathrm{Fr}(\forall x\phi_1)$ and proposition (55) we obtain $\bar{\sigma}(u) = \sigma(u) \neq \sigma(x)$. So we conclude the equality is once again true, which completes our proof of point B. So we now prove point C: using theorem (13) of page 146 once more, we need to show that σ is valid for ϕ_1. However, we already know that σ is valid for $\forall x\phi_1$, and the validity of σ for ϕ_1 follows from proposition (55). This completes our proof of point C. .

3.2.11 Valid Substitution of Totally Clean Proof

There is not much point substituting variables in a proof $\pi \in \mathbf{\Pi}(V)$ according to some map $\sigma : V \to W$, unless the proof $\sigma(\pi)$ has the properties everyone would want it to have. From proposition (193) we have $\mathrm{Hyp}(\sigma(\pi)) = \sigma(\mathrm{Hyp}(\pi))$. So the set of hypothesis of $\sigma(\pi)$ is nicely what we expect it to be, without any assumption on the proof π or substitution σ. However, we also crucially want to control the conclusion of $\sigma(\pi)$ with the equality $\mathrm{Val} \circ \sigma(\pi) = \sigma \circ \mathrm{Val}(\pi)$. As previously discussed, we cannot hope this to be true unless axioms of the proof π remain axioms of first order logic after substitution by σ. By virtue of lemma (19), one way to achieve this is to impose that σ be valid for every axiom of π. However, we also need to make sure any use of the generalization rule of inference in the proof π remains legitimate after substitution by σ. Specifically, if $\nabla x \pi_1$ is a sub-proof of π, the variable $\sigma(x)$ should remain an arbitrary variable of the proof $\sigma(\pi_1)$ so that $\nabla \sigma(x) \sigma(\pi_1)$ can be inferred legitimately. In other words, no free variable of an hypothesis of π_1 should be *captured* by the substitution σ. In definition (79) we introduced the notion of *valid substitution* for proofs with two considerations in mind: on the one hand we wanted to impose conditions on σ which are strong enough to ensure the conclusion of the proof $\sigma(\pi)$ is what we expect. On the other hand, we wanted the theory of capture-avoiding substitutions for proofs to be formally as close as possible if not identical, to the theory of capture-avoiding substitutions for formulas, even if this meant imposing conditions on σ which are slightly stronger than necessary. As we shall see, a huge benefit will be derived from the formal proximity of the notions of validity for proofs and formulas. We shall be able to define a minimal transform and substitution congruence on $\mathbf{\Pi}(V)$, and prove the existence of essential substitutions for proofs in theorem (29) of page 375. This will in turn lead to the substitution theorem (30) of page 388. Now going back to the discussion at hand, the hope is that provided σ is valid for π, the conclusion of $\sigma(\pi)$ is the right one. However, we already saw that imposing a condition on σ was not enough. The example of $\pi = (x \in x) \oplus [(y \in y) \to \bot]$ with $x \neq y$ and $\sigma = [y/x]$ shows that things can go wrong despite σ being valid for π. Since π is derived from a flawed application of modus ponens, its conclusion is $\mathrm{Val}(\pi) = \bot \to \bot$, while the conclusion of $\sigma(\pi) = (y \in y) \oplus [(y \in y) \to \bot]$ is $\mathrm{Val} \circ \sigma(\pi) = \bot$. In definition (73) we introduced the notion of *totally clean proof* so as to focus only on those proofs of $\mathbf{\Pi}(V)$ which do not contain any flawed application of rules of inference or axiom invocation. Unless a proof is totally clean, we cannot say anything sensible about it. Granted its conclusion is provable from its hypothesis, but this is as far as it goes. So we need π to be totally clean and σ to be valid for π, in which case $\sigma(\pi)$ becomes interesting:

Proposition 229 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\pi \in \mathbf{\Pi}(V)$ be totally clean and σ be valid for π. Then $\sigma(\pi)$ is totally clean and:*

$$\mathrm{Val} \circ \sigma(\pi) = \sigma \circ \mathrm{Val}(\pi) \tag{3.25}$$

Proof
For all $\pi \in \mathbf{\Pi}(V)$ we need to show the following implication:

$$(\pi \text{ t-clean}) \wedge (\sigma \text{ valid for } \pi) \;\Rightarrow\; (\sigma(\pi) \text{ t-clean}) \wedge (\text{ eq. (3.25) })$$

We shall do so with a structural induction using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. From definition (73), π is always totally clean in this case. So we assume that σ is valid for π, and we need to show that $\sigma(\pi)$ is totally clean together with equation (3.25). From definition (74) we have $\sigma(\pi) = \sigma(\phi) \in \mathbf{P}(W)$ and consequently $\sigma(\pi)$ is totally clean. Furthermore, we have $\mathrm{Val}(\sigma(\pi)) = \mathrm{Val}(\sigma(\phi)) = \sigma(\phi) = \sigma(\mathrm{Val}(\pi))$ which shows that equation (3.25) is true. This completes the case when $\pi = \phi$ for which the assumption of validity of σ for π was unnecessary. We now assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. We further assume that π is totally clean and σ is valid for π. we need to show that $\sigma(\pi)$ is totally clean together with equation (3.25). From definition (73), having assumed that π is totally clean we obtain $\phi \in \mathbf{A}(V)$, i.e. ϕ is a legitimate axiom. Having assumed that σ is valid for π, in particular from proposition (218) σ is valid for ϕ. It follows from lemma (19) that $\sigma(\phi) \in \mathbf{A}(W)$. Hence, using definition (73) once more we see that $\sigma(\pi) = \partial\sigma(\phi)$ is totally clean. Furthermore from definition (69) we have $\mathrm{Val}(\sigma(\pi)) = \sigma(\phi) = \sigma(\mathrm{Val}(\pi))$ and it follows that equation (3.25) is true. So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs which satisfy our implication. We need to show the same is true of π. So we assume that π is totally clean and furthermore that σ is valid for π. We need to show that $\sigma(\pi)$ is totally clean and equation (3.25) is true. However, using proposition (182) we see that both π_1 and π_2 are totally clean and the following equality holds:

$$\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \to \mathrm{Val}(\pi) \tag{3.26}$$

Furthermore, using proposition (219) we see that σ is valid for π_1 and π_2. Having assumed our induction hypothesis holds for π_1, π_2 it follows that $\sigma(\pi_1)$ and $\sigma(\pi_2)$ are totally clean and equation (3.25) is true for π_1, π_2. So let us prove that $\sigma(\pi)$ is totally clean: since $\sigma(\pi) = \sigma(\pi_1) \oplus \sigma(\pi_2)$, from proposition (182) it is sufficient to prove that $\sigma(\pi_1)$ and $\sigma(\pi_2)$ are totally clean and:

$$\mathrm{Val}(\sigma(\pi_2)) = \mathrm{Val}(\sigma(\pi_1)) \to \mathrm{Val}(\sigma(\pi)) \tag{3.27}$$

We already know that $\sigma(\pi_1)$ and $\sigma(\pi_2)$ are totally clean so we only need to focus on equation (3.27). However, applying $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ on both sides of equation (3.26) we obtain $\sigma(\mathrm{Val}(\pi_2)) = \sigma(\mathrm{Val}(\pi_1)) \to \sigma(\mathrm{Val}(\pi))$, which is:

$$\mathrm{Val}(\sigma(\pi_2)) = \mathrm{Val}(\sigma(\pi_1)) \to \sigma(\mathrm{Val}(\pi)) \tag{3.28}$$

since π_1 and π_2 satisfy equation (3.25). Comparing (3.27) with (3.28) we only need to show that $\mathrm{Val}(\sigma(\pi)) = \sigma(\mathrm{Val}(\pi))$, which is showing that (3.25) is true and which we have to do anyway. In fact, this follows immediately from (3.28) :

$$\mathrm{Val}(\sigma(\pi)) \quad = \quad \mathrm{Val}(\sigma(\pi_1 \oplus \pi_2))$$

$$
\begin{array}{rcl}
 & = & \mathrm{Val}(\sigma(\pi_1) \oplus \sigma(\pi_2)) \\
\text{def. (69)} \ \rightarrow & = & M(\,\mathrm{Val}(\sigma(\pi_1))\,,\,\mathrm{Val}(\sigma(\pi_2))\,) \\
\text{(3.28)} \ \rightarrow & = & M(\,\mathrm{Val}(\sigma(\pi_1))\,,\,\mathrm{Val}(\sigma(\pi_1)) \rightarrow \sigma(\mathrm{Val}(\pi))\,) \\
\text{def. (68)} \ \rightarrow & = & \sigma(\mathrm{Val}(\pi))
\end{array}
$$

This completes the case when $\pi = \pi_1 \oplus \pi_2$. So we now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ satisfies our implication. We need to show the same is true of π. So we assume that π is totally clean and σ is valid for π. We need to show that $\sigma(\pi)$ is totally clean and equation (3.25) is true. However from proposition (183), π_1 is totally clean and $x \notin \mathrm{Sp}(\pi_1)$. Furthermore, using proposition (220) we see that σ is valid for π_1 and for all $u \in V$:

$$
u \in \mathrm{Fr}(\nabla x \pi_1) \ \Rightarrow \ \sigma(u) \neq \sigma(x) \tag{3.29}
$$

Having assumed our induction hypothesis holds for π_1 it follows that $\sigma(\pi_1)$ is totally clean and equation (3.25) is true for π_1. So let us prove that $\sigma(\pi)$ is totally clean: since $\sigma(\pi) = \nabla \sigma(x) \sigma(\pi_1)$, from proposition (183) it is sufficient to prove that $\sigma(\pi_1)$ is totally clean and $\sigma(x) \notin \mathrm{Sp}(\sigma(\pi_1))$. We already know that $\sigma(\pi_1)$ is totally clean so we only need to show that $\sigma(x) \notin \mathrm{Sp}(\sigma(\pi_1))$. So suppose to the contrary that $\sigma(x) \in \mathrm{Sp}(\sigma(\pi_1))$. From proposition (206) we have $\mathrm{Sp}(\sigma(\pi_1)) \subseteq \sigma(\mathrm{Sp}(\pi_1))$ and it follows that $\sigma(x) = \sigma(u)$ for some $u \in \mathrm{Sp}(\pi_1)$. Having established that $x \notin \mathrm{Sp}(\pi_1)$ we must have $u \neq x$ and so $u \in \mathrm{Sp}(\pi_1) \setminus \{x\}$. Using proposition (210), since π_1 is totally clean we have $\mathrm{Sp}(\pi_1) \subseteq \mathrm{Fr}(\pi_1)$ and it follows that $u \in \mathrm{Fr}(\nabla x \pi_1)$ while $\sigma(u) = \sigma(x)$. This contradicts the implication (3.29) above. So we have proved that $\sigma(\pi)$ is totally clean and it remains to show (3.25), which goes as follows:

$$
\begin{array}{rcl}
\mathrm{Val}(\sigma(\pi)) & = & \mathrm{Val}(\sigma(\nabla x \pi_1)) \\
\text{def. (74)} \ \rightarrow & = & \mathrm{Val}(\nabla \sigma(x) \sigma(\pi_1)) \\
\sigma(x) \notin \mathrm{Sp}(\sigma(\pi_1)) \ \rightarrow & = & \forall \sigma(x) \mathrm{Val}(\sigma(\pi_1)) \\
\text{(3.25) true for } \pi_1 \ \rightarrow & = & \forall \sigma(x) \sigma(\mathrm{Val}(\pi_1)) \\
\text{def. (24)} \ \rightarrow & = & \sigma(\forall x \mathrm{Val}(\pi_1)) \\
x \notin \mathrm{Sp}(\pi_1) \ \rightarrow & = & \sigma(\mathrm{Val}(\nabla x \pi_1)) \\
 & = & \sigma(\mathrm{Val}(\pi))
\end{array}
$$

.

So we have made some reasonable progress in our quest towards the substitution theorem (30) of page 388 and the objective to carry over the sequent $\Gamma \vdash \phi$ into $\sigma(\Gamma) \vdash \sigma(\phi)$. Given reasonable assumptions on the proof π and substitution σ, proposition (229) shows that $\sigma(\pi)$ has the right property. Unfortunately, this will not take us very far. Given a sequent $\Gamma \vdash \phi$ with underlying proof π, even if we choose π to be totally clean we have no way to guarantee the validity of σ for π. In effect, proposition (229) is pretty useless. However, we know from proposition (224) that an injective map $\sigma : V \rightarrow W$ will always be valid for any

proof $\pi \in \mathbf{\Pi}(V)$. So we can prove a version of the substitution theorem in the injective case, which is the purpose of proposition (230) below. This is of course a very weak and temporary result. Dull, boring and expected. Is it ever the case that an injective map will fail to *carry over* properties nicely from one space to the other? Actually, coming to think of it, there is a case when injectivity is not enough to make a result trivial: suppose $\Gamma \subseteq \mathbf{P}(V)$ is a consistent subset, i.e. such that the sequent $\Gamma \vdash \bot$ is false. The fact that $\sigma(\Gamma)$ should also be consistent when $\sigma : V \to W$ is injective we feel is not trivial at all. It seems particularly hard when V is a finite set, a point we shall need to resolve later.

Proposition 230 *Let V, W be sets and $\sigma : V \to W$ be an injective map. Then for every subset $\Gamma \subseteq \mathbf{P}(V)$ and formula $\phi \in \mathbf{P}(V)$ we have the implication:*

$$\Gamma \vdash \phi \;\Rightarrow\; \sigma(\Gamma) \vdash \sigma(\phi)$$

where $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ also denotes the associated substitution mapping.

Proof
Let $\pi \in \mathbf{\Pi}(V)$ be a proof underlying the sequent $\Gamma \vdash \phi$. Without loss of generality, from proposition (185) we may assume that π is totally clean. Since σ is an injective map, from proposition (224) it is valid for π. Using proposition (229) it follows that $\mathrm{Val} \circ \sigma(\pi) = \sigma \circ \mathrm{Val}(\pi)$. Hence we see that $\mathrm{Val}(\sigma(\pi)) = \sigma(\phi)$. Furthermore from proposition (193) we obtain $\mathrm{Hyp}(\sigma(\pi)) = \sigma(\mathrm{Hyp}(\pi)) \subseteq \sigma(\Gamma)$. So we have found $\pi^* = \sigma(\pi) \in \mathbf{\Pi}(W)$ such that $\mathrm{Val}(\pi^*) = \sigma(\phi)$ together with $\mathrm{Hyp}(\pi^*) \subseteq \sigma(\Gamma)$. It follows that $\sigma(\Gamma) \vdash \sigma(\phi)$ as requested. **.**

3.3 Proof Modulo and Minimal Transform

3.3.1 Preliminaries

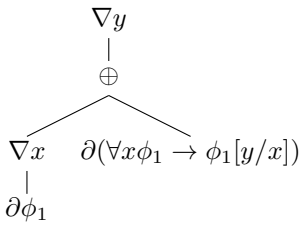
Using proposition (229), we obtained proposition (230) allowing us to carry over sequents from $\Gamma \vdash \phi$ to $\sigma(\Gamma) \vdash \sigma(\phi)$ in the case when $\sigma : V \to W$ is an injective map. There is only so much we can do with proposition (229). The equality $\mathrm{Val} \circ \sigma(\pi) = \sigma \circ \mathrm{Val}(\pi)$ cannot be inferred from it, unless σ is valid for π. In general, we have no way to tell whether a substitution σ is valid for a proof π underlying the sequent $\Gamma \vdash \phi$. We do not know which axioms are being used in the proof, simply by looking at the sequent. We need a whole new strategy.

We have dealt with this problem before. Given a map $\sigma : V \to W$ and a formula $\phi \in \mathbf{P}(V)$, we wanted to define a formula $\sigma(\phi)$ which is meaningful even in the case when σ is not valid for ϕ. Our solution was to introduce the minimal transform $\mathcal{M}(\phi)$ of definition (38) and consider the formula $\bar{\sigma} \circ \mathcal{M}(\phi)$ where all the free variables of ϕ are carried over by σ while avoiding capture. Likewise, given a map $\sigma : V \to W$ which may not be valid for the proof $\pi \in \mathbf{\Pi}(V)$, we want to define a proof $\sigma(\pi)$ which is meaningful even when σ is not valid for π. By *meaningful*, it is understood that the key equality $\mathrm{Val} \circ \sigma(\pi) = \sigma \circ \mathrm{Val}(\pi)$ should be satisfied. Of course, we also need to say something about the set

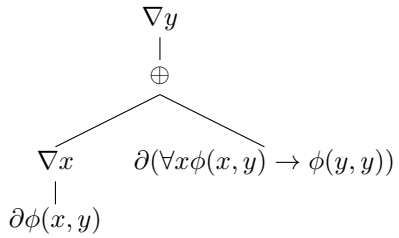
of hypothesis $\mathrm{Hyp}(\sigma(\pi))$ but this is usually a lot easier to achieve. So here is the plan: we should define the minimal transform $\mathcal{M}(\pi)$ which replaces all the bound variables of π by elements of a copy of $\mathbf{N}$ which is disjoint from V, and consider the proof $\bar{\sigma} \circ \mathcal{M}(\pi)$ in the hope that such a proof will have the right property, as the variable substitution will avoid capture. Recall that $\bar{\sigma} : \bar{V} \to \bar{W}$ is the minimal extension of σ as per definition (39). When attempting to define the minimal transform $\mathcal{M}(\pi)$, the obvious choice appears to set $\mathcal{M}(\pi) = \mathcal{M}(\phi)$ whenever $\pi = \phi$, $\mathcal{M}(\partial\phi) = \partial\mathcal{M}(\phi)$, $\mathcal{M}(\pi_1 \oplus \pi_2) = \mathcal{M}(\pi_1) \oplus \mathcal{M}(\pi_2)$ and:

$$\mathcal{M}(\nabla x \pi_1) = \nabla n \mathcal{M}(\pi_1)[n/x]$$

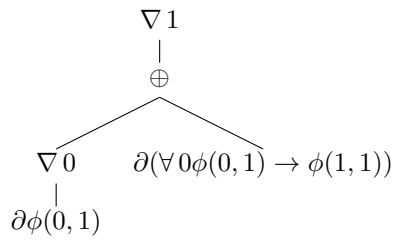
where $n = \min\{k \in \mathbf{N} : [k/x] \text{ valid for } \mathcal{M}(\pi_1)\}$. So let us look at an example:



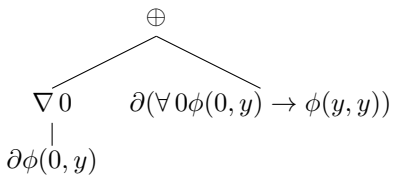
where $\phi_1 \in \mathbf{A}(V)$ is any axiom of first order logic and $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ is an essential substitution of y in place of x. To make our discussion simpler, let us define the map $\phi : V \times V \to \mathbf{A}(V)$ by setting $\phi(x, y) = \bot \to (\,(x \in y) \to \bot\,)$ and pick $\phi_1 = \phi(x, y)$ for some $x \neq y$. Then $\phi_1[y/x] = \phi(y, y)$. Our proof is:



which can be expressed as $\pi = \nabla y[\,\nabla x \partial\phi(x, y) \oplus \partial(\,\forall x \phi(x, y) \to \phi(y, y)\,)\,]$. This is arguably less readable than the tree representation. So $\mathcal{M}(\pi)$ becomes:



The key observation in this case is that $[0/y]$ is not valid for the proof:



and consequently the variable y had to be replaced by 1 instead of 0. Now it appears that the conclusion of $\mathcal{M}(\pi)$ is the formula $\mathrm{Val} \circ \mathcal{M}(\pi) = \forall\, 1\phi(1,1)$, while the conclusion of π is the formula $\mathrm{Val}(\pi) = \forall y \phi(y,y)$. It follows that $\mathcal{M} \circ \mathrm{Val}(\pi) = \forall\, 0\phi(0,0)$ and we are met with the fact that:

$$\mathrm{Val} \circ \mathcal{M}(\pi) \neq \mathcal{M} \circ \mathrm{Val}(\pi)$$

This is hugely disappointing. The conclusion of $\mathcal{M}(\pi)$ is not what we want it to be. Our plan is going to fail. However, it should be noted that $\forall\, 0\phi(0,0)$ and $\forall\, 1\phi(1,1)$ are equivalent modulo the substitution congruence $\sim$ and thus:

$$\mathrm{Val} \circ \mathcal{M}(\pi) \sim \mathcal{M} \circ \mathrm{Val}(\pi)$$

It may be that this equivalence is true at all times. It may also be sufficient for our purpose to carry over sequents $\Gamma \vdash \phi$. Our tentative definition of minimal transform for proofs may be appropriate after all. Unfortunately, this is seemingly not the case: consider the proof $\rho = \pi \oplus \partial(\forall y \phi(y,y) \to \phi(x,x))$. From $\mathrm{Val}(\pi) = \forall y \phi(y,y)$ we obtain $\mathrm{Val}(\rho) = \phi(x,x)$. Hence $\mathcal{M} \circ \mathrm{Val}(\rho) = \phi(x,x)$. In contrast we have $\mathcal{M}(\rho) = \mathcal{M}(\pi) \oplus \partial(\forall\, 0\phi(0,0) \to \phi(x,x))$. From the equality $\mathrm{Val} \circ \mathcal{M}(\pi) = \forall\, 1\phi(1,1)$ we see that $\mathcal{M}(\rho)$ is not a legitimate application of the modus ponens rule of inference and consequently $\mathrm{Val} \circ \mathcal{M}(\rho) = \bot \to \bot$. Thus, the equivalence $\mathrm{Val} \circ \mathcal{M}(\rho) \sim \mathcal{M} \circ \mathrm{Val}(\rho)$ is not even satisfied.

3.3.2 Valuation of Proof Modulo

In the previous section, we saw that a proof of the form $\pi = \pi_1 \oplus \pi_2$ where $\mathrm{Val}(\pi_1) = \forall\, 1\phi(1,1)$ and $\mathrm{Val}(\pi_2) = \forall\, 0\phi(0,0) \to \phi(x,x)$ fails to be a legitimate use of the modus ponens rule of inference. We are not discovering anything, as we knew this all along. We are deliberately being dumb, refusing to understand the proof π while any ordinary mathematician would most likely accept it as a legitimate proof of $\phi(x,x)$, provided both π_1 and π_2 are themselves acceptable. This is how we defined our key semantics on $\mathbf{\Pi}(V)$. From definition (69), the valuation mapping $\mathrm{Val} : \mathbf{\Pi}(V) \to \mathbf{P}(V)$ will not return anything sensible unless its argument is a totally clean proof, as per definition (73). The benefit of this approach is that we were able to define a notion of provability and sequent $\Gamma \vdash \phi$ in definition (70) while keeping to a minimum the complexity associated with the substitution congruence. As you may recall, we were not able to completely strip out references to this congruence, as our specialization axioms namely $\forall x \phi_1 \to \phi_1[y/x]$ are defined in terms of essential substitutions of y in place of x,

as per definition (62). However, we avoided the use of quotients and equivalence classes, while staying well clear of any informal treatment where the reader is casually invited to assume renaming of variables is continually taking place to avoid variable capture. In short, we kept it simple but without waving our hands on variable binding, capture and α-equivalence. It is all very nice, but we have now discovered a major flaw in this approach: as explained in the previous section, our very natural definition of minimal transform for proofs is failing, seemingly because $\pi = \pi_1 \oplus \pi_2$ is not regarded as a legitimate use of the modus ponens rule of inference, despite the equivalence $\forall 1\phi(1,1) \sim \forall 0\phi(0,0)$. So we are back to the drawing board. We are committed to defining a minimal transform mapping on $\mathbf{\Pi}(V)$ and our tentative definition is so natural that we do not believe it should be changed: what is wrong is our deductive system.

Luckily, we can address this issue with minimal work. We defined our set of proofs as a set of abstract formal expressions. $\mathbf{\Pi}(V)$ is a free universal algebra. This is as general as it gets. We allowed a proof $\pi_1 \oplus \pi_2$ to be meaningful at all times. A generalization $\nabla x \pi_1$ always exists. Even an axiom invocation $\partial\phi$ can be done without ϕ being an axiom of first order logic. A proof is just a skeleton. It doesn't say much about provability which is defined solely in terms of semantics. What matters is not so much the proof, but our interpretation of it. If we need to adjust our deductive system, we simply need to change the semantics. Right now, we have a valuation $\mathrm{Val} : \mathbf{\Pi}(V) \to \mathbf{P}(V)$ which maps every proof $\pi \in \mathbf{\Pi}(V)$ to its conclusion $\mathrm{Val}(\pi) \in \mathbf{P}(V)$. Although this map is a total function, it is only truly meaningful when π is totally clean, as per definition (73). In effect, the domain of the valuation Val is the set of totally clean proofs. This is our kernel for provability. We now wish to extend this kernel by defining a new valuation $\mathrm{Val}^+ : \mathbf{\Pi}(V) \to \mathbf{P}(V)$ which coincides with Val on totally clean proofs, but has a wider domain of acceptable proofs. We want this new valuation to be clever: it should know about α-equivalence and be flexible about it. It should not require that ϕ be an axiom of first order logic to accept $\partial\phi$ as a legitimate axiom invocation, but should return $\mathrm{Val}^+(\partial\phi) = \phi$ as long as ϕ is equivalent to an axiom. With this in mind, we define:

Definition 81 *Let V be a set and $\sim$ be the substitution congruence. We say that $\phi \in \mathbf{P}(V)$ is an* axiom modulo *if and only if there exists an axiom $\psi \in \mathbf{A}(V)$ such that $\phi \sim \psi$. The set of axioms modulo on $\mathbf{P}(V)$ is denoted $\mathbf{A}^+(V)$.*

So we should have $\mathrm{Val}^+(\partial\phi) = \phi$ whenever ϕ is an axiom modulo, which improves on $\mathrm{Val}(\partial\phi) = \bot \to \bot$ which may occur if ϕ is not strictly an axiom of first order logic. Thus, the valuation Val^+ will have more flexibility than Val with regards to axioms. We also want more flexibility with regards to modus ponens. At this point, we have $\mathrm{Val}(\pi_1 \oplus \pi_2) = M(\mathrm{Val}(\pi_1), \mathrm{Val}(\pi_2))$ where $M : \mathbf{P}(V)^2 \to \mathbf{P}(V)$ is the modus ponens mapping of definition (68). This mapping does not allow any equality modulo and insists on the strict equality $\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \to \phi$ for some $\phi \in \mathbf{P}(V)$. We shall introduce more flexibility in the valuation Val^+ by defining $\mathrm{Val}^+(\pi_1 \oplus \pi_2) = M^+(\mathrm{Val}^+(\pi_1), \mathrm{Val}^+(\pi_2))$ where $M^+ : \mathbf{P}(V)^2 \to \mathbf{P}(V)$ understands α-equivalence. Note that the fol-

lowing definition uses a notational shortcut for readability: the mathematical statement 'if $\phi_2 = \psi_1 \to \psi_2$ and $\psi_1 \sim \phi_1$' should be rightly understood to mean 'if there exist $\psi_1, \psi_2 \in \mathbf{P}(V)$ such that $\phi_2 = \psi_1 \to \psi_2$ and $\psi_1 \sim \phi_1$':

Definition 82 *Let V be a set and $\sim$ be the substitution congruence. We call* modus ponens mapping modulo *the map $M^+ : \mathbf{P}(V)^2 \to \mathbf{P}(V)$ defined by:*

$$\forall \phi_1, \phi_2 \in \mathbf{P}(V)\ ,\ M^+(\phi_1, \phi_2) = \begin{cases} \psi_2 & \text{if} \quad \phi_2 = \psi_1 \to \psi_2 \text{ and } \psi_1 \sim \phi_1 \\ \bot \to \bot & \text{otherwise} \end{cases}$$

It remains to deal with generalization. At this point, we have the equality $\mathrm{Val}(\nabla x \pi_1) = \bot \to \bot$ whenever x is not an arbitrary variable, i.e. $x \in \mathrm{Sp}(\pi_1)$. Such a variable is called a *specific* variable of the proof π_1 as per definition (67). The specific variables of π_1 are the free variables of the hypothesis of π_1. The free variables of any axiom involved in π_1 are considered *arbitrary*, i.e. not specific. If x is not a specific variable of π_1, then we have $\mathrm{Val}(\nabla x \pi_1) = \forall x \mathrm{Val}(\pi_1)$. When it comes to defining our extended valuation $\mathrm{Val}^+ : \mathbf{\Pi}(V) \to \mathbf{P}(V)$, there is not much flexibility which can be added with regards to generalization. We want Val^+ to be clever. We do not want it to accept proofs which are irretrievably flawed. We cannot allow a mathematician to generalize with respect to a variable which is not arbitrary. So we shall keep $\mathrm{Val}^+(\nabla x \pi_1) = \forall x \mathrm{Val}^+(\pi_1)$ whenever $x \notin \mathrm{Sp}(\pi_1)$ and set $\mathrm{Val}^+(\nabla x \pi_1) = \bot \to \bot$ otherwise, just like we did for Val :

Definition 83 *Let V be a set. We call* valuation mapping modulo *on $\mathbf{\Pi}(V)$ the map $\mathrm{Val}^+ : \mathbf{\Pi}(V) \to \mathbf{P}(V)$ defined by the recursion, given $\pi \in \mathbf{\Pi}(V)$:*

$$\mathrm{Val}^+(\pi) = \begin{cases} \phi & \text{if} \quad \pi = \phi \in \mathbf{P}(V) \\ \phi & \text{if} \quad \pi = \partial\phi,\ \phi \in \mathbf{A}^+(V) \\ \bot \to \bot & \text{if} \quad \pi = \partial\phi,\ \phi \notin \mathbf{A}^+(V) \\ M^+\left(\mathrm{Val}^+(\pi_1), \mathrm{Val}^+(\pi_2)\right) & \text{if} \quad \pi = \pi_1 \oplus \pi_2 \\ \forall x \mathrm{Val}^+(\pi_1) & \text{if} \quad \pi = \nabla x \pi_1,\ x \notin \mathrm{Sp}(\pi_1) \\ \bot \to \bot & \text{if} \quad \pi = \nabla x \pi_1,\ x \in \mathrm{Sp}(\pi_1) \end{cases}$$

where $M^+ : \mathbf{P}(V)^2 \to \mathbf{P}(V)$ refers to the modus ponens mapping modulo.

Proposition 231 *The structural recursion of* definition (82) *is legitimate.*

Proof
We need to prove the existence and uniqueness of $\mathrm{Val}^+ : \mathbf{\Pi}(V) \to \mathbf{P}(V)$, which satisfies the six conditions of definition (82). We cannot apply theorem (4) of page 42 in this case. The reason for this is that we do not wish $\mathrm{Val}^+(\nabla x \pi_1)$ to be simply a function of $\mathrm{Val}^+(\pi_1)$. Indeed, the conclusion modulo of the proof $\nabla x \pi_1$ depends on whether $x \in \mathrm{Sp}(\pi_1)$ or not. So we want $\mathrm{Val}^+(\nabla x \pi_1)$ to be a function of both $\mathrm{Val}^+(\pi_1)$ and π_1. So the main point is to define the mapping $h(\nabla x) : \mathbf{P}(V) \times \mathbf{\Pi}(V) \to \mathbf{P}(V)$ by $h(\nabla x)(\phi_1, \pi_1) = \forall x \phi_1$ if $x \notin \mathrm{Sp}(\pi_1)$ and $h(\nabla x)(\phi_1, \pi_1) = \bot \to \bot$ otherwise. We can then apply theorem (5) of page 44. Note that the mapping $h(\partial\phi) : \mathbf{P}(V)^0 \times \mathbf{\Pi}(V)^0 \to \mathbf{P}(V)$ should be defined

differently, depending on whether ϕ is an axiom modulo or not. If $\phi \in \mathbf{A}^+(V)$ we set $h(\partial\phi)(0,0) = \phi$ and otherwise $h(\partial\phi)(0,0) = \bot \to \bot$. .

From the beginning, our intention was to define an extension of the valuation Val from the domain of totally clean proofs to a wider domain. Having defined $\mathrm{Val}^+ : \mathbf{\Pi}(V) \to \mathbf{P}(V)$, our first step is to confirm Val^+ is indeed an extension:

Proposition 232 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$ be a totally clean proof. Then:*

$$\mathrm{Val}^+(\pi) = \mathrm{Val}(\pi)$$

Proof
We need to show the implication (π totally clean) $\Rightarrow$ $\mathrm{Val}^+(\pi) = \mathrm{Val}(\pi)$. We shall do so with a structural induction argument, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then π is always totally clean and we have $\mathrm{Val}^+(\pi) = \phi = \mathrm{Val}(\pi)$. Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. We need to show the implication is true for π. So we assume that π is totally clean. From definition (73) we obtain $\phi \in \mathbf{A}(V)$. So $\phi \in \mathbf{A}^+(V)$ and it follows that $\mathrm{Val}^+(\pi) = \phi = \mathrm{Val}(\pi)$. Next we assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs satisfying the implication. We need to show the same is true of π. So we assume that π is totally clean. From proposition (182) it follows that both π_1 and π_2 are totally clean and furthermore $\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \to \mathrm{Val}(\pi)$. Having assumed the implication is true for π_1, π_2, it follows that $\mathrm{Val}^+(\pi_1) = \mathrm{Val}(\pi_1)$ and $\mathrm{Val}^+(\pi_2) = \mathrm{Val}(\pi_2)$ and consequently $\mathrm{Val}^+(\pi_2) = \mathrm{Val}^+(\pi_1) \to \mathrm{Val}(\pi)$. In particular, we see that $\mathrm{Val}^+(\pi_2) = \psi_1 \to \psi_2$ with $\psi_1 \sim \mathrm{Val}^+(\pi_1)$ for some $\psi_1, \psi_2 \in \mathbf{P}(V)$, where $\sim$ is the substitution congruence on $\mathbf{P}(V)$. Using definition (82) it follows that $\mathrm{Val}^+(\pi) = \psi_2 = \mathrm{Val}(\pi)$. So we now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof satisfying the implication. We need to show the same is true of π. So we assume that π is totally clean. From proposition (183) it follows that π_1 is itself totally clean and furthermore $x \notin \mathrm{Sp}(\pi_1)$. Having assumed the implication is true for π_1, we see that $\mathrm{Val}^+(\pi_1) = \mathrm{Val}(\pi_1)$ and consequently:

$$\begin{array}{rcl}
\mathrm{Val}^+(\pi) & = & \mathrm{Val}^+(\nabla x \pi_1) \\
x \notin \mathrm{Sp}(\pi_1) \ \to & = & \forall x \mathrm{Val}^+(\pi_1) \\
& = & \forall x \mathrm{Val}(\pi_1) \\
x \notin \mathrm{Sp}(\pi_1) \ \to & = & \mathrm{Val}(\nabla x \pi_1) \\
& = & \mathrm{Val}(\pi)
\end{array}$$

.

From the valuation modulo $\mathrm{Val}^+ : \mathbf{\Pi}(V) \to \mathbf{P}(V)$ corresponds a notion of provability modulo and sequent modulo. In order for $\pi \in \mathbf{\Pi}(V)$ to be a proof modulo of ϕ from Γ, we are asking for the strict equality $\mathrm{Val}^+(\pi) = \phi$ and not simply for the substitution equivalence $\mathrm{Val}^+(\pi) \sim \phi$. We also require the inclusion $\mathrm{Hyp}(\pi) \subseteq \Gamma$ rather than a weaker condition involving α-equivalence. As we shall see in theorem (22) below, we could equally provide a definition of provability modulo with weaker conditions. However, we wanted the following

definition to mirror exactly definition (70) and emphasize a key fact: all we are doing is change the semantics on $\mathbf{\Pi}(V)$ from Val to Val^+ :

Definition 84 *Let V be a set. Let $\Gamma \subseteq \mathbf{P}(V)$ and $\phi \in \mathbf{P}(V)$. We say that $\pi \in \mathbf{\Pi}(V)$ is a* proof modulo of the formula ϕ from Γ *if and only if we have:*

$$\mathrm{Val}^+(\pi) = \phi \text{ and } \mathrm{Hyp}(\pi) \subseteq \Gamma$$

We say that ϕ is provable modulo from Γ *or that* Γ entails ϕ modulo *denoted:*

$$\Gamma \vdash_+ \phi$$

if and only if there exists a proof modulo $\pi \in \mathbf{\Pi}(V)$ of the formula ϕ from Γ.

As the following proposition shows, the notation $\Gamma \vdash_+ \phi$ is unlikely to be used again, as it is simply equivalent to $\Gamma \vdash \phi$. Thus, our new notion of *provability modulo* is in fact equivalent to our initial definition (70). This is of course extremely reassuring. We want our new valuation $\mathrm{Val}^+ : \mathbf{\Pi}(V) \to \mathbf{P}(V)$ to be clever enough to cope with the substitution congruence, in order to make sense of minimal transforms on $\mathbf{\Pi}(V)$. We do not want Val^+ to change the set of provable formulas on $\mathbf{P}(V)$. Somehow we believe '$\vdash \phi$' is an *absolute* on $\mathbf{P}(V)$.

Proposition 233 *Let V be a set. Let $\Gamma \subseteq \mathbf{P}(V)$ and $\phi \in \mathbf{P}(V)$. Then we have:*

$$\Gamma \vdash \phi \;\Leftrightarrow\; \Gamma \vdash_+ \phi$$

i.e. ϕ is provable from Γ if and only if ϕ is provable modulo from Γ.

Proof
First we show $\Rightarrow$: so we assume that $\Gamma \vdash \phi$, i.e. there exists $\pi \in \mathbf{\Pi}(V)$ which is a proof of ϕ from Γ. Using proposition (185), without loss of generality we may assume that π is totally clean. So we have found a totally clean proof $\pi \in \mathbf{\Pi}(V)$ such that $\mathrm{Hyp}(\pi) \subseteq \Gamma$ and $\mathrm{Val}(\pi) = \phi$. Since π is totally clean, from proposition (232) we have $\mathrm{Val}^+(\pi) = \mathrm{Val}(\pi)$. It follows that $\mathrm{Hyp}(\pi) \subseteq \Gamma$ and $\mathrm{Val}^+(\pi) = \phi$. This shows that π is a proof modulo of ϕ from Γ, and so $\Gamma \vdash_+ \phi$. We now prove $\Leftarrow$: in order to prove this implication, it is sufficient to show:

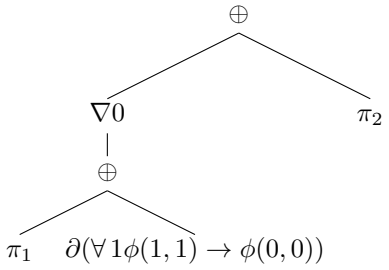
$$\mathrm{Hyp}(\pi) \vdash \mathrm{Val}^+(\pi) \tag{3.30}$$

for all $\pi \in \mathbf{\Pi}(V)$. In other words, the valuation modulo of a proof is provable from its hypothesis. Suppose this property has been proved. We shall show that the implication $\Leftarrow$ is true. So we assume that $\Gamma \vdash_+ \phi$. We need to show that $\Gamma \vdash \phi$. By assumption, there exists a proof $\pi \in \mathbf{\Pi}(V)$ such that $\mathrm{Hyp}(\pi) \subseteq \Gamma$ and $\mathrm{Val}^+(\pi) = \phi$. Having assumed that (3.30) is true we obtain $\mathrm{Hyp}(\pi) \vdash \phi$. From $\mathrm{Hyp}(\pi) \subseteq \Gamma$ we conclude that $\Gamma \vdash \phi$ as requested. So it remains to show that (3.30) is true. We shall do so with a structural induction argument, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. From definition (82) we have $\mathrm{Val}^+(\pi) = \phi$. Hence we need to show that $\{\phi\} \vdash \phi$ which

is clear. Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. We shall distinguish two cases: first we assume that ϕ is not an axiom modulo, i.e. $\phi \notin \mathbf{A}^+(V)$. From definition (82) we have $\mathrm{Val}^+(\pi) = \bot \to \bot$. Hence we need to show that $\vdash (\bot \to \bot)$ which follows from lemma (18). Next we assume that ϕ is an axiom modulo, i.e. $\phi \in \mathbf{A}^+(V)$. From definition (82) we have $\mathrm{Val}^+(\pi) = \phi$. So we need to show that $\vdash \phi$. However, from $\phi \in \mathbf{A}^+(V)$ and definition (80), there exists an axiom $\psi \in \mathbf{A}(V)$ such that $\phi \sim \psi$, where $\sim$ is the substitution congruence on $\mathbf{P}(V)$. Since ψ is an axiom, from proposition (160) it is provable i.e. we have $\vdash \psi$. It follows that $\vdash \psi$ and $\psi \sim \phi$, and from proposition (179) we conclude that $\vdash \phi$ as requested. So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs which satisfy the entailment (3.30). We need to show the same is true of π. We shall distinguish two cases: First we assume that $\mathrm{Val}^+(\pi_2)$ cannot be written as $\mathrm{Val}^+(\pi_2) = \psi_1 \to \psi_2$ where $\psi_1 \sim \mathrm{Val}^+(\pi_1)$. From definition (82) we have $\mathrm{Val}^+(\pi) = \bot \to \bot$ and we need to show that $\mathrm{Hyp}(\pi) \vdash (\bot \to \bot)$ which is clear. Next we assume that $\mathrm{Val}^+(\pi_2) = \psi_1 \to \psi_2$ where $\psi_1, \psi_2 \in \mathbf{P}(V)$ and $\psi_1 \sim \mathrm{Val}^+(\pi_1)$. From definition (82) we have $\mathrm{Val}^+(\pi) = \psi_2$ and we need to show that $\mathrm{Hyp}(\pi) \vdash \psi_2$. Using the modus ponens property of proposition (161) it is sufficient to prove that $\mathrm{Hyp}(\pi) \vdash \psi_1$ and $\mathrm{Hyp}(\pi) \vdash \psi_1 \to \psi_2$. First we show that $\mathrm{Hyp}(\pi) \vdash \psi_1 \to \psi_2$: We need to show that $\mathrm{Hyp}(\pi) \vdash \mathrm{Val}^+(\pi_2)$ which follows immediately from $\mathrm{Hyp}(\pi) \supseteq \mathrm{Hyp}(\pi_2)$ and the entailment (3.30) applied to π_2. So we now show that $\mathrm{Hyp}(\pi) \vdash \psi_1$. Since $\psi_1 \sim \mathrm{Val}^+(\pi_1)$, from proposition (179) it is sufficient to show that $\mathrm{Hyp}(\pi) \vdash \mathrm{Val}^+(\pi_1)$ which follows immediately from $\mathrm{Hyp}(\pi) \supseteq \mathrm{Hyp}(\pi_1)$ and the entailment (3.30) applied to π_1. This completes our induction argument in the case when $\pi = \pi_1 \oplus \pi_2$. So we now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof which satisfies the entailment (3.30). We need to show the same is true of π. We shall distinguish two cases: first we assume that $x \in \mathrm{Sp}(\pi_1)$. From definition (82) we have $\mathrm{Val}^+(\pi) = \bot \to \bot$ and we need to show that $\mathrm{Hyp}(\pi) \vdash (\bot \to \bot)$ which is clear. Next we assume that $x \notin \mathrm{Sp}(\pi_1)$. From definition (82) we have $\mathrm{Val}^+(\pi) = \forall x \mathrm{Val}^+(\pi_1)$ and we need to show that $\mathrm{Hyp}(\pi) \vdash \forall x \mathrm{Val}^+(\pi_1)$. Since $\mathrm{Hyp}(\pi) = \mathrm{Hyp}(\pi_1)$ we have to show that $\mathrm{Hyp}(\pi_1) \vdash \forall x \mathrm{Val}^+(\pi_1)$. Since $x \notin \mathrm{Sp}(\pi_1) = \mathrm{Fr}(\mathrm{Hyp}(\pi_1))$, from the generalization property of proposition (162) it is sufficient to prove that $\mathrm{Hyp}(\pi_1) \vdash \mathrm{Val}^+(\pi_1)$ which follows from the entailment (3.30) applied to π_1. .

Using proposition (233), we can now prove a sequent $\Gamma \vdash \phi$ with less work than before. Until now, we needed to find a proof $\pi \in \mathbf{\Pi}(V)$ with $\mathrm{Val}(\pi) = \phi$ and $\mathrm{Hyp}(\pi) \subseteq \Gamma$. We no longer need to have the equality $\mathrm{Val}(\pi) = \phi$ anymore. It is sufficient to have $\mathrm{Val}^+(\pi) = \phi$. So let us go back to our initial example of $\pi = \pi_1 \oplus \pi_2$ where $\mathrm{Val}(\pi_1) = \forall 1 \phi(1,1)$ and $\mathrm{Val}(\pi_2) = \forall 0 \phi(0,0) \to \phi(x,x)$. From the equality $\mathrm{Val}^+(\pi) = \phi(x,x)$ we can now claim that $\phi(x,x)$ is provable from $\Gamma = \mathrm{Hyp}(\pi)$ without any further justification. Without proposition (233), we would need to specialize the proof π_1 using the axiom of first order logic

$\forall 1\phi(1,1) \to \phi(0,0)$ and generalize with respect to 0 so as to obtain:



which is a proof π^* such that $\mathrm{Val}(\pi^*) = \phi(x,x)$ (assuming generalization in 0 is legitimate). So proposition (233) is an improvement allowing us to establish provability with the leaner proof $\pi_1 \oplus \pi_2$ instead of π^*. However, we can still do better than this: if $\sim$ is the substitution congruence on $\mathbf{P}(V)$, we know from proposition (179) that the sequent $\Gamma \vdash \phi$ is true whenever $\Gamma \vdash \psi$ and $\psi \sim \phi$. Hence the equality $\mathrm{Val}^+(\pi) = \phi$ should not be required. It should be sufficient to have $\mathrm{Val}^+(\pi) \sim \phi$. Similarly by virtue of the deduction theorem (21) of page 226, the inclusion $\mathrm{Hyp}(\pi) \subseteq \Gamma$ should not be required either. It should be sufficient that every element of $\mathrm{Hyp}(\pi)$ be equivalent to some element of Γ. Thus, in order to establish the sequent $\Gamma \vdash \phi$ it should be sufficient to find a proof $\pi \in \mathbf{\Pi}(V)$ such that $\mathrm{Val}^+(\pi) \sim \phi$ and $\mathrm{Hyp}(\pi) \precsim \Gamma$, where $\precsim$ is an inclusion modulo. We shall prove this fact in theorem (22) below. Before we can do so, we shall make precise the notion of *inclusion modulo*:

Definition 85 *Let V be a set and $\simeq$ be a congruence on $\mathbf{P}(V)$. We call* inclusion modulo *associated with $\simeq$ the relation $\precsim$ on $\mathcal{P}(\mathbf{P}(V))$ defined by the equivalence $\Gamma \precsim \Delta$ if and only if for all $\phi \in \Gamma$ there exists $\psi \in \Delta$ with $\phi \simeq \psi$.*

The notion of inclusion modulo leads naturally to that of *equality modulo* for subsets, which we shall use again in proposition (306). For reference:

Definition 86 *Let V be a set and $\simeq$ be a congruence on $\mathbf{P}(V)$. We call* equality modulo *associated with $\simeq$ the relation on $\mathcal{P}(\mathbf{P}(V))$ defined by:*

$$\Gamma \simeq \Delta \;\Leftrightarrow\; (\Gamma \precsim \Delta) \wedge (\Delta \precsim \Gamma)$$

where $\precsim$ is the inclusion modulo associated with the congruence $\simeq$.

Before we can prove theorem (22), we shall establish an easy consequence of proposition (179) and the transitivity of the consequence relation $\vdash$:

Proposition 234 *Let V be a set. Let $\Gamma, \Delta \subseteq \mathbf{P}(V)$ and $\phi \in \mathbf{P}(V)$. Then:*

$$(\Gamma \succsim \Delta) \wedge (\Delta \vdash \phi) \;\Rightarrow\; \Gamma \vdash \phi$$

where $\precsim$ denotes the inclusion modulo the substitution congruence on $\mathbf{P}(V)$.

Proof
Using the transitivity of the consequence relation $\vdash$ in the form of proposition (169) it is sufficient to prove that $\Gamma \vdash \psi$ for all $\psi \in \Delta$. So let $\psi \in \Delta$. We need to show that $\Gamma \vdash \psi$. However, from the assumption $\Gamma \succsim \Delta$, there exists $\phi \in \Gamma$ such that $\phi \sim \psi$, where $\sim$ is the substitution congruence on $\mathbf{P}(V)$. It is clear that $\Gamma \vdash \phi$. Hence from proposition (179) we obtain $\Gamma \vdash \psi$ as requested. **.**

We can now prove theorem (22) which is the main result of this section, and provide the weakest conditions allowing us to establish provability so far:

Theorem 22 *Let V be a set. Let $\Gamma \subseteq \mathbf{P}(V)$ and $\phi \in \mathbf{P}(V)$. Then the sequent $\Gamma \vdash \phi$ is true if and only if there exists a proof $\pi \in \mathbf{\Pi}(V)$ such that:*

$$\mathrm{Val}^+(\pi) \sim \phi \text{ and } \mathrm{Hyp}(\pi) \precsim \Gamma$$

where $\precsim$ denotes the inclusion modulo the substitution congruence $\sim$ on $\mathbf{P}(V)$.

Proof
First we show the 'only if' part: so we assume that $\Gamma \vdash \phi$. Using proposition (233) it follows that ϕ is provable modulo from Γ. Thus, there exists a proof $\pi \in \mathbf{\Pi}(V)$ such that $\mathrm{Val}^+(\pi) = \phi$ and $\mathrm{Hyp}(\pi) \subseteq \Gamma$. In particular we have $\mathrm{Val}^+(\pi) \sim \phi$ and $\mathrm{Hyp}(\pi) \precsim \Gamma$ as requested. We now prove the 'if' part: so we assume that $\pi \in \mathbf{\Pi}(V)$ is a proof such that $\mathrm{Val}^+(\pi) \sim \phi$ and $\mathrm{Hyp}(\pi) \precsim \Gamma$. We need to show that $\Gamma \vdash \phi$. From proposition (179) it is sufficient to prove $\Gamma \vdash \mathrm{Val}^+(\pi)$. However, since $\mathrm{Hyp}(\pi) \precsim \Gamma$, using proposition (234) it is sufficient to show that $\mathrm{Hyp}(\pi) \vdash \mathrm{Val}^+(\pi)$. Finally, using proposition (233) we simply need to show that $\mathrm{Val}^+(\pi)$ is provable modulo from $\mathrm{Hyp}(\pi)$. This is clear from definition (83) since π is a proof modulo of $\mathrm{Val}^+(\pi)$ from $\mathrm{Hyp}(\pi)$. **.**

We have now achieved the aim motivating this section. We wanted to change our deductive system by creating a valuation $\mathrm{Val}^+ : \mathbf{\Pi}(V) \to \mathbf{P}(V)$ which extends $\mathrm{Val} : \mathbf{\Pi}(V) \to \mathbf{P}(V)$ from totally clean proofs to a wider domain, thereby introducing flexibility and awareness of α-equivalence. This allowed us to prove theorem (22) providing a convenient way to establish the truth of any sequent $\Gamma \vdash \phi$. It will also allow us to define the minimal transform $\mathcal{M}(\pi)$ of any proof $\pi \in \mathbf{\Pi}(V)$. Before we complete this section, we shall establish a few elementary results regarding the valuation Val^+. We start with the fact that variables of conclusions of sub-proofs are variables of the proof:

Proposition 235 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$. Then we have:*

$$\cup\{\, \mathrm{Var}(\mathrm{Val}^+(\rho)) \;:\; \rho \preceq \pi \,\} \subseteq \mathrm{Var}(\pi) \tag{3.31}$$

i.e. the variables of conclusions modulo of sub-proofs of π are variables of π.

Proof
We shall prove inclusion (3.31) with a structural induction argument, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. From definition (19), the only sub-proof of π is π itself. Hence we need to show

the inclusion $\mathrm{Var}(\mathrm{Val}^+(\pi)) \subseteq \mathrm{Var}(\pi)$ which follows from $\mathrm{Var}(\pi) = \mathrm{Var}(\phi)$ and $\mathrm{Val}^+(\pi) = \phi$. Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then again the only sub-proof of π is π itself and we need to show that $\mathrm{Var}(\mathrm{Val}^+(\pi)) \subseteq \mathrm{Var}(\pi)$. We shall distinguish two cases: first we assume that $\phi \in \mathbf{A}^+(V)$. Then we have $\mathrm{Val}^+(\pi) = \phi$ while $\mathrm{Var}(\pi) = \mathrm{Var}(\phi)$ so the inclusion is clear. Next we assume that $\phi \notin \mathbf{A}^+(V)$. Then $\mathrm{Val}^+(\pi) = \bot \to \bot$ so $\mathrm{Var}(\mathrm{Val}^+(\pi)) = \emptyset$ and the inclusion is also true. So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs for which the inclusion (3.31) is true. Then we have:

$$\begin{array}{rcl}
\mathrm{Var}(\pi) & = & \mathrm{Var}(\pi_1 \oplus \pi_2) \\
& = & \mathrm{Var}(\pi_1) \cup \mathrm{Var}(\pi_2) \\
& \supseteq & (\cup\{\mathrm{Var}(\mathrm{Val}^+(\rho)) : \rho \preceq \pi_1\}) \cup (\cup\{\mathrm{Var}(\mathrm{Val}^+(\rho)) : \rho \preceq \pi_2\}) \\
& = & \cup\{\mathrm{Var}(\mathrm{Val}^+(\rho)) : \rho \in \mathrm{Sub}(\pi_1) \cup \mathrm{Sub}(\pi_2)\} \\
\text{A: below} \to & = & \cup\{\mathrm{Var}(\mathrm{Val}^+(\rho)) : \rho \in \mathrm{Sub}(\pi_1) \cup \mathrm{Sub}(\pi_2) \cup \{\pi_1 \oplus \pi_2\}\} \\
\text{def. (19)} \to & = & \cup\{\mathrm{Var}(\mathrm{Val}^+(\rho)) : \rho \in \mathrm{Sub}(\pi_1 \oplus \pi_2)\} \\
& = & \cup\{\mathrm{Var}(\mathrm{Val}^+(\rho)) : \rho \preceq \pi\}
\end{array}$$

So it remains to show point A: The inclusion $\subseteq$ is clear. In order to show $\supseteq$ it is sufficient to show that $\rho = \pi_1 \oplus \pi_2$ does not enlarge the set, that is:

$$\mathrm{Var}(\mathrm{Val}^+(\pi_1 \oplus \pi_2)) \subseteq \cup\{\mathrm{Var}(\mathrm{Val}^+(\rho)) : \rho \in \mathrm{Sub}(\pi_1) \cup \mathrm{Sub}(\pi_2)\}$$

We shall distinguish two cases: first we assume that $\mathrm{Val}^+(\pi_1 \oplus \pi_2) = \bot \to \bot$. Then the inclusion is clear. Next we assume that $\mathrm{Val}^+(\pi_1 \oplus \pi_2) \neq \bot \to \bot$. Then we must have $\mathrm{Val}^+(\pi_2) = \psi_1 \to \psi_2$ for some ψ_1, ψ_2 such that $\psi_1 \sim \mathrm{Val}^+(\pi_1)$ and $\psi_2 = \mathrm{Val}^+(\pi_1 \oplus \pi_2)$, where $\sim$ is the substitution congruence. Consequently:

$$\mathrm{Var}(\mathrm{Val}^+(\pi_1 \oplus \pi_2)) = \mathrm{Var}(\psi_2) \subseteq \mathrm{Var}(\mathrm{Val}^+(\pi_2))$$

and the inclusion is also clear. So we now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof for which inclusion (3.31) is true:

$$\begin{array}{rcl}
\mathrm{Var}(\pi) & = & \mathrm{Var}(\nabla x \pi_1) \\
& = & \{x\} \cup \mathrm{Var}(\pi_1) \\
& \supseteq & \{x\} \cup (\cup\{\mathrm{Var}(\mathrm{Val}^+(\rho)) : \rho \in \mathrm{Sub}(\pi_1)\}) \\
\text{A: to be proved} \to & = & \cup\{\mathrm{Var}(\mathrm{Val}^+(\rho)) : \rho \in \mathrm{Sub}(\pi_1) \cup \{\nabla x \pi_1\}\} \\
\text{def. (19)} \to & = & \cup\{\mathrm{Var}(\mathrm{Val}^+(\rho)) : \rho \in \mathrm{Sub}(\nabla x \pi_1)\} \\
& = & \cup\{\mathrm{Var}(\mathrm{Val}^+(\rho)) : \rho \preceq \pi\}
\end{array}$$

So it remains to show point A. We shall distinguish two cases: first we assume that $x \in \mathrm{Sp}(\pi_1)$. Then $\mathrm{Val}^+(\nabla x \pi_1) = \bot \to \bot$ and $\mathrm{Var}(\mathrm{Val}^+(\rho)) = \emptyset$ in the case when $\rho = \nabla x \pi_1$. So the inclusion $\supseteq$ is clear. In order to show $\subseteq$, it is

sufficient to prove that $x \in \mathrm{Var}(\mathrm{Val}^+(\rho))$ for some $\rho \in \mathrm{Sub}(\pi_1)$. However, since $x \in \mathrm{Sp}(\pi_1)$, from definition (67) we have $x \in \mathrm{Fr}(\phi)$ for some $\phi \in \mathrm{Hyp}(\pi_1)$. Defining $\rho = \phi$ from proposition (191) we have $\rho \in \mathrm{Sub}(\pi_1)$ and furthermore since $\mathrm{Val}^+(\rho) = \phi$ and $\mathrm{Fr}(\phi) \subseteq \mathrm{Var}(\phi)$ we conclude that $x \in \mathrm{Var}(\mathrm{Val}^+(\rho))$. So we now assume that $x \notin \mathrm{Sp}(\pi_1)$. Then $\mathrm{Val}^+(\nabla x\pi_1) = \forall x \mathrm{Val}^+(\pi_1)$ and:

$$\mathrm{Var}(\mathrm{Val}^+(\nabla x\pi_1)) = \{x\} \cup \mathrm{Var}(\mathrm{Val}^+(\pi_1)) \tag{3.32}$$

In particular, we see that $x \in \mathrm{Var}(\mathrm{Val}^+(\rho))$ in the case when $\rho = \nabla x\pi_1$ and the inclusion $\subseteq$ is clear. In order to show $\supseteq$ we simply need to prove:

$$\mathrm{Var}(\mathrm{Val}^+(\nabla x\pi_1)) \subseteq \{x\} \cup (\cup\{\mathrm{Var}(\mathrm{Val}^+(\rho)) : \rho \in \mathrm{Sub}(\pi_1)\})$$

which follows immediately from equation (3.32) and the fact that $\pi_1 \in \mathrm{Sub}(\pi_1)$.
.

The free variables of the conclusion modulo of a proof are free variables of the proof itself. Remember that free variables of a sub-proof may not be free variables of the proof. So although we can claim that $\mathrm{Fr}(\mathrm{Val}^+(\rho)) \subseteq \mathrm{Fr}(\rho)$ for every sub-proof $\rho \preceq \pi$, the inclusion $\mathrm{Fr}(\mathrm{Val}^+(\rho)) \subseteq \mathrm{Fr}(\pi)$ is false in general.

Proposition 236 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$. Then we have the inclusion:*

$$\mathrm{Fr}(\mathrm{Val}^+(\pi)) \subseteq \mathrm{Fr}(\pi)$$

i.e. the free variables of the conclusion modulo of π are free variables of π.

Proof
We shall prove this inclusion with a structural induction, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then the inclusion follows immediately from $\mathrm{Val}^+(\phi) = \phi$. Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. We need to show the inclusion holds for π. This is clearly the case if $\mathrm{Val}^+(\pi) = \bot \to \bot$. So we may assume that $\mathrm{Val}^+(\pi) \neq \bot \to \bot$ in which case ϕ is an axiom modulo, i.e. $\phi \in \mathbf{A}^+(V)$ and consequently $\mathrm{Val}^+(\pi) = \phi$. It follows that $\mathrm{Fr}(\mathrm{Val}^+(\pi)) = \mathrm{Fr}(\phi) = \mathrm{Fr}(\partial\phi) = \mathrm{Fr}(\pi)$ and in particular the inclusion holds. So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs satisfying the inclusion. We need to show the same is true of π. This is clearly the case if $\mathrm{Val}^+(\pi) = \bot \to \bot$. So we may assume that $\mathrm{Val}^+(\pi) \neq \bot \to \bot$ in which case $\mathrm{Val}^+(\pi_2) = \psi_1 \to \psi_2$ for some $\psi_1, \psi_2 \in \mathbf{P}(V)$ with $\psi_1 \sim \mathrm{Val}^+(\pi_1)$ and $\psi_2 = \mathrm{Val}^+(\pi)$, where $\sim$ denotes the substitution congruence on $\mathbf{P}(V)$:

$$\begin{aligned}
\mathrm{Fr}(\mathrm{Val}^+(\pi)) &= \mathrm{Fr}(\psi_2) \\
&\subseteq \mathrm{Fr}(\psi_1) \cup \mathrm{Fr}(\psi_2) \\
&= \mathrm{Fr}(\psi_1 \to \psi_2) \\
&= \mathrm{Fr}(\mathrm{Val}^+(\pi_2)) \\
&\subseteq \mathrm{Fr}(\pi_2) \\
&\subseteq \mathrm{Fr}(\pi_1) \cup \mathrm{Fr}(\pi_2) \\
&= \mathrm{Fr}(\pi_1 \oplus \pi_2) \\
&= \mathrm{Fr}(\pi)
\end{aligned}$$

So we now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof satisfying our inclusion. We need to show the same is true of π. This is clearly the case if $\mathrm{Val}^+(\pi) = \bot \to \bot$. So we may assume that $\mathrm{Val}^+(\pi) \neq \bot \to \bot$ in which case we have $x \notin \mathrm{Sp}(\pi_1)$ and $\mathrm{Val}^+(\pi) = \forall x \mathrm{Val}^+(\pi_1)$. Hence:

$$\begin{aligned} \mathrm{Fr}(\mathrm{Val}^+(\pi)) &= \mathrm{Fr}(\forall x \mathrm{Val}^+(\pi_1)) \\ &= \mathrm{Fr}(\mathrm{Val}^+(\pi_1)) \setminus \{x\} \\ &\subseteq \mathrm{Fr}(\pi_1) \setminus \{x\} \\ &= \mathrm{Fr}(\nabla x \pi_1) \\ &= \mathrm{Fr}(\pi) \end{aligned}$$

.

In definition (79) we extended the notion of *valid substitution* from formulas to proofs. We made sure every valid substitution would be valid for every hypothesis and every axiom of a given proof. We also made sure the substitution would avoid variable capture which may arise from generalization. The following proposition may be seen as a vindication of the valuation modulo $\mathrm{Val}^+ : \mathbf{\Pi}(V) \to \mathbf{P}(V)$ as well as of definition (79): every valid substitution is in fact also valid for all intermediary conclusions arising from the proof:

Proposition 237 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\pi \in \mathbf{\Pi}(V)$. Then if σ is valid for π, for all $\rho \in \mathbf{\Pi}(V)$ we have the implication:*

$$\rho \preceq \pi \;\Rightarrow\; \sigma \textit{ valid for } \mathrm{Val}^+(\rho)$$

Proof
Given $\pi \in \mathbf{\Pi}(V)$, it is sufficient to show the following implication:

$$(\sigma \text{ valid for } \pi) \;\Rightarrow\; \sigma \text{ valid for } \mathrm{Val}^+(\pi)$$

Indeed, suppose we have done so. Then if σ is valid for π and $\rho \preceq \pi$, from proposition (217) σ is also valid for ρ and consequently from the implication it is valid for $\mathrm{Val}^+(\rho)$. So the proposition is proved. We shall prove the implication with a structural induction argument, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then the implication follows immediately from $\mathrm{Val}^+(\phi) = \phi$. Next we assume that $\pi = \partial\phi$ for $\phi \in \mathbf{P}(V)$. We need to show the implication is true for π. So we assume that σ is valid for π. We need to show it is valid for $\mathrm{Val}^+(\pi)$. This is obviously the case when $\mathrm{Val}^+(\pi) = \bot \to \bot$. So we may assume that $\mathrm{Val}^+(\pi) \neq \bot \to \bot$ in which case ϕ is an axiom modulo, i.e. $\phi \in \mathbf{A}^+(V)$. It follows that $\mathrm{Val}^+(\pi) = \phi$ and we need to show that σ is valid for ϕ. This follows from proposition (218) and the fact that σ is valid for $\pi = \partial\phi$. So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs satisfying our implication. We need to show the same is true of π. So we assume that σ is valid for π. We need to show that σ is valid for $\mathrm{Val}^+(\pi)$. This is obviously the case if $\mathrm{Val}^+(\pi) = \bot \to \bot$. So we may

assume that $\mathrm{Val}^+(\pi) \neq \bot \to \bot$ in which case we have $\mathrm{Val}^+(\pi_2) = \psi_1 \to \psi_2$ where $\psi_1, \psi_2 \in \mathbf{P}(V)$ are such that $\psi_1 \sim \mathrm{Val}^+(\pi_1)$ and $\psi_2 = \mathrm{Val}^+(\pi)$, where $\sim$ denotes substitution congruence on $\mathbf{P}(V)$. So we need to show that σ is valid for ψ_2. Using proposition (54), it is sufficient to prove that σ is valid for $\mathrm{Val}^+(\pi_2)$. Having assumed the implication is true for π_2, we simply need to show that σ is valid for π_2 which follows from proposition (219) and the validity of σ for π. So we now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof satisfying our implication. We need to show the same is true of π. So we assume that σ is valid for π. We need to show it is valid for $\mathrm{Val}^+(\pi)$. This is obviously the case if $\mathrm{Val}^+(\pi) = \bot \to \bot$. So we may assume that $\mathrm{Val}^+(\pi) \neq \bot \to \bot$ in which case $x \notin \mathrm{Sp}(\pi_1)$ and $\mathrm{Val}^+(\pi) = \forall x \mathrm{Val}^+(\pi_1)$. So we need to show that σ is valid for $\forall x \mathrm{Val}^+(\pi_1)$. Using proposition (55), it is sufficient to show that σ is valid for $\mathrm{Val}^+(\pi_1)$ and furthermore given $u \in \mathrm{Fr}(\forall x \mathrm{Val}^+(\pi_1))$, that $\sigma(u) \neq \sigma(x)$. However, using proposition (236) we have $\mathrm{Fr}(\mathrm{Val}^+(\pi_1)) \subseteq \mathrm{Fr}(\pi_1)$ and so:

$$\mathrm{Fr}(\forall x \mathrm{Val}^+(\pi_1)) \subseteq \mathrm{Fr}(\pi_1) \setminus \{x\} = \mathrm{Fr}(\nabla x \pi_1)$$

So it is sufficient to show the implication $u \in \mathrm{Fr}(\nabla x \pi_1) \Rightarrow \sigma(u) \neq \sigma(x)$ which follows from proposition (220) and the validity of σ for $\pi = \nabla x \pi_1$. So it remains to show that σ is valid for $\mathrm{Val}^+(\pi_1)$. Having assumed our implication is true for π_1, we simply need to prove that σ is valid for π_1 which follows once again from proposition (220) and the validity of σ for $\pi = \nabla x \pi_1$. .

3.3.3 Clean Proof

In the previous section, we introduced a new semantics on our free universal algebra of proofs $\mathbf{\Pi}(V)$. The new valuation $\mathrm{Val}^+ : \mathbf{\Pi}(V) \to \mathbf{P}(V)$ was designed to be more flexible and specifically to cope with the substitution congruence, commonly known as α-equivalence. We made sure that Val^+ would be an extension of $\mathrm{Val} : \mathbf{\Pi}(V) \to \mathbf{P}(V)$ from the domain of totally clean proofs to a larger domain on which we shall now focus. It would be wrong to think that the new flexibility embedded in Val^+ allows it it to return a meaningful conclusion $\mathrm{Val}^+(\pi)$ for every $\pi \in \mathbf{\Pi}(V)$. Some elements of $\mathbf{\Pi}(V)$ are regarded as *flawed*, as they contain steps which are not legitimate. For example, the proof $\pi = \partial\phi$ is not a legitimate axiom invocation unless ϕ is an axiom modulo, namely $\phi \in \mathbf{A}^+(V)$ as per definition (80). The proof $\pi = \pi_1 \oplus \pi_2$ is not a legitimate use of the modus ponens rule of inference unless the conclusion modulo of π_2 is of the form $\mathrm{Val}^+(\pi_2) = \psi_1 \to \psi_2$ for some $\psi_1, \psi_2 \in \mathbf{P}(V)$ where ψ_1 is substitution equivalent to the conclusion modulo of π_1. The proof $\pi = \nabla x \pi_1$ is not a legitimate use of the generalization rule of inference unless the variable x is truly arbitrary, i.e. is not a specific variable of the proof π_1. In this section, we intend to study those proof $\pi \in \mathbf{\Pi}(V)$ which do not contain any flawed steps in relation to the valuation modulo Val^+. These proofs constitute the true domain of Val^+ and will be called *clean proofs*. Although $\mathrm{Val}^+ : \mathbf{\Pi}(V) \to \mathbf{P}(V)$ is a total function and $\mathrm{Val}^+(\pi)$ is provable for all $\pi \in \mathbf{\Pi}(V)$, the clean proofs play an important role for us as their behavior is predictable in relation to Val^+,

just like totally clean proofs were seen to be predictable in relation to Val. In particular, we shall see that the crucial equality $\mathrm{Val}^+ \circ \sigma(\pi) = \sigma \circ \mathrm{Val}^+(\pi)$ does hold for clean proofs in proposition (248), provided σ is valid for π. We shall also prove the α-equivalence $\mathrm{Val}^+ \circ \mathcal{M}(\pi) \sim \mathcal{M} \circ \mathrm{Val}^+(\pi)$ in proposition (254), which will vindicate our chosen definition of minimal transform for proofs and our design of Val^+. In definition (73) we defined totally clean proofs in terms of a *strength mapping* $s : \mathbf{\Pi}(V) \to 2$ and showed in proposition (184) that totally clean proofs were simply proofs without flawed steps. In this section, we shall define clean proofs directly in the spirit of proposition (184). A clean proof is simply a proof without *flawed steps*, after *flawlessness* has been redefined. Note that the mathematical statement (ii) of the following definition is a notational shortcut, where '*there exists* $\psi_1, \psi_2 \in \mathbf{P}(V)$ *such that...*' has been omitted:

Definition 87 *Let V be a set and $\sim$ be the substitution congruence. A proof $\pi \in \mathbf{\Pi}(V)$ is* clean *if and only if for all $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$, $\phi \in \mathbf{P}(V)$ and $x \in V$:*

$$(i) \quad \partial\phi \preceq \pi \;\Rightarrow\; \phi \in \mathbf{A}^+(V)$$

$$(ii) \quad \pi_1 \oplus \pi_2 \preceq \pi \;\Rightarrow\; \mathrm{Val}^+(\pi_2) = \psi_1 \to \psi_2 \text{ where } \psi_1 \sim \mathrm{Val}^+(\pi_1)$$

$$(iii) \quad \nabla x \pi_1 \preceq \pi \;\Rightarrow\; x \notin \mathrm{Sp}(\pi_1)$$

We claimed that Val^+ was an extension of Val and indeed we proved in proposition (232) that $\mathrm{Val}^+(\pi) = \mathrm{Val}(\pi)$ whenever π is totally clean. Strictly speaking, in order for Val^+ to qualify as an *extension* of Val, it should have a wider domain than Val. A totally clean proof should also be clean:

Proposition 238 *Let V be a set. If $\pi \in \mathbf{\Pi}(V)$ is totally clean, then it is clean.*

Proof
We assume that π is totally clean. We need to show that π is clean, namely that (i), (ii) and (iii) of definition (86) hold. First we show (i): so we assume that $\partial\phi$ is a sub-proof of π. We need to show that ϕ is an axiom modulo. However, from proposition (184) we have $\phi \in \mathbf{A}(V)$, i.e. ϕ is an axiom. In particular, from definition (80) we obtain $\phi \in \mathbf{A}^+(V)$ as requested. Next we show (ii): so we assume that $\pi_1 \oplus \pi_2$ is a sub-proof of π. We need to show that $\mathrm{Val}^+(\pi_2) = \psi_1 \to \psi_2$ for some $\psi_1, \psi_2 \in \mathbf{P}(V)$ such that $\psi_1 \sim \mathrm{Val}^+(\pi_1)$. However, since $\pi_1 \preceq \pi$ and $\pi_2 \preceq \pi$ from proposition (181) both π_1 and π_2 are totally clean proofs. It follows from proposition (232) that $\mathrm{Val}^+(\pi_1) = \mathrm{Val}(\pi_1)$ and $\mathrm{Val}^+(\pi_2) = \mathrm{Val}(\pi_2)$. Hence we need to show that $\mathrm{Val}(\pi_2) = \psi_1 \to \psi_2$ for some $\psi_1, \psi_2 \in \mathbf{P}(V)$ such that $\psi_1 \sim \mathrm{Val}(\pi_1)$. However since $\pi_1 \oplus \pi_2 \preceq \pi$ and π is totally clean, from proposition (184) we obtain $\mathrm{Val}(\pi_2) = \psi_1 \to \psi_2$ as requested where $\psi_1 = \mathrm{Val}(\pi_1)$ and $\psi_2 = \mathrm{Val}(\pi_1 \oplus \pi_2)$. So we now prove (iii): we assume that $\nabla x \pi_1 \preceq \pi$. From proposition (184) we obtain $x \notin \mathrm{Sp}(\pi_1)$. **.**

A proof is clean if it is *flawless*. So every sub-proof should also be *flawless*. Conversely if every sub-proof is clean, we should expect the proof to be clean. This is similar to proposition (181) which was established for totally clean proofs:

Proposition 239 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$. Then the proof π is clean if and only if every sub-proof $\rho \preceq \pi$ of π is itself clean.*

Proof
Since π is a sub-proof of itself, the 'if' part is clear. So we assume that π is clean and $\rho \preceq \pi$. We need to show that ρ is clean. This follows immediately from the transitivity of the sub-proof partial order on $\mathbf{\Pi}(V)$: if $\partial\phi \preceq \rho$ then $\partial\phi \preceq \pi$ and consequently $\phi \in \mathbf{A}^+(V)$. If $\pi_1 \oplus \pi_2 \preceq \rho$, then $\pi_1 \oplus \pi_2 \preceq \pi$ and consequently $\mathrm{Val}^+(\pi_2) = \psi_1 \rightarrow \psi_2$ for some $\psi_1, \psi_2 \in \mathbf{P}(V)$ such that $\psi_1 \sim \mathrm{Val}^+(\pi_1)$. If $\nabla x \pi_1 \preceq \rho$ then $\nabla x \pi_1 \preceq \pi$ and consequently we have $x \notin \mathrm{Sp}(\pi_1)$. .

Just like in the case of totally clean proofs, we need the appropriate tools to perform structural induction arguments on clean proofs. Thus we need to say something on clean proofs of the form $\pi_1 \oplus \pi_2$ and $\nabla x \pi_1$ in relation to π_1 and π_2. The following proposition is the counterpart of proposition (182):

Proposition 240 *Let V be a set and π be a proof of the form $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$. Let $\sim$ be the substitution congruence on $\mathbf{P}(V)$. Then π is a clean proof if and only if both π_1, π_2 are clean and we have the equality:*

$$\mathrm{Val}^+(\pi_2) = \psi_1 \rightarrow \psi_2$$

for some $\psi_1, \psi_2 \in \mathbf{P}(V)$ such that $\psi_1 \sim \mathrm{Val}^+(\pi_1)$ in which case $\psi_2 = \mathrm{Val}^+(\pi)$.

Proof
If $\mathrm{Val}^+(\pi_2) = \psi_1 \rightarrow \psi_2$ where $\psi_1 \sim \mathrm{Val}^+(\pi_1)$ then from definition (82) :

$$\begin{array}{rcl} \mathrm{Val}^+(\pi) & = & \mathrm{Val}^+(\pi_1 \oplus \pi_2) \\ & = & M^+\left(\mathrm{Val}^+(\pi_1), \mathrm{Val}^+(\pi_2)\right) \\ & = & M^+\left(\mathrm{Val}^+(\pi_1), \psi_1 \rightarrow \psi_2\right) \\ \text{def. (81), } \psi_1 \sim \mathrm{Val}^+(\pi_1) \rightarrow & = & \psi_2 \end{array}$$

So it remains to show the equivalence. First we show the 'only if' part: so we assume that $\pi = \pi_1 \oplus \pi_2$ is a clean proof. Since $\pi_1 \preceq \pi$ and $\pi_2 \preceq \pi$, from proposition (239) we see that both π_1 and π_2 are clean. Furthermore, from $\pi_1 \oplus \pi_2 \preceq \pi$ and (ii) of definition (86) we see that $\mathrm{Val}^+(\pi_2) = \psi_1 \rightarrow \psi_2$ as requested for some $\psi_1, \psi_2 \in \mathbf{P}(V)$ such that $\psi_1 \sim \mathrm{Val}^+(\pi_1)$. We now show the 'if' part: so we assume that both π_1, π_2 are clean and furthermore that $\mathrm{Val}^+(\pi_2) = \psi_1 \rightarrow \psi_2$ where $\psi_1 \sim \mathrm{Val}^+(\pi_1)$. We need to show that $\pi = \pi_1 \oplus \pi_2$ is clean, namely that (i), (ii) and (iii) of definition (86) hold. First we show (i). So we assume that $\partial\phi \preceq \pi = \pi_1 \oplus \pi_2$. From theorem (2) of page 21, we cannot possibly have $\partial\phi = \pi_1 \oplus \pi_2$. It follows that $\partial\phi \preceq \pi_1$ or $\partial\phi \preceq \pi_2$, and $\phi \in \mathbf{A}^+(V)$ follows from the fact that both π_1 and π_2 are clean. We now prove (iii). So we assume that $\nabla x \rho_1 \preceq \pi = \pi_1 \oplus \pi_2$. Once again we cannot possibly have $\nabla x \rho_1 = \pi_1 \oplus \pi_2$ and it follows that $\nabla x \rho_1 \preceq \pi_1$ or $\nabla x \rho_1 \preceq \pi_2$. So $x \notin \mathrm{Sp}(\rho_1)$ follows from the fact that π_1 and π_2 are clean proofs. We now prove (ii). So we assume that $\rho_1 \oplus \rho_2 \preceq \pi = \pi_1 \oplus \pi_2$. We need to show that $\mathrm{Val}^+(\rho_2) = \psi_1 \rightarrow \psi_2$ for some ψ_1, ψ_2 with $\psi_1 \sim \mathrm{Val}^+(\rho_1)$. If $\rho_1 \oplus \rho_2 = \pi$ then from theorem (2) of page 21 we have $\rho_1 = \pi_1$ and $\rho_2 = \pi_2$ and the conclusion is true by assumption. Otherwise, if $\rho_1 \oplus \rho_2 \neq \pi$ then $\rho_1 \oplus \rho_2 \preceq \pi_1$ or $\rho_1 \oplus \rho_2 \preceq \pi_2$, and the conclusion follows from the fact that both π_1 and π_2 are clean proofs. .

The following is the counterpart of proposition (183) for clean proofs:

Proposition 241 *Let V be a set and $\pi = \nabla x \pi_1$ where $\pi_1 \in \mathbf{\Pi}(V)$ and $x \in V$. Then π is a clean proof if and only if π_1 is itself clean and $x \notin \mathrm{Sp}(\pi_1)$.*

Proof
First we show the 'only if' part: so we assume that $\pi = \nabla x \pi_1$ is a clean proof. Since $\pi_1 \preceq \pi$ we see that π_1 is itself clean from proposition (239). Since $\nabla x \pi_1 \preceq \pi$, from (iii) of definition (86) we obtain $x \notin \mathrm{Sp}(\pi_1)$. We now show the 'if' part: so we assume that π_1 is a clean proof and $x \notin \mathrm{Sp}(\pi_1)$. We need to show that $\pi = \nabla x \pi_1$ is itself clean. So we need to prove (i), (ii) and (iii) of definition (86). First we show (i): so we assume that $\partial\phi \preceq \pi = \nabla x \pi_1$. From theorem (2) of page 21 we cannot possibly have $\partial\phi = \nabla x \pi_1$. Hence $\partial\phi \preceq \pi_1$ and $\phi \in \mathbf{A}^+(V)$ follows from the fact that π_1 is a clean proof. We now show (ii): so we assume that $\rho_1 \oplus \rho_2 \preceq \pi = \nabla x \pi_1$. Once again we cannot have the equality $\rho_1 \oplus \rho_2 = \nabla x \pi_1$ and consequently $\rho_1 \oplus \rho_2 \preceq \pi_1$. Having assumed that π_1 is a clean proof, we obtain $\mathrm{Val}^+(\rho_2) = \psi_1 \to \psi_2$ as requested where $\psi_1 \sim \mathrm{Val}^+(\rho_1)$ and $\sim$ is the substitution congruence. We now show (iii): so we assume that $\nabla y \rho_1 \preceq \pi = \nabla x \pi_1$. We need to show that $y \notin \mathrm{Sp}(\rho_1)$. We shall distinguish two cases: first we assume that $\nabla y \rho_1 = \pi$. Then from theorem (2) of page 21 we obtain $y = x$ and $\rho_1 = \pi_1$ and the conclusion $y \notin \mathrm{Sp}(\rho_1)$ is true by assumption. Next we assume that $\nabla y \rho_1 \neq \pi$. Then we must have $\nabla y \rho_1 \preceq \pi_1$ and the conclusion $y \notin \mathrm{Sp}(\rho_1)$ follows from the fact that π_1 is a clean proof. **.**

In proposition (235) we showed that the variables of the conclusion modulo of any sub-proof were variables of the proof itself, a statement which is best summarized as $\mathrm{Var}(\mathrm{Val}^+(\rho)) \subseteq \mathrm{Var}(\pi)$ for all $\rho \preceq \pi$. In general, the converse is not true. A variable of the proof may not appear at all in any conclusion modulo of any sub-proof. We know from $\pi = (x \in x) \oplus ((x \in x) \to (y \in y))$ with $x \neq y$ that a variable of π has no reason to be a variable for $\mathrm{Val}^+(\pi)$. However, we should expect it to appear somewhere in one of the conclusion modulo of a sub-proof of π. This is not the case. Simply consider $\pi = \partial\phi$ where ϕ fails to be an axiom modulo and $\mathrm{Var}(\phi) \neq \emptyset$. Then $\mathrm{Val}^+(\pi) = \bot \to \bot$. This is what happens with proofs which are not clean. They behave unpredictably. Fortunately, our expectations are met when dealing with clean proofs:

Proposition 242 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$ be a clean proof. Then:*

$$\cup\{\, \mathrm{Var}(\mathrm{Val}^+(\rho)) \;:\; \rho \preceq \pi \,\} = \mathrm{Var}(\pi) \tag{3.33}$$

i.e. the variables of conclusions modulo of sub-proofs of π are the variables of π.

Proof
By virtue of proposition (235), we only need to show the implication:

$$(\pi \text{ clean}) \;\Rightarrow\; \mathrm{Var}(\pi) \subseteq \cup\{\, \mathrm{Var}(\mathrm{Val}^+(\rho)) \;:\; \rho \preceq \pi \,\}$$

We shall do so with a structural induction argument, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then π is always a clean proof. From definition (19), the only sub-proof of π is π itself. Hence we need to show the inclusion $\mathrm{Var}(\pi) \subseteq \mathrm{Var}(\mathrm{Val}^+(\pi))$ which follows from the

equalities $\mathrm{Var}(\pi) = \mathrm{Var}(\phi)$ and $\mathrm{Val}^+(\pi) = \phi$. Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Furthermore we assume that π is a clean proof. Since $\partial\phi \preceq \pi$, from definition (86) we have $\phi \in \mathbf{A}^+(V)$. Once again the only sub-proof of π is π itself and we need to show that $\mathrm{Var}(\pi) \subseteq \mathrm{Var}(\mathrm{Val}^+(\pi))$. However since $\phi \in \mathbf{A}^+(V)$ we obtain $\mathrm{Val}^+(\pi) = \phi$ while $\mathrm{Var}(\pi) = \mathrm{Var}(\phi)$ so the inclusion is again clear. So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs for which the implication is true. We need to show the same is true of π. So we assume that π is a clean proof and we need to show the inclusion is true for π. However, from proposition (240) we see that both π_1 and π_2 are clean proofs. So π_1 and π_2 satisfy the inclusion and consequently we have:

$$\begin{array}{rcl}
\mathrm{Var}(\pi) & = & \mathrm{Var}(\pi_1 \oplus \pi_2) \\
& = & \mathrm{Var}(\pi_1) \cup \mathrm{Var}(\pi_2) \\
& \subseteq & (\cup\{\mathrm{Var}(\mathrm{Val}^+(\rho)) : \rho \preceq \pi_1\}) \cup (\cup\{\mathrm{Var}(\mathrm{Val}^+(\rho)) : \rho \preceq \pi_2\}) \\
& = & \cup\{\mathrm{Var}(\mathrm{Val}^+(\rho)) : \rho \in \mathrm{Sub}(\pi_1) \cup \mathrm{Sub}(\pi_2)\} \\
& \subseteq & \cup\{\mathrm{Var}(\mathrm{Val}^+(\rho)) : \rho \in \mathrm{Sub}(\pi_1) \cup \mathrm{Sub}(\pi_2) \cup \{\pi_1 \oplus \pi_2\}\} \\
\text{def. (19)} \ \rightarrow & = & \cup\{\mathrm{Var}(\mathrm{Val}^+(\rho)) : \rho \in \mathrm{Sub}(\pi_1 \oplus \pi_2)\} \\
& = & \cup\{\mathrm{Var}(\mathrm{Val}^+(\rho)) : \rho \preceq \pi\}
\end{array}$$

So we now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof for which the implication is true. We need to show the same is true of π. So we assume that π is a clean proof and we need to show the inclusion is true for π. However, from proposition (241) we see that π_1 is itself clean. Having assumed the implication is true for π_1, it satisfies the inclusion and consequently:

$$\begin{array}{rcl}
\mathrm{Var}(\pi) & = & \mathrm{Var}(\nabla x \pi_1) \\
& = & \{x\} \cup \mathrm{Var}(\pi_1) \\
& \subseteq & \{x\} \cup (\cup\{\mathrm{Var}(\mathrm{Val}(\rho)) : \rho \in \mathrm{Sub}(\pi_1)\}) \\
\text{A: to be proved} \ \rightarrow & \subseteq & \cup\{\mathrm{Var}(\mathrm{Val}(\rho)) : \rho \in \mathrm{Sub}(\pi_1) \cup \{\nabla x \pi_1\}\} \\
\text{def. (19)} \ \rightarrow & = & \cup\{\mathrm{Var}(\mathrm{Val}(\rho)) : \rho \in \mathrm{Sub}(\nabla x \pi_1)\} \\
& = & \cup\{\mathrm{Var}(\mathrm{Val}(\rho)) : \rho \preceq \pi\}
\end{array}$$

So it remains to show point A, for which it is sufficient to prove $x \in \mathrm{Var}(\mathrm{Val}^+(\rho))$ for $\rho = \nabla x \pi_1$. This follows from π being clean and $\mathrm{Val}^+(\rho) = \forall x \mathrm{Val}^+(\pi_1)$. .

Since Val^+ is an extension of Val from the domain of totally clean proofs to that of clean proofs, the previous proposition (242) can be restricted to the case of totally clean proofs and the valuation $\mathrm{Val} : \mathbf{\Pi}(V) \to \mathbf{P}(V)$:

Proposition 243 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$ be a totally clean proof. Then:*

$$\cup\{\, \mathrm{Var}(\mathrm{Val}(\rho)) \ : \ \rho \preceq \pi \,\} = \mathrm{Var}(\pi) \tag{3.34}$$

i.e. the variables of conclusions of sub-proofs of π are the variables of π.

Proof
We assume that π is totally clean. Then in particular from proposition (238) it is a clean proof. Applying proposition (242) we obtain:

$$\cup\{\, \mathrm{Var}(\mathrm{Val}^+(\rho)) \;:\; \rho \preceq \pi \,\} = \mathrm{Var}(\pi)$$

However, every $\rho \preceq \pi$ is totally clean by virtue of proposition (181). It follows from proposition (232) that $\mathrm{Val}^+(\rho) = \mathrm{Val}(\rho)$ and equation (3.34) follows. **.**

Given $\pi \in \mathbf{\Pi}(V)$, the specific variables of π are the free variables of the elements of $\mathrm{Hyp}(\pi)$. If π is a clean proof, it contains no flawed application of the generalization rule of inference. In other words, no generalization occurs with respect to a variable which is not truly arbitrary. So no specific variable should get bound and the elements of $\mathrm{Sp}(\pi)$ should remain free variables:

Proposition 244 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$ be a clean proof. Then:*

$$\mathrm{Sp}(\pi) \subseteq \mathrm{Fr}(\pi)$$

Proof
For every proof $\pi \in \mathbf{\Pi}(V)$ we need to show the following implication:

$$(\pi \text{ clean}) \;\Rightarrow\; \mathrm{Sp}(\pi) \subseteq \mathrm{Fr}(\pi)$$

We shall do so with a structural induction, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then π is always clean in this case and we simply need to prove the inclusion which follows from:

$$\mathrm{Sp}(\phi) = \mathrm{Fr}(\mathrm{Hyp}(\phi)) = \mathrm{Fr}(\{\phi\}) = \mathrm{Fr}(\phi)$$

We now assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then $\mathrm{Sp}(\pi) = \emptyset$ and the inclusion is always true, and so is the implication. So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs satisfying our implication. We need to show the same is true for π. So we assume that π is clean. We need to show the inclusion is true for π. However, from proposition (240) both π_1 and π_2 are clean and it follows that the inclusion is true for π_1 and π_2. Hence:

$$\begin{array}{rcl}
\mathrm{Sp}(\pi) & = & \mathrm{Sp}(\pi_1 \oplus \pi_2) \\
\text{prop. (204)} \;\rightarrow & = & \mathrm{Sp}(\pi_1) \cup \mathrm{Sp}(\pi_2) \\
& \subseteq & \mathrm{Fr}(\pi_1) \cup \mathrm{Fr}(\pi_2) \\
& = & \mathrm{Fr}(\pi_1 \oplus \pi_2) \\
& = & \mathrm{Fr}(\pi)
\end{array}$$

We now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof satisfying our implication. We need to show the same is true of π. So we assume that π is clean. We need to show the inclusion is true for π. However, from proposition (241) we see that π_1 is clean and $x \notin \mathrm{Sp}(\pi_1)$. Hence:

$$\mathrm{Sp}(\pi) \;=\; \mathrm{Sp}(\nabla x \pi_1)$$

$$\begin{array}{rcll} \text{prop. (204)} & \rightarrow & = & \mathrm{Sp}(\pi_1) \\ x \notin \mathrm{Sp}(\pi_1) & \rightarrow & = & \mathrm{Sp}(\pi_1) \setminus \{x\} \\ & & \subseteq & \mathrm{Fr}(\pi_1) \setminus \{x\} \\ & & = & \mathrm{Fr}(\nabla x \pi_1) \\ & & = & \mathrm{Fr}(\pi) \end{array}$$

.

This completes our section on clean proofs which brings the final touches to the study of the new valuation $\mathrm{Val}^+ : \mathbf{\Pi}(V) \rightarrow \mathbf{P}(V)$ which we hope will fulfill its promise. We were driven to define Val^+ after realizing that Val would not allow us to write $\mathrm{Val} \circ \mathcal{M}(\pi) \sim \mathcal{M} \circ \mathrm{Val}(\pi)$ despite opting for a very natural definition of minimal transform for proofs. So we now hope to have the equivalence $\mathrm{Val}^+ \circ \mathcal{M}(\pi) \sim \mathcal{M} \circ \mathrm{Val}^+(\pi)$. However, we should also extend proposition (229) and obtain $\mathrm{Val}^+ \circ \sigma(\pi) = \sigma \circ \mathrm{Val}^+(\pi)$ for clean proofs when σ is valid for π. Unless we can prove this equality (or possibly equivalence modulo substitution), the introduction of Val^+ would hardly be a step forward.

3.3.4 Valid Substitution of Axiom Modulo

Having introduced the valuation modulo $\mathrm{Val}^+ : \mathbf{\Pi}(V) \rightarrow \mathbf{P}(V)$ in definition (82) and clarified its domain of clean proofs in definition (86), one of the first task facing us is to extend proposition (229) and establish a result of the form $\mathrm{Val}^+ \circ \sigma(\pi) = \sigma \circ \mathrm{Val}^+(\pi)$ whenever π is a clean proof and $\sigma : V \rightarrow W$ is valid for π. As it turns out, the result is true and will be proved in proposition (248). What may be seen as somewhat surprising is the fact that the equality is true, rather than the mere substitution equivalence $\mathrm{Val}^+ \circ \sigma(\pi) \sim \sigma \circ \mathrm{Val}^+(\pi)$. So we shall have a stronger result than expected. Now if proposition (248) is going to be true, then it must be true when π is of the form $\pi = \partial\phi$. We should be used to this idea by now: the proof $\sigma(\pi)$ cannot be meaningful unless the substitution σ behaves adequately on the *axioms* of the proof. So suppose $\pi = \partial\phi$ is a clean proof. Then ϕ must be an axiom modulo and consequently $\mathrm{Val}^+(\pi) = \phi$. Since $\sigma(\pi) = \partial\sigma(\phi)$, we cannot hope to have the equality $\mathrm{Val}^+ \circ \sigma(\pi) = \sigma \circ \mathrm{Val}^+(\pi)$ unless $\sigma(\phi)$ is itself an axiom modulo. Hence, we need to establish that if σ is valid for an axiom modulo ϕ, then $\sigma(\phi)$ is itself an axiom modulo. This will be done in proposition (246) below. Now let $\phi \in \mathbf{A}^+(V)$ be an arbitrary axiom modulo, From definition (80), the formula ϕ is substitution equivalent to an axiom of first order logic ψ. We want to show that $\sigma(\phi)$ is also an axiom modulo, and the first thing which comes to mind is to attempt proving the equivalence $\sigma(\phi) \sim \sigma(\psi)$. From proposition (19) we know that $\sigma(\psi)$ is itself an axiom of first order logic, provided σ is valid for ψ. Unfortunately, this approach is not going to work. We are assuming that σ is valid for ϕ. We have no control on whether σ is also valid for ψ. So we need to find another route and think in terms of minimal transforms which have proved very handy in the past. From the equivalence $\phi \sim \psi$ and theorem (14) of page 149 we obtain $\mathcal{M}(\phi) = \mathcal{M}(\psi)$ and consequently $\bar{\sigma} \circ \mathcal{M}(\phi) = \bar{\sigma} \circ \mathcal{M}(\psi)$. Having assumed that σ is valid for ϕ

we can apply theorem (13) of page 146 and obtain $\mathcal{M} \circ \sigma(\phi) = \bar{\sigma} \circ \mathcal{M}(\psi)$. Since ψ is an axiom of first order logic, it is not unreasonable to hope that $\mathcal{M}(\psi)$ is also an axiom of first order logic. We also know from proposition (100) that $\bar{\sigma}$ is always valid for $\mathcal{M}(\psi)$ and it follows from proposition (19) that $\bar{\sigma} \circ \mathcal{M}(\psi)$ is an axiom of first order logic. Hence we see that the minimal transform of $\sigma(\phi)$ is an axiom of first order logic. This may be enough for us to conclude that $\sigma(\phi)$ is an axiom modulo. So here is the plan: on the on hand, we need to show that $\mathcal{M}(\psi)$ is an axiom, i.e. we need to establish that the minimal transform of an axiom is an axiom. This will be done in lemma (20) below. On the other hand, we need to prove that if the minimal transform of a formula is an axiom of first order logic, then the formula is an axiom modulo. This will be the object of lemma (21).

Lemma 20 *Let V be a set. Then for all $\phi \in \mathbf{P}(V)$ we have the implication:*

$$\phi \in \mathbf{A}(V) \;\Rightarrow\; \mathcal{M}(\phi) \in \mathbf{A}(\bar{V})$$

In other words, the minimal transform of an axiom is an axiom.

Proof
We shall prove this implication by considering the five possible types of axioms of definition (63): first we assume that ϕ is a simplification axiom as per definition (58). Then $\phi = \phi_1 \to (\phi_2 \to \phi_1)$ for some $\phi_1, \phi_2 \in \mathbf{P}(V)$ and from definition (38) we obtain $\mathcal{M}(\phi) = \psi_1 \to (\psi_2 \to \psi_1)$ where $\psi_1 = \mathcal{M}(\phi_1)$ and $\psi_2 = \mathcal{M}(\phi_2)$. So $\mathcal{M}(\phi)$ is itself a simplification axiom on $\mathbf{P}(\bar{V})$, and we have $\mathcal{M}(\phi) \in \mathbf{A}(\bar{V})$. We now assume that ϕ is a Frege axiom as per definition (59). Then $\phi = [\phi_1 \to (\phi_2 \to \phi_3)] \to [(\phi_1 \to \phi_2) \to (\phi_1 \to \phi_3)]$ and consequently:

$$\mathcal{M}(\phi) = [\psi_1 \to (\psi_2 \to \psi_3)] \to [(\psi_1 \to \psi_2) \to (\psi_1 \to \psi_3)]$$

where $\psi_1 = \mathcal{M}(\phi_1)$, $\psi_2 = \mathcal{M}(\phi_2)$ and $\psi_3 = \mathcal{M}(\phi_3)$. So $\mathcal{M}(\phi)$ is itself a Frege axiom. Likewise, if ϕ is a transposition axiom as per definition (60), then $\phi = [(\phi_1 \to \bot) \to \bot] \to \phi_1$ for some $\phi_1 \in \mathbf{P}(V)$ and it is clear that $\mathcal{M}(\phi)$ is itself a transposition axiom. So we now assume that ϕ is a quantification axiom as per definition (61). Then $\phi = \forall x(\phi_1 \to \phi_2) \to (\phi_1 \to \forall x \phi_2)$ for some $\phi_1, \phi_2 \in \mathbf{P}(V)$ such that $x \notin \mathrm{Fr}(\phi_1)$. Using definition (38) once more:

$$\mathcal{M}(\phi) = \forall n(\, \mathcal{M}(\phi_1)[n/x] \to \mathcal{M}(\phi_2)[n/x]\,) \to (\, \mathcal{M}(\phi_1) \to \forall m \mathcal{M}(\phi_2)[m/x]\,)$$

where n is the smallest integer k such that $[k/x]$ is valid for $\mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2)$, and m is the smallest integer $k \in \mathbf{N}$ such that $[k/x]$ is valid for $\mathcal{M}(\phi_2)$. Let us accept for now that $n = m$ and furthermore that $\mathcal{M}(\phi_1)[n/x] = \mathcal{M}(\phi_1)$. Then:

$$\mathcal{M}(\phi) = \forall n(\, \mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2)[n/x]\,) \to (\, \mathcal{M}(\phi_1) \to \forall n \mathcal{M}(\phi_2)[n/x]\,)$$

which can be expressed as:

$$\mathcal{M}(\phi) = \forall n(\psi_1 \to \psi_2) \to (\psi_1 \to \forall n \psi_2)$$

where $\psi_1 = \mathcal{M}(\phi_1)$ and $\psi_2 = \mathcal{M}(\phi_2)[n/x]$. So we see that $\mathcal{M}(\phi)$ is itself a quantification axiom on $\mathbf{P}(\bar{V})$, provided we show $n \notin \mathrm{Fr}(\psi_1)$. So a few things remain to be proved. First we show that $\mathcal{M}(\phi_1)[n/x] = \mathcal{M}(\phi_1)$. Using proposition (36) it is sufficient to show that $[n/x](u) = u$ for all $u \in \mathrm{Var}(\mathcal{M}(\phi_1))$. It is therefore sufficient to prove that $x \notin \mathrm{Var}(\mathcal{M}(\phi_1))$. So suppose to the contrary that $x \in \mathrm{Var}(\mathcal{M}(\phi_1))$. Since $x \in V$ we obtain $x \in \mathrm{Var}(\mathcal{M}(\phi_1)) \cap V$ and it follows from proposition (97) that $x \in \mathrm{Fr}(\phi_1)$ which contradicts our assumption. We now show that $n \notin \mathrm{Fr}(\psi_1)$. This follows once again from proposition (97), since $n \in \mathrm{Fr}(\psi_1) = \mathrm{Fr}(\mathcal{M}(\phi_1))$ implies $n \in \mathrm{Fr}(\phi_1)$ and consequently $n \in V$ which contradicts $V \cap \mathbf{N} = \emptyset$. So it remains to show that $n = m$, for which it is sufficient to show the equivalence:

$$[k/x] \text{ valid for } \mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2) \;\Leftrightarrow\; [k/x] \text{ valid for } \mathcal{M}(\phi_2)$$

The implication $\Rightarrow$ follows immediately from proposition (54) and it remains to show $\Leftarrow$: so we assume that $k \in \mathbf{N}$ is such that $[k/x]$ is valid for $\mathcal{M}(\phi_2)$. We need to show that it is also valid for $\mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2)$. Using proposition (54), we simply need to show that $[k/x]$ is valid for $\mathcal{M}(\phi_1)$. Using proposition (59), the identity mapping $i : \bar{V} \to \bar{V}$ being valid for $\mathcal{M}(\phi_1)$, it is sufficient to prove that $\mathcal{M}(\phi_1)[k/x] = \mathcal{M}(\phi_1)$, which follows from the established fact that $x \notin \mathrm{Var}(\mathcal{M}(\phi_1))$. This completes our proof in the case when ϕ is a quantification axiom on $\mathbf{P}(V)$. So we now assume that ϕ is a specialization axiom as per definition (62). Then $\phi = \forall x \phi_1 \to \phi_1[y/x]$ where $\phi_1 \in \mathbf{P}(V)$, $x, y \in V$ and $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ is an essential substitution of y in place of x. We have:

$$\mathcal{M}(\phi) = \forall n \psi_1 \to \psi_1^*$$

where $\psi_1 = \mathcal{M}(\phi_1)[n/x]$, $\psi_1^* = \mathcal{M} \circ [y/x](\phi_1)$ and n is the smallest integer $k \in \mathbf{N}$ such that $[k/x]$ is valid for $\mathcal{M}(\phi_1)$. Using proposition (157), in order to show that $\mathcal{M}(\phi)$ is itself a specialization axiom, it is sufficient to prove that $\psi_1^* \sim \psi_1[y/n]$ where $[y/n] : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{V})$ is an essential substitution of y in place for n, and $\sim$ is the substitution congruence on $\mathbf{P}(\bar{V})$. Using the minimal transform mapping $\bar{\mathcal{M}} : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{\bar{V}})$, by virtue of theorem (14) of page 149 we simply need to prove that $\bar{\mathcal{M}}(\psi_1^*) = \bar{\mathcal{M}} \circ [y/n](\psi_1)$. Before we do so, let us say a few words on the single variable substitutions involved in the proof so as to avoid any possible confusion: first we have the essential substitution $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ which is associated to the map $[y/x] : V \to V$. We also have the minimal extension $\overline{[y/x]} : \bar{V} \to \bar{V}$ which turns out to be exactly the substitution of y in place of x, so $\overline{[y/x]} = [y/x]$ this time on $\bar{V}$ rather than V. From $[y/x] : \bar{V} \to \bar{V}$ we also obtain the minimal extension $[y/x] : \bar{\bar{V}} \to \bar{\bar{V}}$, and of course we also have the associated substitutions $[y/x] : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{V})$ and $[y/x] : \mathbf{P}(\bar{\bar{V}}) \to \mathbf{P}(\bar{\bar{V}})$ as per definition (24) (i.e. non-essential). Hence the notation $[y/x]$ has several possible meanings depending on the context. We have $[y/x] : A \to A$ where $A = V, \bar{V}$ and $\bar{\bar{V}}$. We have $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ (essential) and $[y/x] : \mathbf{P}(A) \to \mathbf{P}(A)$ (non-essential) with $A = \bar{V}$ and $A = \bar{\bar{V}}$. Likewise, we have $[n/x] : \bar{V} \to \bar{V}$ with minimal extension $[n/x] : \bar{\bar{V}} \to \bar{\bar{V}}$ and the

(non-essential) substitutions $[n/x] : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{V})$ and $[n/x] : \mathbf{P}(\bar{\bar{V}}) \to \mathbf{P}(\bar{\bar{V}})$. We also have the essential substitution $[y/n] : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{V})$ and its associated $[y/n] : \bar{V} \to \bar{V}$ with minimal extension $[y/n] : \bar{\bar{V}} \to \bar{\bar{V}}$ and its associated (non-essential) substitution $[y/n] : \mathbf{P}(\bar{\bar{V}}) \to \mathbf{P}(\bar{\bar{V}})$. From $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$:

$$\begin{array}{rcl}
\bar{\mathcal{M}}(\psi_1^*) & = & \bar{\mathcal{M}} \circ \mathcal{M} \circ [y/x](\phi_1) \\
[y/x] : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{V}) \ \to & = & \bar{\mathcal{M}} \circ [y/x] \circ \mathcal{M}(\phi_1) \\
\text{Th. (13) p. 146, } [y/x] \text{ valid for } \mathcal{M}(\phi_1) \ \to & = & [y/x] \circ \bar{\mathcal{M}} \circ \mathcal{M}(\phi_1) \\
\text{A: to be proved} \ \to & = & [y/n] \circ [n/x] \circ \bar{\mathcal{M}} \circ \mathcal{M}(\phi_1) \\
[n/x] \text{ valid for } \mathcal{M}(\phi_1) \ \to & = & [y/n] \circ \bar{\mathcal{M}} \circ [n/x] \circ \mathcal{M}(\phi_1) \\
[y/n] : \mathbf{P}(\bar{\bar{V}}) \to \mathbf{P}(\bar{\bar{V}}) \ \to & = & [y/n] \circ \bar{\mathcal{M}}(\psi_1) \\
[y/n] : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{V}) \text{ essential} \ \to & = & \bar{\mathcal{M}} \circ [y/n](\psi_1)
\end{array}$$

So it remains to show point A: using proposition (36) it is sufficient to show that the maps $[y/x] : \bar{\bar{V}} \to \bar{\bar{V}}$ and $[y/n] \circ [n/x] : \bar{\bar{V}} \to \bar{\bar{V}}$ coincide on $\mathrm{Var}(\bar{\mathcal{M}} \circ \mathcal{M}(\phi_1))$. So let $u \in \mathrm{Var}(\bar{\mathcal{M}} \circ \mathcal{M}(\phi_1))$. We need to show that $[y/x](u) = [y/n] \circ [n/x](u)$. Since $\bar{\bar{V}} = \bar{V} \uplus \bar{\mathbf{N}}$, we shall distinguish two cases: first we assume that $u \in \bar{\mathbf{N}}$. Since $\bar{V} \cap \bar{\mathbf{N}} = \emptyset$, in particular we have $u \notin \{x, n\}$ and the equality is clear. Next we assume that $u \in \bar{V}$. Then we have $u \in \mathrm{Var}(\bar{\mathcal{M}} \circ \mathcal{M}(\phi_1)) \cap \bar{V}$ and it follows from proposition (97) that $u \in \mathrm{Fr}(\mathcal{M}(\phi_1)) = \mathrm{Fr}(\phi_1) \subseteq V$. Since $V \cap \mathbf{N} = \emptyset$, in particular we have $u \neq n$. We shall distinguish two further cases: first we assume that $u = x$. Then the equality is clear. Next we assume that $u \neq x$. Then we have $u \notin \{x, n\}$ and the equality is again clear. **.**

The following lemma is hard. By this we mean the amount of small technical details to check is substantial. The probability of getting it wrong is a lot higher than in any other results. Most of the things we do in these notes are easy and can be followed without any pain. In fact, many of the proofs are so obvious that they hardly need to be checked. They are proofs which would be omitted in a typical mathematical textbook. The following proof should not be omitted. It is boring and tedious but we are very keen to make sure the lemma is true.

Lemma 21 *Let V be a set. Then for all $\phi \in \mathbf{P}(V)$ we have the implication:*

$$\mathcal{M}(\phi) \in \mathbf{A}(\bar{V}) \ \Rightarrow \ \phi \in \mathbf{A}^+(V)$$

i.e. if the minimal transform of ϕ is an axiom then ϕ is an axiom modulo.

Proof
We shall prove the implication by considering the five possible cases of axioms as per definition (63). First we assume that $\mathcal{M}(\phi)$ is a simplification axiom as per definition (58). Then $\mathcal{M}(\phi) = \psi_1 \to (\psi_2 \to \psi_1)$ where $\psi_1, \psi_2 \in \mathbf{P}(\bar{V})$. We need to show that ϕ is an axiom modulo. Using theorem (2) of page 21, the formula ϕ can be of four possible types: we can have $\phi = (x \in y)$ for some $x, y \in V$ or $\phi = \bot$ or $\phi = \phi_1 \to \phi_2$ for some $\phi_1, \phi_2 \in \mathbf{P}(V)$ or $\phi = \forall x \phi_1$ for some $\phi_1 \in \mathbf{P}(V)$ and $x \in V$. Looking at definition (38), the corresponding values for

$\mathcal{M}(\phi)$ are $\mathcal{M}(\phi) = (x \in y)$ or $\mathcal{M}(\phi) = \bot$ or $\mathcal{M}(\phi) = \mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2)$ or $\mathcal{M}(\phi) = \forall n \mathcal{M}(\phi_1)[n/x]$ for some $n \in \mathbf{N}$. Since $\mathcal{M}(\phi) = \psi_1 \to (\psi_2 \to \psi_1)$, the uniqueness property of theorem (2) tells us the only possible case is $\phi = \phi_1 \to \phi_2$ and $\mathcal{M}(\phi) = \mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2)$, and furthermore we have $\mathcal{M}(\phi_1) = \psi_1$ and $\mathcal{M}(\phi_2) = \psi_2 \to \psi_1$. Pushing this argument further, we see that ϕ_2 must be of the form $\phi_2 = \phi_3 \to \phi_4$ and we have $\mathcal{M}(\phi_3) = \psi_2$ and $\mathcal{M}(\phi_4) = \psi_1$. So we have proved that $\phi = \phi_1 \to (\phi_3 \to \phi_4)$ where $\mathcal{M}(\phi_1) = \mathcal{M}(\phi_4)$. If we define the formula $\phi^* = \phi_1 \to (\phi_3 \to \phi_1)$, then ϕ^* is a simplification axiom which satisfies $\mathcal{M}(\phi) = \mathcal{M}(\phi^*)$. From theorem (14) of page 149, it follows that $\phi \sim \phi^*$ where $\sim$ is the substitution congruence on $\mathbf{P}(V)$, and we have proved that ϕ is an axiom modulo, i.e. $\phi \in \mathbf{A}^+(V)$ as requested. So we now assume that $\mathcal{M}(\phi)$ is a Frege axiom as per definition (59). Then we have the equality:

$$\mathcal{M}(\phi) = [\psi_1 \to (\psi_2 \to \psi_3)] \to [(\psi_1 \to \psi_2) \to (\psi_1 \to \psi_3)]$$

for some $\psi_1, \psi_2, \psi_3 \in \mathbf{P}(\bar{V})$. From our previous argument we see that ϕ must be of the form $\phi = \phi_1 \to \phi_2$ with $\mathcal{M}(\phi_1) = \psi_1 \to (\psi_2 \to \psi_3)$ together with $\mathcal{M}(\phi_2) = (\psi_1 \to \psi_2) \to (\psi_1 \to \psi_3)$. So ϕ_1 must be of the form $\phi_1 = \phi_3 \to \phi_4$ with $\mathcal{M}(\phi_3) = \psi_1$ and $\mathcal{M}(\phi_4) = \psi_2 \to \psi_3$. Pushing this argument further, and renaming the formulas involved, we see that ϕ must be of the form:

$$\phi = [\phi_1 \to (\phi_2 \to \phi_3)] \to [(\phi_4 \to \phi_5) \to (\phi_6 \to \phi_7)]$$

with $\mathcal{M}(\phi_1) = \mathcal{M}(\phi_4) = \mathcal{M}(\phi_6)$, $\mathcal{M}(\phi_2) = \mathcal{M}(\phi_5)$ and $\mathcal{M}(\phi_3) = \mathcal{M}(\phi_7)$. Let:

$$\phi^* = [\phi_1 \to (\phi_2 \to \phi_3)] \to [(\phi_1 \to \phi_2) \to (\phi_1 \to \phi_3)]$$

Then $\mathcal{M}(\phi) = \mathcal{M}(\phi^*)$ and consequently $\phi \sim \phi^*$, so ϕ is an axiom modulo. We now assume that $\mathcal{M}(\phi)$ is a transposition axiom as per definition (60). Then $\mathcal{M}(\phi) = [(\psi_1 \to \bot) \to \bot] \to \psi_1$ for some $\psi \in \mathbf{P}(\bar{V})$, and it follows that ϕ must be of the form $\phi = [(\phi_1 \to \bot) \to \bot] \to \phi_2$ where $\mathcal{M}(\phi_1) = \mathcal{M}(\phi_2)$. Defining $\phi^* = [(\phi_1 \to \bot) \to \bot] \to \phi_1$ we obtain $\mathcal{M}(\phi) = \mathcal{M}(\phi^*)$ which is $\phi \sim \phi^*$ and ϕ is an axiom modulo as requested. So we now assume that $\mathcal{M}(\phi)$ is a quantification axiom as per definition (61). Then we have the equality:

$$\mathcal{M}(\phi) = \forall z(\psi_1 \to \psi_2) \to (\psi_1 \to \forall z \psi_2)$$

for some $\psi_1, \psi_2 \in \mathbf{P}(\bar{V})$ and $z \in \bar{V}$ such that $z \notin \mathrm{Fr}(\psi_1)$. So ϕ must be of the form $\phi = \phi_7 \to \phi_8$ with $\mathcal{M}(\phi_7) = \forall z(\psi_1 \to \psi_2)$ and $\mathcal{M}(\phi_8) = \psi_1 \to \forall z \psi_2$. So ϕ_7 must be of the form $\phi_7 = \forall x \phi_5$ for some $x \in V$ and $\phi_5 \in \mathbf{P}(V)$, where $\mathcal{M}(\phi_5)[n/x] = \psi_1 \to \psi_2$ and $n = z$, and n is also the smallest integer k such that $[k/x]$ is valid for $\mathcal{M}(\phi_5)$. Furthermore, ϕ_8 must be of the form $\phi_8 = \phi_3 \to \phi_6$ where $\mathcal{M}(\phi_3) = \psi_1$ and $\mathcal{M}(\phi_6) = \forall n \psi_2$. Continuing in this way, we see that ϕ_5 must be of the form $\phi_5 = \phi_1 \to \phi_2$ where $\mathcal{M}(\phi_1)[n/x] = \psi_1$ together with $\mathcal{M}(\phi_2)[n/x] = \psi_2$, while ϕ_6 must be of the form $\phi_6 = \forall y \phi_4$ for some $y \in V$ and $\phi_4 \in \mathbf{P}(V)$, with $\mathcal{M}(\phi_4)[n/y] = \psi_2$. Note that n is also the smallest integer such that $[k/y]$ is valid for $\mathcal{M}(\phi_4)$. So we have proved that ϕ is of the form:

$$\phi = \forall x(\phi_1 \to \phi_2) \to (\phi_3 \to \forall y \phi_4)$$

where $\mathcal{M}(\phi_1)[n/x] = \mathcal{M}(\phi_3)$, $\mathcal{M}(\phi_2)[n/x] = \mathcal{M}(\phi_4)[n/y]$ and $n = z \in \mathbf{N}$. We also proved that $n = z$ is the smallest integer k such that $[k/x]$ is valid for $\mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2)$ and it is also the smallest integer k such that $[k/y]$ is valid for $\mathcal{M}(\phi_4)$. We now consider the formula ϕ^* defined as:

$$\phi^* = \forall x(\phi_1 \to \phi_2) \to (\phi_1 \to \forall x \phi_2)$$

Let us accept for now that $x \notin \mathrm{Fr}(\phi_1)$. Then ϕ^* is a quantification axiom, and in order to show that ϕ is an axiom modulo it is sufficient to prove that $\phi \sim \phi^*$. So it is sufficient to show that $\phi_1 \sim \phi_3$ and $\forall x \phi_2 \sim \forall y \phi_4$. First we show that $\phi_1 \sim \phi_3$. We need to show that $\mathcal{M}(\phi_1) = \mathcal{M}(\phi_3)$. Having established that $\mathcal{M}(\phi_1)[n/x] = \mathcal{M}(\phi_3)$, we simply need to prove that $\mathcal{M}(\phi_1) = \mathcal{M}(\phi_1)[n/x]$. Using proposition (36), it is sufficient to prove that $u = [n/x](u)$ for every $u \in \mathrm{Var}(\mathcal{M}(\phi_1))$. So it is sufficient to show $x \notin \mathrm{Var}(\mathcal{M}(\phi_1))$. So suppose to the contrary that $x \in \mathrm{Var}(\mathcal{M}(\phi_1))$. Since $x \in V$ we obtain $x \in \mathrm{Var}(\mathcal{M}(\phi_1)) \cap V$ and it follows from proposition (97) that $x \in \mathrm{Fr}(\phi_1)$ which is a contradiction. We now prove that $\forall x \phi_2 \sim \forall y \phi_4$. We need to show $\mathcal{M}(\forall x \phi_2) = \mathcal{M}(\forall y \phi_4)$. We already know that n is the smallest integer k such that $[k/y]$ is valid for $\mathcal{M}(\phi_4)$. So $\mathcal{M}(\forall y \phi_4) = \forall n \mathcal{M}(\phi_4)[n/y]$. Let us accept for now that n is also the smallest integer k such that $[k/x]$ is valid for $\mathcal{M}(\phi_2)$. Then $\mathcal{M}(\forall x \phi_2) = \forall n \mathcal{M}(\phi_2)[n/x]$ and the equality $\mathcal{M}(\forall x \phi_2) = \mathcal{M}(\forall y \phi_4)$ follows from the established fact that $\mathcal{M}(\phi_2)[n/x] = \mathcal{M}(\phi_4)[n/y]$. So it remains to show that n is indeed the smallest integer k such that $[k/x]$ is valid for $\mathcal{M}(\phi_2)$. However, we have established the fact it is the smallest integer k such that $[k/x]$ is valid for $\mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2)$. It is therefore sufficient to prove the equivalence:

$$[k/x] \text{ valid for } \mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2) \;\Leftrightarrow\; [k/x] \text{ valid for } \mathcal{M}(\phi_2)$$

The implication $\Rightarrow$ follows immediately from proposition (54). So it remains to show $\Leftarrow$: so we assume that $k \in \mathbf{N}$ is such that $[k/x]$ is valid for $\mathcal{M}(\phi_2)$. We need to show that $[k/x]$ is also valid for $\mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2)$. Using proposition (54) it is sufficient to show that $[k/x]$ is valid for $\mathcal{M}(\phi_1)$. The identity mapping $i : \bar{V} \to \bar{V}$ being valid for $\mathcal{M}(\phi_1)$, using proposition (59), it is sufficient to prove that $\mathcal{M}(\phi_1) = \mathcal{M}(\phi_1)[k/x]$ which follows from the established fact that $x \notin \mathrm{Var}(\mathcal{M}(\phi_1))$. So we have proved that $\phi \sim \phi^*$ and ϕ is indeed an axiom modulo, provided we show $x \notin \mathrm{Fr}(\phi_1)$. So suppose to the contrary that $x \in \mathrm{Fr}(\phi_1)$. Using proposition (97) we obtain $x \in \mathrm{Fr}(\mathcal{M}(\phi_1))$. However, recall that $\mathcal{M}(\phi_1)[n/x] = \psi_1$ and furthermore $[n/x]$ is valid for $\mathcal{M}(\phi_1)$. Using proposition (52) we obtain $n = [n/x](x) \in [n/x](\,\mathrm{Fr}(\mathcal{M}(\phi_1))\,) = \mathrm{Fr}(\psi_1)$. So we see that $n \in \mathrm{Fr}(\psi_1)$, i.e. $z \in \mathrm{Fr}(\psi_1)$ which contradicts our initial assumption. This completes our proof in the case when $\mathcal{M}(\phi)$ is a quantification axiom. We now assume that $\mathcal{M}(\phi)$ is a specialization axiom as per definition (62). Then:

$$\mathcal{M}(\phi) = \forall z \psi_1 \to \psi_1[y/z]$$

for some $\psi_1 \in \mathbf{P}(\bar{V})$ and $y, z \in \bar{V}$, where $[y/z] : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{V})$ is an essential substitution of y in place of z. So ϕ must be of the form $\phi = \phi_3 \to \phi_2$ where

$\mathcal{M}(\phi_3) = \forall z \psi_1$ and $\mathcal{M}(\phi_2) = \psi_1[y/z]$. It follows that ϕ_3 must be of the form $\phi_3 = \forall x \phi_1$ for some $\phi_1 \in \mathbf{P}(V)$ and $x \in V$ such that $\mathcal{M}(\phi_1)[n/x] = \psi_1$ where $n = z \in \mathbf{N}$ and n is also the smallest integer k such that $[k/x]$ is valid for $\mathcal{M}(\phi_1)$. So we have proved that ϕ is of the form $\phi = \forall x \phi_1 \to \phi_2$. In order to show that ϕ is an axiom modulo, it is sufficient to show that ϕ is actually a specialization axiom. in order to do so, we shall crucially distinguish two cases: we first consider the case when $y \in \bar{V}$ is in fact an element of V. Using proposition (157), it is sufficient to prove that $\phi_2 \sim \phi_1[y/x]$ where $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ is an essential substitution of y in place of x. Note that we cannot apply proposition (157) unless y is indeed an element of V. So it is sufficient to prove that $\mathcal{M}(\phi_2) = \mathcal{M} \circ [y/x](\phi_1)$. Using proposition (112) it is in fact sufficient to prove the equivalence $\mathcal{M}(\phi_2) \sim \mathcal{M} \circ [y/x](\phi_1)$ where $\sim$ also denotes the substitution congruence on $\mathbf{P}(\bar{V})$. It is therefore sufficient to prove the equality $\bar{\mathcal{M}} \circ \mathcal{M}(\phi_2) = \bar{\mathcal{M}} \circ \mathcal{M} \circ [y/x](\phi_1)$. It may seem a bit odd that we do not attempt to prove the equality $\mathcal{M}(\phi_2) = \mathcal{M} \circ [y/x](\phi_1)$ directly, and choose instead to make use of the minimal transform $\bar{\mathcal{M}} : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{\bar{V}})$. However, remember that $\mathcal{M}(\phi_2) = \psi_1[y/z]$ and $[y/z] : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{V})$ is an essential substitution. From proposition (114), an essential substitution can always be redefined modulo the substitution congruence. So it is very hard to say anything about the exact value of $[y/z](\psi_1)$. However, in this case we know that $[y/z](\psi_1)$ is the minimal transform of ϕ_2. So this allows us to conclude, and the easy way to do so is to use $\bar{\mathcal{M}}$. So we need to show that $\bar{\mathcal{M}} \circ \mathcal{M}(\phi_2) = \bar{\mathcal{M}} \circ \mathcal{M} \circ [y/x](\phi_1)$:

$$
\begin{array}{rcl}
\bar{\mathcal{M}} \circ \mathcal{M}(\phi_2) & = & \bar{\mathcal{M}} \circ [y/z](\psi_1) \\
z = n \ \to & = & \bar{\mathcal{M}} \circ [y/n](\psi_1) \\
[y/n] \text{ essential } \to & = & [y/n] \circ \bar{\mathcal{M}}(\psi_1) \\
\mathcal{M}(\phi_1)[n/x] = \psi_1 \ \to & = & [y/n] \circ \bar{\mathcal{M}} \circ [n/x] \circ \mathcal{M}(\phi_1) \\
\text{Th. (13) p. 146, } [n/x] \text{ valid for } \mathcal{M}(\phi_1) \ \to & = & [y/n] \circ [n/x] \circ \bar{\mathcal{M}} \circ \mathcal{M}(\phi_1) \\
\text{A: to be proved } \to & = & [y/x] \circ \bar{\mathcal{M}} \circ \mathcal{M}(\phi_1) \\
\text{B: to be proved } \to & = & \bar{\mathcal{M}} \circ [y/x] \circ \mathcal{M}(\phi_1) \\
[y/x] \text{ essential } \to & = & \bar{\mathcal{M}} \circ \mathcal{M} \circ [y/x](\phi_1)
\end{array}
$$

So it remains to show point A and B. We shall first deal with point A, for which it is sufficient to prove the equality $[y/n] \circ [n/x](u) = [y/x](u)$ for all $u \in \mathrm{Var}(\, \bar{\mathcal{M}} \circ \mathcal{M}(\phi_1)\,)$. Since $\bar{\bar{V}} = \bar{V} \uplus \bar{\mathbf{N}}$ we shall distinguish two cases: first we assume that $u \in \bar{\mathbf{N}}$. Then $u \notin \{x, n\}$ and the equality is clear. Next we assume that $u \in \bar{V}$. Then using proposition (97) we obtain the equality $u \in \mathrm{Fr}(\mathcal{M}(\phi_1)) = \mathrm{Fr}(\phi_1) \subseteq V$ and in particular $u \neq n \in \mathbf{N}$. We shall distinguish two further cases: if $u = x$ then the equality is clear. If $u \neq x$ then $u \notin \{x, n\}$ and the equality is again clear. We now deal with point B: here we crucially need our assumption that $y \in V$. So the substitution $[y/x]$ of y in place of x is meaningful as a map $[y/x] : V \to V$, whose minimal extension is $[y/x] : \bar{V} \to \bar{V}$.

Using proposition (100), this minimal extension is valid for $\mathcal{M}(\phi_1)$ and point B follows from theorem (13) of page 146. This completes our proof in the case when $y \in \bar{V}$ is in fact an element of V. It remains to show that ϕ is a specialization axiom in the case when $y \notin V$. In this case, we shall see that $x \notin \mathrm{Fr}(\phi_1)$. So let us accept this is true for now. Applying proposition (157) with $y = x$ and the essential substitution $[x/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ being the identity mapping, in order to show that ϕ is a specialization axiom it is sufficient to prove that $\phi_2 \sim \phi_1$. Once again, we need to show that $\bar{\mathcal{M}} \circ \mathcal{M}(\phi_2) = \bar{\mathcal{M}} \circ \mathcal{M}(\phi_1)$, and our previous computation is still perfectly valid up to the point:

$$\bar{\mathcal{M}} \circ \mathcal{M}(\phi_2) = [y/x] \circ \bar{\mathcal{M}} \circ \mathcal{M}(\phi_1)$$

Hence, we need to show that $[y/x] \circ \bar{\mathcal{M}} \circ \mathcal{M}(\phi_1) = \bar{\mathcal{M}} \circ \mathcal{M}(\phi_1)$. Using proposition (36), we need to show that $[y/x](u) = u$ for all $u \in \mathrm{Var}(\bar{\mathcal{M}} \circ \mathcal{M}(\phi_1))$. In other words we need to prove that $x \notin \mathrm{Var}(\bar{\mathcal{M}} \circ \mathcal{M}(\phi_1))$. So suppose to the contrary that $x \in \mathrm{Var}(\bar{\mathcal{M}} \circ \mathcal{M}(\phi_1))$. Since $x \in V \subseteq \bar{V}$ we obtain:

$$x \in \mathrm{Var}(\bar{\mathcal{M}} \circ \mathcal{M}(\phi_1)) \cap \bar{V} = \mathrm{Fr}(\mathcal{M}(\phi_1)) = \mathrm{Fr}(\phi_1)$$

where we have made use of proposition (97). So we obtain $x \in \mathrm{Fr}(\phi_1)$, contradicting our accepted fact that $x \notin \mathrm{Fr}(\phi_1)$. So it remains to show that $x \notin \mathrm{Fr}(\phi_1)$. So suppose to the contrary that $x \in \mathrm{Fr}(\phi_1)$. Then we have $x \in \mathrm{Fr}(\mathcal{M}(\phi_1))$. Since $\mathcal{M}(\phi_1)[n/x] = \psi_1$ and $[n/x]$ is valid for $\mathcal{M}(\phi_1)$, using proposition (52) we obtain $\mathrm{Fr}(\psi_1) = [n/x](\mathrm{Fr}(\mathcal{M}(\phi_1))$ and it follows that $n \in \mathrm{Fr}(\psi_1)$. Since $\mathcal{M}(\phi_2) = \psi_1[y/n]$ and $[y/n] : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{V})$ is an essential substitution, from proposition (120) we have $\mathrm{Fr}(\mathcal{M}(\phi_2)) = [y/n](\mathrm{Fr}(\psi_1))$ and it follows that $y \in \mathrm{Fr}(\mathcal{M}(\phi_2)) = \mathrm{Fr}(\phi_2)$, which contradicts $y \notin V$. **.**

The following proposition summarizes the results obtained in lemma (20) and lemma (21) with the additional fact that if a minimal transform $\mathcal{M}(\phi)$ is an axiom modulo, then it is in fact an axiom of first order logic.

Proposition 245 *Let V be a set and $\phi \in \mathbf{P}(V)$. The following are equivalent:*

$$\begin{array}{ll} (i) & \phi \in \mathbf{A}^+(V) \text{ , i.e. } \phi \text{ is an axiom modulo} \\ (ii) & \mathcal{M}(\phi) \in \mathbf{A}(\bar{V}) \text{ , i.e. } \mathcal{M}(\phi) \text{ is an axiom} \\ (iii) & \mathcal{M}(\phi) \in \mathbf{A}^+(\bar{V}) \text{ , i.e. } \mathcal{M}(\phi) \text{ is an axiom modulo} \end{array}$$

where $\mathcal{M} : \mathbf{P}(V) \to \mathbf{P}(\bar{V})$ is the minimal transform mapping of definition (38).

Proof
First we assume the equivalence $(i) \Leftrightarrow (ii)$ has been proved, and we shall show $(ii) \Leftrightarrow (iii)$. From definition (80) we have $\mathbf{A}(\bar{V}) \subseteq \mathbf{A}^+(\bar{V})$ and the implication $(ii) \Rightarrow (iii)$ is clear. We now show $(iii) \Rightarrow (ii)$: so we assume that $\mathcal{M}(\phi)$ is an axiom modulo, i.e. $\mathcal{M}(\phi) \in \mathbf{A}^+(\bar{V})$. We need to show that $\mathcal{M}(\phi)$ is in fact an axiom, i.e. $\mathcal{M}(\phi) \in \mathbf{A}(\bar{V})$. However, from $\mathcal{M}(\phi) \in \mathbf{A}^+(\bar{V})$ and the implication $(i) \Rightarrow (ii)$ we see that $\bar{\mathcal{M}} \circ \mathcal{M}(\phi) \in \mathbf{A}(\bar{\bar{V}})$ where $\bar{\mathcal{M}} : \mathbf{P}(\bar{V}) \to \mathbf{P}(\bar{\bar{V}})$ is the minimal transform mapping. Consider the map $p : \bar{\bar{V}} \to \bar{V}$ of definition (43).

Then from lemma (14) we know that p is valid for $\bar{\mathcal{M}} \circ \mathcal{M}(\phi)$. Hence using lemma (19) we obtain $p \circ \bar{\mathcal{M}} \circ \mathcal{M}(\phi) \in \mathbf{A}(\bar{V})$. However, $\mathcal{N} = p \circ \bar{\mathcal{M}}$ is the weak transform of definition (43), and applying proposition (13) to the identity mapping $\sigma : V \to V$ we obtain $\mathcal{N} \circ \mathcal{M}(\phi) = \mathcal{M}(\phi)$. Having proved that $\mathcal{N} \circ \mathcal{M}(\phi) \in \mathbf{A}(\bar{V})$ we conclude that $\mathcal{M}(\phi) \in \mathbf{A}(\bar{V})$ as requested. So we now prove the equivalence $(i) \Leftrightarrow (ii)$ starting with $(i) \Rightarrow (ii)$: we assume that ϕ is an axiom modulo, i.e. $\phi \in \mathbf{A}^+(V)$. We need to show that $\mathcal{M}(\phi)$ is an axiom, i.e. $\mathcal{M}(\phi) \in \mathbf{A}(\bar{V})$. However, from definition (80), there exists an axiom $\psi \in \mathbf{A}(V)$ such that $\phi \sim \psi$, where $\sim$ is the substitution congruence. Using theorem (14) of page 149 we have $\mathcal{M}(\phi) = \mathcal{M}(\psi)$. It is therefore sufficient to prove that $\mathcal{M}(\psi) \in \mathbf{A}(\bar{V})$ which follows immediately from $\psi \in \mathbf{A}(V)$ and lemma (20). It remains to show the implication $(ii) \Rightarrow (i)$ which follows from lemma (21). **.**

As discussed in the beginning of this section, we need to show that the image of an axiom modulo by a valid substitution is an axiom modulo. Having proved proposition (245) we can safely rely on minimal transforms and prove the result:

Proposition 246 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\phi \in \mathbf{A}^+(V)$:*

$$(\sigma \text{ valid for } \phi) \Rightarrow \sigma(\phi) \in \mathbf{A}^+(W)$$

i.e. the image of an axiom modulo by a valid substitution is an axiom modulo.

Proof
We assume that ϕ is an axiom modulo i.e. $\phi \in \mathbf{A}^+(V)$. We also assume that σ is valid for ϕ. We need to show that $\sigma(\phi)$ is an axiom modulo, i.e. $\sigma(\phi) \in \mathbf{A}^+(W)$. From $\phi \in \mathbf{A}^+(V)$ and proposition (245) we obtain $\mathcal{M}(\phi) \in \mathbf{A}(\bar{V})$, i.e. the minimal transform $\mathcal{M}(\phi)$ is an axiom. Using proposition (100) the minimal extension $\bar{\sigma} : \bar{V} \to \bar{W}$ is valid for $\mathcal{M}(\phi)$. Applying lemma (19) we obtain $\bar{\sigma} \circ \mathcal{M}(\phi) \in \mathbf{A}(\bar{W})$, i.e. $\bar{\sigma} \circ \mathcal{M}(\phi)$ is an axiom. However, having assumed that σ is valid for ϕ, from theorem (13) of page 146 we have $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M} \circ \sigma(\phi)$. It follows that $\mathcal{M} \circ \sigma(\phi) \in \mathbf{A}(\bar{W})$ and from proposition (245), $\sigma(\phi) \in \mathbf{A}^+(W)$. **.**

The proof of proposition (246) actually works unchanged for essential substitutions $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$. Hence, without any additional work, we see that the image by an essential substitution of an axiom modulo is an axiom modulo.

Proposition 247 *Let V, W be sets and $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ be an essential substitution. Then for all $\phi \in \mathbf{P}(V)$ we have the following implication:*

$$\phi \in \mathbf{A}^+(V) \Rightarrow \sigma(\phi) \in \mathbf{A}^+(W)$$

i.e. the essential substitution image of an axiom modulo is an axiom modulo.

Proof
We assume that $\phi \in \mathbf{A}^+(V)$. We need to show that $\sigma(\phi) \in \mathbf{A}^+(W)$. From $\phi \in \mathbf{A}^+(V)$ and proposition (245) we obtain $\mathcal{M}(\phi) \in \mathbf{A}(\bar{V})$. Recall that from definition (44) the essential substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is associated to a unique map $\sigma : V \to W$. Using proposition (100) the minimal extension $\bar{\sigma}$:

$\bar{V} \to \bar{W}$ is valid for $\mathcal{M}(\phi)$. Applying lemma (19) we obtain $\bar{\sigma} \circ \mathcal{M}(\phi) \in \mathbf{A}(\bar{W})$. However from definition (44) we have $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M} \circ \sigma(\phi)$. It follows that $\mathcal{M} \circ \sigma(\phi) \in \mathbf{A}(\bar{W})$ and from proposition (245), $\sigma(\phi) \in \mathbf{A}^+(W)$. **.**

This completes our section where we have carried out the study of axioms modulo, and their images by minimal transforms, valid substitutions and essential substitutions. We are now well-equipped to establish the equality $\mathrm{Val}^+ \circ \sigma(\pi) = \sigma \circ \mathrm{Val}^+(\pi)$ in the case when π is a clean proof and σ is valid for π. This is the object of proposition (248) in the next section.

3.3.5 Valid Substitution of Clean Proof

We created the valuation $\mathrm{Val}^+ : \mathbf{\Pi}(V) \to \mathbf{P}(V)$ in definition (82) so as to allow us to define a notion of minimal transform for proofs which would behave sensibly, namely with the equivalence $\mathrm{Val}^+ \circ \mathcal{M}(\pi) \sim \mathcal{M} \circ \mathrm{Val}^+(\pi)$ for a *reasonable* proof π, where $\sim$ is the substitution congruence on $\mathbf{P}(\bar{V})$. We now know that a *reasonable* proof is simply a clean proof as per definition (86). However, before we proceed with minimal transforms on $\mathbf{\Pi}(V)$, we need to check that Val^+ successfully passes its second test. Remember that some degree of validation for Val^+ was already obtained when we established in proposition (233) that Val^+ does lead to an equivalent notion of provability. However, we now need to go further and make sure that the three key notions of Val^+, *clean* proof and valid substitution for proofs of definition (79) all make sense:

Proposition 248 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\pi \in \mathbf{\Pi}(V)$ be a clean proof and let σ be valid for π. Then $\sigma(\pi)$ is also a clean proof and:*

$$\mathrm{Val}^+ \circ \sigma(\pi) = \sigma \circ \mathrm{Val}^+(\pi) \tag{3.35}$$

Proof
For every proof $\pi \in \mathbf{\Pi}(V)$, we need to show the following implication:

$$(\pi \text{ clean}) \wedge (\sigma \text{ valid for } \pi) \;\Rightarrow\; (\sigma(\pi) \text{ clean}) \wedge (\text{eq. (3.35)})$$

We shall do so with a structural induction using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. From definition (86), π is always a clean proof in this case. So we assume that σ is valid for π, and we need to show that $\sigma(\pi)$ is a clean proof together with equation (3.35). From definition (74) we have $\sigma(\pi) = \sigma(\phi) \in \mathbf{P}(W)$ and consequently $\sigma(\pi)$ is a clean proof. Furthermore, we have $\mathrm{Val}^+(\sigma(\pi)) = \mathrm{Val}^+(\sigma(\phi)) = \sigma(\phi) = \sigma(\mathrm{Val}^+(\pi))$ which shows that equation (3.35) is true. This completes the case when $\pi = \phi$ for which the assumption of validity of σ for π was unnecessary. We now assume $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. We further assume that π is a clean proof and σ is valid for π. We need to show that $\sigma(\pi)$ is clean together with equation (3.35). From definition (86), having assumed that π is a clean proof we obtain $\phi \in \mathbf{A}^+(V)$, i.e. ϕ is an axiom modulo. Having assumed that σ is valid for π, from proposition (218) σ is valid for ϕ. It follows from proposition (246) that $\sigma(\phi) \in \mathbf{A}^+(W)$. Hence, using definition (86) once more we see that $\sigma(\pi) = \partial\sigma(\phi)$ is a clean proof. Furthermore from definition (82) we have $\mathrm{Val}^+(\sigma(\pi)) = \sigma(\phi) = \sigma(\mathrm{Val}^+(\pi))$ and it

follows that equation (3.35) is true. So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs which satisfy our implication. We need to show the same is true of π. So we assume that π is a clean proof and furthermore that σ is valid for π. We need to show that $\sigma(\pi)$ is clean and equation (3.35) is true. However, using proposition (240) we see that both π_1 and π_2 are clean proofs, and furthermore that $\mathrm{Val}^+(\pi_2) = \psi_1 \to \psi_2$ for some $\psi_1, \psi_2 \in \mathbf{P}(V)$ such that $\psi_1 \sim \mathrm{Val}^+(\pi_1)$ and $\psi_2 = \mathrm{Val}^+(\pi)$, where $\sim$ is the substitution congruence on $\mathbf{P}(V)$. Moreover, using proposition (219) we see that σ is valid for both π_1 and π_2. Having assumed our induction hypothesis holds for π_1, π_2 it follows that $\sigma(\pi_1)$ and $\sigma(\pi_2)$ are both clean proofs, and equation (3.35) is true for π_1 and π_2. So let us prove that $\sigma(\pi)$ is a clean proof: since $\sigma(\pi) = \sigma(\pi_1) \oplus \sigma(\pi_2)$, from proposition (240) it is sufficient to show that $\sigma(\pi_1)$ and $\sigma(\pi_2)$ are clean which we already know, and furthermore that $\mathrm{Val}^+(\sigma(\pi_2)) = \chi_1 \to \chi_2$ where $\chi_1 \sim \mathrm{Val}^+(\sigma(\pi_1))$. If this last property is true, then $\chi_2 = \mathrm{Val}^+(\sigma(\pi))$. So let us prove this is indeed the case. Applying $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ on both sides of $\mathrm{Val}^+(\pi_2) = \psi_1 \to \psi_2$ we obtain $\sigma \circ \mathrm{Val}^+(\pi_2) = \sigma(\psi_1) \to \sigma(\psi_2)$. Since equation (3.35) is true for π_2 it follows that $\mathrm{Val}^+(\sigma(\pi_2)) = \chi_1 \to \chi_2$ where $\chi_1 = \sigma(\psi_1)$ and $\chi_2 = \sigma(\psi_2)$. In order to show that $\sigma(\pi)$ is a clean proof, it remains to show that $\sigma(\psi_1) \sim \mathrm{Val}^+(\sigma(\pi_1))$ where $\sim$ is the substitution congruence on $\mathbf{P}(W)$. Since equation (3.35) is true for π_1, this amounts to showing that $\sigma(\psi_1) \sim \sigma(\mathrm{Val}^+(\pi_1))$. Since $\psi_1 \sim \mathrm{Val}^+(\pi_1)$, using theorem (15) of page 152 it is sufficient to show that σ is valid for both ψ_1 and $\mathrm{Val}^+(\pi_1)$. The validity of σ for $\mathrm{Val}^+(\pi_1)$ follows from proposition (237) and the validity of σ for π_1. So it remains to show that σ is valid for ψ_1. Since $\mathrm{Val}^+(\pi_2) = \psi_1 \to \psi_2$, from proposition (54) it is sufficient to show that σ is valid for $\mathrm{Val}^+(\pi_2)$ which follows from proposition (237) and the validity of σ for π_2. So we have proved that $\sigma(\pi)$ is a clean proof, and it remains to show that equation (3.35) is true. However as already indicated, we have $\mathrm{Val}^+(\sigma(\pi)) = \chi_2 = \sigma(\psi_2) = \sigma(\mathrm{Val}^+(\pi))$ which completes our induction argument in the case when $\pi = \pi_1 \oplus \pi_2$. So we now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof which satisfies our implication. We need to show the same is true of π. So we assume that π is a clean proof and furthermore that σ is valid for π. We need to show that $\sigma(\pi)$ is clean and equation (3.35) is true. However from proposition (241), π_1 is a clean proof and $x \notin \mathrm{Sp}(\pi_1)$. Furthermore, using proposition (220), σ is valid for π_1 and furthermore for all $u \in V$ we have the implication:

$$u \in \mathrm{Fr}(\nabla x \pi_1) \;\Rightarrow\; \sigma(u) \neq \sigma(x) \tag{3.36}$$

Having assumed our induction hypothesis holds for π_1 it follows that $\sigma(\pi_1)$ is a clean proof and equation (3.35) is true for π_1. So let us prove that $\sigma(\pi)$ is a clean proof: since $\sigma(\pi) = \nabla \sigma(x) \sigma(\pi_1)$, from proposition (241) it is sufficient to prove that $\sigma(\pi_1)$ is clean and $\sigma(x) \notin \mathrm{Sp}(\sigma(\pi_1))$. We already know that $\sigma(\pi_1)$ is a clean proof so we only need to show that $\sigma(x) \notin \mathrm{Sp}(\sigma(\pi_1))$. So suppose to the contrary that $\sigma(x) \in \mathrm{Sp}(\sigma(\pi_1))$. From proposition (206) we have $\mathrm{Sp}(\sigma(\pi_1)) \subseteq \sigma(\mathrm{Sp}(\pi_1))$ and it follows that $\sigma(x) = \sigma(u)$ for some $u \in \mathrm{Sp}(\pi_1)$. Having established that $x \notin \mathrm{Sp}(\pi_1)$ we must have $u \neq x$ and consequently $u \in \mathrm{Sp}(\pi_1) \setminus \{x\}$. However, since π_1 is a clean proof, from proposition (244) we

have $\mathrm{Sp}(\pi_1) \subseteq \mathrm{Fr}(\pi_1)$. It follows that $u \in \mathrm{Fr}(\nabla x \pi_1)$ while $\sigma(u) = \sigma(x)$. This contradicts the implication (3.36). So we have proved that $\sigma(\pi)$ is clean and it remains to prove equation (3.35) which goes as follows:

$$\begin{array}{rcl}
\mathrm{Val}^+(\sigma(\pi)) & = & \mathrm{Val}^+(\sigma(\nabla x \pi_1)) \\
\text{def. (74)} \ \rightarrow & = & \mathrm{Val}^+(\nabla \sigma(x) \sigma(\pi_1)) \\
\sigma(x) \notin \mathrm{Sp}(\sigma(\pi_1)) \ \rightarrow & = & \forall \sigma(x) \mathrm{Val}^+(\sigma(\pi_1)) \\
\text{(3.35) true for } \pi_1 \ \rightarrow & = & \forall \sigma(x) \sigma(\mathrm{Val}^+(\pi_1)) \\
\text{def. (24)} \ \rightarrow & = & \sigma(\forall x \mathrm{Val}^+(\pi_1)) \\
x \notin \mathrm{Sp}(\pi_1) \ \rightarrow & = & \sigma(\mathrm{Val}^+(\nabla x \pi_1)) \\
& = & \sigma(\mathrm{Val}^+(\pi))
\end{array}$$

.

3.3.6 Minimal Transform of Proof

The following definition introduces a concept of minimal transform for proofs. Comparing with the existing definition (38) of minimal transform for formulas, we see that our suggestion of $\mathcal{M}(\pi)$ for $\pi \in \mathbf{\Pi}(V)$ is as natural as it can be. However we saw that despite its simplicity, this definition failed to give us the sensible outcome $\mathrm{Val} \circ \mathcal{M}(\pi) \sim \mathcal{M} \circ \mathrm{Val}(\pi)$ where $\sim$ is the substitution congruence on $\mathbf{P}(\bar{V})$. Nevertheless, we stood our ground and decided to review our deductive system rather than contemplate an alternative definition of minimal transform for proofs. We defined a new valuation $\mathrm{Val}^+ : \mathbf{\Pi}(V) \rightarrow \mathbf{P}(V)$ which was flexible enough on α-equivalence, while leading to an equivalent set of sequents $\Gamma \vdash \phi$ as demonstrated by proposition (233). This new valuation will allow us to write $\mathrm{Val}^+ \circ \mathcal{M}(\pi) \sim \mathcal{M} \circ \mathrm{Val}^+(\pi)$ whenever π is a clean proof, a fact we shall prove in proposition (254). Needless to say that minimal transforms for proofs are likely to be a key notion just as they were for formulas. We shall be able to show the existence of *essential substitutions* for proofs of definition (95) and establish the substitution theorem (30) of page 388, allowing us to carry over the sequent $\Gamma \vdash \phi$ into $\sigma(\Gamma) \vdash \sigma(\phi)$ whenever $\sigma : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$ is an essential substitution. This is a beautiful result we think, as it no longer contains the ugly caveats on variable capture which are so common in mathematical textbooks. Note that the following definition of minimal transform abides with a key principle which we have adopted throughout these notes. Since $\mathbf{P}(V) \subseteq \mathbf{\Pi}(V)$, we made sure this new definition of $\mathcal{M}(\pi)$ is compatible with the existing definition (38) whenever $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Thus, when confronted with the notation $\mathcal{M}(\phi)$ we do not need to worry as to whether ϕ is regarded as a formula or as a proof. We are now ready to quote:

Definition 88 *Let V be a set with minimal extension $\bar{V}$. We call* minimal

transform mapping on $\mathbf{\Pi}(V)$ *the map* $\mathcal{M} : \mathbf{\Pi}(V) \to \mathbf{\Pi}(\bar{V})$ *defined by:*

$$\forall \pi \in \mathbf{\Pi}(V)\ ,\ \mathcal{M}(\pi) = \begin{cases} \mathcal{M}(\phi) & \textit{if} \quad \pi = \phi \in \mathbf{P}(V) \\ \partial\mathcal{M}(\phi) & \textit{if} \quad \pi = \partial\phi \\ \mathcal{M}(\pi_1) \oplus \mathcal{M}(\pi_2) & \textit{if} \quad \pi = \pi_1 \oplus \pi_2 \\ \nabla n \mathcal{M}(\pi_1)[n/x] & \textit{if} \quad \pi = \nabla x \pi_1 \end{cases} \tag{3.37}$$

where $n = \min\{k \in \mathbf{N} : [k/x]$ *valid for* $\mathcal{M}(\pi_1)\}$.

Proposition 249 *The structural recursion of* definition (87) *is legitimate.*

Proof
We need to show the existence and uniqueness of the map $\mathcal{M} : \mathbf{\Pi}(V) \to \mathbf{\Pi}(\bar{V})$ satisfying the four conditions of (3.37). We shall do so using theorem (4) of page 42. So we take $X = \mathbf{\Pi}(V)$ with free generator $X_0 = \mathbf{P}(V)$ and we choose $A = \mathbf{\Pi}(\bar{V})$. We define $g_0 : X_0 \to A$ by setting $g_0(\phi) = \mathcal{M}(\phi) \in \mathbf{P}(\bar{V}) \subseteq A$, which takes care of the first condition. For every $\phi \in \mathbf{P}(V)$, we define the map $h(\partial\phi) : A^0 \to A$ by setting $h(\partial\phi)(0) = \partial\mathcal{M}(\phi)$ which takes care of the second condition. We also define $h(\oplus) : A^2 \to A$ by setting $h(\oplus)(\pi_1, \pi_2) = \pi_1 \oplus \pi_2$ which takes care of the third condition. Finally, for all $x \in V$ we define the map $h(\nabla x) : A^1 \to A$ by setting $h(\nabla x)(\pi_1) = \nabla n \pi_1[n/x]$, where:

$$n = n(\nabla x)(\pi_1) = \min\{k \in \mathbf{N}\ :\ [k/x] \text{ valid for } \pi_1\}$$

.

As we shall see, many properties of minimal transforms apply to both proofs and formulas. The following property does not. By showing the equality $\mathrm{Sp}(\mathcal{M}(\pi)) = \mathrm{Sp}(\pi)$ for clean proofs, we shall be able to argue that minimal transforms of clean proofs are clean. Note that the equality fails when π is not clean. For example, if $\pi = \nabla x(x \in x)$ we have $\mathcal{M}(\pi) = \nabla\, 0(0 \in 0)$. Thus, we see that $\mathrm{Sp}(\pi) = \{x\}$ while $\mathrm{Sp}(\mathcal{M}(\pi)) = \{0\}$ and $\{x\} \neq \{0\}$ since $V \cap \mathbf{N} = \emptyset$.

Proposition 250 *Let* V *be a set and* $\pi \in \mathbf{\Pi}(V)$ *be a clean proof. Then:*

$$\mathrm{Sp}(\mathcal{M}(\pi)) = \mathrm{Sp}(\pi)$$

Proof
For every proof $\pi \in \mathbf{\Pi}(V)$ we need to show the following implication:

$$(\pi \text{ clean}) \ \Rightarrow\ \mathrm{Sp}(\mathcal{M}(\pi)) = \mathrm{Sp}(\pi)$$

We shall do so with a structural induction, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then π is always a clean proof, and we need to show that $\mathrm{Fr}(\mathcal{M}(\phi)) = \mathrm{Fr}(\phi)$ which follows from proposition (97). Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then we have:

$$\mathrm{Sp}(\mathcal{M}(\pi)) = \mathrm{Sp}(\,\partial\mathcal{M}(\phi)\,) = \emptyset = \mathrm{Sp}(\pi)$$

Whether or not π is a clean proof, i.e. whether or not ϕ is an axiom modulo is irrelevant in this case. So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$

are proofs which satisfy our implication. We need to show the same is true of π. So we assume that π is a clean proof. From proposition (240) it follows in particular that both π_1 and π_2 are clean proofs. Consequently:

$$\begin{array}{rcl} \mathrm{Sp}(\mathcal{M}(\pi)) & = & \mathrm{Sp}(\,\mathcal{M}(\pi_1 \oplus \pi_2)\,) \\ & = & \mathrm{Sp}(\,\mathcal{M}(\pi_1) \oplus \mathcal{M}(\pi_2)\,) \\ \text{prop. (204)} \;\rightarrow & = & \mathrm{Sp}(\mathcal{M}(\pi_1)) \cup \mathrm{Sp}(\mathcal{M}(\pi_2)) \\ \pi_1, \pi_2 \text{ clean} \;\rightarrow & = & \mathrm{Sp}(\pi_1) \cup \mathrm{Sp}(\pi_2) \\ \text{prop. (204)} \;\rightarrow & = & \mathrm{Sp}(\pi_1 \oplus \pi_2) \\ & = & \mathrm{Sp}(\pi) \end{array}$$

So we now assume that $\pi = \nabla x \pi_1$ for some $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ which satisfies our implication. We need to show the same is true of π. So we assume that π is a clean proof. From proposition (241) it follows that π_1 is itself a clean proof and furthermore $x \notin \mathrm{Sp}(\pi_1)$. Hence, we have the following equalities:

$$\begin{array}{rcl} \mathrm{Sp}(\mathcal{M}(\pi)) & = & \mathrm{Sp}(\mathcal{M}(\nabla x \pi_1)) \\ n = \min\{k : [k/x] \text{ valid for } \mathcal{M}(\pi_1)\} \;\rightarrow & = & \mathrm{Sp}(\,\nabla n \mathcal{M}(\pi_1)[n/x]\,) \\ \text{prop. (204)} \;\rightarrow & = & \mathrm{Sp}(\,\mathcal{M}(\pi_1)[n/x]\,) \\ \text{prop. (222), } [n/x] \text{ valid for } \mathcal{M}(\pi_1) \;\rightarrow & = & [n/x](\,\mathrm{Sp}(\mathcal{M}(\pi_1))\,) \\ \pi_1 \text{ clean} \;\rightarrow & = & [n/x](\,\mathrm{Sp}(\pi_1)\,) \\ x \notin \mathrm{Sp}(\pi_1) \;\rightarrow & = & \mathrm{Sp}(\pi_1) \\ \text{prop. (204)} \;\rightarrow & = & \mathrm{Sp}(\nabla x \pi_1) \\ & = & \mathrm{Sp}(\pi) \end{array}$$

.

We have spent a lot of time discussing the importance of the equivalence $\mathrm{Val}^+ \circ \mathcal{M}(\pi) \sim \mathcal{M} \circ \mathrm{Val}^+(\pi)$, where $\sim$ is the substitution congruence on $\mathbf{P}(\bar{V})$. The notion of minimal transform $\mathcal{M}(\pi)$ cannot be interesting unless we can say something sensible about its conclusion or conclusion modulo. However, we should not forget that controlling the hypothesis of a proof is as important as controlling its conclusion. So we need to make sure $\mathrm{Hyp}(\mathcal{M}(\pi))$ is also sensible.

Proposition 251 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$ be a clean proof. Then:*

$$\mathrm{Hyp}(\mathcal{M}(\pi)) = \mathcal{M}(\mathrm{Hyp}(\pi))$$

Proof
For every proof $\pi \in \mathbf{\Pi}(V)$ we need to show the following implication:

$$(\pi \text{ clean}) \;\Rightarrow\; \mathrm{Hyp}(\mathcal{M}(\pi)) = \mathcal{M}(\mathrm{Hyp}(\pi))$$

We shall do so with a structural induction, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then π is always clean in this case and we simply need to prove the equality which goes as follows:

$$\mathrm{Hyp}(\mathcal{M}(\phi)) = \{\mathcal{M}(\phi)\} = \mathcal{M}(\{\phi\}) = \mathcal{M}(\mathrm{Hyp}(\phi))$$

We now assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then we have:

$$\begin{aligned}
\mathrm{Hyp}(\mathcal{M}(\pi)) &= \mathrm{Hyp}(\mathcal{M}(\partial\phi)) \\
&= \mathrm{Hyp}(\,\partial\mathcal{M}(\phi)\,) \\
&= \emptyset \\
&= \mathcal{M}(\emptyset) \\
&= \mathcal{M}(\mathrm{Hyp}(\partial\phi)) \\
&= \mathcal{M}(\mathrm{Hyp}(\pi))
\end{aligned}$$

So the equality is always true and so is the implication. So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs satisfying our implication. We need to show the same is true of π. So we assume that π is clean. We need to show the equality is true for π. However, from proposition (240) both π_1 and π_2 are clean and the equality is therefore true for π_1 and π_2. Hence:

$$\begin{aligned}
\mathrm{Hyp}(\mathcal{M}(\pi)) &= \mathrm{Hyp}(\mathcal{M}(\pi_1 \oplus \pi_2)) \\
&= \mathrm{Hyp}(\,\mathcal{M}(\pi_1) \oplus \mathcal{M}(\pi_2)\,) \\
&= \mathrm{Hyp}(\mathcal{M}(\pi_1)) \cup \mathrm{Hyp}(\mathcal{M}(\pi_2)) \\
&= \mathcal{M}(\mathrm{Hyp}(\pi_1)) \cup \mathcal{M}(\mathrm{Hyp}(\pi_2)) \\
&= \mathcal{M}(\,\mathrm{Hyp}(\pi_1) \cup \mathrm{Hyp}(\pi_2)\,) \\
&= \mathcal{M}(\mathrm{Hyp}(\pi_1 \oplus \pi_2)) \\
&= \mathcal{M}(\mathrm{Hyp}(\pi))
\end{aligned}$$

We now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof satisfying our implication. We need to show the same is true of π. So we assume that π is clean. We need to show the equality is true for π. However, from proposition (241) we see that π_1 is clean and $x \notin \mathrm{Sp}(\pi_1)$. Hence:

$$\begin{aligned}
\mathrm{Hyp}(\mathcal{M}(\pi)) &= \mathrm{Hyp}(\mathcal{M}(\nabla x \pi_1)) \\
&= \mathrm{Hyp}(\,\nabla n \mathcal{M}(\pi_1)[n/x]\,) \\
&= \mathrm{Hyp}(\mathcal{M}(\pi_1)[n/x]) \\
\text{prop. (193)} \;\rightarrow\; &= [n/x](\,\mathrm{Hyp}(\mathcal{M}(\pi_1))\,) \\
&= [n/x](\,\mathcal{M}(\mathrm{Hyp}(\pi_1))\,) \\
\text{A: to be proved} \;\rightarrow\; &= \mathcal{M}(\mathrm{Hyp}(\pi_1)) \\
&= \mathcal{M}(\mathrm{Hyp}(\nabla x \pi_1)) \\
&= \mathcal{M}(\mathrm{Hyp}(\pi))
\end{aligned}$$

So it remains to prove point A, for which is it sufficient to show the equality $[n/x](\psi) = \psi$ for all $\psi \in \mathcal{M}(\mathrm{Hyp}(\pi_1))$. So it is sufficient to show the equality

$[n/x] \circ \mathcal{M}(\phi) = \mathcal{M}(\phi)$ for all $\phi \in \mathrm{Hyp}(\pi_1)$. So let $\phi \in \mathrm{Hyp}(\pi_1)$. Using proposition (36), we simply need to show that $[n/x](u) = u$ for all $u \in \mathrm{Var}(\mathcal{M}(\phi))$. It is therefore sufficient to prove that $x \notin \mathrm{Var}(\mathcal{M}(\phi))$. So suppose to the contrary that $x \in \mathrm{Var}(\mathcal{M}(\phi))$. Since $x \in V$ we have $x \in \mathrm{Var}(\mathcal{M}(\phi)) \cap V$ and it follows from proposition (97) that $x \in \mathrm{Fr}(\phi)$ while $\phi \in \mathrm{Hyp}(\pi_1)$. Hence we see that $x \in \mathrm{Sp}(\pi_1)$ which is a contradiction, and completes our induction argument. .

The whole point of minimal transforms is to create logical copies of formulas and proofs in which free and bound variables have been segregated. The free variables remain in the set V while the bound variables belong to a copy of $\mathbf{N}$ which is disjoint from V. The following is the counterpart of proposition (97):

Proposition 252 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$. Then we have the equality:*

$$\mathrm{Fr}(\mathcal{M}(\pi)) = \mathrm{Var}(\mathcal{M}(\pi)) \cap V = \mathrm{Fr}(\pi)$$

where $\mathcal{M}(\pi) \in \mathbf{\Pi}(\bar{V})$ is the minimal transform of $\pi \in \mathbf{\Pi}(V)$.

Proof
We shall prove this equality with a structural induction, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then the equality follows immediately from proposition (97). So we now assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then using proposition (97) once more we obtain:

$$\begin{array}{rcl}
\mathrm{Var}(\mathcal{M}(\pi)) \cap V & = & \mathrm{Var}(\mathcal{M}(\partial\phi)) \cap V \\
& = & \mathrm{Var}(\partial\mathcal{M}(\phi)) \cap V \\
& = & \mathrm{Var}(\mathcal{M}(\phi)) \cap V \\
\text{prop. (97)} \ \rightarrow & = & \mathrm{Fr}(\phi) \\
& = & \mathrm{Fr}(\partial\phi) \\
& = & \mathrm{Fr}(\pi)
\end{array}$$

as well as:

$$\begin{array}{rcl}
\mathrm{Fr}(\mathcal{M}(\pi)) & = & \mathrm{Fr}(\mathcal{M}(\partial\phi)) \\
& = & \mathrm{Fr}(\partial\mathcal{M}(\phi)) \\
& = & \mathrm{Fr}(\mathcal{M}(\phi)) \\
\text{prop. (97)} \ \rightarrow & = & \mathrm{Fr}(\phi) \\
& = & \mathrm{Fr}(\partial\phi) \\
& = & \mathrm{Fr}(\pi)
\end{array}$$

So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs satisfying our equality. We need to show the same is true of π. On the one hand we have:

$$\mathrm{Var}(\mathcal{M}(\pi)) \cap V \quad = \quad \mathrm{Var}(\mathcal{M}(\pi_1 \oplus \pi_2)) \cap V$$

$$
\begin{array}{rcl}
 & = & \mathrm{Var}(\,\mathcal{M}(\pi_1)\oplus\mathcal{M}(\pi_2)\,)\cap V \\
 & = & (\,\mathrm{Var}(\mathcal{M}(\pi_1))\cup\mathrm{Var}(\mathcal{M}(\pi_2))\,)\cap V \\
 & = & \mathrm{Var}(\mathcal{M}(\pi_1))\cap V\ \cup\ \mathrm{Var}(\mathcal{M}(\pi_2))\cap V \\
 & = & \mathrm{Fr}(\pi_1)\cup\mathrm{Fr}(\pi_2) \\
 & = & \mathrm{Fr}(\pi_1\oplus\pi_2) \\
 & = & \mathrm{Fr}(\pi)
\end{array}
$$

while on the other hand:

$$
\begin{array}{rcl}
\mathrm{Fr}(\mathcal{M}(\pi)) & = & \mathrm{Fr}(\mathcal{M}(\pi_1\oplus\pi_2)) \\
 & = & \mathrm{Fr}(\,\mathcal{M}(\pi_1)\oplus\mathcal{M}(\pi_2)\,) \\
 & = & \mathrm{Fr}(\mathcal{M}(\pi_1))\cup\mathrm{Fr}(\mathcal{M}(\pi_2)) \\
 & = & \mathrm{Fr}(\pi_1)\cup\mathrm{Fr}(\pi_2) \\
 & = & \mathrm{Fr}(\pi_1\oplus\pi_2) \\
 & = & \mathrm{Fr}(\pi)
\end{array}
$$

We now assume that $\pi = \nabla x\pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof satisfying our equality. We need to show the same is true of π. On the one hand we have:

$$
\begin{array}{rcl}
\mathrm{Var}(\mathcal{M}(\pi))\cap V & = & \mathrm{Var}(\mathcal{M}(\nabla x\pi_1))\cap V \\
 & = & \mathrm{Var}(\,\nabla n\mathcal{M}(\pi_1)[n/x]\,)\cap V \\
 & = & (\,\{n\}\cup\mathrm{Var}(\,\mathcal{M}(\pi_1)[n/x]\,)\,)\cap V \\
n\notin V\ \rightarrow & = & \mathrm{Var}(\,\mathcal{M}(\pi_1)[n/x]\,)\cap V \\
\text{prop. (201)}\ \rightarrow & = & [n/x](\,\mathrm{Var}(\mathcal{M}(\pi_1))\,)\cap V \\
n\notin V\ \rightarrow & = & [n/x](\,\mathrm{Var}(\mathcal{M}(\pi_1))\setminus\{x\}\,)\cap V \\
u\neq x\Rightarrow[n/x](u)=u\ \rightarrow & = & (\,\mathrm{Var}(\mathcal{M}(\pi_1))\setminus\{x\}\,)\cap V \\
 & = & (\,\mathrm{Var}(\mathcal{M}(\pi_1))\cap V\,)\setminus\{x\} \\
 & = & \mathrm{Fr}(\pi_1)\setminus\{x\} \\
 & = & \mathrm{Fr}(\nabla x\pi_1) \\
 & = & \mathrm{Fr}(\pi)
\end{array}
$$

while on the other hand:

$$
\begin{array}{rcl}
\mathrm{Fr}(\mathcal{M}(\pi)) & = & \mathrm{Fr}(\mathcal{M}(\nabla x\pi_1)) \\
n=\min\{k:[k/x]\text{ valid for }\mathcal{M}(\pi_1)\}\ \rightarrow & = & \mathrm{Fr}(\nabla n\mathcal{M}(\pi_1)[n/x]) \\
 & = & \mathrm{Fr}(\mathcal{M}(\pi_1)[n/x])\setminus\{n\} \\
[n/x]\text{ valid, prop. (223)}\ \rightarrow & = & [n/x](\,\mathrm{Fr}(\mathcal{M}(\pi_1))\,)\setminus\{n\} \\
[n/x](x)=n\ \rightarrow & = & [n/x](\,\mathrm{Fr}(\mathcal{M}(\pi_1))\setminus\{x\}\,)\setminus\{n\} \\
u\neq x\Rightarrow\ [n/x](u)=u\ \rightarrow & = & \mathrm{Fr}(\mathcal{M}(\pi_1))\setminus\{x\}\setminus\{n\}
\end{array}
$$

$$\begin{array}{rcl} & = & \mathrm{Fr}(\pi_1) \setminus \{x\} \setminus \{n\} \\ n \notin V \ \rightarrow & = & \mathrm{Fr}(\pi_1) \setminus \{x\} \\ & = & \mathrm{Fr}(\nabla x \pi_1) \\ & = & \mathrm{Fr}(\pi) \end{array}$$

.

The following is the counterpart of proposition (98) :

Proposition 253 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$. Then we have the equality:*

$$\mathrm{Bnd}(\mathcal{M}(\pi)) = \mathrm{Var}(\mathcal{M}(\pi)) \cap \mathbf{N}$$

where $\mathcal{M}(\pi) \in \mathbf{\Pi}(\bar{V})$ is the minimal transform of $\pi \in \mathbf{\Pi}(V)$.

Proof
We shall prove this equality with a structural induction, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then the equality follows immediately from proposition (98). Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then we have the following equalities:

$$\begin{array}{rcl} \mathrm{Bnd}(\mathcal{M}(\pi)) & = & \mathrm{Bnd}(\mathcal{M}(\partial\phi)) \\ & = & \mathrm{Bnd}(\partial\mathcal{M}(\phi)) \\ & = & \mathrm{Bnd}(\mathcal{M}(\phi)) \\ \text{prop. (98)} \ \rightarrow & = & \mathrm{Var}(\mathcal{M}(\phi)) \cap \mathbf{N} \\ & = & \mathrm{Var}(\partial\mathcal{M}(\phi)) \cap \mathbf{N} \\ & = & \mathrm{Var}(\mathcal{M}(\partial\phi)) \cap \mathbf{N} \\ & = & \mathrm{Var}(\mathcal{M}(\pi)) \cap \mathbf{N} \end{array}$$

So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs satisfying our equality. We need to show the same is true of π, which goes as follows:

$$\begin{array}{rcl} \mathrm{Bnd}(\mathcal{M}(\pi)) & = & \mathrm{Bnd}(\mathcal{M}(\pi_1 \oplus \pi_2)) \\ & = & \mathrm{Bnd}(\, \mathcal{M}(\pi_1) \oplus \mathcal{M}(\pi_2) \,) \\ & = & \mathrm{Bnd}(\mathcal{M}(\pi_1)) \cup \mathrm{Bnd}(\mathcal{M}(\pi_2)) \\ & = & (\mathrm{Var}(\mathcal{M}(\pi_1)) \cap \mathbf{N}) \cup (\mathrm{Var}(\mathcal{M}(\pi_2)) \cap \mathbf{N}) \\ & = & (\, \mathrm{Var}(\mathcal{M}(\pi_1)) \cup \mathrm{Var}(\mathcal{M}(\pi_2)) \,) \cap \mathbf{N} \\ & = & \mathrm{Var}(\, \mathcal{M}(\pi_1) \oplus \mathcal{M}(\pi_2) \,) \cap \mathbf{N} \\ & = & \mathrm{Var}(\mathcal{M}(\pi_1 \oplus \pi_2)) \cap \mathbf{N} \\ & = & \mathrm{Var}(\mathcal{M}(\pi)) \cap \mathbf{N} \end{array}$$

We now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof satisfying our equality. We need to show the same is true for π which goes as follows:

$$\mathrm{Bnd}(\mathcal{M}(\pi)) \quad = \quad \mathrm{Bnd}(\mathcal{M}(\nabla x \pi_1))$$

$$
\begin{array}{rrcl}
 & & = & \mathrm{Bnd}(\,\nabla n\mathcal{M}(\pi_1)[n/x]\,) \\
 & & = & \{n\} \cup \mathrm{Bnd}(\mathcal{M}(\pi_1)[n/x]) \\
 & \text{prop. (215)} \;\rightarrow & = & \{n\} \cup [n/x](\,\mathrm{Bnd}(\mathcal{M}(\pi_1))\,) \\
 & [n/x](x) = n \;\rightarrow & = & \{n\} \cup [n/x](\,\mathrm{Bnd}(\mathcal{M}(\pi_1)) \setminus \{x\}\,) \\
u \neq x \Rightarrow & [n/x](u) = u \;\rightarrow & = & \{n\} \cup \mathrm{Bnd}(\mathcal{M}(\pi_1)) \setminus \{x\} \\
 & & = & \{n\} \cup (\,\mathrm{Var}(\mathcal{M}(\pi_1)) \cap \mathbf{N}\,) \setminus \{x\} \\
 & & = & (\,\{n\} \cup \mathrm{Var}(\mathcal{M}(\pi_1)) \setminus \{x\}\,) \cap \mathbf{N} \\
u \neq x \Rightarrow & [n/x](u) = u \;\rightarrow & = & (\,\{n\} \cup [n/x](\,\mathrm{Var}(\mathcal{M}(\pi_1)) \setminus \{x\}\,)\,) \cap \mathbf{N} \\
 & [n/x](x) = n \;\rightarrow & = & (\,\{n\} \cup [n/x](\,\mathrm{Var}(\mathcal{M}(\pi_1))\,)\,) \cap \mathbf{N} \\
 & \text{prop. (201)} \;\rightarrow & = & (\,\{n\} \cup \mathrm{Var}(\mathcal{M}(\pi_1)[n/x])\,) \cap \mathbf{N} \\
 & & = & \mathrm{Var}(\,\nabla n\mathcal{M}(\pi_1)[n/x]\,) \cap \mathbf{N} \\
 & & = & \mathrm{Var}(\mathcal{M}(\nabla x\pi_1)) \cap \mathbf{N} \\
 & & = & \mathrm{Var}(\mathcal{M}(\pi)) \cap \mathbf{N}
\end{array}
$$

.

3.3.7 Minimal Transform of Clean Proof

As already pointed out, the equivalence $\mathrm{Val}^+ \circ \mathcal{M}(\pi) \sim \mathcal{M} \circ \mathrm{Val}^+(\pi)$ is hugely important. The fact that we are able to obtain it serves as a vindication of both definition (82) of the valuation modulo $\mathrm{Val}^+ : \mathbf{\Pi}(V) \rightarrow \mathbf{P}(V)$ and of definition (87) of the minimal transform $\mathcal{M} : \mathbf{\Pi}(V) \rightarrow \mathbf{\Pi}(\bar{V})$. After much preliminary work we are at last in a position to prove it:

Proposition 254 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$ be a clean proof. Then the minimal transform $\mathcal{M}(\pi)$ is itself a clean proof and furthermore we have:*

$$\mathrm{Val}^+ \circ \mathcal{M}(\pi) \sim \mathcal{M} \circ \mathrm{Val}^+(\pi) \tag{3.38}$$

where $\sim$ denotes the substitution congruence on $\mathbf{P}(\bar{V})$.

Proof
For every proof $\pi \in \mathbf{\Pi}(V)$, we need to show the following implication:

$$(\,\pi \text{ clean}\,) \;\Rightarrow (\,\mathcal{M}(\pi) \text{ clean}\,) \wedge (\,\text{eq. (3.38)}\,)$$

We shall do so with a structural induction using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. From definition (86), π is always a clean proof in this case. From definition (87) we have $\mathcal{M}(\pi) = \mathcal{M}(\phi)$ which is also a clean proof. Furthermore, from definition (82) we have the equality $\mathrm{Val}^+ \circ \mathcal{M}(\pi) = \mathcal{M}(\phi) = \mathcal{M} \circ \mathrm{Val}^+(\pi)$ which shows in particular that the substitution equivalence (3.38) is true. So we now assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. We need to show that the implication is true for π. So we assume that π

is a clean proof. From definition (86) we have $\phi \in \mathbf{A}^+(V)$, i.e. ϕ is an axiom modulo. We need to show that $\mathcal{M}(\pi)$ is a clean proof and the equivalence (3.38) holds. However from proposition (245), $\mathcal{M}(\phi) \in \mathbf{A}^+(\bar{V})$ and consequently we see that $\mathcal{M}(\pi) = \partial\mathcal{M}(\phi)$ is a clean proof. Furthermore, we have $\mathrm{Val}^+ \circ \mathcal{M}(\pi) = \mathcal{M}(\phi) = \mathcal{M} \circ \mathrm{Val}^+(\pi)$ and in particular the substitution equivalence (3.38) is true. So we now assume that $\pi = \pi_1 \oplus \pi_2$ where π_1, π_2 are proofs which satisfy our implication. We need to show the same is true of π. So we assume that π is a clean proof. We need to show that $\mathcal{M}(\pi)$ is itself a clean proof, and furthermore that the equivalence (3.38) holds. However, from proposition (240) we see that both π_1 and π_2 are clean and:

$$\mathrm{Val}^+(\pi_2) = \psi_1 \to \psi_2 \tag{3.39}$$

for some $\psi_1, \psi_2 \in \mathbf{P}(V)$ such that $\psi_1 \sim \mathrm{Val}^+(\pi_1)$ and $\psi_2 = \mathrm{Val}^+(\pi)$, where $\sim$ also denotes the substitution congruence on $\mathbf{P}(V)$. Having assumed our implication is true for π_1 and π_2, it follows that $\mathcal{M}(\pi_1)$ and $\mathcal{M}(\pi_2)$ are clean and the equivalence (3.38) is true for π_1 and π_2. So let us prove that $\mathcal{M}(\pi)$ is a clean proof: since $\mathcal{M}(\pi) = \mathcal{M}(\pi_1) \oplus \mathcal{M}(\pi_2)$, from proposition (240) it is sufficient to show that both $\mathcal{M}(\pi_1)$ and $\mathcal{M}(\pi_2)$ are clean which we already know, and furthermore that we have the equality:

$$\mathrm{Val}^+ \circ \mathcal{M}(\pi_2) = \chi_1 \to \chi_2 \tag{3.40}$$

for some $\chi_1, \chi_2 \in \mathbf{P}(\bar{V})$ such that $\chi_1 \sim \mathrm{Val}^+ \circ \mathcal{M}(\pi_1)$, in which case we shall have $\chi_2 = \mathrm{Val}^+ \circ \mathcal{M}(\pi)$. However, taking the minimal transform on both sides of the equality (3.39) we obtain $\mathcal{M} \circ \mathrm{Val}^+(\pi_2) = \mathcal{M}(\psi_1) \to \mathcal{M}(\psi_2)$. Having established the fact that the equivalence (3.38) is true for π_2, it follows that $\mathrm{Val}^+ \circ \mathcal{M}(\pi_2) \sim \mathcal{M}(\psi_1) \to \mathcal{M}(\psi_2)$. Using theorem (12) of page 132 we see that equation (3.40) is therefore true for some $\chi_1, \chi_2 \in \mathbf{P}(\bar{V})$ such that $\chi_1 \sim \mathcal{M}(\psi_1)$ and $\chi_2 \sim \mathcal{M}(\psi_2)$. In order to show that $\mathcal{M}(\pi)$ is a clean proof, it remains to prove that $\mathcal{M}(\psi_1) \sim \mathrm{Val}^+ \circ \mathcal{M}(\pi_1)$. However, from $\psi_1 \sim \mathrm{Val}^+(\pi_1)$ and theorem (14) of page 149 we obtain $\mathcal{M}(\psi_1) = \mathcal{M} \circ \mathrm{Val}^+(\pi_1)$. So it is sufficient to prove that $\mathcal{M} \circ \mathrm{Val}^+(\pi_1) \sim \mathrm{Val}^+ \circ \mathcal{M}(\pi_1)$ which follows from the established fact that the equivalence (3.38) is true for π_1. So we have proved that $\mathcal{M}(\pi)$ is a clean proof and it remains to prove the equivalence (3.38) for π:

$$\mathrm{Val}^+ \circ \mathcal{M}(\pi) = \chi_2 \sim \mathcal{M}(\psi_2) = \mathcal{M} \circ \mathrm{Val}^+(\pi)$$

This completes our structural induction in the case when $\pi = \pi_1 \oplus \pi_2$. So we now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is a proof which satisfies our implication. We need to show the same is true of π. So we assume that π is a clean proof. We need to show that $\mathcal{M}(\pi)$ is itself a clean proof, and furthermore that the equivalence (3.38) is true for π. However, from proposition (241) we see that π_1 is a clean proof and $x \notin \mathrm{Sp}(\pi_1)$. Having assumed π_1 satisfies our implication, it follows that $\mathcal{M}(\pi_1)$ is clean, and the equivalence (3.38) is true for π_1. So let us prove that $\mathcal{M}(\pi)$ is a clean proof: since $\mathcal{M}(\pi) = \nabla n \mathcal{M}(\pi_1)[n/x]$, from proposition (241) it is sufficient to show

that $\mathcal{M}(\pi_1)[n/x]$ is a clean proof and furthermore that $n \notin \mathrm{Sp}(\,\mathcal{M}(\pi_1)[n/x]\,)$. First we show that $\mathcal{M}(\pi_1)[n/x]$ is clean: this follows from proposition (248) and the fact that $\mathcal{M}(\pi_1)$ is a clean proof while $[n/x]$ is valid for $\mathcal{M}(\pi_1)$ by virtue of definition (87). We now show that $n \notin \mathrm{Sp}(\,\mathcal{M}(\pi_1)[n/x]\,)$. So suppose to the contrary that $n \in \mathrm{Sp}(\,\mathcal{M}(\pi_1)[n/x]\,)$. From proposition (206) we have $\mathrm{Sp}(\,\mathcal{M}(\pi_1)[n/x]\,) \subseteq [n/x](\,\mathrm{Sp}(\mathcal{M}(\pi_1))\,)$. Furthermore, since π_1 is a clean proof, from proposition (250) we have $\mathrm{Sp}(\mathcal{M}(\pi_1)) = \mathrm{Sp}(\pi_1)$. It follows that $\mathrm{Sp}(\,\mathcal{M}(\pi_1)[n/x]\,) \subseteq [n/x](\mathrm{Sp}(\pi_1))$, and consequently $n = [n/x](u)$ for some $u \in \mathrm{Sp}(\pi_1) \subseteq V$. Having established that $x \notin \mathrm{Sp}(\pi_1)$ we obtain $u \neq x$ and finally $n = u$. This contradicts the fact $n \in \mathbf{N}$ while $u \in V$ and $V \cap \mathbf{N} = \emptyset$. So we have proved that $\mathcal{M}(\pi)$ is indeed a clean proof. We now show the equivalence (3.38) is true for π, which goes as follows:

$$
\begin{array}{rcl}
\mathrm{Val}^+ \circ \mathcal{M}(\pi) & = & \mathrm{Val}^+ \circ \mathcal{M}(\nabla x \pi_1) \\
n = \min\{k : [k/x] \text{ valid for } \mathcal{M}(\pi_1)\} \;\rightarrow & = & \mathrm{Val}^+(\,\nabla n \mathcal{M}(\pi_1)[n/x]\,) \\
n \notin \mathrm{Sp}(\,\mathcal{M}(\pi_1)[n/x]\,) \;\rightarrow & = & \forall n\, \mathrm{Val}^+ \circ [n/x] \circ \mathcal{M}(\pi_1) \\
\text{A: to be proved} \;\rightarrow & = & \forall n\, [n/x] \circ \mathrm{Val}^+ \circ \mathcal{M}(\pi_1) \\
& = & [n/x](\,\forall x\, \mathrm{Val}^+ \circ \mathcal{M}(\pi_1)\,) \\
\text{B: to be proved} \;\rightarrow & \sim & \forall x\, \mathrm{Val}^+ \circ \mathcal{M}(\pi_1) \\
\text{(3.38) true for } \pi_1 \;\rightarrow & \sim & \forall x\, \mathcal{M} \circ \mathrm{Val}^+(\pi_1) \\
\text{C: to be proved} \;\rightarrow & \sim & [m/x](\,\forall x\, \mathcal{M} \circ \mathrm{Val}^+(\pi_1)\,) \\
& = & \forall m\, \mathcal{M}(\mathrm{Val}^+(\pi_1))[m/x] \\
m = \min\{k : [k/x] \text{ valid for } \mathcal{M}(\mathrm{Val}^+(\pi_1))\} \;\rightarrow & = & \mathcal{M}(\,\forall x\, \mathrm{Val}^+(\pi_1)\,) \\
x \notin \mathrm{Sp}(\pi_1) \;\rightarrow & = & \mathcal{M} \circ \mathrm{Val}^+(\nabla x \pi_1) \\
& = & \mathcal{M} \circ \mathrm{Val}^+(\pi)
\end{array}
$$

It remains to justify points A,B and C . First we start with point A, which follows from proposition (248) and the fact that $\mathcal{M}(\pi_1)$ is a clean proof while $[n/x]$ is valid for $\mathcal{M}(\pi_1)$. We shall now establish point B: using proposition (77), it is sufficient to show that $[n/x] : \bar{V} \rightarrow \bar{V}$ is an admissible substitution for $\forall x\, \mathrm{Val}^+ \circ \mathcal{M}(\pi_1)$ as per definition (34). So we need to show that $[n/x]$ is valid for $\forall x\, \mathrm{Val}^+ \circ \mathcal{M}(\pi_1)$, and furthermore that $[n/x](u) = u$ for all $u \in \mathrm{Fr}(\,\forall x\, \mathrm{Val}^+ \circ \mathcal{M}(\pi_1)\,)$. This last equality is clear since any such u would satisfy $u \neq x$. So we can focus on the validity of $[n/x]$. Using proposition (55), it is sufficient to show that $[n/x]$ is valid for $\mathrm{Val}^+ \circ \mathcal{M}(\pi_1)$ and furthermore, given $u \in \mathrm{Fr}(\,\forall x\, \mathrm{Val}^+ \circ \mathcal{M}(\pi_1)\,)$ we have $[n/x](u) \neq [n/x](x)$. This last requirement can be expressed as $u \neq n$ which follows from $V \cap \mathbf{N} = \emptyset$ provided we show that $u \in V$. However since (3.38) is true for π_1, from proposition (79) we have $\mathrm{Fr}(\,\mathrm{Val}^+ \circ \mathcal{M}(\pi_1)\,) = \mathrm{Fr}(\,\mathcal{M} \circ \mathrm{Val}^+(\pi_1)\,) \subseteq V$, where this last inclusion follows from proposition (97). Hence we have $u \in V$ as requested. So it remains to show that $[n/x]$ is valid for $\mathrm{Val}^+ \circ \mathcal{M}(\pi_1)$ which follows from the validity of $[n/x]$ for $\mathcal{M}(\pi_1)$ and proposition (237). It remains to justify point C : similarly to the previous point, it is sufficient to prove that $[m/x] : \bar{V} \rightarrow \bar{V}$ is an admissible substitution for $\forall x\, \mathcal{M} \circ \mathrm{Val}^+(\pi_1)$.

It is clear that $[m/x](u) = u$ for all $u \in \mathrm{Fr}(\,\forall x\,\mathcal{M} \circ \mathrm{Val}^+(\pi_1)\,)$. So we simply need to show that $[m/x]$ is valid for $\forall x\,\mathcal{M} \circ \mathrm{Val}^+(\pi_1)$. As the integer m is chosen to be the smallest integer k such that $[k/x]$ is valid for $\mathcal{M} \circ \mathrm{Val}^+(\pi_1)$, in particular $[m/x]$ is valid for $\mathcal{M} \circ \mathrm{Val}^+(\pi_1)$. Using proposition (55) it is therefore sufficient to prove that $[m/x](u) \neq [m/x](x)$, which is $u \neq m$ for all $u \in \mathrm{Fr}(\,\forall x\,\mathcal{M} \circ \mathrm{Val}^+(\pi_1)\,)$. This follows from $u \in V$, itself a consequence of proposition (97). **.**

We have defined an notion of minimal transform for proofs which extends the existing notion for formulas. From proposition (254) we now know that the conclusion modulo of $\mathcal{M}(\pi)$ has the correct shape modulo α-equivalence. We also know from proposition (251) that the hypothesis of $\mathcal{M}(\pi)$ does make sense. This is enough for us to carry over sequents from $\Gamma \vdash \phi$ into $\mathcal{M}(\Gamma) \vdash \mathcal{M}(\phi)$, just as we carried over sequents from $\Gamma \vdash \phi$ into $\sigma(\Gamma) \vdash \sigma(\phi)$ for injective maps in proposition (230) following proposition (229). However, the ability to carry over sequents $\Gamma \vdash \phi$ into their minimal transform counterparts is not hugely interesting. What would be interesting is to have the equivalence:

$$\Gamma \vdash \phi \;\Leftrightarrow\; \mathcal{M}(\Gamma) \vdash \mathcal{M}(\phi)$$

Such equivalence would allow us to establish provability results while focussing on minimal transforms, which is arguably a lot easier. Unfortunately, this result (if true) is out of reach for the time being. Take $\phi = \forall x \forall y (x \in y) \to \forall x (y \in x)$ with $V = \{x, y\}$ and $x \neq y$. The only reason $\vdash \phi$ is true is we made sure it was an axiom, thanks to an essential substitution of y in place of x. By contrast, the sequent $\vdash \mathcal{M}(\phi)$ can be proved without *essential* specialization axioms. so if $\vdash \mathcal{M}(\phi) \;\Rightarrow \vdash \phi$ happens to be true, it crucially has to do with our larger set of axioms made possible by the use of essential substitutions. It looks deeper.

Proposition 255 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. Let $\phi \in \mathbf{P}(V)$. Then we have:*

$$\Gamma \vdash \phi \;\Rightarrow\; \mathcal{M}(\Gamma) \vdash \mathcal{M}(\phi)$$

where $\mathcal{M} : \mathbf{P}(V) \to \mathbf{P}(\bar{V})$ is the minimal transform mapping of definition (38)*.*

Proof
We assume that $\Gamma \vdash \phi$. There exists a proof $\pi \in \mathbf{\Pi}(V)$ such that $\mathrm{Val}(\pi) = \phi$ and $\mathrm{Hyp}(\pi) \subseteq \Gamma$. Without lost of generality, from proposition (185) we may assume that π is a totally clean proof. In particular, from proposition (238) π is clean. Furthermore, from proposition (232) we have $\mathrm{Val}^+(\pi) = \mathrm{Val}(\pi)$. Applying proposition (254) we see that $\mathrm{Val}^+ \circ \mathcal{M}(\pi) \sim \mathcal{M} \circ \mathrm{Val}^+(\pi)$, where $\sim$ is the substitution congruence on $\mathbf{P}(\bar{V})$. It follows that $\mathrm{Val}^+ \circ \mathcal{M}(\pi) \sim \mathcal{M}(\phi)$. Using theorem (22) of page 293, in order to prove $\mathcal{M}(\Gamma) \vdash \mathcal{M}(\phi)$ it is therefore sufficient to show the inclusion $\mathrm{Hyp}(\mathcal{M}(\pi)) \precsim \mathcal{M}(\Gamma)$ modulo the substitution congruence. In particular, it is sufficient to prove that $\mathrm{Hyp}(\mathcal{M}(\pi)) \subseteq \mathcal{M}(\Gamma)$. Since π is a clean proof, from proposition (251) it remains to show that $\mathcal{M}(\mathrm{Hyp}(\pi)) \subseteq \mathcal{M}(\Gamma)$ which follows from $\mathrm{Hyp}(\pi) \subseteq \Gamma$ and which completes our proof. **.**

3.3.8 Minimal Transform and Valid Substitution

There are many reasons why minimal transforms are so useful. One of them is their ability to characterize α-equivalence with a simple equality $\mathcal{M}(\phi) = \mathcal{M}(\psi)$ as illustrated by theorem (14) of page 149. Another reason is the fact that $\mathcal{M}(\phi)$ is essentially a copy of ϕ as can be seen from the equivalence $\mathcal{M}(\phi) \sim i(\phi)$ of proposition (99). However, this copy $\mathcal{M}(\phi)$ is a lot more convenient to handle, which leads us to our third and most fundamental reason: the formula $\mathcal{M}(\phi)$ can be acted upon by any map $\sigma : V \to W$ without caveats on variable capture. This is the whole point of minimal transforms. It can be expressed formally by saying that the minimal extension $\bar{\sigma} : \bar{V} \to \bar{W}$ is always valid for the formula $\mathcal{M}(\phi)$, a fact which was proved in proposition (100). So why is this important? It is crucially important as we are able to consider the formula $\bar{\sigma} \circ \mathcal{M}(\phi)$ which is meaningful as the substitution avoids variable capture. This formula is essentially what we mean by '$\sigma(\phi)$', even when σ is not valid for ϕ. In fact whenever σ is valid for ϕ, from theorem (13) of page 146 we have the equality $\bar{\sigma} \circ \mathcal{M}(\phi) = \mathcal{M} \circ \sigma(\phi)$ which shows that our formula $\bar{\sigma} \circ \mathcal{M}(\phi)$ essentially coincides with what we intended to describe, namely $\sigma(\phi)$. So minimal transforms allow us to give meaning to $\sigma(\phi)$ despite the fact σ may not be capture-avoiding. Minimal transforms are the key to essential substitutions.

We are now hoping to replicate these same ideas from formulas to proofs. We have extended the notion of minimal transform to proofs and established some of its important properties, among which is the substitution equivalence $\mathrm{Val}^+ \circ \mathcal{M}(\pi) \sim \mathcal{M} \circ \mathrm{Val}^+(\pi)$ of proposition (254) which is true for clean proofs. We shall now prove that the minimal extension $\bar{\sigma} : \bar{V} \to \bar{W}$ is always valid for the minimal transform $\mathcal{M}(\pi)$, followed by the commutation property $\bar{\sigma} \circ \mathcal{M}(\pi) = \mathcal{M} \circ \sigma(\pi)$ whenever σ is valid for π. Note that these results are true without qualification on π being a clean proof. They are purely syntactic and do not rely on the semantics $\mathrm{Val}^+ : \mathbf{\Pi}(V) \to \mathbf{P}(V)$. In fact, these results are immediate replication of what was done for formulas. Their proofs are a case of 'cut-and-paste' which is somewhat embarrassing and symptomatic of poor design. We know this should not be done, in computing or mathematics alike. This is what abstraction and generalization are meant to achieve: to avoid the duplication of code. On the positive side, our duplicated approach has allowed us to offer plenty of motivational background, making the material a lot more accessible. Furthermore, when we do attempt to abstract and generalize on the next occasion, we shall have a far greater insight of what needs to be done. the following proposition is the counterpart of proposition (100) :

Proposition 256 *Let $\sigma : V \to W$ be a map. Then for all $\pi \in \mathbf{\Pi}(V)$ the minimal extension $\bar{\sigma} : \bar{V} \to \bar{W}$ is valid for the minimal transform $\mathcal{M}(\pi)$.*

Proof
We need to check the three properties of proposition (228) are met in relation to $\bar{\sigma} : \bar{V} \to \bar{W}$ and $\mathcal{M}(\pi)$ with $V_0 = \mathbf{N}$. First we show property (i): we need to show that $\mathrm{Bnd}(\mathcal{M}(\pi)) \subseteq \mathbf{N}$ which follows from proposition (253). Next we show property (ii): we need to show that $\bar{\sigma}_{|\mathbf{N}}$ is injective which is clear

from definition (39). We finally show property (iii): we need to show that $\bar{\sigma}(\mathbf{N}) \cap \bar{\sigma}(\mathrm{Var}(\mathcal{M}(\pi)) \setminus \mathbf{N}) = \emptyset$. This follows from $\bar{\sigma}(\mathbf{N}) \subseteq \mathbf{N}$ and $\bar{\sigma}(\mathrm{Var}(\mathcal{M}(\pi)) \setminus \mathbf{N}) \subseteq \bar{\sigma}(V) = \sigma(V) \subseteq W$, while $W \cap \mathbf{N} = \emptyset$. .

Our next result is theorem (23) below, showing the commutation property $\bar{\sigma} \circ \mathcal{M}(\pi) = \mathcal{M} \circ \sigma(\pi)$ whenever σ is valid for π. However before we deal with this theorem, we shall need to prove a couple of lemmas. The following is the counterpart of lemma (10) which was established for formulas:

Lemma 22 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\pi = \nabla x \pi_1$ where $\pi_1 \in \mathbf{\Pi}(V)$ and $x \in V$ such that $\sigma(x) \notin \sigma(\mathrm{Fr}(\pi))$. Then for all $n \in \mathbf{N}$ we have:*

$$\bar{\sigma} \circ [n/x] \circ \mathcal{M}(\pi_1) = [n/\sigma(x)] \circ \bar{\sigma} \circ \mathcal{M}(\pi_1)$$

where $\bar{\sigma} : \bar{V} \to \bar{W}$ is the minimal extension of $\sigma : V \to W$.

Proof
Using proposition (202), we only need to show that the mappings $\bar{\sigma} \circ [n/x]$ and $[n/\sigma(x)] \circ \bar{\sigma}$ coincide on $\mathrm{Var}(\mathcal{M}(\pi_1))$. So let $u \in \mathrm{Var}(\mathcal{M}(\pi_1)) \subseteq \bar{V}$. We want:

$$\bar{\sigma} \circ [n/x](u) = [n/\sigma(x)] \circ \bar{\sigma}(u) \tag{3.41}$$

Since $\bar{V}$ is the disjoint union of V and $\mathbf{N}$, we shall distinguish two cases: first we assume that $u \in \mathbf{N}$. From $V \cap \mathbf{N} = \emptyset$ we obtain $u \neq x$ and consequently $\bar{\sigma} \circ [n/x](u) = \bar{\sigma}(u) = u$. From $W \cap \mathbf{N} = \emptyset$ we obtain $u \neq \sigma(x)$ and consequently $[n/\sigma(x)] \circ \bar{\sigma}(u) = [n/\sigma(x)](u) = u$. So equation (3.41) is indeed satisfied. Next we assume that $u \in V$. We shall distinguish two further cases: first we assume that $u = x$. Then $\bar{\sigma} \circ [n/x](u) = \bar{\sigma}(n) = n$ and $[n/\sigma(x)] \circ \bar{\sigma}(u) = [n/\sigma(x)](\sigma(x)) = n$ and we see that equation (3.41) is again satisfied. Next we assume that $u \neq x$. Then $\bar{\sigma} \circ [n/x](u) = \bar{\sigma}(u) = \sigma(u)$, and furthermore $[n/\sigma(x)] \circ \bar{\sigma}(u) = [n/\sigma(x)](\sigma(u))$. In order to establish equation (3.41), it is therefore sufficient to prove that $\sigma(u) \neq \sigma(x)$. However, since $u \in \mathrm{Var}(\mathcal{M}(\pi_1))$ and $u \in V$, it follows from proposition (252) that $u \in \mathrm{Fr}(\pi_1)$. Having assumed that $u \neq x$ we in fact have $u \in \mathrm{Fr}(\nabla x \pi_1) = \mathrm{Fr}(\pi)$. Having assumed that $\sigma(x) \notin \sigma(\mathrm{Fr}(\pi))$ it follows that $\sigma(u) \neq \sigma(x)$ as requested. .

The following lemma is the counterpart of lemma (11):

Lemma 23 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\pi = \nabla x \pi_1$ where $\pi_1 \in \mathbf{\Pi}(V)$ and $x \in V$ such that $\sigma(x) \notin \sigma(\mathrm{Fr}(\pi))$. Then for all $k \in \mathbf{N}$ we have:*

$$[k/x] \text{ valid for } \mathcal{M}(\pi_1) \;\Leftrightarrow\; [k/\sigma(x)] \text{ valid for } \bar{\sigma} \circ \mathcal{M}(\pi_1)$$

where $\bar{\sigma} : \bar{V} \to \bar{W}$ is the minimal extension of $\sigma : V \to W$.

Proof
First we show $\Leftarrow$: So we assume that $[k/\sigma(x)]$ is valid for $\bar{\sigma} \circ \mathcal{M}(\pi_1)$. We need to show that $[k/x]$ is valid for $\mathcal{M}(\pi_1)$. However, we know from proposition (256) that $\bar{\sigma}$ is valid for $\mathcal{M}(\pi_1)$. Hence, from the validity of $[k/\sigma(x)]$ for $\bar{\sigma} \circ \mathcal{M}(\pi_1)$

and proposition (226) we see that $[k/\sigma(x)] \circ \bar{\sigma}$ is valid for $\mathcal{M}(\pi_1)$. Furthermore, having assumed $\sigma(x) \notin \sigma(\mathrm{Fr}(\pi))$, we can use lemma (22) to obtain:

$$\bar{\sigma} \circ [k/x] \circ \mathcal{M}(\pi_1) = [k/\sigma(x)] \circ \bar{\sigma} \circ \mathcal{M}(\pi_1) \tag{3.42}$$

It follows from proposition (227) that $\bar{\sigma} \circ [k/x]$ is valid for $\mathcal{M}(\pi_1)$, and in particular, using proposition (226) once more, we conclude that $[k/x]$ is valid for $\mathcal{M}(\pi_1)$ as requested. We now show $\Rightarrow$: so we assume that $[k/x]$ is valid for $\mathcal{M}(\pi_1)$. We need to show that $[k/\sigma(x)]$ is valid for $\bar{\sigma} \circ \mathcal{M}(\pi_1)$. However, from proposition (226) it is sufficient to prove that $[k/\sigma(x)] \circ \bar{\sigma}$ is valid for $\mathcal{M}(\pi_1)$. Using equation (3.42) and proposition (227) once more, we simply need to show that $\bar{\sigma} \circ [k/x]$ is valid for $\mathcal{M}(\pi_1)$. Having assumed that $[k/x]$ is valid for $\mathcal{M}(\pi_1)$, from proposition (226) it is sufficient to show that $\bar{\sigma}$ is valid for $[k/x] \circ \mathcal{M}(\pi_1)$. We shall do so with an application of proposition (228) to $V_0 = \mathbf{N}$. First we need to check that $\mathrm{Bnd}(\, [k/x] \circ \mathcal{M}(\pi_1)\,) \subseteq \mathbf{N}$. However, from proposition (215) we have $\mathrm{Bnd}(\, [k/x] \circ \mathcal{M}(\pi_1)\,) = [k/x](\, \mathrm{Bnd}(\mathcal{M}(\pi_1))\,)$ and from proposition (253) we have $\mathrm{Bnd}(\mathcal{M}(\pi_1)) \subseteq \mathbf{N}$. So the desired inclusion follows. Next we need to show that $\bar{\sigma}_{|\mathbf{N}}$ is injective which is clear from definition (39). Finally, we need to check that $\bar{\sigma}(\mathbf{N}) \cap \bar{\sigma}(\, \mathrm{Var}([k/x] \circ \mathcal{M}(\pi_1)) \setminus \mathbf{N}\,) = \emptyset$. This follows from $\bar{\sigma}(\mathbf{N}) \subseteq \mathbf{N}$ and $\bar{\sigma}(\, \mathrm{Var}([k/x] \circ \mathcal{M}(\pi_1)) \setminus \mathbf{N}\,) \subseteq \bar{\sigma}(V) = \sigma(V) \subseteq W$, while $W \cap \mathbf{N} = \emptyset$. **.**

We are now ready to prove theorem (23) which his the counterpart of theorem (13) of page 146. The equality $\bar{\sigma} \circ \mathcal{M}(\pi) = \mathcal{M} \circ \sigma(\pi)$ for σ valid for π will turn out to be very useful, just as it was for formulas. More fundamentally, this equality vindicates our belief that $\bar{\sigma} \circ \mathcal{M}(\pi)$ is *essentially* the right definition for '$\sigma(\pi)$' when σ is not valid for π, since the two coincide in the valid case.

Theorem 23 *Let V and W be sets. Let $\sigma : V \to W$ be a map. Let $\pi \in \mathbf{\Pi}(V)$. If σ is valid for π, then it commutes with minimal transforms, specifically:*

$$\bar{\sigma} \circ \mathcal{M}(\pi) = \mathcal{M} \circ \sigma(\pi) \tag{3.43}$$

where $\bar{\sigma} : \bar{V} \to \bar{W}$ is the minimal extension of $\sigma : V \to W$.

Proof
Before we start, it should be noted that σ in equation (3.43) refers to the substitution mapping $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ while the $\mathcal{M}$ on the right-hand-side refers to the minimal transform mapping $\mathcal{M} : \mathbf{\Pi}(W) \to \mathbf{\Pi}(\bar{W})$. The other $\mathcal{M}$ which appears on the left-hand-side refers to the minimal transform mapping $\mathcal{M} : \mathbf{\Pi}(V) \to \mathbf{\Pi}(\bar{V})$, and $\bar{\sigma}$ is the substitution mapping $\bar{\sigma} : \mathbf{\Pi}(\bar{V}) \to \mathbf{\Pi}(\bar{W})$. So everything makes sense. For all $\pi \in \mathbf{\Pi}(V)$, we need to show the property:

$$(\sigma \text{ valid for } \pi) \;\Rightarrow\; \bar{\sigma} \circ \mathcal{M}(\pi) = \mathcal{M} \circ \sigma(\pi)$$

We shall do so by structural induction using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. We need to show the property is true for π. So we assume that σ is valid for $\pi = \phi$. We need to show the equality $\bar{\sigma} \circ \mathcal{M}(\pi) = \mathcal{M} \circ \sigma(\pi)$ which follows immediately from theorem (13)

of page 146. Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. We need to show that the property is true for π. So we assume that σ is valid for π. Using proposition (218) this means that σ is valid for ϕ. Hence we have:

$$\begin{aligned}
\bar{\sigma} \circ \mathcal{M}(\pi) &= \bar{\sigma} \circ \mathcal{M}(\partial\phi) \\
&= \bar{\sigma}(\partial\mathcal{M}(\phi)) \\
&= \partial\bar{\sigma} \circ \mathcal{M}(\phi) \\
\text{Th. (13), } \sigma \text{ valid for } \phi \ \rightarrow \ &= \partial\mathcal{M} \circ \sigma(\phi) \\
&= \mathcal{M}(\partial\sigma(\phi)) \\
&= \mathcal{M} \circ \sigma(\partial\phi) \\
&= \mathcal{M} \circ \sigma(\pi)
\end{aligned}$$

Next we assume that $\pi = \pi_1 \oplus \pi_2$ where the property is true for $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$. We need to show the property is also true for π. So we assume that σ is valid for π. We need to show equation (3.43) holds for π. However, from proposition (219), the substitution σ is valid for both π_1 and π_2. Having assumed the property is true for π_1 and π_2, it follows that equation (3.43) holds for π_1 and π_2. Hence, we have the following equalities:

$$\begin{aligned}
\bar{\sigma} \circ \mathcal{M}(\pi) &= \bar{\sigma} \circ \mathcal{M}(\pi_1 \oplus \pi_2) \\
&= \bar{\sigma}(\, \mathcal{M}(\pi_1) \oplus \mathcal{M}(\pi_2)\,) \\
&= \bar{\sigma}(\mathcal{M}(\pi_1)) \oplus \bar{\sigma}(\mathcal{M}(\pi_2)) \\
&= \mathcal{M}(\sigma(\pi_1)) \oplus \mathcal{M}(\sigma(\pi_2)) \\
&= \mathcal{M}(\, \sigma(\pi_1) \oplus \sigma(\pi_2)\,) \\
&= \mathcal{M}(\sigma(\pi_1 \oplus \pi_2)) \\
&= \mathcal{M} \circ \sigma(\pi)
\end{aligned}$$

Finally we assume that $\pi = \nabla x \pi_1$ where $x \in V$ and the property is true for $\pi_1 \in \mathbf{\Pi}(V)$. We need to show the property is also true for π. So we assume that σ is valid for π. We need to show equation (3.43) holds for π. However, from proposition (220), the substitution σ is also valid for π_1. Having assumed the property is true for π_1, it follows that equation (3.43) holds for π_1. Hence:

$$\begin{aligned}
\bar{\sigma} \circ \mathcal{M}(\pi) &= \bar{\sigma} \circ \mathcal{M}(\nabla x \pi_1) \\
n = \min\{k : [k/x] \text{ valid for } \mathcal{M}(\pi_1)\} \ \rightarrow \ &= \bar{\sigma}(\, \nabla n \mathcal{M}(\pi_1)[n/x]\,) \\
&= \nabla\bar{\sigma}(n)\bar{\sigma}(\, \mathcal{M}(\pi_1)[n/x]\,) \\
&= \nabla n\, \bar{\sigma} \circ [n/x] \circ \mathcal{M}(\pi_1) \\
\text{A: to be proved} \ \rightarrow \ &= \nabla n\, [n/\sigma(x)] \circ \bar{\sigma} \circ \mathcal{M}(\pi_1) \\
&= \nabla n\, [n/\sigma(x)] \circ \mathcal{M} \circ \sigma(\pi_1) \\
&= \nabla n\, \mathcal{M}[\sigma(\pi_1)][n/\sigma(x)] \\
\text{B: to be proved} \ \rightarrow \ &= \nabla m\, \mathcal{M}[\sigma(\pi_1)][m/\sigma(x)]
\end{aligned}$$

$$
\begin{array}{rcl}
m = \min\{k : [k/\sigma(x)] \text{ valid for } \mathcal{M}[\sigma(\pi_1)]\} \ \rightarrow & = & \mathcal{M}(\nabla\sigma(x)\sigma(\pi_1)) \\
& = & \mathcal{M}(\sigma(\nabla x\pi_1)) \\
& = & \mathcal{M}\circ\sigma(\pi)
\end{array}
$$

So we have two more points A and B to justify. First we deal with point A. It is sufficient for us to prove the following equality:

$$\bar{\sigma}\circ[n/x]\circ\mathcal{M}(\pi_1) = [n/\sigma(x)]\circ\bar{\sigma}\circ\mathcal{M}(\pi_1)$$

Using lemma (22) it is sufficient to show that $\sigma(x) \notin \sigma(\mathrm{Fr}(\pi))$. So suppose to the contrary that $\sigma(x) \in \sigma(\mathrm{Fr}(\pi))$. Then there exists $u \in \mathrm{Fr}(\pi)$ such that $\sigma(u) = \sigma(x)$. This contradicts proposition (220) and the fact that σ is valid for π, which completes the proof of point A. So we now turn to point B. We need to prove that $n = m$, for which it is sufficient to show the equivalence:

$$[k/x] \text{ valid for } \mathcal{M}(\pi_1) \ \Leftrightarrow \ [k/\sigma(x)] \text{ valid for } \mathcal{M}[\sigma(\pi_1)]$$

This follows from lemma (23) and the fact that $\sigma(x) \notin \sigma(\mathrm{Fr}(\pi))$, together with the induction hypothesis $\bar{\sigma}\circ\mathcal{M}(\pi_1) = \mathcal{M}\circ\sigma(\pi_1)$. .

3.4 The Substitution Congruence for Proofs

3.4.1 The Substitution Congruence

It all began with our desire to carry over sequents from $\Gamma \vdash \phi$ to $\sigma(\Gamma) \vdash \sigma(\phi)$. We had no control over the axioms potentially being used in a proof underlying a sequent. Without validity, we could not say anything sensible about proofs which arise from a blind substitution of variables. We needed variable substitutions to avoid capture at all times. We knew the minimal extension $\bar{\sigma} : \bar{V} \rightarrow \bar{W}$ was always valid for the minimal transform $\mathcal{M}(\phi)$ of any formula ϕ. It was clear we needed minimal transforms to be extended from formulas to proofs. This extension has now been done. We have a minimal transform for proofs and sure enough $\bar{\sigma}$ is always valid for $\mathcal{M}(\pi)$, as can be seen from proposition (256). We also have the equality $\bar{\sigma}\circ\mathcal{M}(\pi) = \mathcal{M}\circ\sigma(\pi)$ whenever σ is valid for π, as follows from theorem (23) of page 327. In fact, a pattern has emerged: we have found ourselves shamelessly duplicating results from formulas to proofs, while providing identical arguments. There is an obvious parallel between the free algebras $\mathbf{P}(V)$ and $\mathbf{\Pi}(V)$. This should not be too surprising. After all, both are formal languages with variable binding and similar signatures. However, the realization of this close parallel between $\mathbf{P}(V)$ and $\mathbf{\Pi}(V)$ is raising a new question: how far can it go? Can we define an essential substitution $\sigma : \mathbf{\Pi}(V) \rightarrow \mathbf{\Pi}(W)$ for proofs just as we did for formulas? Can we define a substitution congruence on $\mathbf{\Pi}(V)$? In fact, this last question has never occurred to us. Of course we know the argument: 'Let x such that $p(x)\ldots$ therefore $q(x)$. QED' does not rely on what the variable x really is. There is clearly a notion of α-equivalence for proofs. But why should we care? We are interested in provability. We want

to establish sequents $\Gamma \vdash \phi$. We do not necessarily want to spend too much time investigating little niceties of congruences on $\mathbf{\Pi}(V)$. There needs to be a real purpose. So here it is: it all begins with our desire to carry over sequents from $\Gamma \vdash \phi$ to $\sigma(\Gamma) \vdash \sigma(\phi)$. It now occurs to us that essential substitutions could also be defined for proofs. This would be a powerful tool: an essential substitution $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ would allow us to generate a new proof $\sigma(\pi)$ from an older proof π, and this without variable capture. This is exactly what we need. However, we cannot speak of *essential* substitutions for proofs without formalizing the notion of what *essential* is. So we need to define a substitution congruence for proofs, which is the purpose of this section.

Now we have a choice: unlike the situation we were facing when dealing with formulas, we now have a few tools and some insight at our disposal. In particular, it is very tempting to define a substitution congruence $\equiv$ on $\mathbf{\Pi}(V)$ simply with the equality $\mathcal{M}(\pi) = \mathcal{M}(\rho)$ in light of theorem (14) of page 149. It is clear that whatever choices we make, the end result should be that α-equivalence for proofs be characterized by minimal transforms, just as it is for formulas. So one option is to start directly from there. However, we can also define a substitution congruence on $\mathbf{\Pi}(V)$ from a generator, following definition (35). We shall adopt the latter which is the safe option, simply following a trail:

Definition 89 *Let V be a set. We call substitution congruence on $\mathbf{\Pi}(V)$ the congruence on $\mathbf{\Pi}(V)$ generated by $R_0 \cup R_1 \cup R_2 \subseteq \mathbf{\Pi}(V) \times \mathbf{\Pi}(V)$ where the set R_0 and R_1 are defined by $R_0 = \{(\phi, \psi) : \phi \sim \psi\}$, $R_1 = \{(\partial\phi, \partial\psi) : \phi \sim \psi\}$ and:*

$$R_2 = \{\ (\nabla x \pi_1, \nabla y \pi_1[y{:}x]) : \pi_1 \in \mathbf{\Pi}(V)\ ,\ x, y \in V\ ,\ x \neq y\ ,\ y \notin \mathrm{Fr}(\pi_1)\ \}$$

where $\sim$ is the substitution congruence on $\mathbf{P}(V)$, and $[y{:}x]$ as per definition (27).

Let $\sim$ and $\equiv$ denote the substitution congruence on $\mathbf{P}(V)$ and $\mathbf{\Pi}(V)$ respectively. Let $\phi, \psi \in \mathbf{P}(V)$. If $\phi \sim \psi$ then the ordered pair (ϕ, ψ) is an element of R_0 and in particular $\phi \equiv \psi$. However, if $\phi \equiv \psi$ it is not obvious at this stage that $\phi \sim \psi$. The equivalence shall be proved later in proposition (270). In the meantime, we shall be very careful to avoid any possible confusion between $\phi \sim \psi$ and $\phi \equiv \psi$.

Following definition (34), we shall now introduce the notion of *admissible substitutions* for proofs. Admissible substitutions $\sigma : V \to W$ only apply to the case when $W = V$. Admissibility is a stronger notion than validity, as we also require that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\pi)$. Admissible substitutions have proved useful as a tool to establish cases of α-equivalence $\phi \sim \psi$ in the case when $\psi = \sigma(\phi)$ for some $\sigma : V \to V$. The proof simply relies on showing that σ is admissible for ϕ. We shall establish a similar criterion for proofs.

Definition 90 *Let V be a set and $\sigma : V \to V$ be a map. Let $\pi \in \mathbf{\Pi}(V)$. We say that σ is an* admissible substitution *for π if and only if it satisfies:*

$$\begin{array}{ll} (i) & \sigma \text{ valid for } \pi \\ (ii) & \forall u \in \mathrm{Fr}(\pi)\ ,\ \sigma(u) = u \end{array}$$

Given a formula $\phi \in \mathbf{P}(V)$ and a map $\sigma : V \to V$, the terminology σ is *admissible for* ϕ is potentially ambiguous. Since $\mathbf{P}(V) \subseteq \mathbf{\Pi}(V)$, it may refer to the usual notion of admissibility as per definition (34), or to the new notion of definition (89) applied to the proof $\pi = \phi$. Luckily, the two notions coincide. The following proposition is the counterpart of proposition (77). Note however that we shall not be able to provide a counterpart of proposition (78) which shows that ordered pairs $(\phi, \sigma(\phi))$ with σ admissible for ϕ form a generator of the substitution congruence on $\mathbf{P}(V)$. This is one of the rare cases we shall encounter, where the parallel between formulas and proofs is broken. However, this will be of little significance and all other expected results will hold.

Proposition 257 *Let $\equiv$ be the substitution congruence on $\mathbf{\Pi}(V)$ where V is a set. Let $\pi \in \mathbf{\Pi}(V)$ and $\sigma : V \to V$ be an admissible substitution for π. Then:*

$$\pi \equiv \sigma(\pi)$$

Proof
We need to show the property $\forall\sigma[\,(\sigma \text{ admissible for } \pi) \;\Rightarrow\; \pi \equiv \sigma(\pi)\,]$ for all $\pi \in \mathbf{\Pi}(V)$. We shall do so by structural induction, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. We need to show the property is true for ϕ. So we assume that σ is admissible for ϕ. Then from proposition (77) we obtain $\phi \sim \sigma(\phi)$, where $\sim$ denotes the substitution congruence on $\mathbf{P}(V)$. In particular, the ordered pair $(\phi, \sigma(\phi))$ is an element of the set R_0 of definition (88). It follows that $\phi \equiv \sigma(\phi)$ as requested. We now assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. We need to show the property is true for π. So we assume that σ is admissible for π. From proposition (218) it follows that σ is valid for ϕ. Since $\mathrm{Fr}(\pi) = \mathrm{Fr}(\phi)$ we see that σ is in fact admissible for ϕ. Using proposition (77) once more, we obtain $\phi \sim \sigma(\phi)$. Hence we see that the ordered pair $(\partial\phi, \partial\sigma(\phi)) = (\pi, \sigma(\pi))$ is an element of the set R_1 of definition (88). In particular we obtain $\pi \equiv \sigma(\pi)$ as requested. We now check that the property is true for $\pi = \pi_1 \oplus \pi_2$ if it is true for $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$. So we assume that $\sigma : V \to V$ is an admissible substitution for π. We need to show that $\pi \equiv \sigma(\pi)$. Since $\pi = \pi_1 \oplus \pi_2$ and $\sigma(\pi) = \sigma(\pi_1) \oplus \sigma(\pi_2)$, the substitution congruence being a congruent relation on $\mathbf{\Pi}(V)$, it is sufficient to show that $\pi_1 \equiv \sigma(\pi_1)$ and $\pi_2 \equiv \sigma(\pi_2)$. First we show that $\pi_1 \equiv \sigma(\pi_1)$. Having assumed the property is true for π_1, it is sufficient to show that σ is an admissible substitution for π_1. Since σ admissible for π, in particular it is valid for π and it follows from proposition (219) that it is also valid for π_1. So it remains to show that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\pi_1)$ which follows immediately from $\mathrm{Fr}(\pi) = \mathrm{Fr}(\pi_1) \cup \mathrm{Fr}(\pi_2)$ and the fact that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\pi)$. So we have proved that $\pi_1 \equiv \sigma(\pi_1)$ and we show similarly that $\pi_2 \equiv \sigma(\pi_2)$. We now need to check that the property is true for $\pi = \nabla x \pi_1$ if it is true for $\pi_1 \in \mathbf{\Pi}(V)$. So we assume that $\sigma : V \to V$ is an admissible substitution for π. We need to show that $\pi \equiv \sigma(\pi)$. We shall distinguish two cases: first we assume that $\sigma(x) = x$. Then $\sigma(\pi) = \nabla x\, \sigma(\pi_1)$ and in order to show $\pi \equiv \sigma(\pi)$, the substitution congruence being a congruent relation on $\mathbf{\Pi}(V)$, it is sufficient to show that $\pi_1 \equiv \sigma(\pi_1)$. Having assumed the property is true for π_1, it is therefore

sufficient to prove that σ is an admissible substitution for π_1. Since σ admissible for π, in particular it is valid for π and it follows from proposition (220) that it is also valid for π_1. So it remains to show that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\pi_1)$. We shall distinguish two further cases: first we assume that $u = x$. Then $\sigma(u) = u$ is true from our assumption $\sigma(x) = x$. So we assume that $u \neq x$. It follows that $u \in \mathrm{Fr}(\pi_1) \setminus \{x\} = \mathrm{Fr}(\pi)$, and since σ is admissible for π, we conclude that $\sigma(u) = u$. This completes our proof of $\pi \equiv \sigma(\pi)$ in the case when $\sigma(x) = x$. We now assume that $\sigma(x) \neq x$. Let $y = \sigma(x)$. Then $\sigma(\pi) = \nabla y\, \sigma(\pi_1)$ and we need to show that $\nabla x \pi_1 \equiv \nabla y\, \sigma(\pi_1)$. However, since $[y:x] \circ [y:x]$ is the identity mapping we have $\sigma = [y:x] \circ \sigma^*$ where the map $\sigma^* : V \to V$ is defined as $\sigma^* = [y:x] \circ \sigma$. It follows that $\sigma(\pi_1) = \sigma^*(\pi_1)[y:x]$ and we need to show that $\nabla x \pi_1 \equiv \nabla y\, \sigma^*(\pi_1)[y:x]$. Let us accept for now that $y \notin \mathrm{Fr}(\sigma^*(\pi_1))$. Then from definition (88) we obtain $\nabla x \sigma^*(\pi_1) \equiv \nabla y \sigma^*(\pi_1)[y:x]$, and it is therefore sufficient to prove that $\nabla x \pi_1 \equiv \nabla x \sigma^*(\pi_1)$. So we see that it is sufficient to prove $\pi_1 \equiv \sigma^*(\pi_1)$ provided we can justify the fact that $y \notin \mathrm{Fr}(\sigma^*(\pi_1))$. First we show that $\pi_1 \equiv \sigma^*(\pi_1)$. Having assumed our property is true for π_1 it is sufficient to prove that σ^* is admissible for π_1. However, we have already seen that σ is valid for π_1. Furthermore, since $[y:x]$ is an injective map, from proposition (224) it is a valid substitution for $\sigma(\pi_1)$. It follows from proposition (226) that $\sigma^* = [y:x] \circ \sigma$ is valid for π_1. So in order to prove that σ^* is admissible for π_1, it remains to show that $\sigma^*(u) = u$ for all $u \in \mathrm{Fr}(\pi_1)$. So let $u \in \mathrm{Fr}(\pi_1)$. We shall distinguish two cases: first we assume that $u = x$. Then $\sigma^*(u) = [y:x](\sigma(x)) = [y:x](y) = x = u$. Next we assume that $u \neq x$. Then u is in fact an element of $\mathrm{Fr}(\pi)$. Having assumed σ is admissible for π we obtain $\sigma(u) = u$. We also obtain the fact that σ is valid for $\pi = \nabla x \pi_1$ and consequently $\sigma(u) \neq \sigma(x)$, i.e. $u \neq y$. Thus $\sigma^*(u) = [y:x](\sigma(u)) = [y:x](u) = u$. This completes our proof that σ^* is admissible for π_1 and $\pi_1 \equiv \sigma^*(\pi_1)$. It remains to show that $y \notin \mathrm{Fr}(\sigma^*(\pi_1))$. So suppose to the contrary that $y \in \mathrm{Fr}(\sigma^*(\pi_1))$. We shall obtain a contradiction. Using proposition (209) there exists $u \in \mathrm{Fr}(\pi_1)$ such that $y = \sigma^*(u)$. Having proven that σ^* is admissible for π_1 we have $\sigma^*(u) = u$ and consequently $y = u \in \mathrm{Fr}(\pi_1)$. From the assumption $y = \sigma(x) \neq x$ we in fact have $y \in \mathrm{Fr}(\pi)$. So from the admissibility of σ for π we obtain $\sigma(y) = y$ and furthermore from the validity of σ for $\pi = \nabla x \pi_1$ we obtain $\sigma(y) \neq \sigma(x)$. So we conclude that $y \neq \sigma(x)$ which contradicts our very definition of y. **.**

3.4.2 Characterization of the Substitution Congruence

The purpose of this section is to provide a characterization of the substitution congruence on $\mathbf{\Pi}(V)$ similar to theorem (12) of page 132 for $\mathbf{P}(V)$. The result will be proved in theorem (24) below. This type of theorem is very useful as it confirms the natural belief that α-equivalence can only occur between proofs which are *structurally identical*. So if $\equiv$ and $\sim$ denote the substitution congruence on $\mathbf{\Pi}(V)$ and $\mathbf{P}(V)$ respectively, then the equivalence $\pi \equiv \rho$ can only arise when π and ρ are both elements of $\mathbf{P}(V)$ with $\pi \sim \rho$, or both 'axioms' with $\pi = \partial\phi$, $\rho = \partial\psi$ and $\phi \sim \psi$, or both of the form $\pi = \pi_1 \oplus \pi_2$, $\rho = \rho_1 \oplus \rho_2$ and $\pi_1 \equiv \rho_1$, $\pi_2 \equiv \rho_2$ etc. We start by showing that equivalent proofs have the

same free variables, which is the counterpart of proposition (79).

Proposition 258 *Let $\equiv$ denote the substitution congruence on $\mathbf{\Pi}(V)$ where V is a set. Then for all $\pi, \rho \in \mathbf{\Pi}(V)$ we have the implication:*

$$\pi \equiv \rho \;\Rightarrow\; \mathrm{Fr}(\pi) = \mathrm{Fr}(\rho)$$

Proof
Let $\simeq$ be the relation on $\mathbf{\Pi}(V)$ defined by $\pi \simeq \rho \;\Leftrightarrow\; \mathrm{Fr}(\pi) = \mathrm{Fr}(\rho)$. We need to show that $\pi \equiv \rho \;\Rightarrow\; \pi \simeq \rho$ or equivalently that the inclusion $\equiv \subseteq \simeq$ holds. Since $\equiv$ is the substitution congruence on $\mathbf{\Pi}(V)$, it is the smallest congruence on $\mathbf{\Pi}(V)$ which contains the sets R_0, R_1 and R_2 of definition (88). In order to show the inclusion $\equiv \subseteq \simeq$ it is therefore sufficient to show that $\simeq$ is a congruence on $\mathbf{\Pi}(V)$ such that $R_i \subseteq \simeq$ for $i \in 3$. However, we already know from proposition (211) that $\simeq$ is a congruence on $\mathbf{\Pi}(V)$. So it remains to show that $R_i \subseteq \simeq$ for $i \in 3$. First we show that $R_0 \subseteq \simeq$. So let $\phi, \psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$ where $\sim$ denotes the substitution congruence on $\mathbf{P}(V)$. We need to show that $\phi \simeq \psi$ i.e. that $\mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$ which follows from proposition (79). We now show that $R_1 \subseteq \simeq$. So let $\phi, \psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$. We need to show that $\partial\phi \simeq \partial\psi$ which is $\mathrm{Fr}(\partial\phi) = \mathrm{Fr}(\partial\psi)$ or equivalently $\mathrm{Fr}(\phi) = \mathrm{Fr}(\psi)$. Once again, this follows from proposition (79). So we now show that $R_2 \subseteq \simeq$. Let $\pi_1 \in \mathbf{\Pi}(V)$ and $x, y \in V$ such that $x \neq y$ and $y \notin \mathrm{Fr}(\pi_1)$. Define $\pi = \nabla x \pi_1$ and $\rho = \nabla y \pi_1[y{:}x]$. We need to show that $\pi \simeq \rho$, i.e. that $\mathrm{Fr}(\pi) = \mathrm{Fr}(\rho)$. However, from proposition (224), the map $[y{:}x]$ is valid for π_1. Hence:

$$\begin{array}{rcl}
\mathrm{Fr}(\rho) & = & \mathrm{Fr}(\,\nabla y \pi_1[y{:}x]\,) \\
 & = & \mathrm{Fr}(\pi_1[y{:}x]) \setminus \{y\} \\
\text{prop. (223)} \;\rightarrow & = & [y{:}x](\mathrm{Fr}(\pi_1)) \setminus \{y\} \\
y \notin \mathrm{Fr}(\pi_1) \;\rightarrow & = & [y{:}x](\,\mathrm{Fr}(\pi_1) \setminus \{y\}\,) \setminus \{y\} \\
[y{:}x](x) = y \;\rightarrow & = & [y{:}x](\,\mathrm{Fr}(\pi_1) \setminus \{x, y\}\,) \setminus \{y\} \\
u \notin \{x, y\} \Rightarrow [y{:}x](u) = u \;\rightarrow & = & (\mathrm{Fr}(\pi_1) \setminus \{x, y\}) \setminus \{y\} \\
 & = & \mathrm{Fr}(\pi_1) \setminus \{x, y\} \\
y \notin \mathrm{Fr}(\pi_1) \;\rightarrow & = & \mathrm{Fr}(\pi_1) \setminus \{x\} \\
 & = & \mathrm{Fr}(\nabla x \pi_1) \\
 & = & \mathrm{Fr}(\pi)
\end{array}$$

.

The following proposition is the counterpart of proposition (80):

Proposition 259 *Let $\equiv$ denote the substitution congruence on $\mathbf{\Pi}(V)$ where V is a set. Then for all $\pi_1 \in \mathbf{\Pi}(V)$ and $x, y \in V$ such that $x, y \notin \mathrm{Fr}(\pi_1)$ we have:*

$$\nabla x \pi_1 \equiv \nabla y \pi_1$$

Proof
From $y \notin \mathrm{Fr}(\pi_1)$ and definition (88) we see that $\nabla x \pi_1 \equiv \nabla y \pi_1[y:x]$. So we need to show that $\nabla y \pi_1[y:x] \equiv \forall y \pi_1$. Hence it is sufficient to prove that $\pi_1[y:x] \equiv \pi_1$. Using proposition (257), we simply need to argue that $[y:x]$ is an admissible substitution for π_1. Being injective, from proposition (224) it is a valid substitution for π_1. So it remains to show that $[y:x](u) = u$ for all $u \in \mathrm{Fr}(\pi_1)$ which follows immediately from $x, y \notin \mathrm{Fr}(\pi_1)$. .

An injective substitution preserves α-equivalence. This is of course a temporary results which will be extended from injective to valid substitutions in theorem (27) of page 350. The following is the counterpart of proposition (81):

Proposition 260 *Let V and W be sets and $\sigma : V \to W$ be an injective map. Let $\equiv$ be the substitution congruence both on $\mathbf{\Pi}(V)$ and $\mathbf{\Pi}(W)$. Then:*

$$\pi \equiv \rho \;\Rightarrow\; \sigma(\pi) \equiv \sigma(\rho)$$

for all $\pi, \rho \in \mathbf{\Pi}(V)$, where $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ is also the substitution mapping.

Proof
Let $\simeq$ be the relation on $\mathbf{\Pi}(V)$ defined by $\pi \simeq \rho \;\Leftrightarrow\; \sigma(\pi) \equiv \sigma(\rho)$. We need to show that $\pi \equiv \rho \;\Rightarrow\; \pi \simeq \rho$ or equivalently that the inclusion $\equiv \subseteq \simeq$ holds. Since $\equiv$ is the substitution congruence on $\mathbf{\Pi}(V)$, it is the smallest congruence on $\mathbf{\Pi}(V)$ which contains the sets R_0, R_1 and R_2 of definition (88). In order to show the inclusion $\equiv \subseteq \simeq$ it is therefore sufficient to show that $\simeq$ is a congruence on $\mathbf{\Pi}(V)$ such that $R_i \subseteq \simeq$ for $i \in 3$. However, we already know from proposition (190) that $\simeq$ is a congruence on $\mathbf{\Pi}(V)$. So it remains to show that $R_i \subseteq \simeq$ for $i \in 3$. First we show that $R_0 \subseteq \simeq$. So let $\phi, \psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$, where $\sim$ denotes the substitution congruence on $\mathbf{P}(V)$. We need to show that $\phi \simeq \psi$ or equivalently that $\sigma(\phi) \equiv \sigma(\psi)$. Looking at definition (88) it is sufficient to show that $\sigma(\phi) \sim \sigma(\psi)$ where $\sim$ now denotes the substitution congruence on $\mathbf{P}(W)$. However, the equivalence $\sigma(\phi) \sim \sigma(\psi)$ follows immediately from the injectivity of σ and proposition (81). We now show that $R_1 \subseteq \simeq$. So let $\phi, \psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$. We need to show that $\partial\phi \simeq \partial\psi$ or equivalently $\sigma(\partial\phi) \equiv \sigma(\partial\psi)$ which is $\partial\sigma(\phi) \equiv \partial\sigma(\psi)$. Once again from definition (88) it is sufficient to show that $\sigma(\phi) \sim \sigma(\psi)$ which follows from the injectivity of σ. We now show that $R_2 \subseteq \simeq$. So let $\pi_1 \in \mathbf{\Pi}(V)$ and $x, y \in V$ be such that $x \neq y$ and $y \notin \mathrm{Fr}(\pi_1)$. Define $\pi = \nabla x \pi_1$ and $\rho = \nabla y\, \pi_1[y:x]$. We need to show that $\pi \simeq \rho$ or equivalently that $\sigma(\pi) \equiv \sigma(\rho)$. In order to do so, it is sufficient to show that the ordered pair $(\sigma(\pi), \sigma(\rho))$ belongs to the set R_2' of the substitution congruence on $\mathbf{\Pi}(W)$ as per definition (88). In other words, it is sufficient to show the existence of $\pi_1' \in \mathbf{\Pi}(W)$ and $x', y' \in W$ with $x' \neq y'$ and $y' \notin \mathrm{Fr}(\pi_1')$, such that $\sigma(\pi) = \nabla x' \pi_1'$ and $\sigma(\rho) = \nabla y'\, \pi_1'[y':x']$. Take $\pi_1' = \sigma(\pi_1) \in \mathbf{\Pi}(W)$ together with $x' = \sigma(x) \in W$ and $y' = \sigma(y) \in W$. Then:

$$\sigma(\pi) = \sigma(\nabla x \pi_1) = \nabla \sigma(x)\, \sigma(\pi_1) = \nabla x' \pi_1'$$

Furthermore, from proposition (37) we have $\sigma \circ [y:x] = [\sigma(y):\sigma(x)] \circ \sigma$ and so:

$$\sigma(\rho) \quad = \quad \sigma(\nabla y\, \pi_1[y:x])$$

$$
\begin{aligned}
&= \nabla\sigma(y)\,\sigma(\pi_1[y:x]) \\
&= \nabla y'\,\sigma\circ[y:x]\,(\pi_1) \\
&= \nabla y'\,[\sigma(y):\sigma(x)]\circ\sigma\,(\pi_1) \\
&= \nabla y'\,[y':x'](\pi_1') \\
&= \nabla y'\,\pi_1'[y':x']
\end{aligned}
$$

So it remains to show that $x' \neq y'$ and $y' \notin \mathrm{Fr}(\pi_1')$. Since $\sigma : V \to W$ is an injective map, $x' \neq y'$ follows immediately from $x \neq y$. We now show that $y' \notin \mathrm{Fr}(\pi_1')$. So suppose to the contrary that $y' \in \mathrm{Fr}(\pi_1')$. We shall arrive at a contradiction. Since $\pi_1' = \sigma(\pi_1)$, from proposition (209) there exists $u \in \mathrm{Fr}(\pi_1)$ such that $y' = \sigma(u)$. However, $y' = \sigma(y)$ and $\sigma : V \to W$ is an injective map. Hence we see that $u = y$ and consequently $y \in \mathrm{Fr}(\pi_1)$ which contradicts our initial assumption of $y \notin \mathrm{Fr}(\pi_1)$ and completes our proof. **.**

We shall now follow a familiar strategy leading to theorem (24) of page 339. We shall first define a new relation $\simeq$ on $\mathbf{\Pi}(V)$ reflecting our best estimate of what the substitution congruence $\equiv$ should be like. We shall then show that $\simeq$ is in fact a congruence which is indeed equal to $\equiv$ as expected. Note that some of the mathematical statements of the following definition have been shortened in the interest of readability. So in the case of (iii), what is meant is 'there exist π_1, π_2 and ρ_1, ρ_2 such that $\pi = \pi_1 \oplus \pi_2$, $\rho = \rho_1 \oplus \rho_2$, $\pi_1 \equiv \rho_1$ and $\pi_2 \equiv \rho_2$' etc.

Definition 91 *Let $\equiv$ and $\sim$ be the substitution congruence on $\mathbf{\Pi}(V)$ and $\mathbf{P}(V)$ respectively where V is a set. Let $\pi, \rho \in \mathbf{\Pi}(V)$. We say that π is* almost equivalent to ρ *denoted $\pi \simeq \rho$, if and only if one of the following is the case:*

$$
\begin{aligned}
&(i) && \pi = \phi\ ,\ \rho = \psi\ ,\ \textit{for some } \phi, \psi \in \mathbf{P}(V) \textit{ and } \phi \sim \psi \\
&(ii) && \pi = \partial\phi\ ,\ \rho = \partial\psi\ ,\ \textit{for some } \phi, \psi \in \mathbf{P}(V) \textit{ and } \phi \sim \psi \\
&(iii) && \pi = \pi_1 \oplus \pi_2\ ,\ \rho = \rho_1 \oplus \rho_2\ ,\ \pi_1 \equiv \rho_1 \textit{ and } \pi_2 \equiv \rho_2 \\
&(iv) && \pi = \nabla x \pi_1\ ,\ \rho = \nabla x \rho_1 \textit{ and } \pi_1 \equiv \rho_1 \\
&(v) && \pi = \nabla x \pi_1\ ,\ \rho = \nabla y \rho_1\ ,\ x \neq y\ ,\ \rho_1 \equiv \pi_1[y:x]\ ,\ y \notin \mathrm{Fr}(\pi_1)
\end{aligned}
$$

Proposition 261 *$(i), (ii), (iii), (iv), (v)$ of* def. (90) *are mutually exclusive.*

Proof
This is an immediate consequence of theorem (2) of page 21 applied to the free universal algebra $\mathbf{\Pi}(V)$ with free generator $\mathbf{P}(V)$, where a proof $\pi \in \mathbf{\Pi}(V)$ is either an element of $\mathbf{P}(V)$, or an element of the form $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$, or the result of a modus ponens application $\pi = \pi_1 \oplus \pi_2$, or a generalization $\pi = \nabla x \pi_1$, but cannot be equal to any two of those things simultaneously. Since (v) can only occur with $x \neq y$, it also follows from theorem (2) that (v) cannot occur at the same time as (iv) which completes our proof. **.**

Proposition 262 *Let $\simeq$ be the almost equivalence relation on $\mathbf{\Pi}(V)$ where V is a set. Then $\simeq$ contains the sets R_0, R_1 and R_2 of* definition (88).

Proof
First we show that $R_0 \subseteq \simeq$. So let $\phi, \psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$. We need to show that $\phi \simeq \psi$ which is clear from (i) of definition (90). Next we show that $R_1 \subseteq \simeq$. So let $\phi, \psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$. We need to show that $\partial\phi \simeq \partial\psi$ which is clear from (ii) of definition (90). We finally show $R_3 \subseteq \simeq$. So we assume $x, y \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ are such that $x \neq y$ and $y \notin \mathrm{Fr}(\pi_1)$. Note that this cannot happen unless V has at least two elements. We define $\pi = \nabla x \pi_1$ and $\rho = \nabla y\, \pi_1[y:x]$. We need to show that $\pi \simeq \rho$. We shall do so by proving that (v) of definition (90) is the case. Define $\rho_1 = \pi_1[y:x]$. Then we have $\pi = \nabla x \pi_1$, $\rho = \nabla y \rho_1$, $x \neq y$ and $y \notin \mathrm{Fr}(\pi_1)$. So it remains to show that $\rho_1 \equiv \pi_1[y:x]$ which is immediate from the reflexivity of $\equiv$. .

Proposition 263 *The almost equivalence relation on $\mathbf{\Pi}(V)$ is reflexive.*

Proof
Let $\pi \in \mathbf{\Pi}(V)$. We need to show that $\pi \simeq \pi$. From theorem (2) of page 21 we know that π is either an element of $\mathbf{P}(V)$, or $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$ or $\pi = \pi_1 \oplus \pi_2$ or $\pi = \nabla x \pi_1$ for some $\pi_1, \pi_2 \in \mathbf{P}(V)$ and $x \in V$. In every one of these cases, it is clear that $\pi \simeq \pi$ from the reflexivity of $\equiv$ and $\sim$. .

Proposition 264 *The almost equivalence relation on $\mathbf{\Pi}(V)$ is symmetric.*

Proof
Let $\pi, \rho \in \mathbf{\Pi}(V)$ be such that $\pi \simeq \rho$. We need to show that $\rho \simeq \pi$. We shall consider the five possible cases of definition (90): it is clear that $\rho \simeq \pi$ is true in cases $(i) - (iv)$ from the symmetry of $\equiv$ and $\sim$. So we consider the last possible case of $\pi = \nabla x \pi_1$, $\rho = \nabla y \rho_1$ with $x \neq y$, $\rho_1 \equiv \pi_1[y:x]$ and $y \notin \mathrm{Fr}(\pi_1)$. We need to show that $\pi_1 \equiv \rho_1[x:y]$ and $x \notin \mathrm{Fr}(\rho_1)$. First we show that $\pi_1 \equiv \rho_1[x:y]$. Note that $[x:y]$ and $[y:x]$ are in fact the same substitutions. So we need to show that $\pi_1 \equiv \rho_1[y:x]$. Since $\rho_1 \equiv \pi_1[y:x]$ and $[y:x] : V \to V$ is injective, from proposition (260) we obtain $\rho_1[y:x] \equiv \pi_1[y:x][y:x]$. It is therefore sufficient to show that $\pi_1 = \pi_1[y:x][y:x]$ which follows from proposition (188) and the fact that $[y:x] \circ [y:x]$ is the identity mapping. We now show that $x \notin \mathrm{Fr}(\rho_1)$. From $\rho_1 \equiv \pi_1[y:x]$ and proposition (258) we obtain $\mathrm{Fr}(\rho_1) = \mathrm{Fr}(\pi_1[y:x])$. So we need to show that $x \notin \mathrm{Fr}(\pi_1[y:x])$. So suppose to the contrary that $x \in \mathrm{Fr}(\pi_1[y:x])$. From proposition (209) we have $\mathrm{Fr}(\pi_1[y:x]) \subseteq [y:x](\mathrm{Fr}(\pi_1))$ and consequently there exists $u \in \mathrm{Fr}(\pi_1)$ such that $x = [y:x](u)$. By injectivity, It follows that $u = y$ which contradicts the assumption $y \notin \mathrm{Fr}(\pi_1)$. .

As is now usual, establishing transitivity is the hardest part:

Proposition 265 *The almost equivalence relation on $\mathbf{\Pi}(V)$ is transitive.*

Proof
Let π, ρ and $\kappa \in \mathbf{\Pi}(V)$ be such that $\pi \simeq \rho$ and $\rho \simeq \kappa$. We need to show that $\pi \simeq \kappa$. We shall consider the five possible cases of definition (90) in relation to $\pi \simeq \rho$. Suppose first that $\pi = \phi$ and $\rho = \psi$ for some $\phi, \psi \in \mathbf{P}(V)$ with $\phi \sim \psi$. Then from $\rho \simeq \kappa$ we obtain that $\kappa = \chi$ for some $\chi \in \mathbf{P}(V)$ and $\psi \sim \chi$. It follows

that $\pi = \phi$, $\kappa = \chi$ with $\phi \sim \chi$. Hence we see that $\pi \simeq \kappa$ as requested. We now assume that $\pi = \partial\phi$ and $\rho = \partial\psi$ for some $\phi, \psi \in \mathbf{P}(V)$ with $\phi \sim \psi$. Then from $\rho \simeq \kappa$ we obtain that $\kappa = \partial\chi$ for some $\chi \in \mathbf{P}(V)$ and $\psi \sim \chi$. It follows that $\pi = \partial\phi$, $\kappa = \partial\chi$ with $\phi \sim \chi$. Once again we see that $\pi \simeq \kappa$ as requested. We now assume that $\pi = \pi_1 \oplus \pi_2$ and $\rho = \rho_1 \oplus \rho_2$ with $\pi_1 \equiv \rho_1$ and $\pi_2 \equiv \rho_2$. From $\rho \simeq \kappa$ we obtain $\kappa = \kappa_1 \oplus \kappa_2$ with $\rho_1 \equiv \kappa_1$ and $\rho_2 \equiv \kappa_2$. It follows that $\pi_1 \equiv \kappa_1$ and $\pi_2 \equiv \kappa_2$. Hence we see that $\pi \simeq \kappa$ as requested. We now assume that $\pi = \nabla x \pi_1$ and $\rho = \nabla x \rho_1$ with $\pi_1 \equiv \rho_1$, for some $x \in V$. From $\rho \simeq \kappa$ only the cases (iv) and (v) of definition (90) are possible. First we assume that (iv) is the case. Then $\kappa = \nabla x \kappa_1$ with $\rho_1 \equiv \kappa_1$. Hence we obtain $\pi_1 \equiv \kappa_1$ and consequently $\pi \simeq \kappa$ as requested. We now assume that (v) is the case. Then $\kappa = \nabla y \kappa_1$ for some $y \in V$ with $x \neq y$, $\kappa_1 \equiv \rho_1[y:x]$ and $y \notin \mathrm{Fr}(\rho_1)$. In order to prove $\pi \simeq \kappa$ it is sufficient to show that $\kappa_1 \equiv \pi_1[y:x]$ and $y \notin \mathrm{Fr}(\pi_1)$. First we show that $\kappa_1 \equiv \pi_1[y:x]$. It is sufficient to prove that $\pi_1[y:x] \equiv \rho_1[y:x]$ which follows from $\pi_1 \equiv \rho_1$, using proposition (260) and the fact that $[y:x] : V \to V$ is injective. We now show that $y \notin \mathrm{Fr}(\pi_1)$. From $\pi_1 \equiv \rho_1$ and proposition (258) we obtain $\mathrm{Fr}(\pi_1) = \mathrm{Fr}(\rho_1)$. Hence it is sufficient to show that $y \notin \mathrm{Fr}(\rho_1)$ which is true by assumption. It remains to consider the last possible case of definition (90). So we assume that $\pi = \nabla x \pi_1$ and $\rho = \nabla y \rho_1$ with $x \neq y$, $\rho_1 \equiv \pi_1[y:x]$ and $y \notin \mathrm{Fr}(\pi_1)$. From $\rho \simeq \kappa$ only the cases (iv) and (v) of definition (90) are possible. First we assume that (iv) is the case. Then $\kappa = \nabla y \kappa_1$ with $\rho_1 \equiv \kappa_1$. Then, we obtain $\kappa_1 \equiv \pi_1[y:x]$ and consequently $\pi \simeq \kappa$. We now assume that (v) is the case. Then $\kappa = \nabla z \kappa_1$ for some $z \in V$ with $y \neq z$, $\kappa_1 \equiv \rho_1[z:y]$ and $z \notin \mathrm{Fr}(\rho_1)$. We shall now distinguish two cases. First we assume that $x = z$. Then $\pi = \nabla x \pi_1$ and $\kappa = \nabla x \kappa_1$ and in order to show that $\pi \simeq \kappa$ it is sufficient to prove that $\pi_1 \equiv \kappa_1$. From $\kappa_1 \equiv \rho_1[z:y]$ and $z = x$ we obtain $\kappa_1 \equiv \rho_1[y:x]$ and it is therefore sufficient to prove that $\pi_1 \equiv \rho_1[y:x]$. However, we know that $\rho_1 \equiv \pi_1[y:x]$ and since $[y:x] : V \to V$ is injective, from proposition (260) we obtain $\rho_1[y:x] \equiv \pi_1[y:x][y:x] = \pi_1$. This completes our proof in the case when $x = z$. We now assume that $x \neq z$. So we have $x \neq y$, $y \neq z$ and $x \neq z$, with $\pi = \nabla x \pi_1$, $\rho = \nabla y \rho_1$ and $\kappa = \nabla z \kappa_1$. Furthermore, $\rho_1 \equiv \pi_1[y:x]$ and $\kappa_1 \equiv \rho_1[z:y]$ while we have $y \notin \mathrm{Fr}(\pi_1)$ and $z \notin \mathrm{Fr}(\rho_1)$, and we need to show that $\pi \simeq \kappa$. So we need to prove that $\kappa_1 \equiv \pi_1[z:x]$ and $z \notin \mathrm{Fr}(\pi_1)$. First we show that $z \notin \mathrm{Fr}(\pi_1)$. So suppose to the contrary that $z \in \mathrm{Fr}(\pi_1)$. We shall derive a contradiction. Since $[y:x]$ is injective it is valid for π_1 and from proposition (223) we have $\mathrm{Fr}(\pi_1[y:x]) = [y:x](\mathrm{Fr}(\pi_1))$. It follows that $z = [y:x](z)$ is also an element of $\mathrm{Fr}(\pi_1[y:x])$. However we have $\rho_1 \equiv \pi_1[y:x]$ and consequently from proposition (258) we obtain $\mathrm{Fr}(\rho_1) = \mathrm{Fr}(\pi_1[y:x])$. Hence we see that $z \in \mathrm{Fr}(\rho_1)$ which is our desired contradiction. We shall now prove that $\kappa_1 \equiv \pi_1[z:x]$. Since $\kappa_1 \equiv \rho_1[z:y]$, it is sufficient to show that $\rho_1[z:y] \equiv \pi_1[z:x]$. However we know that $\rho_1 \equiv \pi_1[y:x]$ and since $[z:y] : V \to V$ is injective, from proposition (260) we obtain $\rho_1[z:y] \equiv \pi_1[y:x][z:y]$. It is therefore sufficient to show that $\pi_1[y:x][z:y] \equiv \pi_1[z:x]$. Let us accept for now:

$$[z:x] = [y:x] \circ [z:y] \circ [y:x] \tag{3.44}$$

Then we simply need to show that $\pi_1[y:x][z:y] \equiv \pi_1[y:x][z:y][y:x]$. Using

proposition (257), it is therefore sufficient to prove that $[y:x]$ is an admissible substitution for $\pi_1[y:x][z:y]$. Since $[y:x] : V \to V$ is injective, from proposition (224) it is valid for $\pi_1[y:x][z:y]$. So it remains to show that $[y:x](u) = u$ for all $u \in \mathrm{Fr}(\pi_1[y:x][z:y])$. It is therefore sufficient to prove that neither x nor y are elements of $\mathrm{Fr}(\pi_1[y:x][z:y])$. However, from proposition (209) we have $\mathrm{Fr}(\pi_1[y:x][z:y]) \subseteq [z:y] \circ [y:x](\mathrm{Fr}(\pi_1))$. So it is sufficient to show that x and y do not belong to $[z:y] \circ [y:x](\mathrm{Fr}(\pi_1))$. First we do this for x. Suppose $x = [z:y] \circ [y:x](u)$ for some $u \in \mathrm{Fr}(\pi_1)$. By injectivity we must have $u = y$, contradicting the assumption $y \notin \mathrm{Fr}(\pi_1)$. We now deal with y. So suppose $y = [z:y] \circ [y:x](u)$ for some $u \in \mathrm{Fr}(\pi_1)$. By injectivity we must have $u = z$, contradicting the fact that $z \notin \mathrm{Fr}(\pi_1)$ which we have already proven. It remains to prove that equation (3.44) holds. So let $u \in V$. We need:

$$[z:x](u) = [y:x] \circ [z:y] \circ [y:x](u)$$

This is the case when $u \notin \{x, y, z\}$. The cases $u = x$, $u = y$ and $u = z$ are easy. .

The almost equivalence is stronger than the substitution congruence:

Proposition 266 *Let $\simeq$ be the almost equivalence and $\equiv$ be the substitution congruence on $\mathbf{\Pi}(V)$, where V is a set. Then for all $\pi, \rho \in \mathbf{\Pi}(V)$ we have:*

$$\pi \simeq \rho \;\Rightarrow\; \pi \equiv \rho$$

Proof
Let $\pi, \rho \in \mathbf{\Pi}(V)$ such that $\pi \simeq \rho$. We need to show that $\pi \equiv \rho$. We shall consider the five possible cases of definition (90) in relation to $\pi \simeq \rho$. Suppose first that $\pi = \phi$ and $\rho = \psi$ for some $\phi, \psi \in \mathbf{P}(V)$ with $\phi \sim \psi$. Then the ordered pair (π, ρ) belongs to the set R_0 of definition (88) and in particular $\pi \equiv \rho$. Suppose next that $\pi = \partial\phi$ and $\rho = \partial\psi$ for some $\phi, \psi \in \mathbf{P}(V)$ with $\phi \sim \psi$. Then the ordered pair (π, ρ) belongs to the set R_1 of definition (88) and in particular $\pi \equiv \rho$. We now assume that $\pi = \pi_1 \oplus \pi_2$ and $\rho = \rho_1 \oplus \rho_2$ where $\pi_1 \equiv \rho_1$ and $\pi_2 \equiv \rho_2$. The substitution congruence being a congruent relation on $\mathbf{\Pi}(V)$, we obtain $\pi \equiv \rho$. Next we assume that $\pi = \nabla x \pi_1$ and $\rho = \nabla x \rho_1$ where $\pi_1 \equiv \rho_1$ and $x \in V$. Again, the substitution congruence being a congruent relation we obtain $\pi \equiv \rho$. Finally we assume that $\pi = \nabla x \pi_1$ and $\rho = \nabla y \rho_1$ where $x \neq y$, $\rho_1 \equiv \pi_1[y:x]$ and $y \notin \mathrm{Fr}(\pi_1)$. For the last time, the substitution congruence being a congruent relation we obtain $\rho \equiv \nabla y\, \pi_1[y:x]$. Hence in order to show $\pi \equiv \rho$ it is sufficient to show that $\nabla x \pi_1 \equiv \nabla y\, \pi_1[y:x]$ which follows immediately from $x \neq y$, $y \notin \mathrm{Fr}(\pi_1)$ and the definition of R_2 of definition (88). .

Proposition 267 *The almost equivalence relation on $\mathbf{\Pi}(V)$ is congruent.*

Proof
From proposition (263), the almost equivalence $\simeq$ is reflexive and so $\partial\phi \simeq \partial\phi$ for all $\phi \in \mathbf{P}(V)$. We now assume that $\pi = \pi_1 \oplus \pi_2$ and $\rho = \rho_1 \oplus \rho_2$ where $\pi_1 \simeq \rho_1$ and $\pi_2 \simeq \rho_2$. We need to show that $\pi \simeq \rho$. However from proposition (266) we

obtain $\pi_1 \equiv \rho_1$ and $\pi_2 \equiv \rho_2$ and it follows from definition (90) that $\pi \simeq \rho$. We now assume that $\pi = \nabla x \pi_1$ and $\rho = \nabla x \rho_1$ where $\pi_1 \simeq \rho_1$ and $x \in V$. We need to show that $\pi \simeq \rho$. Once again from proposition (266) we have $\pi_1 \equiv \rho_1$ and consequently from definition (90) we obtain $\pi \simeq \rho$ as requested. .

Proposition 268 *The almost equivalence relation on $\mathbf{\Pi}(V)$ is a congruence.*

Proof
We need to show that $\simeq$ is reflexive, symmetric, transitive and that it is a congruent relation on $\mathbf{\Pi}(V)$. From proposition (263), the relation $\simeq$ is reflexive. From proposition (264) it is symmetric while from proposition (265) it is transitive. Finally from proposition (267) the relation $\simeq$ is a congruent relation. .

Proposition 269 *Let $\simeq$ be the almost equivalence and $\equiv$ be the substitution congruence on $\mathbf{\Pi}(V)$, where V is a set. For all $\pi, \rho \in \mathbf{\Pi}(V)$ we have:*

$$\pi \simeq \rho \;\Leftrightarrow\; \pi \equiv \rho$$

Proof
From proposition (266) it is sufficient to show the implication $\Leftarrow$ or equivalently the inclusion $\equiv \subseteq \simeq$. Since $\equiv$ is the substitution congruence on $\mathbf{\Pi}(V)$, it is the smallest congruence on $\mathbf{\Pi}(V)$ which contains the sets R_0, R_1 and R_2 of definition (88). In order to show the inclusion $\equiv \subseteq \simeq$ it is therefore sufficient to show that $\simeq$ is a congruence on $\mathbf{\Pi}(V)$ such that $R_i \subseteq \simeq$ for $i \in 3$. The fact that it is a congruence stems from proposition (268). The fact that $R_i \subseteq \simeq$ for $i \in 3$ follows from proposition (262), which completes our proof. .

The almost equivalence $\simeq$ can now be forgotten. We obtain:

Theorem 24 *Let $\equiv$ be the substitution congruence on $\mathbf{\Pi}(V)$ where V is a set. For all $\pi, \rho \in \mathbf{\Pi}(V)$, $\pi \equiv \rho$ if and only if one of the following is the case:*

$$\begin{array}{ll}
(i) & \pi = \phi \ ,\ \rho = \psi \ ,\ \textit{for some } \phi, \psi \in \mathbf{P}(V) \textit{ and } \phi \sim \psi \\
(ii) & \pi = \partial\phi \ ,\ \rho = \partial\psi \ ,\ \textit{for some } \phi, \psi \in \mathbf{P}(V) \textit{ and } \phi \sim \psi \\
(iii) & \pi = \pi_1 \oplus \pi_2 \ ,\ \rho = \rho_1 \oplus \rho_2 \ ,\ \pi_1 \equiv \rho_1 \textit{ and } \pi_2 \equiv \rho_2 \\
(iv) & \pi = \nabla x \pi_1 \ ,\ \rho = \nabla x \rho_1 \textit{ and } \pi_1 \equiv \rho_1 \\
(v) & \pi = \nabla x \pi_1 \ ,\ \rho = \nabla y \rho_1 \ ,\ x \neq y \ ,\ \rho_1 \equiv \pi_1[y:x] \ ,\ y \notin \mathrm{Fr}(\pi_1)
\end{array}$$

where $\sim$ denotes the substitution congruence on $\mathbf{P}(V)$.

Proof
Immediately follows from proposition (269) and definition (90). .

We can now prove what we claimed at the beginning of this section: if $\sim$ and $\equiv$ denote the substitution congruence on $\mathbf{P}(V)$ and $\mathbf{\Pi}(V)$ respectively, then $\phi \sim \psi$ is equivalent to $\phi \equiv \psi$. It will no longer be necessary for us to use two different notations for the substitution congruence, and we shall stick to the familiar $\sim$ going forward. When confronted with the equivalence $\phi \sim \psi$, we do not need to worry as to whether ϕ, ψ are regarded as formulas or proofs.

Proposition 270 *Let V be a set and $\pi = \phi$, $\rho = \psi$ for some $\phi, \psi \in \mathbf{P}(V)$:*

$$\pi \equiv \rho \;\Leftrightarrow\; \phi \sim \psi$$

where $\equiv$ and $\sim$ are the substitution congruence on $\mathbf{\Pi}(V)$ and $\mathbf{P}(V)$ respectively.

Proof
First we show $\Leftarrow$: So we assume that $\phi \sim \psi$. Then the ordered pair (π, ρ) is an element of the set R_0 of definition (88). In particular we have $\pi \equiv \rho$. We now prove $\Rightarrow$: so we assume that $\pi \equiv \rho$. Using theorem (24), the only possibility with $\pi, \rho \in \mathbf{P}(V)$ is (i), in which case $\phi \sim \psi$ as requested. **.**

Given $\phi, \psi \in \mathbf{P}(V)$, we already knew from definition (88) that $\partial\phi \equiv \partial\psi$ whenever $\phi \sim \psi$. However, the converse was not obvious until now:

Proposition 271 *Let V be a set and $\pi = \partial\phi$, $\rho = \partial\psi$ for some $\phi, \psi \in \mathbf{P}(V)$:*

$$\pi \equiv \rho \;\Leftrightarrow\; \phi \sim \psi$$

where $\equiv$ and $\sim$ are the substitution congruence on $\mathbf{\Pi}(V)$ and $\mathbf{P}(V)$ respectively.

Proof
First we show $\Leftarrow$: So we assume that $\phi \sim \psi$. Then the ordered pair (π, ρ) is an element of the set R_1 of definition (88). In particular we have $\pi \equiv \rho$. We now prove $\Rightarrow$: so we assume that $\pi \equiv \rho$. Using theorem (24), the only possibility with $\pi = \partial\phi$ and $\rho = \partial\psi$ is (ii), in which case $\phi \sim \psi$ as requested. **.**

3.4.3 Local Inversion of Substitution for Proofs

A substitution congruence for proofs will never be acceptable to us unless it has the same connection to the minimal transform which it has for formulas. So we need to prove the implication $\mathcal{M}(\pi) = \mathcal{M}(\rho) \;\Rightarrow\; \pi \sim \rho$. At some point we shall be faced with an equality $\mathcal{M}(\pi_1)[n/x] = \mathcal{M}(\rho_1)[n/x]$ from which we shall want to argue that $\mathcal{M}(\pi_1) = \mathcal{M}(\rho_1)$. So we shall need to have a local inversion theorem for proofs just as we have theorem (10) of page 105 for formulas. So the purpose of this section is to establish theorem (25) of page 345 below. A local inversion theorem allows us to derive $\pi = \rho$ from an equality $\sigma(\pi) = \sigma(\rho)$ in certain conditions, especially in cases when the proof substitution $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ associated with $\sigma : V \to W$ may not be an injective map. We are pretty sure we could find ways to achieve our purpose without a local inversion theorem. But the result is interesting in its own right. So rather than redesigning old proofs based on the equivalence $\mathcal{M}(\phi) \sim i(\phi)$ where $i : V \to \bar{V}$ is the inclusion mapping, we have decided to keep a local inversion theorem for proofs in our list of objectives. The material that follows is relatively technical and dry. It is simply an extension of the work previously done for formulas. A lot of motivational background can be found in the discussions preceding lemma (9). We start with the notion of *dual substitution* $\tau : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ associated with an ordered pair (τ_0, τ_1) of maps

$\tau_0, \tau_1 : V \to W$. The underlying idea is that the proof $\tau(\pi)$ should correspond to the proof π, where all free variables have been substituted in accordance to the map τ_0 and bound variables in accordance to the map τ_1. The main issue here is that $\tau(\pi)$ cannot be defined directly with a simple recursion. A recursive formula would not be able to tell whether a variable will remain free in the final proof being considered. So the proof $\tau(\pi)$ needs to be defined in two stages. We start by defining a map $\tau^\circ : \mathbf{\Pi}(V) \to [\mathcal{P}(V) \to \mathbf{\Pi}(W)]$ so that $\tau^\circ(\pi)$ rather than being a proof, is a map $\tau^\circ(\pi) : \mathcal{P}(V) \to \mathbf{\Pi}(W)$. If $U \subseteq V$ is a set of variables, then $\tau^\circ(\pi)(U)$ is the proof obtained from π, τ_0 and τ_1 assuming all variables in U are free, except those being bound by the recursive formula. We then define $\tau(\pi)$ as $\tau(\pi) = \tau^\circ(\pi)(V)$. More explanations can be found in the discussion preceding definition (31). The following definition is in fact the counterpart of definition (31) which defines a map $\tau^* : \mathbf{P}(V) \to [\mathcal{P}(V) \to \mathbf{P}(W)]$ for formulas which corresponds to our $\tau^\circ : \mathbf{\Pi}(V) \to [\mathcal{P}(V) \to \mathbf{\Pi}(W)]$ for proofs. The key point of note in definition (91) below is that $\tau^\circ(\pi)(U)$ is defined in terms of $\tau^\circ(\pi_1)(U \setminus \{x\})$ whenever π is of the form $\pi = \nabla x \pi_1$. Loosely speaking, the recursive formula has now become aware that x is no longer a free variable.

Definition 92 *Let V, W be sets and $\tau_0, \tau_1 : V \to W$ be maps. We call* dual variable substitution *associated with (τ_0, τ_1) the map $\tau : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ defined by $\tau(\pi) = \tau^\circ(\pi)(V)$, where the map $\tau^\circ : \mathbf{\Pi}(V) \to [\mathcal{P}(V) \to \mathbf{\Pi}(W)]$ is defined by the following structural recursion, given $\pi \in \mathbf{\Pi}(V)$ and $U \in \mathcal{P}(V)$:*

$$\tau^\circ(\pi)(U) = \begin{cases} \tau^*(\phi)(U) & \text{if} \quad \pi = \phi \in \mathbf{P}(V) \\ \partial\tau^*(\phi)(U) & \text{if} \quad \pi = \partial\phi \\ \tau^\circ(\pi_1)(U) \oplus \tau^\circ(\pi_2)(U) & \text{if} \quad \pi = \pi_1 \oplus \pi_2 \\ \nabla\tau_1(x)\tau^\circ(\pi_1)(U \setminus \{x\}) & \text{if} \quad \pi = \nabla x \pi_1 \end{cases} \tag{3.45}$$

where the map $\tau^* : \mathbf{P}(V) \to [\mathcal{P}(V) \to \mathbf{P}(W)]$ is as per definition (31)

Proposition 272 *The structural recursion of* definition (91) *is legitimate.*

Proof
We need to prove the existence and uniqueness of $\tau^\circ : \mathbf{\Pi}(V) \to [\mathcal{P}(V) \to \mathbf{\Pi}(W)]$ satisfying equation (3.45). We shall do so using theorem (4) of page 42. So we take $X = \mathbf{\Pi}(V)$, $X_0 = \mathbf{P}(V)$ and $A = [\mathcal{P}(V) \to \mathbf{\Pi}(W)]$. We consider the map $g_0 : X_0 \to A$ defined by $g_0(\phi)(U) = \tau^*(\phi)(U)$ where it is understood that $\tau^* : \mathbf{P}(V) \to [\mathcal{P}(V) \to \mathbf{P}(W)]$ is as per definition (31). Given $\phi \in \mathbf{P}(V)$ we define $h(\partial\phi) : A^0 \to A$ by setting $h(\partial\phi)(0)(U) = \partial\tau^*(\phi)(U)$ and $h(\oplus) : A^2 \to A$ by setting $h(\oplus)(v)(U) = v(0)(U) \oplus v(1)(U)$. Finally, we define $h(\nabla x) : A^1 \to A$:

$$h(\nabla x)(v)(U) = \nabla\tau_1(x)v(0)(U \setminus \{x\})$$

From theorem (4) there exists a unique map $\tau^\circ : X \to A$ with $\tau^\circ(\pi) = g_0(\pi)$ whenever $\pi \in \mathbf{P}(V)$ and $\tau^\circ(f(\pi)) = h(f)(\tau^\circ(\pi))$ for all $f = \partial\phi, \oplus, \nabla x$ and $\pi \in X^{\alpha(f)}$. So let us check that this works: from $\tau^\circ(\pi) = g_0(\pi)$ whenever $\pi = \phi$

for some $\phi \in \mathbf{P}(V)$ we obtain $\tau^\circ(\pi)(U) = g_0(\phi)(U) = \tau^*(\phi)(U)$ which is the first line of equation (3.45). Take $f = \partial\phi$ for some $\phi \in \mathbf{P}(V)$ and $\pi = \partial\phi$:

$$\begin{aligned}
\tau^\circ(\pi)(U) &= \tau^\circ(\partial\phi)(U) \\
\text{proper notation } \rightarrow &= \tau^\circ(\partial\phi(0))(U) \\
&= \tau^\circ(f(0))(U) \\
\tau^\circ : X^0 \rightarrow A^0 \ \rightarrow &= h(f)(\tau^\circ(0))(U) \\
&= h(f)(0)(U) \\
&= h(\partial\phi)(0)(U) \\
&= \partial\tau^*(\phi)(U)
\end{aligned}$$

which is the second line of equation (3.45). Recall that the τ° which appears in the fourth equality refers to the unique mapping $\tau^\circ : X^0 \rightarrow A^0$. We now take $f = \oplus$ and $\pi = \pi_1 \oplus \pi_2$ for some $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$. Then we have:

$$\begin{aligned}
\tau^\circ(\pi)(U) &= \tau^\circ(\pi_1 \oplus \pi_2)(U) \\
\pi^*(0) = \pi_1,\ \pi^*(1) = \pi_2 \ \rightarrow &= \tau^\circ(f(\pi^*))(U) \\
\tau^\circ : X^2 \rightarrow A^2 \ \rightarrow &= h(f)(\tau^\circ(\pi^*))(U) \\
&= h(\oplus)(\tau^\circ(\pi^*))(U) \\
&= \tau^\circ(\pi^*)(0)(U) \oplus \tau^\circ(\pi^*)(1)(U) \\
&= \tau^\circ(\pi^*(0))(U) \oplus \tau^\circ(\pi^*(1))(U) \\
&= \tau^\circ(\pi_1)(U) \oplus \tau^\circ(\pi_2)(U)
\end{aligned}$$

This is the third line of equation (3.45). Finally consider $f = \nabla x$ and $\pi = \nabla x \pi_1$:

$$\begin{aligned}
\tau^\circ(\pi)(U) &= \tau^\circ(\nabla x \pi_1)(U) \\
\pi^*(0) = \pi_1 \ \rightarrow &= \tau^\circ(f(\pi^*))(U) \\
\tau^\circ : X^1 \rightarrow A^1 \ \rightarrow &= h(f)(\tau^\circ(\pi^*))(U) \\
&= h(\nabla x)(\tau^\circ(\pi^*))(U) \\
&= \nabla\tau_1(x)\tau^\circ(\pi^*)(0)(U \setminus \{x\}) \\
&= \nabla\tau_1(x)\tau^\circ(\pi^*(0))(U \setminus \{x\}) \\
&= \nabla\tau_1(x)\tau^\circ(\pi_1)(U \setminus \{x\})
\end{aligned}$$

and this is the last line of equation (3.45). .

The following lemma is the counterpart of lemma (9) prior to which some motivational discussion may be found. It is the main lemma of this section allowing us to prove the local inversion theorem (25) below. The purpose of the theorem is to derive $\pi = \rho$ from the equality $\sigma(\pi) = \sigma(\rho)$ in cases when σ behaves nicely enough on π and ρ. Specifically, we require that σ be an injective map when acting on the free variables of π and ρ, and also when acting on the

bound variables of π and ρ. We also require that σ be valid for π and ρ so that no confusion arises between the free and bound variables. The strategy to obtain the equality $\pi = \rho$ is simply to construct a *local inverse* of σ, namely a map $\tau : \mathbf{\Pi}(W) \to \mathbf{\Pi}(V)$ for which the equality $\tau \circ \sigma(\pi) = \pi$ holds in some *neighborhood* Π of π and ρ. The map $\tau : \mathbf{\Pi}(W) \to \mathbf{\Pi}(V)$ is defined as a *dual substitution* as per definition (91) associated with a pair (τ_0, τ_1) which are left-inverses of σ when restricted to the free and bound variables respectively. The main difficulty is to check the whole construction works, namely that the equality $\tau \circ \sigma(\pi) = \pi$ holds. The argument needs to be done by structural induction which is the purpose of this lemma leading to equation (3.46) below. The lemma is carefully designed so that the induction hypothesis carries through nicely at every step of the structural induction argument, as it should.

Lemma 24 *Let V, W be sets and $\sigma : V \to W$ be a map. Let V_0, V_1 be subsets of V and $\tau_0, \tau_1 : W \to V$ be maps such that for all $x \in V$:*

$$\begin{array}{ll} (i) & x \in V_0 \;\Rightarrow\; \tau_0 \circ \sigma(x) = x \\ (ii) & x \in V_1 \;\Rightarrow\; \tau_1 \circ \sigma(x) = x \end{array}$$

Let $\tau^\circ : \mathbf{\Pi}(W) \to [\mathcal{P}(W) \to \mathbf{\Pi}(V)]$ be the map associated with (τ_0, τ_1) as per definition (91). *Then for all $U \in \mathcal{P}(V)$ and $\pi \in \mathbf{\Pi}(V)$ we have:*

$$\tau^\circ(\sigma(\pi))(W \setminus \sigma(U)) = \pi \tag{3.46}$$

provided U and π satisfy the following properties:

$$\begin{array}{ll} (iii) & (\,\mathrm{Fr}(\pi) \setminus U \subseteq V_0\,) \wedge (\,\mathrm{Bnd}(\pi) \cup U \subseteq V_1\,) \\ (iv) & (\,\sigma \text{ valid for } \pi\,) \wedge (\,\sigma(U) \cap \sigma(\mathrm{Fr}(\pi) \setminus U) = \emptyset\,) \end{array}$$

Proof
We assume $\sigma : V \to W$ is given together with the subsets V_0, V_1 and the maps $\tau_0, \tau_1 : W \to V$ satisfying (i) and (ii). Let $\tau^\circ : \mathbf{\Pi}(W) \to [\mathcal{P}(W) \to \mathbf{\Pi}(V)]$ be the map associated with the ordered pair (τ_0, τ_1) as per definition (91) of page 341. Given $U \subseteq V$ and $\pi \in \mathbf{\Pi}(V)$ consider the property $q(U, \pi)$ defined by (iii) and (iv). Then we need to show that for all $\pi \in \mathbf{\Pi}(V)$ we have:

$$\forall U \subseteq V\ ,\ [\,q(U,\pi) \;\Rightarrow\; \tau^\circ(\sigma(\pi))(W \setminus \sigma(U)) = \pi\,]$$

We shall do so by a structural induction argument, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Let $U \subseteq V$ and suppose $q(U, \pi)$ is true. We need to show that equation (3.46) holds. We have:

$$\begin{array}{rcl} \tau^\circ(\sigma(\pi))(W \setminus \sigma(U)) & = & \tau^\circ(\sigma(\phi))(W \setminus \sigma(U)) \\ \text{def. (91)} \;\rightarrow & = & \tau^*(\sigma(\phi))(W \setminus \sigma(U)) \\ \text{lemma (9)} \;\rightarrow & = & \phi \\ & = & \pi \end{array}$$

Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then we have:

$$\begin{aligned}
\tau^\circ(\sigma(\pi))(W \setminus \sigma(U)) &= \tau^\circ(\sigma(\partial\phi))(W \setminus \sigma(U)) \\
&= \tau^\circ(\partial\sigma(\phi))(W \setminus \sigma(U)) \\
\text{def. (91)} \ \rightarrow \ &= \partial\tau^*(\sigma(\phi))(W \setminus \sigma(U)) \\
\text{A: to be proved} \ \rightarrow \ &= \partial\phi \\
&= \pi
\end{aligned}$$

It remains to justify point A for which we need to show $\tau^*(\sigma(\phi))(W \setminus \sigma(U)) = \phi$. This follows once again from an application of lemma (9), provided we can check the assumptions of the lemma are indeed satisfied whenever $q(U, \partial\phi)$ is itself satisfied. This follows from $\mathrm{Fr}(\partial\phi) = \mathrm{Fr}(\phi)$, $\mathrm{Bnd}(\partial\phi) = \mathrm{Bnd}(\phi)$ and the fact that the validity of σ for $\partial\phi$ is equivalent to the validity of σ for ϕ, as proven from proposition (218). So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ satisfy our desired property. We need to show the same is true of π. So let $U \subseteq V$ and suppose $q(U, \pi)$ is true. We need to show that equation (3.46) holds:

$$\begin{aligned}
\tau^\circ(\sigma(\pi))(W \setminus \sigma(U)) &= \tau^\circ(\sigma(\pi_1 \oplus \pi_2))(W \setminus \sigma(U)) \\
\text{define } U^* = W \setminus \sigma(U) \ \rightarrow \ &= \tau^\circ(\sigma(\pi_1 \oplus \pi_2))(U^*) \\
&= \tau^\circ(\, \sigma(\pi_1) \oplus \sigma(\pi_2)\,)(U^*) \\
\text{definition (91)} \ \rightarrow \ &= \tau^\circ(\sigma(\pi_1))(U^*) \oplus \tau^\circ(\sigma(\pi_2))(U^*) \\
\text{A: to be proved} \ \rightarrow \ &= \pi_1 \oplus \pi_2 \\
&= \pi
\end{aligned}$$

So it remains to show that equation (3.46) holds for π_1 and π_2. However, from our induction hypothesis, our property is true for π_1 and π_2. Hence, it is sufficient to prove that $q(U, \pi_1)$ and $q(U, \pi_2)$ are true. First we show that $q(U, \pi_1)$ is true. We need to prove that (iii) and (iv) above are true for π_1 :

$$\mathrm{Fr}(\pi_1) \setminus U \subseteq \mathrm{Fr}(\pi) \setminus U \subseteq V_0$$

where the second inclusion follows from our assumption of $q(U, \pi)$. Furthermore:

$$\mathrm{Bnd}(\pi_1) \cup U \subseteq \mathrm{Bnd}(\pi) \cup U \subseteq V_1$$

So (iii) is now established for π_1. Also from $q(U, \pi)$ we obtain:

$$\sigma(U) \cap \sigma(\mathrm{Fr}(\pi_1) \setminus U) \subseteq \sigma(U) \cap \sigma(\mathrm{Fr}(\pi) \setminus U) = \emptyset$$

So it remains to show that σ is valid for π_1, which follows immediately from proposition (219) and the validity of σ for $\pi = \pi_1 \oplus \pi_2$. This completes our proof of $q(U, \pi_1)$. The proof of $q(U, \pi_2)$ being identical, we are now done with the case $\pi = \pi_1 \oplus \pi_2$. So we now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ satisfy our induction hypothesis. We need to show the same is true for π. So let $U \subseteq V$ and suppose $q(U, \pi)$ is true. We need to show equation (3.46) :

$$\tau^\circ(\sigma(\pi))(W \setminus \sigma(U)) = \tau^\circ(\sigma(\nabla x \pi_1))(W \setminus \sigma(U))$$

$$\begin{aligned}
\text{define } U^* = W \setminus \sigma(U) \;\to\; &= \tau^\circ(\sigma(\nabla x \pi_1))(U^*) \\
&= \tau^\circ(\,\nabla\sigma(x)\sigma(\pi_1)\,)(U^*) \\
\text{definition (91)} \;\to\; &= \nabla\tau_1 \circ \sigma(x)\,\tau^\circ(\sigma(\pi_1))(\,U^* \setminus \{\sigma(x)\}\,) \\
(ii) \text{ and } x \in \mathrm{Bnd}(\pi) \subseteq V_1 \;\to\; &= \nabla x\,\tau^\circ(\sigma(\pi_1))(\,U^* \setminus \{\sigma(x)\}\,) \\
\text{define } U_1^* = U^* \setminus \{\sigma(x)\} \;\to\; &= \nabla x\,\tau^\circ(\sigma(\pi_1))(U_1^*) \\
\text{A: to be proved} \;\to\; &= \nabla x \pi_1 \\
&= \pi
\end{aligned}$$

So it remains to show that $\tau^\circ(\sigma(\pi_1))(U_1^*) = \pi_1$. From $U^* = W \setminus \sigma(U)$ and $U_1^* = U^* \setminus \{\sigma(x)\}$ we obtain $U_1^* = W \setminus \sigma(U_1)$ where $U_1 = U \cup \{x\}$. So it remains to show that $\tau^\circ(\sigma(\pi_1))(W \setminus \sigma(U_1)) = \pi_1$, or equivalently that equation (3.46) holds for U_1 and π_1. Having assumed π_1 satisfies our induction hypothesis, it is therefore sufficient to prove that $q(U_1, \pi_1)$ is true. So we need to show that (iii) and (iv) above are true for U_1 and π_1, which goes as follows:

$$\begin{aligned}
\mathrm{Fr}(\pi_1) \setminus U_1 &= \mathrm{Fr}(\pi_1) \setminus \{x\} \setminus U \\
&= \mathrm{Fr}(\pi) \setminus U \\
q(U,\pi) \;\to\; &\subseteq V_0
\end{aligned}$$

Furthermore:

$$\begin{aligned}
\mathrm{Bnd}(\pi_1) \cup U_1 &= \mathrm{Bnd}(\pi_1) \cup \{x\} \cup U \\
&= \mathrm{Bnd}(\pi) \cup U \\
q(U,\pi) \;\to\; &\subseteq V_1
\end{aligned}$$

and:

$$\begin{aligned}
\sigma(U_1) \cap \sigma(\mathrm{Fr}(\pi_1) \setminus U_1) &= \sigma(U_1) \cap \sigma(\,\mathrm{Fr}(\pi_1) \setminus \{x\} \setminus U\,) \\
&= \sigma(U_1) \cap \sigma(\mathrm{Fr}(\pi) \setminus U) \\
&= (\sigma(U) \cup \{\sigma(x)\}) \cap \sigma(\mathrm{Fr}(\pi) \setminus U) \\
q(U,\pi) \;\to\; &= \{\sigma(x)\} \cap \sigma(\mathrm{Fr}(\pi) \setminus U) \\
&\subseteq \{\sigma(x)\} \cap \sigma(\mathrm{Fr}(\pi)) \\
\text{A: to be proved} \;\to\; &= \emptyset
\end{aligned}$$

So we need to show that $\sigma(u) \neq \sigma(x)$ whenever $u \in \mathrm{Fr}(\pi)$, which follows immediately from proposition (220) and the validity of σ for $\pi = \nabla x \pi_1$, itself a consequence of our assumption $q(U, \pi)$. So we are almost done proving $q(U_1, \pi_1)$ and it remains to show that σ is valid for π_1, which is another immediate consequence of proposition (220). This completes our induction argument. .

We are now ready to conclude with our local inversion theorem which is the counterpart of theorem (10) of page 105 and follows from lemma (24).

Theorem 25 *Let V, W be sets and $\sigma : V \to W$ be a map. Let V_0, V_1 be subsets of V such that $\sigma_{|V_0}$ and $\sigma_{|V_1}$ are injective maps. Let Π be the subset of $\mathbf{\Pi}(V)$:*

$$\Pi = \{\pi \in \mathbf{\Pi}(V) : (\mathrm{Fr}(\pi) \subseteq V_0) \wedge (\mathrm{Bnd}(\pi) \subseteq V_1) \wedge (\sigma \textit{ valid for } \pi)\}$$

Then, there exits $\tau : \mathbf{\Pi}(W) \to \mathbf{\Pi}(V)$ *such that:*

$$\forall \pi \in \Pi \ , \ \tau \circ \sigma(\pi) = \pi$$

where $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ *also denotes the associated proof substitution mapping.*

Proof
Let $\sigma : V \to W$ be a map and $V_0, V_1 \subseteq V$ be such that $\sigma_{|V_0}$ and $\sigma_{|V_1}$ are injective maps. We shall distinguish two cases: first we assume that $V = \emptyset$. Then for all $\pi \in \mathbf{\Pi}(V)$ the inclusions $\mathrm{Fr}(\pi) \subseteq V_0$ and $\mathrm{Bnd}(\pi) \subseteq V_1$ are always true. Furthermore, from definition (79) the substitution σ is always valid for π. Hence we have $\Pi = \mathbf{\Pi}(V)$ and we need to find $\tau : \mathbf{\Pi}(W) \to \mathbf{\Pi}(V)$ such that $\tau \circ \sigma(\pi) = \pi$ for all $\pi \in \mathbf{\Pi}(V)$. Our first step is to apply theorem (10) of page (105) to obtain a map $\tau^* : \mathbf{P}(W) \to \mathbf{P}(V)$ such that $\tau^* \circ \sigma(\phi) = \phi$ for all $\phi \in \Gamma$ where $\Gamma = \{\phi \in \mathbf{P}(V) : (\mathrm{Fr}(\phi) \subseteq V_0) \wedge (\mathrm{Bnd}(\phi) \subseteq V_1) \wedge (\sigma \text{ valid for } \phi)\}$. However, since $V = \emptyset$ we have $\Gamma = \mathbf{P}(V)$ and so $\tau^* \circ \sigma(\phi) = \phi$ for all $\phi \in \mathbf{P}(V)$. We define τ with the following recursion on $\mathbf{\Pi}(W)$:

$$\tau(\rho) = \begin{cases} \tau^*(\psi) & \text{if} \quad \rho = \psi \in \mathbf{P}(W) \\ \partial\tau^*(\psi) & \text{if} \quad \rho = \partial\psi \\ \tau(\rho_1) \oplus \tau(\rho_2) & \text{if} \quad \rho = \rho_1 \oplus \rho_2 \\ \bot & \text{if} \quad \rho = \nabla u \rho_1 \end{cases} \tag{3.47}$$

We do not really care how $\tau(\rho)$ is defined in the case when $\rho = \nabla u \rho_1$ so we are setting $\tau(\rho) = \bot$ which is the proof with single hypothesis $\bot$ and conclusion $\bot$. We shall now prove that $\tau \circ \sigma(\pi) = \pi$ using a structural induction argument. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then we have:

$$\begin{aligned} \tau \circ \sigma(\pi) &= \tau \circ \sigma(\phi) \\ \text{eq. (3.47)} \ \to \ &= \tau^* \circ \sigma(\phi) \\ &= \phi \\ &= \pi \end{aligned}$$

Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then we have:

$$\begin{aligned} \tau \circ \sigma(\pi) &= \tau \circ \sigma(\partial\phi) \\ \tau \circ \sigma(\pi) &= \tau(\partial\sigma(\phi)) \\ \text{eq. (3.47)} \ \to \ &= \partial\tau^* \circ \sigma(\phi) \\ &= \partial\phi \\ &= \pi \end{aligned}$$

Next we assume that $\pi = \pi_1 \oplus \pi_2$ with $\tau \circ \sigma(\pi_1) = \pi_1$ and $\tau \circ \sigma(\pi_2) = \pi_2$. Then:

$$\begin{aligned} \tau \circ \sigma(\pi) &= \tau \circ \sigma(\pi_1 \oplus \pi_2) \\ &= \tau(\, \sigma(\pi_1) \oplus \sigma(\pi_2)\,) \\ \text{eq. (3.47)} \ \to \ &= \tau \circ \sigma(\pi_1) \oplus \tau \circ \sigma(\pi_2) \\ &= \pi_1 \oplus \pi_2 \\ &= \pi \end{aligned}$$

Since $V = \emptyset$ there is nothing to check in the case when $\pi = \nabla x \pi_1$. So this completes our proof when $V = \emptyset$, and we now assume that $V \neq \emptyset$. Let $x_0 \in V$ and consider $\tau_0 : \sigma(V_0) \to V$ and $\tau_1 : \sigma(V_1) \to V$ to be the inverse mappings of $\sigma_{|V_0}$ and $\sigma_{|V_1}$ respectively. Extend τ_0 and τ_1 to the whole of W by setting $\tau_0(u) = x_0$ if $u \notin \sigma(V_0)$ and $\tau_1(u) = x_0$ if $u \notin \sigma(V_1)$. Then $\tau_0, \tau_1 : W \to V$ are left-inverse of σ on V_0 and V_1 respectively, i.e. we have:

$$\begin{array}{ll} (i) & x \in V_0 \ \Rightarrow \ \tau_0 \circ \sigma(x) = x \\ (ii) & x \in V_1 \ \Rightarrow \ \tau_1 \circ \sigma(x) = x \end{array}$$

Let $\tau : \mathbf{\Pi}(W) \to \mathbf{\Pi}(V)$ be the dual variable substitution associated with the ordered pair (τ_0, τ_1) as per definition (91). We shall complete the proof of the theorem by showing that $\tau \circ \sigma(\pi) = \pi$ for all $\pi \in \Pi$ where:

$$\Pi = \{\pi \in \mathbf{\Pi}(V) : (\mathrm{Fr}(\pi) \subseteq V_0) \wedge (\mathrm{Bnd}(\pi) \subseteq V_1) \wedge (\sigma \text{ valid for } \pi)\}$$

So let $\pi \in \Pi$. Then in particular π satisfies property (iii) and (iv) of lemma (24) in the particular case when $U = \emptyset$. So applying lemma (24) for $U = \emptyset$, we see that $\tau^\circ(\sigma(\pi))(W \setminus \sigma(\emptyset)) = \pi$ where $\tau^\circ : \mathbf{\Pi}(W) \to [\mathcal{P}(W) \to \mathbf{\Pi}(V)]$ is the map associated with τ. Hence we conclude that $\tau \circ \sigma(\pi) = \tau^\circ(\sigma(\pi))(W) = \pi$. **.**

3.4.4 Minimal Transform and Substitution Congruence

In definition (87) we extended the notion of minimal transform to proofs. In definition (88) we introduced a substitution congruence on the algebra $\mathbf{\Pi}(V)$. In light of theorem (14) of page 149, we expect that $\mathcal{M}(\pi) = \mathcal{M}(\rho)$ be equivalent to $\pi \sim \rho$. In this section we prove that it is indeed the case. This will be the object of theorem (26) below. We shall also provide an immediate consequence of theorem (26) showing that α-equivalence is preserved by valid substitutions. This will be the object of theorem (27). We start by showing that the equality $\mathcal{M}(\pi) = \mathcal{M}(\rho)$ defines a congruence on the free universal algebra $\mathbf{\Pi}(V)$.

Proposition 273 *Let V be a set and $\equiv$ be the relation on $\mathbf{\Pi}(V)$ defined by:*

$$\pi \equiv \rho \ \Leftrightarrow \ \mathcal{M}(\pi) = \mathcal{M}(\rho)$$

for all $\pi, \rho \in \mathbf{\Pi}(V)$. Then $\equiv$ is a congruence on $\mathbf{\Pi}(V)$.

Proof
The relation $\equiv$ is clearly reflexive, symmetric and transitive. So it is an equivalence relation on $\mathbf{\Pi}(V)$ and we simply need to prove that it is a congruent relation, as per definition (15) of page 49. We already know that $\partial\phi \equiv \partial\phi$ for all $\phi \in \mathbf{P}(V)$. So let $\pi = \pi_1 \oplus \pi_2$ and $\rho = \rho_1 \oplus \rho_2$ where $\pi_1 \equiv \rho_1$ and $\pi_2 \equiv \rho_2$. We need to show that $\pi \equiv \rho$, which goes as follows:

$$\begin{array}{rcl} \mathcal{M}(\pi) & = & \mathcal{M}(\pi_1 \oplus \pi_2) \\ & = & \mathcal{M}(\pi_1) \oplus \mathcal{M}(\pi_2) \\ (\pi_1 \equiv \rho_1) \wedge (\pi_2 \equiv \rho_2) \ \rightarrow & = & \mathcal{M}(\rho_1) \oplus \mathcal{M}(\rho_2) \\ & = & \mathcal{M}(\rho_1 \oplus \rho_2) \\ & = & \mathcal{M}(\rho) \end{array}$$

Next we assume that $\pi = \nabla x \pi_1$ and $\rho = \nabla x \rho_1$ where $x \in V$ and $\pi_1 \equiv \rho_1$. We need to show that $\pi \equiv \rho$, which goes as follows:

$$\begin{aligned} \mathcal{M}(\pi) &= \mathcal{M}(\nabla x \pi_1) \\ n = \min\{k : [k/x] \text{ valid for } \mathcal{M}(\pi_1)\} \ \rightarrow &= \nabla n \mathcal{M}(\pi_1)[n/x] \\ \pi_1 \equiv \rho_1 \ \rightarrow &= \nabla n \mathcal{M}(\rho_1)[n/x] \\ \pi_1 \equiv \rho_1 \Rightarrow n = m \ \rightarrow &= \nabla m \mathcal{M}(\rho_1)[m/x] \\ m = \min\{k : [k/x] \text{ valid for } \mathcal{M}(\rho_1)\} \ \rightarrow &= \mathcal{M}(\nabla x \rho_1) \\ &= \mathcal{M}(\rho) \end{aligned}$$

.

The following theorem is the counterpart of theorem (14) of page 149. We provide an identical proof which relies on the local inversion theorem (25).

Theorem 26 *Let $\sim$ be the substitution congruence on $\mathbf{\Pi}(V)$ where V is a set. Then for all $\pi, \rho \in \mathbf{\Pi}(V)$ we have the equivalence:*

$$\pi \sim \rho \ \Leftrightarrow \ \mathcal{M}(\pi) = \mathcal{M}(\rho)$$

where $\mathcal{M}(\pi)$ and $\mathcal{M}(\rho)$ are the minimal transforms as per definition (87).

Proof
First we show $\Rightarrow$: consider the relation $\equiv$ on $\mathbf{\Pi}(V)$ defined by $\pi \equiv \rho$ if and only if $\mathcal{M}(\pi) = \mathcal{M}(\rho)$. We need to show the inclusion $\sim \subseteq \equiv$. However, we know from proposition (273) that $\equiv$ is a congruence on $\mathbf{\Pi}(V)$. Since $\sim$ is the smallest congruence on $\mathbf{\Pi}(V)$ which contains the sets R_0, R_1 and R_2 of definition (88) we simply need to show that $R_i \subseteq \equiv$ for $i \in 3$. First we show that $R_0 \subseteq \equiv$: so let $\pi = \phi$ and $\rho = \psi$ for some $\phi, \psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$, where $\sim$ also denotes the substitution congruence on $\mathbf{P}(V)$. We need to show that $\pi \equiv \rho$ which is $\mathcal{M}(\phi) = \mathcal{M}(\psi)$ which follows immediately from theorem (14) of page 149. Next we show that $R_1 \subseteq \equiv$: so let $\pi = \partial\phi$ and $\rho = \partial\psi$ for some $\phi, \psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$. We need to show that $\pi \equiv \rho$ which is $\mathcal{M}(\pi) = \mathcal{M}(\rho)$. Since $\mathcal{M}(\pi) = \partial\mathcal{M}(\phi)$ and $\mathcal{M}(\rho) = \partial\mathcal{M}(\psi)$, we simply need to show that $\mathcal{M}(\phi) = \mathcal{M}(\psi)$ which also follows from theorem (14). We now show that $R_2 \subseteq \equiv$: so let $\pi = \nabla x \pi_1$ and $\rho = \nabla y \pi_1[y : x]$ where $x \neq y$ and $y \notin \mathrm{Fr}(\pi_1)$. We need to show that $\pi \equiv \rho$ which is $\mathcal{M}(\pi) = \mathcal{M}(\rho)$. However, we have $\rho = \sigma(\pi)$ where $\sigma : V \to V$ is the single variable permutation $\sigma = [y : x]$. So we need to show that $\mathcal{M}(\pi) = \mathcal{M} \circ \sigma(\pi)$. Let $\bar{\sigma} : \bar{V} \to \bar{V}$ be the minimal extension of σ as per definition (39) of page 144. Since σ is an injective map, in particular from proposition (224) σ is valid for π. So we can apply theorem (23) of page 327 from which we obtain $\mathcal{M} \circ \sigma(\pi) = \bar{\sigma} \circ \mathcal{M}(\pi)$. It is therefore sufficient to prove that $\mathcal{M}(\pi) = \bar{\sigma} \circ \mathcal{M}(\pi)$. Let $i : \bar{V} \to \bar{V}$ be the identity mapping. We need to show that $i \circ \mathcal{M}(\pi) = \bar{\sigma} \circ \mathcal{M}(\pi)$ and from proposition (202) it is sufficient to prove that i and $\bar{\sigma}$ coincide on $\mathrm{Var}(\mathcal{M}(\pi))$. So let $u \in \mathrm{Var}(\mathcal{M}(\pi))$. We need to show that $\bar{\sigma}(u) = u$. Since $\bar{V}$ is the disjoint union of V and $\mathbf{N}$, we shall distinguish two cases: first we assume that $u \in \mathbf{N}$. Then $\bar{\sigma}(u) = u$ is immediate

from definition (39). Next we assume that $u \in V$. Then from $u \in \mathrm{Var}(\mathcal{M}(\pi))$ and proposition (252) it follows that $u \in \mathrm{Fr}(\pi) = \mathrm{Fr}(\pi_1) \setminus \{x\}$. In particular we obtain $u \neq x$. Furthermore, having assumed $y \notin \mathrm{Fr}(\pi_1)$, we must have $u \neq y$. Hence we see that $u \notin \{x, y\}$ and consequently since $u \in V$ we obtain the equality $\bar{\sigma}(u) = \sigma(u) = [y:x](u) = u$ as requested. We now prove $\Leftarrow$: we need to show that every $\pi \in \mathbf{\Pi}(V)$ satisfies the property:

$$\forall \rho \in \mathbf{\Pi}(V)\ ,\ [\,\mathcal{M}(\pi) = \mathcal{M}(\rho)\ \Rightarrow\ \pi \sim \rho\,]$$

We shall do so by a structural induction argument using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Let $\rho \in \mathbf{\Pi}(V)$ with the property $\mathcal{M}(\pi) = \mathcal{M}(\phi) = \mathcal{M}(\rho)$. We need to show that $\pi \sim \rho$. From theorem (2) of page 21 the proof ρ can be of one and only one of four types: first it can be of the form $\rho = \psi$ for some $\psi \in \mathbf{P}(V)$. Next, it can be of the form $\rho = \partial\psi$, and possibly of the form $\rho = \rho_1 \oplus \rho_2$ with $\rho_1, \rho_2 \in \mathbf{\Pi}(V)$. Finally, it can be $\rho = \nabla u \rho_1$ for some $u \in V$ and $\rho_1 \in \mathbf{\Pi}(V)$. Looking at definition (87) we see that the minimal transform $\mathcal{M}(\rho)$ has the same basic structure as ρ. Thus, from the equality $\mathcal{M}(\rho) = \mathcal{M}(\phi) \in \mathbf{P}(\bar{V})$ it follows that ρ can only be of the form $\rho = \psi$ for some $\psi \in \mathbf{P}(V)$. So we obtain $\mathcal{M}(\rho) = \mathcal{M}(\psi) = \mathcal{M}(\phi)$ and consequently from theorem (14) of page 149 we obtain $\phi \sim \psi$ which is $\pi \sim \rho$ as requested. So we now assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Let $\rho \in \mathbf{\Pi}(V)$ be such that $\mathcal{M}(\pi) = \mathcal{M}(\rho)$. We need to show that $\pi \sim \rho$. However, since $\mathcal{M}(\pi) = \partial\mathcal{M}(\phi)$ we see that ρ must be of the form $\rho = \partial\psi$ for some $\psi \in \mathbf{P}(V)$. It follows that $\partial\mathcal{M}(\phi) = \partial\mathcal{M}(\psi)$ and thus $\mathcal{M}(\phi) = \mathcal{M}(\psi)$ which implies that $\phi \sim \psi$ by virtue of theorem (14). Hence we have $\partial\phi \sim \partial\psi$ which is $\pi \sim \rho$ as requested. We now assume that $\pi = \pi_1 \oplus \pi_2$ where π_1, π_2 satisfy our property. We need to show the same if true of π. So let $\rho \in \mathbf{\Pi}(V)$ such that $\mathcal{M}(\pi) = \mathcal{M}(\pi_1) \oplus \mathcal{M}(\pi_2) = \mathcal{M}(\rho)$. We need to show that $\pi \sim \rho$. From $\mathcal{M}(\rho) = \mathcal{M}(\pi_1) \oplus \mathcal{M}(\pi_2)$ we see that ρ can only be of the form $\rho = \rho_1 \oplus \rho_2$. It follows that $\mathcal{M}(\rho) = \mathcal{M}(\rho_1) \oplus \mathcal{M}(\rho_2)$ and consequently we obtain $\mathcal{M}(\pi_1) \oplus \mathcal{M}(\pi_2) = \mathcal{M}(\rho_1) \oplus \mathcal{M}(\rho_2)$. Hence, using theorem (2) of page 21 we have $\mathcal{M}(\pi_1) = \mathcal{M}(\rho_1)$ and $\mathcal{M}(\pi_2) = \mathcal{M}(\rho_2)$. Having assumed π_1 and π_2 satisfy our induction property, it follows that $\pi_1 \sim \rho_1$ and $\pi_2 \sim \rho_2$ and consequently $\pi_1 \oplus \pi_2 \sim \rho_1 \oplus \rho_2$. So we have proved that $\pi \sim \rho$ as requested. We now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ satisfies our property. We need to show the same is true of π. So let $\rho \in \mathbf{\Pi}(V)$ such that $\mathcal{M}(\pi) = \mathcal{M}(\rho)$. We need to show that $\pi \sim \rho$. We have:

$$\mathcal{M}(\pi) = \nabla n \mathcal{M}(\pi_1)[n/x] \tag{3.48}$$

where $n = \min\{k \in \mathbf{N} : [k/x] \text{ valid for } \mathcal{M}(\pi_1)\}$. Hence from the equality $\mathcal{M}(\pi) = \mathcal{M}(\rho)$ we see that ρ can only be of the form $\rho = \nabla y \rho_1$ for some $y \in V$ and $\rho_1 \in \mathbf{\Pi}(V)$. We shall distinguish two cases: first we assume that $y = x$. Then we need to show that $\nabla x \pi_1 \sim \nabla x \rho_1$ and it is therefore sufficient to prove that $\pi_1 \sim \rho_1$. Having assumed π_1 satisfy our property, we simply need to show that $\mathcal{M}(\pi_1) = \mathcal{M}(\rho_1)$. However we have the equality:

$$\mathcal{M}(\rho) = \nabla m \mathcal{M}(\rho_1)[m/x] \tag{3.49}$$

where $m = \min\{k \in \mathbf{N} : [k/x] \text{ valid for } \mathcal{M}(\rho_1)\}$. Comparing (3.48) and (3.49), from $\mathcal{M}(\pi) = \mathcal{M}(\rho)$ and theorem (2) of page 21 we obtain $n = m$ and thus:

$$\mathcal{M}(\pi_1)[n/x] = \mathcal{M}(\rho_1)[n/x] \tag{3.50}$$

Consider the substitution $\sigma : \bar{V} \to \bar{V}$ defined by $\sigma = [n/x]$. We shall conclude that $\mathcal{M}(\pi_1) = \mathcal{M}(\rho_1)$ by inverting equation (3.50) using the local inversion theorem (25) of page 345 on the substitution σ. So consider the sets $V_0 = V$ and $V_1 = \mathbf{N}$. It is clear that both $\sigma_{|V_0}$ and $\sigma_{|V_1}$ are injective maps. Define:

$$\Pi = \{\kappa \in \mathbf{\Pi}(\bar{V}) : (\mathrm{Fr}(\kappa) \subseteq V_0) \wedge (\mathrm{Bnd}(\kappa) \subseteq V_1) \wedge (\sigma \text{ valid for } \kappa)\}$$

Then using theorem (25) there exits $\tau : \mathbf{\Pi}(\bar{V}) \to \mathbf{\Pi}(\bar{V})$ such that $\tau \circ \sigma(\kappa) = \kappa$ for all $\kappa \in \Pi$. Hence from equation (3.50) it is sufficient to prove that $\mathcal{M}(\pi_1) \in \Pi$ and $\mathcal{M}(\rho_1) \in \Pi$. First we show that $\mathcal{M}(\pi_1) \in \Pi$. We already know that $\sigma = [n/x]$ is a valid substitution for $\mathcal{M}(\pi_1)$. The fact that $\mathrm{Fr}(\mathcal{M}(\pi_1)) \subseteq V_0$ follows from proposition (252). The fact that $\mathrm{Bnd}(\mathcal{M}(\pi_1)) \subseteq V_1$ follows from proposition (253). So we have proved that $\mathcal{M}(\pi_1) \in \Pi$ as requested. The proof of $\mathcal{M}(\rho_1) \in \Pi$ is identical, which completes our proof of $\pi \sim \rho$ in the case when $\rho = \forall y \rho_1$ and $y = x$. We now assume that $y \neq x$. Consider the proof $\rho^* = \nabla x \rho_1[x\,{:}\,y]$ where $[x\,{:}\,y]$ is the permutation mapping as per definition (27) of page 79. Suppose we have proved the equivalence $\rho \sim \rho^*$. Then in order to prove $\pi \sim \rho$ it is sufficient by transitivity to show that $\pi \sim \rho^*$. However, having already proved the implication $\Rightarrow$ of this theorem, we know that $\rho \sim \rho^*$ implies $\mathcal{M}(\rho) = \mathcal{M}(\rho^*)$. Hence, if we have $\rho \sim \rho^*$, it is sufficient to prove $\pi \sim \rho^*$ knowing that $\mathcal{M}(\pi) = \mathcal{M}(\rho^*)$ and $\rho^* = \nabla x \rho_1^*$ where $\rho_1^* = \rho_1[x\,{:}\,y]$. So we are back to the case when $y = x$, a case we have already dealt with. It follows that we can complete our induction argument simply by showing $\rho \sim \rho^*$. Since $\rho = \nabla y \rho_1$ and $\rho^* = \nabla x \rho_1[x\,{:}\,y]$ with $x \neq y$, from definition (88) of page 330 we simply need to check that $x \notin \mathrm{Fr}(\rho_1)$. So suppose to the contrary that $x \in \mathrm{Fr}(\rho_1)$. Since $x \neq y$ we obtain $x \in \mathrm{Fr}(\rho)$. From proposition (252) it follows that $x \in \mathrm{Fr}(\mathcal{M}(\rho))$. Having assumed that $\mathcal{M}(\pi) = \mathcal{M}(\rho)$ we obtain $x \in \mathrm{Fr}(\mathcal{M}(\pi))$ and finally using proposition (252) once more, we obtain $x \in \mathrm{Fr}(\pi)$. This is our desired contradiction since $\pi = \nabla x \pi_1$. This completes our induction argument.

.

As an immediate consequence of theorem (26), we now provide the following theorem which is the counterpart of theorem (15) of page 152. We know from proposition (260) that α-equivalence is preserved by injective maps. From proposition (224) injective maps are valid substitutions. Hence, the following theorem greatly improves on proposition (260) by showing that α-equivalence is in fact preserved by valid substitutions, as we would expect.

Theorem 27 *Let V and W be sets and $\sigma : V \to W$ be a map. Let $\sim$ be the substitution congruence on $\mathbf{\Pi}(V)$ and $\mathbf{\Pi}(W)$. Then if σ is valid for π and ρ:*

$$\pi \sim \rho \;\Rightarrow\; \sigma(\pi) \sim \sigma(\rho)$$

for all $\pi, \rho \in \mathbf{\Pi}(V)$, where $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ is also the substitution mapping.

Proof
We assume that $\pi \sim \rho$ and $\sigma : V \to W$ is valid for π and ρ. We need to show that $\sigma(\pi) \sim \sigma(\rho)$. Using theorem (26) it is sufficient to prove that $\mathcal{M} \circ \sigma(\pi) = \mathcal{M} \circ \sigma(\rho)$. Since σ is valid for π and ρ, using theorem (23) of page 327 it is therefore sufficient to prove that $\bar{\sigma} \circ \mathcal{M}(\pi) = \bar{\sigma} \circ \mathcal{M}(\rho)$, which follows immediately from $\mathcal{M}(\pi) = \mathcal{M}(\rho)$, itself a consequence of $\pi \sim \rho$. **.**

We shall complete this section by providing a counterpart of proposition (99). This result establishes the equivalence $\mathcal{M}(\pi) \sim i(\pi)$ where $i : V \to \bar{V}$ is the inclusion mapping. It is an elementary result which is not a consequence of theorem (26) or theorem (27). In fact, its corresponding proposition (99) is provided shortly after minimal transforms have been defined. In the case of proofs, we defined minimal transforms before we had any idea of substitution congruence on $\mathbf{\Pi}(V)$. So we had to wait. We suspect the following proposition could be used to design an alternative proof of theorem (26) which does not involve the local inversion theorem (25) of page 345. From the equality $\mathcal{M}(\pi) = \mathcal{M}(\rho)$ we would infer $i(\pi) \sim i(\rho)$. We would still need to find a way to conclude $\pi \sim \rho$ from the equivalence $i(\pi) \sim i(\rho)$. Assuming $V \neq \emptyset$ for the purpose of this discussion, we could define a left inverse $j : \bar{V} \to V$ of $i : V \to \bar{V}$. We would then need to extend proposition (260) by weakening its assumption and showing that the equivalence $\pi \sim \rho$ is preserved simply by assuming the map $\sigma : V \to W$ is injective on $\mathrm{Var}(\pi) \cup \mathrm{Var}(\rho)$, rather than injective on V.

Proposition 274 *Let V be a set and $i : V \to \bar{V}$ be the inclusion map. We denote $\sim$ the substitution congruence on $\mathbf{\Pi}(\bar{V})$. Then for all $\pi \in \mathbf{\Pi}(V)$:*

$$\mathcal{M}(\pi) \sim i(\pi)$$

Proof
We shall prove the equivalence $\mathcal{M}(\pi) \sim i(\pi)$ by a structural induction argument, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then the equivalence follows from proposition (99). Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Using proposition (99) once more:

$$\mathcal{M}(\pi) = \partial\mathcal{M}(\phi) \sim \partial i(\phi) = i(\pi)$$

We now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ satisfy the equivalence:

$$\begin{aligned} \mathcal{M}(\pi) &= \mathcal{M}(\pi_1 \oplus \pi_2) \\ &= \mathcal{M}(\pi_1) \oplus \mathcal{M}(\pi_2) \\ &\sim i(\pi_1) \oplus i(\pi_2) \\ &= i(\pi_1 \oplus \pi_2) \\ &= i(\pi) \end{aligned}$$

Finally we assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ satisfies the equivalence. In this case we have the following equalities:

$$\mathcal{M}(\pi) = \mathcal{M}(\nabla x \pi_1)$$

$$
\begin{array}{rrcl}
n = \min\{k : [k/x] \text{ valid for } \mathcal{M}(\pi_1)\} & \rightarrow & = & \nabla n \mathcal{M}(\pi_1)[n/x] \\
 & & = & [n/x](\nabla x \mathcal{M}(\pi_1)) \\
\text{A: to be proved} & \rightarrow & \sim & \nabla x \mathcal{M}(\pi_1) \\
 & & \sim & \nabla x\, i(\pi_1) \\
 & & = & \nabla i(x)\, i(\pi_1) \\
 & & = & i(\nabla x \pi_1) \\
 & & = & i(\pi)
\end{array}
$$

So it remains to show that $[n/x](\nabla x \mathcal{M}(\pi_1)) \sim \nabla x \mathcal{M}(\pi_1)$. Hence, from proposition (257) it is sufficient to prove that $[n/x]$ is an admissible substitution for $\nabla x \mathcal{M}(\pi_1)$. We already know that $[n/x]$ is valid for $\mathcal{M}(\pi_1)$. Using proposition (220), given $u \in \text{Fr}(\nabla x \mathcal{M}(\pi_1))$, in order to prove that $[n/x]$ is valid for $\nabla x \mathcal{M}(\pi_1)$ we need to show that $[n/x](u) \neq [n/x](x)$. So it is sufficient to show that $[n/x](u) \neq n$. Since $u \in \text{Fr}(\nabla x \mathcal{M}(\pi_1))$, in particular we have $u \neq x$. Hence, we have to show that $u \neq n$. Using proposition (252) we have:

$$u \in \text{Fr}(\nabla x \mathcal{M}(\pi_1)) \subseteq \text{Fr}(\mathcal{M}(\pi_1)) \subseteq V$$

and consequently from $V \cap \mathbf{N} = \emptyset$ we conclude that $u \neq n$. In order to show that $[n/x]$ is an admissible substitution for $\nabla x \mathcal{M}(\pi_1)$ it remains to prove that $[n/x](u) = u$ for all $u \in \text{Fr}(\nabla x \mathcal{M}(\pi_1))$, which follows from $u \neq x$. .

3.4.5 Proof with Clean Minimal Transform

As you may recall, we defined a minimal transform for proofs which naturally led to the notion of substitution congruence on $\mathbf{\Pi}(V)$. We gave a result to characterize this α-equivalence in theorem (24) of page 339. We also established the equivalence between $\pi \sim \rho$ and $\mathcal{M}(\pi) = \mathcal{M}(\rho)$ in theorem (26) of page 348 which serves as a neat validation of our definition choices so far. One other thing to check is that two equivalent proofs are indeed *the same*. Specifically, if $\sim$ denotes the substitution congruence on $\mathbf{\Pi}(V)$ and $\pi \sim \rho$, we want to make sure the *fundamental properties* of π are also those of ρ. So if π is a clean proof, we should expect ρ to be clean as well. We should also expect π and ρ to have equivalent valuation modulo, i.e. $\text{Val}^+(\pi) \sim \text{Val}^+(\rho)$ where $\sim$ now denotes the substitution congruence on $\mathbf{P}(V)$. Finally, we would want to check we have the equality $\text{Hyp}(\pi) \sim \text{Hyp}(\rho)$ modulo the substitution congruence, as per definition (85). In short, two equivalent proofs should prove the same thing from the same hypothesis, modulo α-equivalence, and they should both be clean if one of them is. These results will be established in the next section. For now, we shall focus on proving the following proposition from which every thing else will flow. From proposition (254) we already know that the minimal transform of a clean proof is clean. The following proposition establishes the reverse implication ($\mathcal{M}(\pi)$ is clean) $\Rightarrow$ (π is clean). This type of result requires proofs which are more elaborate than usual. It is very similar to lemma (21) where we proved the implication ($\mathcal{M}(\phi)$ is an axiom) $\Rightarrow$ (ϕ is an axiom modulo). As we shall

see, the proof of proposition (275) below will rely on the local inversion theorem for proofs, which is theorem (25) of page 345. Until now, the local inversion theorem was only ever used to prove the implication $\mathcal{M}(\pi) = \mathcal{M}(\rho) \Rightarrow \pi \sim \rho$.

Proposition 275 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$. Then we have the equivalence:*

$$(\pi \text{ is clean}) \Leftrightarrow (\mathcal{M}(\pi) \text{ is clean})$$

where $\mathcal{M}(\pi)$ is the minimal transform of π as per definition (87).

Proof
The implication $\Rightarrow$ is already known from proposition (254). We shall prove $\Leftarrow$ with an induction argument, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then from definition (86) we see that π is always clean in this case, so our implication is true. Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. We need to show our implication is true for π. So we assume that $\mathcal{M}(\pi)$ is clean. We need to show that π is also clean. However, we have $\mathcal{M}(\pi) = \partial\mathcal{M}(\phi)$ and it follows that $\mathcal{M}(\phi)$ is an axiom modulo, i.e. $\mathcal{M}(\phi) \in \mathbf{A}^+(\bar{V})$. Using proposition (245) we see that $\phi \in \mathbf{A}^+(V)$, i.e. ϕ is itself an axiom modulo. So π is clean as requested. We now assume that $\pi = \pi_1 \oplus \pi_2$, where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are proofs satisfying our implication. We need to show the same is true of π. So we assume that $\mathcal{M}(\pi) = \mathcal{M}(\pi_1) \oplus \mathcal{M}(\pi_2)$ is clean. We need to show that π is itself clean. However, from proposition (240) we see that both $\mathcal{M}(\pi_1)$ and $\mathcal{M}(\pi_2)$ are clean, and furthermore $\mathrm{Val}^+ \circ \mathcal{M}(\pi_2) = \chi_1 \to \chi_2$ for some $\chi_1, \chi_2 \in \mathbf{P}(\bar{V})$ such that $\chi_1 \sim \mathrm{Val}^+ \circ \mathcal{M}(\pi_1)$, where $\sim$ refers to the substitution congruence on $\mathbf{P}(\bar{V})$. Having assumed our implication is true for π_1 and π_2, it follows that both π_1 and π_2 are clean. Using proposition (240), in order to show that π is clean it remains to prove that $\mathrm{Val}^+(\pi_2) = \psi_1 \to \psi_2$ for some $\psi_1, \psi_2 \in \mathbf{P}(V)$ such that $\psi_1 \sim \mathrm{Val}^+(\pi_1)$, where $\sim$ is now the substitution congruence on $\mathbf{P}(V)$. However, using proposition (254) and the fact that π_2 is clean, we obtain $\mathcal{M} \circ \mathrm{Val}^+(\pi_2) \sim \mathrm{Val}^+ \circ \mathcal{M}(\pi_2) = \chi_1 \to \chi_2$. From theorem (12) of page 132 it follows that $\mathcal{M} \circ \mathrm{Val}^+(\pi_2) = \chi_1' \to \chi_2'$ for some $\chi_1', \chi_2' \in \mathbf{P}(\bar{V})$ such that $\chi_1 \sim \chi_1'$ and $\chi_2 \sim \chi_2'$. Looking at definition (38) of the minimal transform and arguing from the uniqueness property of theorem (2) or page 21, we see that $\mathrm{Val}^+(\pi_2)$ must be of the form $\mathrm{Val}^+(\pi_2) = \psi_1 \to \psi_2$ for some $\psi_1, \psi_2 \in \mathbf{P}(V)$ such that $\chi_1' = \mathcal{M}(\psi_1)$. In order to show that π is clean, it remains to prove that $\psi_1 \sim \mathrm{Val}^+(\pi_1)$. From theorem (14) of page 149, this amounts to showing the equality $\mathcal{M}(\psi_1) = \mathcal{M} \circ \mathrm{Val}^+(\pi_1)$, for which it is in fact sufficient to show the equivalence $\mathcal{M}(\psi_1) \sim \mathcal{M} \circ \mathrm{Val}^+(\pi_1)$ by virtue of proposition (112). Since π_1 is clean, we can apply proposition (254) and obtain:

$$\begin{array}{rcl} \mathcal{M}(\psi_1) & = & \chi_1' \\ & \sim & \chi_1 \\ & \sim & \mathrm{Val}^+ \circ \mathcal{M}(\pi_1) \\ \text{prop. (254)} \ \to & \sim & \mathcal{M} \circ \mathrm{Val}^+(\pi_1) \end{array}$$

So we have proved that π is clean as requested. We now assume that $\pi = \nabla x \pi_1$ for some $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ satisfying our implication. We need to show the same is true of π. So we assume that $\mathcal{M}(\pi)$ is clean. We need to show that π is itself clean. Using proposition (241), it is sufficient to show that π_1 is clean and furthermore that $x \notin \mathrm{Sp}(\pi_1)$. However from definition (87) we obtain the equality $\mathcal{M}(\pi) = \nabla n \mathcal{M}(\pi_1)[n/x]$ where $n \in \mathbf{N}$ is the smallest natural number for which $[n/x]$ is valid for $\mathcal{M}(\pi_1)$. Having assumed that $\mathcal{M}(\pi)$ is clean, it follows from proposition (241) that $\mathcal{M}(\pi_1)[n/x]$ is clean and furthermore $n \notin \mathrm{Sp}(\mathcal{M}(\pi_1)[n/x])$. So let us show that π_1 is clean: Consider the substitution $\sigma : \bar{V} \to \bar{V}$ defined by $\sigma = [n/x]$. We shall first show that $\mathcal{M}(\pi_1)$ is clean using the local inversion theorem (25) of page 345. So consider the sets $V_0 = V$ and $V_1 = \mathbf{N}$. It is clear that both $\sigma_{|V_0}$ and $\sigma_{|V_1}$ are injective maps. Define:

$$\Pi = \{\kappa \in \mathbf{\Pi}(\bar{V}) : (\mathrm{Fr}(\kappa) \subseteq V_0) \wedge (\mathrm{Bnd}(\kappa) \subseteq V_1) \wedge (\sigma \text{ valid for } \kappa)\}$$

Then using theorem (25) there exits $\tau : \mathbf{\Pi}(\bar{V}) \to \mathbf{\Pi}(\bar{V})$ such that $\tau \circ \sigma(\kappa) = \kappa$ for all $\kappa \in \Pi$. Using propositions (252), (253) and the fact that $[n/x]$ is valid for $\mathcal{M}(\pi_1)$, it follows that $\mathcal{M}(\pi_1) \in \Pi$. Thus we obtain $\tau(\mathcal{M}(\pi_1)[n/x]) = \mathcal{M}(\pi_1)$. Since $\mathcal{M}(\pi_1)[n/x]$ is clean, in order to show that $\mathcal{M}(\pi_1)$ is itself clean it is sufficient to prove that τ is valid for $\mathcal{M}(\pi_1)[n/x]$, by virtue for proposition (248). Using proposition (226), it is therefore sufficient to prove that $\tau \circ [n/x]$ is valid for $\mathcal{M}(\pi_1)$, which follows from proposition (227) and $\tau(\mathcal{M}(\pi_1)[n/x]) = \mathcal{M}(\pi_1)$. So we have proved that $\mathcal{M}(\pi_1)$ is a clean proof and consequently π_1 itself, as follows from the induction hypothesis. We now show that $x \notin \mathrm{Sp}(\pi_1)$: since $[n/x]$ is valid for $\mathcal{M}(\pi_1)$, from proposition (222) we have the equality $\mathrm{Sp}(\mathcal{M}(\pi_1)[n/x]) = [n/x](\,\mathrm{Sp}(\mathcal{M}(\pi_1))\,)$. Hence we have $n \notin [n/x](\,\mathrm{Sp}(\mathcal{M}(\pi_1))\,)$ and consequently $x \notin \mathrm{Sp}(\mathcal{M}(\pi_1))$. However having established that π_1 is a clean proof, from proposition (250) we have $\mathrm{Sp}(\mathcal{M}(\pi_1)) = \mathrm{Sp}(\pi_1)$. We conclude that $x \notin \mathrm{Sp}(\pi_1)$ as requested, which completes our induction argument. **.**

3.4.6 Valuation Modulo and Substitution Congruence

Having established proposition (275) in the previous section, we are now in a position to check that α-equivalence between proofs is a sensible notion. This means that equivalent proofs prove the same thing from the same hypothesis, modulo the substitution congruence, at least when one of them is clean. When this is the case, then both proofs are in fact clean. Note that $\pi \sim \rho$ may not imply $\mathrm{Val}^+(\pi) \sim \mathrm{Val}^+(\rho)$ if π and ρ are not clean proofs. As already pointed out on several occasions, dealing with proofs which are not clean is typically a waste of time as nothing sensible can be said about them. For example, suppose $x \neq y$ and consider $\pi_1 = \nabla x(x \in x)$ and $\rho_1 = \nabla y(y \in y)$. These proofs are not clean and we have $\mathrm{Val}^+(\pi_1) = \bot \to \bot = \mathrm{Val}^+(\rho_1)$. However, from the equivalence $\pi_1 \sim \rho_1$ we see that $\pi \sim \rho$ where $\pi = \nabla x \pi_1$ and $\rho = \nabla x \rho_1$. Furthermore, since $x \in \mathrm{Sp}(\pi_1) = \{x\}$ we have $\mathrm{Val}^+(\pi) = \bot \to \bot$, while from $x \notin \mathrm{Sp}(\rho_1) = \{y\}$ we obtain $\mathrm{Val}^+(\rho) = \forall x \mathrm{Val}^+(\rho_1) = \forall x(\bot \to \bot)$. From theorem (12) of page 132, the formulas $\forall x(\bot \to \bot)$ and $\bot \to \bot$ are not α-equivalent. Thus we see that

it is possible to have the equivalence $\pi \sim \rho$ and $\mathrm{Val}^+(\pi) \not\sim \mathrm{Val}^+(\rho)$. As the following proposition shows, this possibility is removed by assuming one of the proofs π or ρ is a clean proof.

Proposition 276 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$ be a clean proof. Then for all $\rho \in \mathbf{\Pi}(V)$, if we have the equivalence $\pi \sim \rho$ then ρ is itself clean and:*

$$\mathrm{Val}^+(\pi) \sim \mathrm{Val}^+(\rho)$$

where $\sim$ denotes the substitution congruence both on $\mathbf{P}(V)$ and $\mathbf{\Pi}(V)$.

Proof
We assume that π is clean and $\pi \sim \rho$. We need to show that ρ is clean and $\mathrm{Val}^+(\pi) \sim \mathrm{Val}^+(\rho)$. First we show that ρ is clean: from theorem (26) of page 348 we obtain $\mathcal{M}(\pi) = \mathcal{M}(\rho)$. Furthermore since π is clean, from proposition (275) it follows that $\mathcal{M}(\pi)$ is clean. Hence we see that $\mathcal{M}(\rho)$ is clean and using proposition (275) once more we conclude that ρ is a clean proof. In order to show the equivalence $\mathrm{Val}^+(\pi) \sim \mathrm{Val}^+(\rho)$, it is sufficient to show the equality $\mathcal{M} \circ \mathrm{Val}^+(\pi) = \mathcal{M} \circ \mathrm{Val}^+(\rho)$ by virtue of theorem (14) of page 149. In fact, using proposition (112), it is sufficient to show the equivalence $\mathcal{M} \circ \mathrm{Val}^+(\pi) \sim \mathcal{M} \circ \mathrm{Val}^+(\rho)$ where $\sim$ now denotes the substitution congruence on $\mathbf{P}(\bar{V})$. Since π and ρ are clean proofs, using proposition (254) we obtain:

$$\begin{array}{rcl} \mathcal{M} \circ \mathrm{Val}^+(\pi) & \sim & \mathrm{Val}^+ \circ \mathcal{M}(\pi) \\ & = & \mathrm{Val}^+ \circ \mathcal{M}(\rho) \\ \text{prop. (254)} \ \rightarrow & \sim & \mathcal{M} \circ \mathrm{Val}^+(\rho) \end{array}$$

.

We complete this section by showing the hypothesis of equivalent proofs are the same, modulo the substitution congruence, provided these proofs are clean. For a counter-example involving equivalent proofs which are not clean, simply consider $\pi = \nabla x(x \in x)$ and $\rho = \nabla y(y \in y)$ where $x \neq y$.

Proposition 277 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$ be a clean proof. Then for all $\rho \in \mathbf{\Pi}(V)$, if we have the substitution equivalence $\pi \sim \rho$ then we also have:*

$$\mathrm{Hyp}(\pi) \sim \mathrm{Hyp}(\rho)$$

where $\sim$ is the equality modulo the substitution congruence as per definition (85).

Proof
If π is clean and $\pi \sim \rho$ we know that ρ is clean from proposition (276). We have to show that the equality $\mathrm{Hyp}(\pi) \sim \mathrm{Hyp}(\rho)$ modulo the substitution congruence is true. From definition (85), we need to prove the inclusions modulo $\mathrm{Hyp}(\pi) \precsim \mathrm{Hyp}(\rho)$ and $\mathrm{Hyp}(\rho) \precsim \mathrm{Hyp}(\pi)$, and it is clearly sufficient to focus on one of these inclusions. So let $\phi \in \mathrm{Hyp}(\pi)$. From definition (84), we need to show

the existence of $\psi \in \text{Hyp}(\rho)$ such that $\phi \sim \psi$. However, since π is a clean proof, from proposition (251) we have $\text{Hyp}(\mathcal{M}(\pi)) = \mathcal{M}(\text{Hyp}(\pi))$. It follows that $\mathcal{M}(\phi) \in \text{Hyp}(\mathcal{M}(\pi))$. Having assumed that $\pi \sim \rho$, from theorem (26) of page 348 we obtain $\mathcal{M}(\pi) = \mathcal{M}(\rho)$ and consequently $\mathcal{M}(\phi) \in \text{Hyp}(\mathcal{M}(\rho))$. However, ρ is also a clean proof and we have $\text{Hyp}(\mathcal{M}(\rho)) = \mathcal{M}(\text{Hyp}(\rho))$. It follows that $\mathcal{M}(\phi) \in \mathcal{M}(\text{Hyp}(\rho))$ and we see that there exists $\psi \in \text{Hyp}(\rho)$ such that $\mathcal{M}(\phi) = \mathcal{M}(\psi)$ which is $\phi \sim \psi$ by virtue of theorem (14) of page 149. .

3.5 Essential Substitution for Proofs

3.5.1 Substitution Rank of Proof

We are now getting closer to our objective of defining essential proof substitutions $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ associated with a map $\sigma : V \to W$. Our strategy so far has been to follow the trail of what was done to construct essential substitutions $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ for formulas. There is nothing glamorous in doing so, but we do enjoy a reasonable chance of success by exploiting safe routes, with minimal time and effort. Looking back at the work done for formulas, one natural question comes to mind: why do we need to bother about *substitution rank*? Our final result in theorem (18) of page 174 was to prove the existence of essential substitutions $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ associated with $\sigma : V \to W$, provided $|W|$ is an infinite cardinal or $|V| \leq |W|$. This result does not involve *substitution rank* and it is very likely that it could be proved without any reference to it. So why do we care so much about *substitution rank*? The reason is this: as a general comment, it is no good to know that something is true. What is important is to understand why this is the case. We feel so much better about it. When it comes to the existence of essential substitutions $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$, the notion of *substitution rank* brings us some valuable light. It allows us to understand why the restrictions on the cardinals exist. So let us see why this is: given a map $\sigma : V \to W$ and a formula $\phi \in \mathbf{P}(V)$, the formula $\sigma(\phi)$ is essentially $\bar{\sigma} \circ \mathcal{M}(\phi)$. The problem is $\bar{\sigma} \circ \mathcal{M}(\phi)$ is an element of $\mathbf{P}(\bar{W})$. So it needs to be interpreted as an element of $\mathbf{P}(W)$. This cannot be done unless the set $\mathbf{P}(W)$ is *large enough* for the formula $\bar{\sigma} \circ \mathcal{M}(\phi)$ to be *squeezed* into it. In other words, the set W needs to have sufficiently many variables. This naturally leads to the condition $\text{rnk}(\bar{\sigma} \circ \mathcal{M}(\phi)) \leq |W|$ which is where the *substitution rank* comes in. If we want to define an essential substitution as a total map $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$, we need this condition to hold everywhere, which is clearly the case when $|W|$ is an infinite cardinal. Now we have the following inequalities:

$$\text{rnk}(\bar{\sigma} \circ \mathcal{M}(\phi)) \leq \text{rnk}(\mathcal{M}(\phi)) = \text{rnk}(\phi) \leq |\text{Var}(\phi)| \leq |V|$$

It follows that a sufficient condition is $|V| \leq |W|$. This condition is in fact necessary when W is a finite set as it is not difficult to design a formula ϕ for which $\text{rnk}(\bar{\sigma} \circ \mathcal{M}(\phi)) = n$ for any $n \leq |V|$. So here we are: the notion of *substitution rank* gives us the insight we need to understand why the condition

($|W|$ infinite) $\vee$ ($|V| \leq |W|$) is equivalent to the existence of essential substitutions $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ associated to $\sigma : V \to W$. For those who are surprised by the fact that this condition makes no allowance for the specifics of the map $\sigma : V \to W$, one should remember that an *essential substitution of variables* has no impact on closed formulas, modulo α-equivalence. So if a closed formula needs many variables to be expressed in $\mathbf{P}(V)$, it needs an equal number of variables to exist in $\mathbf{P}(W)$. We are now ready to move on and quote:

Definition 93 *Let V be a set and $\sim$ be the substitution congruence on $\mathbf{\Pi}(V)$. For all $\pi \in \mathbf{\Pi}(V)$ we call* substitution rank *of π the integer* $\mathrm{rnk}(\pi)$ *defined by:*

$$\mathrm{rnk}(\pi) = \min\{\, |\mathrm{Var}(\rho)| \ :\ \rho \in \mathbf{\Pi}(V)\ ,\ \pi \sim \rho \,\}$$

where $|\mathrm{Var}(\rho)|$ denotes the cardinal of the set $\mathrm{Var}(\rho)$*, for all $\rho \in \mathbf{\Pi}(V)$.*

Given a formula $\phi \in \mathbf{P}(V)$ the notation $\mathrm{rnk}(\phi)$ is potentially ambiguous. Since $\mathbf{P}(V) \subseteq \mathbf{\Pi}(V)$, it may refer to the usual $\mathrm{rnk}(\phi)$ of definition (41), or to the newly defined integer $\mathrm{rnk}(\pi)$ where $\pi = \phi$ of definition (92). Luckily, the two notions coincide as the following proposition shows:

Proposition 278 *Let V be a set and $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then:*

$$\mathrm{rnk}(\pi) = \mathrm{rnk}(\phi)$$

where $\mathrm{rnk}(\phi)$ *is the substitution rank of ϕ as per* definition (41)*.*

Proof
First we show $\mathrm{rnk}(\pi) \leq \mathrm{rnk}(\phi)$: so let $\psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$, where $\sim$ is also the substitution congruence on $\mathbf{P}(V)$. We need to show $\mathrm{rnk}(\pi) \leq |\mathrm{Var}(\psi)|$. However take $\rho = \psi$. Then ρ is a proof such that $\pi \sim \rho$. It follows from definition (92) that $\mathrm{rnk}(\pi) \leq |\mathrm{Var}(\rho)|$. So $\mathrm{rnk}(\pi) \leq |\mathrm{Var}(\psi)|$ as requested. We now show $\mathrm{rnk}(\phi) \leq \mathrm{rnk}(\pi)$: so let $\rho \in \mathbf{\Pi}(V)$ such that $\pi \sim \rho$. We need to show that $\mathrm{rnk}(\phi) \leq |\mathrm{Var}(\rho)|$. However from $\pi \sim \rho$ and theorem (24) of page 339, we see that ρ must be of the form $\rho = \psi$ for some $\psi \in \mathbf{P}(V)$ with $\phi \sim \psi$. From definition (41) we obtain $\mathrm{rnk}(\phi) \leq |\mathrm{Var}(\psi)|$. It follows that $\mathrm{rnk}(\phi) \leq |\mathrm{Var}(\rho)|$. .

Proposition 279 *Let V be a set and $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then:*

$$\mathrm{rnk}(\pi) = \mathrm{rnk}(\phi)$$

where $\mathrm{rnk}(\phi)$ *is the substitution rank of ϕ as per* definition (41)*.*

Proof
First we show $\mathrm{rnk}(\pi) \leq \mathrm{rnk}(\phi)$: so let $\psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$, where $\sim$ is also the substitution congruence on $\mathbf{P}(V)$. We need to show $\mathrm{rnk}(\pi) \leq |\mathrm{Var}(\psi)|$. However take $\rho = \partial\psi$. Then ρ is a proof such that $\pi \sim \rho$. It follows from definition (92) that $\mathrm{rnk}(\pi) \leq |\mathrm{Var}(\rho)|$. So $\mathrm{rnk}(\pi) \leq |\mathrm{Var}(\psi)|$ as requested. We now show $\mathrm{rnk}(\phi) \leq \mathrm{rnk}(\pi)$: so let $\rho \in \mathbf{\Pi}(V)$ such that $\pi \sim \rho$. We need to show that $\mathrm{rnk}(\phi) \leq |\mathrm{Var}(\rho)|$. However from $\pi \sim \rho$ and theorem (24) of page 339, we see that ρ must be of the form $\rho = \partial\psi$ for some $\psi \in \mathbf{P}(V)$ with $\phi \sim \psi$. From definition (41) we obtain $\mathrm{rnk}(\phi) \leq |\mathrm{Var}(\psi)|$. It follows that $\mathrm{rnk}(\phi) \leq |\mathrm{Var}(\rho)|$. .

The following proposition is the counterpart of proposition (103) :

Proposition 280 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$. Then, we have:*

$$|\mathrm{Fr}(\pi)| \leq \mathrm{rnk}(\pi) \leq |\mathrm{Var}(\pi)|$$

Proof
The inequality $\mathrm{rnk}(\pi) \leq |\mathrm{Var}(\pi)|$ follows immediately from definition (92). So it remains to show that $|\mathrm{Fr}(\pi)| \leq \mathrm{rnk}(\pi)$. So let $\rho \in \mathbf{\Pi}(V)$ such that $\pi \sim \rho$ where $\sim$ is the substitution congruence. We need to show $|\mathrm{Fr}(\pi)| \leq |\mathrm{Var}(\rho)|$. From proposition (258) we have $\mathrm{Fr}(\pi) = \mathrm{Fr}(\rho)$. Hence we need to show that $|\mathrm{Fr}(\rho)| \leq |\mathrm{Var}(\rho)|$ which follows from $\mathrm{Fr}(\rho) \subseteq \mathrm{Var}(\rho)$. **.**

The following proposition is the counterpart of proposition (104). It is the most important result of this section, as everything else depends on it. When attempting to prove anything about $\mathrm{rnk}(\pi)$, it is very important to find some representative $\rho \sim \pi$ such that $\mathrm{rnk}(\pi) = |\mathrm{Var}(\rho)|$. We know that such representative exists from definition (92). However, we usually want to find ρ while controlling the set $\mathrm{Var}(\rho)$. Since $\rho \sim \pi$ we have $\mathrm{Fr}(\rho) = \mathrm{Fr}(\pi)$ so we cannot control $\mathrm{Fr}(\rho)$. However, if $\mathrm{Fr}(\pi) \subseteq V_0$ for some $V_0 \subseteq V$, we can always find ρ such that $\mathrm{Var}(\rho) \subseteq V_0$ provided V_0 is a large enough set. If V_0 is too small to accommodate every variable of ρ, then we can find ρ such that $V_0 \subseteq \mathrm{Var}(\rho)$.

Proposition 281 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$ such that $\mathrm{Fr}(\pi) \subseteq V_0$ for some $V_0 \subseteq V$. Let $\sim$ denote the substitution congruence on $\mathbf{\Pi}(V)$. Then there exists $\rho \in \mathbf{\Pi}(V)$ such that $\pi \sim \rho$ and $|\mathrm{Var}(\rho)| = \mathrm{rnk}(\pi)$ such that:*

$$\begin{array}{ll} (i) & \mathrm{rnk}(\pi) \leq |V_0| \ \Rightarrow \ \mathrm{Var}(\rho) \subseteq V_0 \\ (ii) & |V_0| \leq \mathrm{rnk}(\pi) \ \Rightarrow \ V_0 \subseteq \mathrm{Var}(\rho) \end{array}$$

Proof
Without loss of generality, we may assume that $|\mathrm{Var}(\pi)| = \mathrm{rnk}(\pi)$. Indeed, suppose the proposition has been established with the additional assumption $|\mathrm{Var}(\pi)| = \mathrm{rnk}(\pi)$. We need to show it is then true in the general case. So given $V_0 \subseteq V$, consider $\pi \in \mathbf{\Pi}(V)$ such that $\mathrm{Fr}(\pi) \subseteq V_0$. From definition (92) there exists $\pi_1 \in \mathbf{\Pi}(V)$ such that $\pi \sim \pi_1$ with the equality $|\mathrm{Var}(\pi_1)| = \mathrm{rnk}(\pi)$. From proposition (258) we obtain $\mathrm{Fr}(\pi) = \mathrm{Fr}(\pi_1)$ and so $\mathrm{Fr}(\pi_1) \subseteq V_0$. Hence we see that π_1 satisfies the assumption of the proposition with the additional property $|\mathrm{Var}(\pi_1)| = \mathrm{rnk}(\pi_1)$. Having assumed the proposition is true in this case, we obtain the existence of $\rho \in \mathbf{\Pi}(V)$ such that $\pi_1 \sim \rho$, $|\mathrm{Var}(\rho)| = \mathrm{rnk}(\pi_1)$ and which satisfies (i) and (ii) where π is replaced by π_1. However $\mathrm{rnk}(\pi_1) = \mathrm{rnk}(\pi)$ and replacing π by π_1 in (i) and (ii) has no impact. So ρ satisfies (i) and (ii). Hence we have $\pi \sim \rho$ and $|\mathrm{Var}(\rho)| = \mathrm{rnk}(\pi)$ together with (i) and (ii) which establishes the proposition in the general case. So we now assume without loss of generality that $|\mathrm{Var}(\pi)| = \mathrm{rnk}(\pi)$ and $\mathrm{Fr}(\pi) \subseteq V_0$. We need to show the existence of $\rho \sim \pi$ such that $|\mathrm{Var}(\rho)| = |\mathrm{Var}(\pi)|$ and which satisfies (i) and (ii). Note that if $V = \emptyset$ then $V_0 = \emptyset$ and we can take $\rho = \pi$. So we assume $V \neq \emptyset$. We shall first consider the case when $\mathrm{rnk}(\pi) \leq |V_0|$ and show the existence of ρ such that $\mathrm{Var}(\rho) \subseteq V_0$. Since $\mathrm{Fr}(\pi) \subseteq V_0$ the set V_0 is the disjoint union of $\mathrm{Fr}(\pi)$

and $V_0 \setminus \mathrm{Fr}(\pi)$, giving us the equality $|V_0| = |\mathrm{Fr}(\pi)| + |V_0 \setminus \mathrm{Fr}(\pi)|$. Since we also have $|\mathrm{Var}(\pi)| = |\mathrm{Fr}(\pi)| + |\mathrm{Var}(\pi) \setminus \mathrm{Fr}(\pi)|$, we obtain from $|\mathrm{Var}(\pi)| \leq |V_0|$:

$$|\mathrm{Fr}(\pi)| + |\mathrm{Var}(\pi) \setminus \mathrm{Fr}(\pi)| \leq |\mathrm{Fr}(\pi)| + |V_0 \setminus \mathrm{Fr}(\pi)|$$

Since $|\mathrm{Fr}(\pi)|$ is a finite cardinal it follows that $|\mathrm{Var}(\pi) \setminus \mathrm{Fr}(\pi)| \leq |V_0 \setminus \mathrm{Fr}(\pi)|$. Hence, there is an injection mapping $i : \mathrm{Var}(\pi) \setminus \mathrm{Fr}(\pi) \to V_0 \setminus \mathrm{Fr}(\pi)$. Having assumed $V \neq \emptyset$ consider $x^* \in V$ and define the map $\sigma : V \to V$ as follows:

$$\forall u \in V \ , \ \sigma(u) = \begin{cases} u & \text{if} \quad u \in \mathrm{Fr}(\pi) \\ i(u) & \text{if} \quad u \in \mathrm{Var}(\pi) \setminus \mathrm{Fr}(\pi) \\ x^* & \text{if} \quad u \notin \mathrm{Var}(\pi) \end{cases}$$

Define $\rho = \sigma(\pi)$. It remains to show that ρ has the desired properties, namely that $\rho \sim \pi$, $|\mathrm{Var}(\rho)| = |\mathrm{Var}(\pi)|$ and $\mathrm{Var}(\rho) \subseteq V_0$. First we show $\rho \sim \pi$. Using proposition (257) it is sufficient to prove that σ is an admissible substitution for π. It is clear that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\pi)$. So it remains to show that σ is valid for π. From proposition (224) it is sufficient to prove that $\sigma_{|\mathrm{Var}(\pi)}$ is an injective map. So let $u, v \in \mathrm{Var}(\pi)$ such that $\sigma(u) = \sigma(v)$. We need to show that $u = v$. We shall distinguish four cases: first we assume that $u \in \mathrm{Fr}(\pi)$ and $v \in \mathrm{Fr}(\pi)$. Then the equality $\sigma(u) = \sigma(v)$ leads to $u = v$. Next we assume that $u \notin \mathrm{Fr}(\pi)$ and $v \notin \mathrm{Fr}(\pi)$. Then we obtain $i(u) = i(v)$ which also leads to $u = v$ since $i : \mathrm{Var}(\pi) \setminus \mathrm{Fr}(\pi) \to V_0 \setminus \mathrm{Fr}(\pi)$ is an injective map. So we now assume that $u \in \mathrm{Fr}(\pi)$ and $v \notin \mathrm{Fr}(\pi)$. Then from $\sigma(u) = \sigma(v)$ we obtain $u = i(v)$ which is in fact impossible since $u \in \mathrm{Fr}(\pi)$ and $i(v) \in V_0 \setminus \mathrm{Fr}(\pi)$. The last case $u \notin \mathrm{Fr}(\pi)$ and $v \in \mathrm{Fr}(\pi)$ is equally impossible which completes our proof of $\rho \sim \pi$. So we now prove that $|\mathrm{Var}(\rho)| = |\mathrm{Var}(\pi)|$. From proposition (201) we have $\mathrm{Var}(\rho) = \mathrm{Var}(\sigma(\pi)) = \sigma(\mathrm{Var}(\pi))$. So we need $|\sigma(\mathrm{Var}(\pi))| = |\mathrm{Var}(\pi)|$ which is clear since $\sigma_{|\mathrm{Var}(\pi)} : \mathrm{Var}(\pi) \to \sigma(\mathrm{Var}(\pi))$ is a bijection. So it remains to show that $\mathrm{Var}(\rho) \subseteq V_0$, or equivalently that $\sigma(\mathrm{Var}(\pi)) \subseteq V_0$. So let $u \in \mathrm{Var}(\pi)$. We need to show that $\sigma(u) \in V_0$. We shall distinguish two cases: first we assume that $u \in \mathrm{Fr}(\pi)$. Then $\sigma(u) = u$ and the property $\sigma(u) \in V_0$ follows from the inclusion $\mathrm{Fr}(\pi) \subseteq V_0$. Next we assume that $u \notin \mathrm{Fr}(\pi)$. Then we have $\sigma(u) = i(u) \in V_0 \setminus \mathrm{Fr}(\pi) \subseteq V_0$. So in the case when $\mathrm{rnk}(\pi) \leq |V_0|$ we have been able to prove the existence of ρ satisfying (i). In fact we claim that ρ also satisfies (ii). So let us assume that $|V_0| \leq \mathrm{rnk}(\pi)$. Then we must have $\mathrm{rnk}(\pi) = |V_0|$ and we need to show that $V_0 \subseteq \mathrm{Var}(\rho)$. However, we have $|\mathrm{Var}(\rho)| = \mathrm{rnk}(\pi)$ and consequently $|\mathrm{Var}(\rho)| = |V_0|$ together with $\mathrm{Var}(\rho) \subseteq V_0$. Two finite subsets ordered by inclusion and with the same cardinal must be equal. So $\mathrm{Var}(\rho) = V_0$. We now consider the case when $|V_0| < \mathrm{rnk}(\pi)$. We need to show the existence of $\rho \sim \pi$ such that $|\mathrm{Var}(\rho)| = |\mathrm{Var}(\pi)|$ satisfying (i) and (ii). In the case when $|V_0| < \mathrm{rnk}(\pi)$, (i) is vacuously true, so we simply need to ensure that $V_0 \subseteq \mathrm{Var}(\rho)$. Since $|V_0| < |\mathrm{Var}(\pi)|$ we obtain:

$$\begin{aligned} |V_0 \setminus \mathrm{Var}(\pi)| &= |V_0| - |V_0 \cap \mathrm{Var}(\pi)| \\ &< |\mathrm{Var}(\pi)| - |V_0 \cap \mathrm{Var}(\pi)| \\ &= |\mathrm{Var}(\pi) \setminus V_0| \end{aligned}$$

So there is an injective map $i : V_0 \setminus \mathrm{Var}(\pi) \to \mathrm{Var}(\pi) \setminus V_0$. Given $x^* \in V$, define:

$$\forall u \in V \ , \ \sigma(u) = \begin{cases} u & \text{if} \quad u \in \mathrm{Var}(\pi) \setminus i(\, V_0 \setminus \mathrm{Var}(\pi)\,) \\ i^{-1}(u) & \text{if} \quad u \in i(\, V_0 \setminus \mathrm{Var}(\pi)\,) \\ x^* & \text{if} \quad u \notin \mathrm{Var}(\pi) \end{cases}$$

Let $\rho = \sigma(\pi)$. It remains to show that $\rho \sim \pi$, $|\mathrm{Var}(\rho)| = |\mathrm{Var}(\pi)|$ and furthermore $V_0 \subseteq \mathrm{Var}(\rho)$. First we show that $\rho \sim \pi$. Using proposition (257) it is sufficient to prove that σ is an admissible substitution for π. So let $u \in \mathrm{Fr}(\pi)$. We need to show that $\sigma(u) = u$. So it is sufficient to prove that $u \notin i(\, V_0 \setminus \mathrm{Var}(\pi)\,)$ which follows from the fact that $u \in V_0$, itself a consequence of $\mathrm{Fr}(\pi) \subseteq V_0$. In order to show that σ is also valid for π, from proposition (224) it is sufficient to prove that σ is injective on $\mathrm{Var}(\pi)$. So let $u, v \in \mathrm{Var}(\pi)$ such that $\sigma(u) = \sigma(v)$. We need to prove that $u = v$. The only case when this may not be clear is when $\sigma(u) = u$ and $\sigma(v) = i^{-1}(v)$ or vice versa. So we assume that $u \in \mathrm{Var}(\pi) \setminus i(\, V_0 \setminus \mathrm{Var}(\pi)\,)$ and $v \in i(\, V_0 \setminus \mathrm{Var}(\pi)\,)$. Then we see that $\sigma(u) = u \in \mathrm{Var}(\pi)$ while $\sigma(v) = i^{-1}(v) \in V_0 \setminus \mathrm{Var}(\pi)$. So the equality $\sigma(u) = \sigma(v)$ is in fact impossible, which completes our proof of $\rho \sim \pi$. As before, the fact that $|\mathrm{Var}(\rho)| = |\mathrm{Var}(\pi)|$ follows from the injectivity of $\sigma_{|\mathrm{Var}(\pi)}$ and it remains to prove that $V_0 \subseteq \mathrm{Var}(\rho)$. So let $u \in V_0$ we need to show that $u \in \mathrm{Var}(\rho) = \sigma(\mathrm{Var}(\pi))$ and we shall distinguish two cases: first we assume that $u \in \mathrm{Var}(\pi)$. Since $u \in V_0$, it cannot be an element of $i(\, V_0 \setminus \mathrm{Var}(\pi)\,)$. It follows that $u \in \mathrm{Var}(\pi) \setminus i(\, V_0 \setminus \mathrm{Var}(\pi)\,)$ and thus $u = \sigma(u) \in \sigma(\mathrm{Var}(\pi)) = \mathrm{Var}(\rho)$. Next we assume that $u \in V_0 \setminus \mathrm{Var}(\pi)$. Then $i(u)$ is an element of $i(\, V_0 \setminus \mathrm{Var}(\pi)\,)$ and therefore $\sigma(i(u)) = i^{-1}(i(u)) = u$. Since $i(u)$ is an element of $\mathrm{Var}(\pi) \setminus V_0$ we conclude that $u = \sigma(i(u)) \in \sigma(\mathrm{Var}(\pi)) = \mathrm{Var}(\rho)$, which completes our proof. **.**

Just like it is for formulas, the substitution rank is invariant by injective substitution. The following proposition is the counterpart of proposition (105) :

Proposition 282 *Let V, W be sets and $\sigma : V \to W$ be a map. Then for all $\pi \in \mathbf{\Pi}(V)$, if $\sigma_{|\mathrm{Var}(\pi)}$ is an injective map, we have the equality:*

$$\mathrm{rnk}(\sigma(\pi)) = \mathrm{rnk}(\pi)$$

where $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ denotes the associated substitution mapping.

Proof
Let $\sigma : V \to W$ and $\pi \in \mathbf{\Pi}(V)$ such that $\sigma_{|\mathrm{Var}(\pi)}$ is an injective map. We need to show that $\mathrm{rnk}(\sigma(\pi)) = \mathrm{rnk}(\pi)$. First we shall show $\mathrm{rnk}(\sigma(\pi)) \leq \mathrm{rnk}(\pi)$. Using proposition (281) with $V_0 = \mathrm{Var}(\pi)$, since we have $\mathrm{Fr}(\pi) \subseteq \mathrm{Var}(\pi)$ and $\mathrm{rnk}(\pi) \leq |\mathrm{Var}(\pi)|$, there exists $\rho \in \mathbf{\Pi}(V)$ such that $\pi \sim \rho$, $|\mathrm{Var}(\rho)| = \mathrm{rnk}(\pi)$ and $\mathrm{Var}(\rho) \subseteq \mathrm{Var}(\pi)$. Having assumed σ is injective on $\mathrm{Var}(\pi)$, it is therefore injective on both $\mathrm{Var}(\pi)$ and $\mathrm{Var}(\rho)$. From proposition (224) it follows that σ is a valid substitution for both π and ρ. Hence from theorem (27) of page 350 we obtain $\sigma(\pi) \sim \sigma(\rho)$ and consequently using proposition (201) :

$$\mathrm{rnk}(\sigma(\pi)) \leq |\mathrm{Var}(\sigma(\rho))| = |\sigma(\mathrm{Var}(\rho))| = |\mathrm{Var}(\rho)| = \mathrm{rnk}(\pi)$$

So it remains to show that $\mathrm{rnk}(\pi) \leq \mathrm{rnk}(\sigma(\pi))$. If $V = \emptyset$ then $\mathrm{rnk}(\pi) = 0$ and we are done. So we may assume that $V \neq \emptyset$. So let $x^* \in V$ and define:

$$\forall u \in W \ , \ \tau(u) = \begin{cases} \sigma^{-1}(u) & \text{if} \quad u \in \sigma(\mathrm{Var}(\pi)) \\ x^* & \text{if} \quad u \notin \sigma(\mathrm{Var}(\pi)) \end{cases}$$

Then $\tau : W \to V$ is injective on $\mathrm{Var}(\sigma(\pi)) = \sigma(\mathrm{Var}(\pi))$ and hence:

$$\mathrm{rnk}(\ \tau(\sigma(\pi))\ ) \leq \mathrm{rnk}(\sigma(\pi))$$

So it suffices for us to show that $\tau \circ \sigma(\pi) = \pi$. From proposition (202) it is thus sufficient to show that $\tau \circ \sigma(x) = x$ for all $x \in \mathrm{Var}(\pi)$, which is clear. **.**

The following proposition is the counterpart of proposition (106) :

Proposition 283 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$. Then the proof π and its minimal transform have equal substitution rank, i.e.:*

$$\mathrm{rnk}(\mathcal{M}(\pi)) = \mathrm{rnk}(\pi)$$

Proof
Let $\sim$ denote the substitution congruence on $\mathbf{\Pi}(V)$ and $i : V \to \bar{V}$ be the inclusion map. From proposition (274) we have $\mathcal{M}(\pi) \sim i(\pi)$ and consequently $\mathrm{rnk}(\mathcal{M}(\pi)) = \mathrm{rnk}(i(\pi))$. So we need to show that $\mathrm{rnk}(i(\pi)) = \mathrm{rnk}(\pi)$ which follows from proposition (282) and the fact that $i : V \to \bar{V}$ is injective. **.**

The following proposition is the counterpart of proposition (107) :

Proposition 284 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\pi \in \mathbf{\Pi}(V)$. We assume that σ is valid for π and $\sigma_{|\mathrm{Fr}(\pi)}$ is an injective map. Then:*

$$\mathrm{rnk}(\sigma(\pi)) = \mathrm{rnk}(\pi)$$

where $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ denotes the associated substitution mapping.

Proof
We shall proceed in two steps: first we shall prove the proposition is true in the case when $W = V$. We shall then extend the result to arbitrary W. So let us assume $W = V$. Let $\sigma : V \to V$ valid for $\pi \in \mathbf{\Pi}(V)$ such that $\sigma_{|\mathrm{Fr}(\pi)}$ is an injective map. We need to show that $\mathrm{rnk}(\sigma(\pi)) = \mathrm{rnk}(\pi)$. If $V = \emptyset$ then $\sigma : V \to V$ is the map with empty domain, namely the empty set which is injective on $\mathrm{Var}(\pi) = \emptyset$ and $\mathrm{rnk}(\sigma(\pi)) = \mathrm{rnk}(\pi)$ follows from proposition (282). So we assume that $V \neq \emptyset$. The idea of the proof is to write $\sigma(\pi) = \tau_1 \circ \tau_0(\pi)$ where each substitution τ_0, τ_1 is rank preserving. Having assumed σ injective on $\mathrm{Fr}(\pi)$, we have the equality $|\sigma(\mathrm{Fr}(\pi)| = |\mathrm{Fr}(\pi)|$ and consequently:

$$\begin{aligned} |\mathrm{Var}(\pi) \setminus \mathrm{Fr}(\pi)| &= |\mathrm{Var}(\pi)| - |\mathrm{Fr}(\pi)| \\ &\leq |V| - |\mathrm{Fr}(\pi)| \\ &= |V| - |\,\sigma(\mathrm{Fr}(\pi))\,| \\ &= |\,V \setminus \sigma(\mathrm{Fr}(\pi))\,| \end{aligned}$$

So let $i : \mathrm{Var}(\pi) \setminus \mathrm{Fr}(\pi) \to V \setminus \sigma(\mathrm{Fr}(\pi))$ be an injective map. Let $x^* \in V$ and define the substitution $\tau_0 : V \to V$ as follows:

$$\forall x \in V \ , \ \tau_0(x) = \begin{cases} \sigma(x) & \text{if} \quad x \in \mathrm{Fr}(\pi) \\ i(x) & \text{if} \quad x \in \mathrm{Var}(\pi) \setminus \mathrm{Fr}(\pi) \\ x^* & \text{if} \quad x \notin \mathrm{Var}(\pi) \end{cases}$$

Let us accept for now that τ_0 is injective on $\mathrm{Var}(\pi)$. Then using proposition (282) we obtain $\mathrm{rnk}(\tau_0(\pi)) = \mathrm{rnk}(\pi)$. So consider $\tau_1 : V \to V$:

$$\forall u \in V \ , \ \tau_1(u) = \begin{cases} u & \text{if} \quad u \in \sigma(\mathrm{Fr}(\pi)) \\ \sigma \circ i^{-1}(u) & \text{if} \quad u \in i(\, \mathrm{Var}(\pi) \setminus \mathrm{Fr}(\pi)\,) \\ x^* & \text{otherwise} \end{cases}$$

Note that τ_1 is well defined since $\sigma(\mathrm{Fr}(\pi)) \cap i(\, \mathrm{Var}(\pi) \setminus \mathrm{Fr}(\pi)\,) = \emptyset$. So let us accept for now that τ_1 is admissible for $\tau_0(\pi)$. Then using proposition (257) we obtain $\tau_1 \circ \tau_0(\pi) \sim \tau_0(\pi)$ where $\sim$ is the substitution congruence on $\mathbf{\Pi}(V)$. Hence in particular we have $\mathrm{rnk}(\tau_1 \circ \tau_0(\pi)) = \mathrm{rnk}(\tau_0(\pi)) = \mathrm{rnk}(\pi)$. So in order to show that the proposition is true in the case when $W = V$, it remains to prove that τ_0 is injective on $\mathrm{Var}(\pi)$, τ_1 is admissible for $\tau_0(\pi)$ and furthermore that $\tau_1 \circ \tau_0(\pi) = \sigma(\pi)$. First we show that τ_0 is injective on $\mathrm{Var}(\pi)$. So let $x, y \in \mathrm{Var}(\pi)$ such that $\tau_0(x) = \tau_0(y)$. We need to show that $x = y$. We shall distinguish four cases: first we assume that $x \in \mathrm{Fr}(\pi)$ and $y \in \mathrm{Fr}(\pi)$. Then the equality $\tau_0(x) = \tau_0(y)$ leads to $\sigma(x) = \sigma(y)$. Having assumed $\sigma_{|\mathrm{Fr}(\pi)}$ is an injective map, we obtain $x = y$. Next we assume that $x \in \mathrm{Var}(\pi) \setminus \mathrm{Fr}(\pi)$ and $y \in \mathrm{Var}(\pi) \setminus \mathrm{Fr}(\pi)$. Then the equality $\tau_0(x) = \tau_0(y)$ leads to $i(x) = i(y)$ and consequently $x = y$. So we now assume that $x \in \mathrm{Fr}(\pi)$ and $y \in \mathrm{Var}(\pi) \setminus \mathrm{Fr}(\pi)$. Then $\tau_0(x) = \sigma(x) \in \sigma(\mathrm{Fr}(\pi))$ and $\tau_0(y) = i(y) \in V \setminus \sigma(\mathrm{Fr}(\pi))$. So the equality $\tau_0(x) = \tau_0(y)$ is in fact impossible. We show similarly that the final case $x \in \mathrm{Var}(\pi) \setminus \mathrm{Fr}(\pi)$ and $y \in \mathrm{Fr}(\pi)$ is also impossible which completes the proof that τ_0 is injective on $\mathrm{Var}(\pi)$. We shall now show that $\tau_1 \circ \tau_0(\pi) = \sigma(\pi)$. From proposition (202) it is sufficient to prove that $\tau_1 \circ \tau_0(x) = \sigma(x)$ for all $x \in \mathrm{Var}(\pi)$. We shall distinguish two cases: first we assume that $x \in \mathrm{Fr}(\pi)$. Then $\tau_0(x) = \sigma(x) \in \sigma(\mathrm{Fr}(\pi))$ and consequently $\tau_1 \circ \tau_0(x) = \sigma(x)$ as requested. Next we assume that $x \in \mathrm{Var}(\pi) \setminus \mathrm{Fr}(\pi)$. Then $\tau_0(x) = i(x) \in i(\, \mathrm{Var}(\pi) \setminus \mathrm{Fr}(\pi)\,)$ and consequently $\tau_1 \circ \tau_0(x) = \sigma \circ i^{-1}(i(x)) = \sigma(x)$. So it remains to show that τ_1 is admissible for $\tau_0(\pi)$, i.e. that it is valid for $\tau_0(\pi)$ and $\tau_1(u) = u$ for all $u \in \mathrm{Fr}(\tau_0(\pi))$. So let $u \in \mathrm{Fr}(\tau_0(\pi))$. We need to show that $\tau_1(u) = u$. So it is sufficient to prove that $u \in \sigma(\mathrm{Fr}(\pi))$. However from proposition (209) we have $\mathrm{Fr}(\tau_0(\pi)) \subseteq \tau_0(\mathrm{Fr}(\pi))$ and consequently there exists $x \in \mathrm{Fr}(\pi)$ such that $u = \tau_0(x) = \sigma(x)$. It follows that $u \in \sigma(\mathrm{Fr}(\pi))$ as requested and it remains to show that τ_1 is valid for $\tau_0(\pi)$. From proposition (226) it is sufficient to show that $\tau_1 \circ \tau_0$ is valid for π. However, having proved that $\tau_1 \circ \tau_0(\pi) = \sigma(\pi)$ from proposition (227) it is sufficient to prove that σ is valid for π which is in fact true by assumption. This completes our proof of the proposition in the case when $W = V$. We shall now prove the proposition in the general case. So we assume that $\sigma : V \to W$ is a map and $\pi \in \mathbf{\Pi}(V)$ is such that σ is valid for π

and $\sigma_{|\mathrm{Fr}(\pi)}$ is an injective map. We need to prove that $\mathrm{rnk}(\sigma(\pi)) = \mathrm{rnk}(\pi)$. Let U be the disjoint union of the sets V and W, specifically:

$$U = \{0\} \times V \uplus \{1\} \times W$$

Let $i : V \to U$ and $j : W \to U$ be the corresponding inclusion maps. Consider the proof $\pi^* = i(\pi) \in \mathbf{\Pi}(U)$ and let $\sigma^* : U \to U$ be defined as:

$$\forall u \in U \ , \ \sigma^*(u) = \begin{cases} j \circ \sigma(u) & \text{if} \quad u \in V \\ u & \text{if} \quad u \in W \end{cases}$$

Let us accept for now that σ^* is valid for π^* and that $\sigma^*_{|\mathrm{Fr}(\pi^*)}$ is an injective map. Having proved the proposition in the case when $W = V$, it can be applied to $\sigma^* : U \to U$ and $\pi^* \in \mathbf{\Pi}(U)$. Hence, since i and j are injective maps, using proposition (282) we obtain the following equalities:

$$\begin{array}{rcl} \mathrm{rnk}(\sigma(\pi)) & = & \mathrm{rnk}(j \circ \sigma(\pi)) \\ \text{A: to be proved} \ \rightarrow & = & \mathrm{rnk}(\sigma^*(\pi^*)) \\ \text{case } W = V \ \rightarrow & = & \mathrm{rnk}(\pi^*) \\ & = & \mathrm{rnk}(i(\pi)) \\ \text{prop. (282)} \ \rightarrow & = & \mathrm{rnk}(\pi) \end{array}$$

So it remains to show that $j \circ \sigma(\pi) = \sigma^*(\pi^*)$ and furthermore that σ^* is valid for π^* while $\sigma^*_{|\mathrm{Fr}(\pi^*)}$ is an injective map. First we show that $j \circ \sigma(\pi) = \sigma^*(\pi^*)$. Since $\pi^* = i(\pi)$ from proposition (202) it is sufficient to prove the equality $j \circ \sigma(u) = \sigma^* \circ i(u)$ for all $u \in \mathrm{Var}(\pi)$. So let $u \in \mathrm{Var}(\pi)$. In particular $u \in V$ and consequently $i(u) \in i(V) \subseteq U$. From the above definition of σ^* we obtain immediately $\sigma^*(i(u)) = j \circ \sigma(u)$ as requested. So we now prove that σ^* is valid for $\pi^* = i(\pi)$. Using proposition (226) it is sufficient to prove that $\sigma^* \circ i$ is valid for π. However, having proved that $\sigma^* \circ i(\pi) = j \circ \sigma(\pi)$, from proposition (227) it is sufficient to prove that $j \circ \sigma$ is valid for π. Having assumed that σ is valid for π, using proposition (226) once more it remains to show that j is valid for $\sigma(\pi)$ which follows from the injectivity of j and proposition (224). So it remains to prove that $\sigma^*_{|\mathrm{Fr}(\pi^*)}$ is an injective map. So let $u, v \in \mathrm{Fr}(\pi^*)$ such that $\sigma^*(u) = \sigma^*(v)$. We need to show that $u = v$. However since $\pi^* = i(\pi)$, from proposition (209) we have $\mathrm{Fr}(\pi^*) \subseteq i(\mathrm{Fr}(\pi))$. Hence, there exists $x, y \in \mathrm{Fr}(\pi)$ such that $u = i(x)$ and $v = i(y)$. Having proved that $j \circ \sigma = \sigma^* \circ i$ on $\mathrm{Var}(\pi)$, from the equality $\sigma^*(u) = \sigma^*(v)$ we obtain $j \circ \sigma(x) = j \circ \sigma(y)$. It follows from the injectivity of j that $\sigma(x) = \sigma(y)$. Having assumed that σ is injective on $\mathrm{Fr}(\pi)$ we conclude that $x = y$ and finally that $u = v$ as requested. **.**

The following proposition is the counterpart of proposition (108) :

Proposition 285 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$ of the form $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$. Then the substitution ranks of π, π_1 and π_2 satisfy the equality:*

$$\mathrm{rnk}(\pi) = \max(\, |\mathrm{Fr}(\pi)| \,,\, \mathrm{rnk}(\pi_1) \,,\, \mathrm{rnk}(\pi_2) \,)$$

Proof
First we show that $\max(\,|\mathrm{Fr}(\pi)|\,,\,\mathrm{rnk}(\pi_1)\,,\,\mathrm{rnk}(\pi_2)\,) \leq \mathrm{rnk}(\pi)$. From proposition (280) we already know that $|\mathrm{Fr}(\pi)| \leq \mathrm{rnk}(\pi)$. So it remains to show that $\mathrm{rnk}(\pi_1) \leq \mathrm{rnk}(\pi)$ and $\mathrm{rnk}(\pi_2) \leq \mathrm{rnk}(\pi)$. So let $\sim$ be the substitution congruence on $\mathbf{\Pi}(V)$ and $\rho \sim \pi$. We need to show that $\mathrm{rnk}(\pi_1) \leq |\mathrm{Var}(\rho)|$ and $\mathrm{rnk}(\pi_2) \leq |\mathrm{Var}(\rho)|$. However, from $\rho \sim \pi = \pi_1 \oplus \pi_2$ and theorem (24) of page 339 we see that ρ must be of the form $\rho = \rho_1 \oplus \rho_2$ where $\rho_1 \sim \pi_1$ and $\rho_2 \sim \pi_2$. Hence we have $\mathrm{rnk}(\pi_1) \leq |\mathrm{Var}(\rho_1)| \leq |\mathrm{Var}(\rho)|$ and similarly $\mathrm{rnk}(\pi_2) \leq |\mathrm{Var}(\rho_2)| \leq |\mathrm{Var}(\rho)|$. So it remains to show the inequality $\mathrm{rnk}(\pi) \leq \max(\,|\mathrm{Fr}(\pi)|\,,\,\mathrm{rnk}(\pi_1)\,,\,\mathrm{rnk}(\pi_2)\,)$. We shall distinguish two cases: first we assume that $\max(\mathrm{rnk}(\pi_1), \mathrm{rnk}(\pi_2)) \leq |\mathrm{Fr}(\pi)|$. Since $\mathrm{Fr}(\pi_1) \subseteq \mathrm{Fr}(\pi)$ and $\mathrm{Fr}(\pi_2) \subseteq \mathrm{Fr}(\pi)$ using proposition (281) we obtain the existence of $\rho_1 \sim \pi_1$ and $\rho_2 \sim \pi_2$ such that $|\mathrm{Var}(\rho_1)| = \mathrm{rnk}(\pi_1)$ and $|\mathrm{Var}(\rho_2)| = \mathrm{rnk}(\pi_2)$ with the inclusions $\mathrm{Var}(\rho_1) \subseteq \mathrm{Fr}(\pi)$ and $\mathrm{Var}(\rho_2) \subseteq \mathrm{Fr}(\pi)$. Since $\pi \sim \rho_1 \oplus \rho_2$:

$$\begin{array}{rcl} \mathrm{rnk}(\pi) & \leq & |\mathrm{Var}(\rho_1 \oplus \rho_2)| \\ & = & |\mathrm{Var}(\rho_1) \cup \mathrm{Var}(\rho_2)| \\ \mathrm{Var}(\rho_i) \subseteq \mathrm{Fr}(\pi) \;\rightarrow & \leq & |\mathrm{Fr}(\pi)| \\ & = & \max(\,|\mathrm{Fr}(\pi)|\,,\,\mathrm{rnk}(\pi_1)\,,\,\mathrm{rnk}(\pi_2)\,) \end{array}$$

Next we assume that $|\mathrm{Fr}(\pi)| \leq \max(\mathrm{rnk}(\pi_1), \mathrm{rnk}(\pi_2))$. We shall distinguish two further cases: first we assume that $\mathrm{rnk}(\pi_1) \leq \mathrm{rnk}(\pi_2)$. Since we have both $\mathrm{Fr}(\pi_2) \subseteq \mathrm{Fr}(\pi)$ and $|\mathrm{Fr}(\pi)| \leq \mathrm{rnk}(\pi_2)$, from proposition (281) we can find $\rho_2 \sim \pi_2$ such that $|\mathrm{Var}(\rho_2)| = \mathrm{rnk}(\pi_2)$ and $\mathrm{Fr}(\pi) \subseteq \mathrm{Var}(\rho_2)$. In particular we obtain the inclusion $\mathrm{Fr}(\pi_1) \subseteq \mathrm{Var}(\rho_2)$ and applying proposition (281) once more, from $\mathrm{rnk}(\pi_1) \leq \mathrm{rnk}(\pi_2) = |\mathrm{Var}(\rho_2)|$ we obtain the existence of $\rho_1 \sim \pi_1$ such that $|\mathrm{Var}(\rho_1)| = \mathrm{rnk}(\pi_1)$ and $\mathrm{Var}(\rho_1) \subseteq \mathrm{Var}(\rho_2)$. It follows that:

$$\begin{array}{rcl} \mathrm{rnk}(\pi) & \leq & |\mathrm{Var}(\rho_1 \oplus \rho_2)| \\ & = & |\mathrm{Var}(\rho_1) \cup \mathrm{Var}(\rho_2)| \\ \mathrm{Var}(\rho_1) \subseteq \mathrm{Var}(\rho_2) \;\rightarrow & = & |\mathrm{Var}(\rho_2)| \\ & = & \mathrm{rnk}(\pi_2) \\ & = & \max(\,|\mathrm{Fr}(\pi)|\,,\,\mathrm{rnk}(\pi_1)\,,\,\mathrm{rnk}(\pi_2)\,) \end{array}$$

The case $\mathrm{rnk}(\pi_2) \leq \mathrm{rnk}(\pi_1)$ is dealt with similarly. .

The following proposition is the counterpart of proposition (109) :

Proposition 286 *Let V be a set and $\pi \in \mathbf{\Pi}(V)$ of the form $\pi = \nabla x \pi_1$ where $\pi_1 \in \mathbf{\Pi}(V)$ and $x \in V$. Then the substitution ranks of π and π_1 satisfy:*

$$\mathrm{rnk}(\pi) = \mathrm{rnk}(\pi_1) + \epsilon$$

where $\epsilon \in 2 = \{0, 1\}$ is given by the equivalence $\epsilon = 1$ if and only if:

$$(\, x \notin \mathrm{Fr}(\pi_1)\,) \wedge (\,|\mathrm{Fr}(\pi_1)| = \mathrm{rnk}(\pi_1)\,)$$

Proof
Let $\pi = \nabla x \pi_1$ where $\pi_1 \in \mathbf{\Pi}(V)$ and $x \in V$. Define $\epsilon = \mathrm{rnk}(\pi) - \mathrm{rnk}(\pi_1)$. Then ϵ is an integer, possibly negative. In order to prove that $\epsilon \in 2$ it is therefore sufficient to prove that the following inequalities hold:

$$\mathrm{rnk}(\pi_1) \leq \mathrm{rnk}(\pi) \leq \mathrm{rnk}(\pi_1) + 1 \tag{3.51}$$

This will be the first part of our proof. Next we shall show the equivalence:

$$(\epsilon = 1) \;\Leftrightarrow\; (\, x \notin \mathrm{Fr}(\pi_1)\,) \wedge (\, |\mathrm{Fr}(\pi_1)| = \mathrm{rnk}(\pi_1)\,) \tag{3.52}$$

So first we show that $\mathrm{rnk}(\pi_1) \leq \mathrm{rnk}(\pi)$. Let $\rho \sim \pi$ where $\sim$ denotes the substitution congruence on $\mathbf{\Pi}(V)$. We need to show that $\mathrm{rnk}(\pi_1) \leq |\mathrm{Var}(\rho)|$. Using theorem (24) of page 339, from the equivalence $\rho \sim \pi$ we see that ρ is either of the form $\rho = \nabla x \rho_1$ where $\rho_1 \sim \pi_1$, or ρ is of the form $\rho = \nabla y \rho_1$ where $\rho_1 \sim \pi_1[y:x]$, $x \neq y$ and $y \notin \mathrm{Fr}(\pi_1)$. First we assume that $\rho = \nabla x \rho_1$ where $\rho_1 \sim \pi_1$. Then we have the following inequalities:

$$\begin{aligned} \mathrm{rnk}(\pi_1) &\leq |\mathrm{Var}(\rho_1)| \\ &\leq |\{x\} \cup \mathrm{Var}(\rho_1)| \\ &= |\mathrm{Var}(\nabla x \rho_1)| \\ &= |\mathrm{Var}(\rho)| \end{aligned}$$

Next we assume that $\rho = \nabla y \rho_1$ where $\rho_1 \sim \pi_1[y:x]$, $x \neq y$ and $y \notin \mathrm{Fr}(\pi_1)$. The permutation $[y:x]$ being injective, from proposition (260) we obtain $\rho_1^* \sim \pi_1$ where $\rho_1^* = \rho_1[y:x]$. Furthermore, defining $\rho^* = \nabla x \rho_1^*$ we have $\rho = \rho^*[y:x]$. Using the injectivity of $[y:x]$ once more and proposition (201) we obtain:

$$|\mathrm{Var}(\rho)| = |\mathrm{Var}(\rho^*[y:x])| = |\,[y:x](\mathrm{Var}(\rho^*))\,| = |\mathrm{Var}(\rho^*)|$$

So we need to prove that $\mathrm{rnk}(\pi_1) \leq |\mathrm{Var}(\rho^*)|$ where $\rho^* = \nabla x \rho_1^*$ and $\rho_1^* \sim \pi_1$. Hence we are back to our initial case and we have proved that $\mathrm{rnk}(\pi_1) \leq \mathrm{rnk}(\pi)$. Next we show that $\mathrm{rnk}(\pi) \leq \mathrm{rnk}(\pi_1) + 1$. So let $\rho_1 \sim \pi_1$. We need to show that $\mathrm{rnk}(\pi) - 1 \leq |\mathrm{Var}(\rho_1)|$ or equivalently that $\mathrm{rnk}(\pi) \leq |\mathrm{Var}(\rho_1)| + 1$:

$$\begin{aligned} \mathrm{rnk}(\pi) &= \mathrm{rnk}(\nabla x \pi_1) \\ \nabla x \pi_1 \sim \nabla x \rho_1 \;\rightarrow\; &\leq |\mathrm{Var}(\nabla x \rho_1)| \\ &= |\{x\} \cup \mathrm{Var}(\rho_1)| \\ &\leq |\mathrm{Var}(\rho_1)| + 1 \end{aligned}$$

So we are done proving the inequalities (3.51). We shall complete the proof of this proposition by showing the equivalence (3.52). First we show $\Rightarrow$: so we assume that $\epsilon = 1$. We need to show that $x \notin \mathrm{Fr}(\pi_1)$ and furthermore that $|\mathrm{Fr}(\pi_1)| = \mathrm{rnk}(\pi_1)$. First we show that $x \notin \mathrm{Fr}(\pi_1)$. So suppose to the contrary that $x \in \mathrm{Fr}(\pi_1)$. We shall obtain a contradiction by showing $\epsilon = 0$, that is $\mathrm{rnk}(\pi_1) = \mathrm{rnk}(\pi)$. We already know that $\mathrm{rnk}(\pi_1) \leq \mathrm{rnk}(\pi)$. So we

need to show that $\mathrm{rnk}(\pi) \leq \mathrm{rnk}(\pi_1)$. So let $\rho_1 \sim \pi_1$. We need to show that $\mathrm{rnk}(\pi) \leq |\mathrm{Var}(\rho_1)|$. However, from $\rho_1 \sim \pi_1$ and proposition (258) we obtain $\mathrm{Fr}(\rho_1) = \mathrm{Fr}(\pi_1)$ and in particular $x \in \mathrm{Fr}(\rho_1)$. It follows that:

$$\begin{array}{rcl} \mathrm{rnk}(\pi) & = & \mathrm{rnk}(\nabla x \pi_1) \\ \nabla x \pi_1 \sim \nabla x \rho_1 \ \rightarrow & \leq & |\mathrm{Var}(\nabla x \rho_1)| \\ & = & |\{x\} \cup \mathrm{Var}(\rho_1)| \\ x \in \mathrm{Fr}(\rho_1) \subseteq \mathrm{Var}(\rho_1) \ \rightarrow & = & |\mathrm{Var}(\rho_1)| \end{array}$$

This is our desired contradiction and we conclude that $x \notin \mathrm{Fr}(\pi_1)$. It remains to show that $|\mathrm{Fr}(\pi_1)| = \mathrm{rnk}(\pi_1)$. So suppose this equality does not hold. We shall obtain a contradiction by showing $\epsilon = 0$, that is $\mathrm{rnk}(\pi) \leq \mathrm{rnk}(\pi_1)$. So let $\rho_1 \sim \pi_1$. We need to show once again that $\mathrm{rnk}(\pi) \leq |\mathrm{Var}(\rho_1)|$. However, having assumed the equality $|\mathrm{Fr}(\pi_1)| = \mathrm{rnk}(\pi_1)$ does not hold, from proposition (280) we obtain $|\mathrm{Fr}(\pi_1)| < \mathrm{rnk}(\pi_1)$ and consequently from $\rho_1 \sim \pi_1$ we have:

$$|\mathrm{Fr}(\rho_1)| = |\mathrm{Fr}(\pi_1)| < \mathrm{rnk}(\pi_1) \leq |\mathrm{Var}(\rho_1)|$$

It follows that the set $\mathrm{Var}(\rho_1) \setminus \mathrm{Fr}(\rho_1)$ cannot be empty, and there exists $y \in \mathrm{Var}(\rho_1) \setminus \mathrm{Fr}(\rho_1)$. From $x \notin \mathrm{Fr}(\pi_1)$ and $y \notin \mathrm{Fr}(\rho_1) = \mathrm{Fr}(\pi_1)$ using proposition (259) we obtain the equivalence $\nabla x \pi_1 \sim \nabla y \pi_1$. Hence we also have the equivalence $\nabla x \pi_1 \sim \nabla y \rho_1$ and consequently:

$$\begin{array}{rcl} \mathrm{rnk}(\pi) & = & \mathrm{rnk}(\nabla x \pi_1) \\ \nabla x \pi_1 \sim \nabla y \rho_1 \ \rightarrow & \leq & |\mathrm{Var}(\nabla y \rho_1)| \\ & = & |\{y\} \cup \mathrm{Var}(\rho_1)| \\ y \in \mathrm{Var}(\rho_1) \ \rightarrow & = & |\mathrm{Var}(\rho_1)| \end{array}$$

which is our desired contradiction and we conclude that $|\mathrm{Fr}(\pi_1)| = \mathrm{rnk}(\pi_1)$. This completes our proof of $\Rightarrow$ in the equivalence (3.52). We now prove $\Leftarrow$: so we assume that $x \notin \mathrm{Fr}(\pi_1)$ and $|\mathrm{Fr}(\pi_1)| = \mathrm{rnk}(\pi_1)$. We need to show that $\epsilon = 1$, that is $\mathrm{rnk}(\pi) = \mathrm{rnk}(\pi_1) + 1$. We already have $\mathrm{rnk}(\pi) \leq \mathrm{rnk}(\pi_1) + 1$. So it remains to show that $\mathrm{rnk}(\pi_1) + 1 \leq \mathrm{rnk}(\pi)$ or equivalently $\mathrm{rnk}(\pi_1) < \mathrm{rnk}(\pi)$. So let $\rho \sim \pi$. We need to show that $\mathrm{rnk}(\pi_1) < |\mathrm{Var}(\rho)|$. Once again, using theorem (24) of page 339, from the equivalence $\rho \sim \pi$ we see that ρ is either of the form $\rho = \nabla x \rho_1$ where $\rho_1 \sim \pi_1$, or ρ is of the form $\rho = \nabla y \rho_1$ where $\rho_1 \sim \pi_1[y:x]$, $x \neq y$ and $y \notin \mathrm{Fr}(\pi_1)$. First we assume that $\rho = \nabla x \rho_1$ where $\rho_1 \sim \pi_1$. Hence $\mathrm{rnk}(\pi_1) \leq |\mathrm{Var}(\rho_1)|$ and we shall distinguish two further cases: first we assume that $\mathrm{rnk}(\pi_1) = |\mathrm{Var}(\rho_1)|$. Having assumed that $|\mathrm{Fr}(\pi_1)| = \mathrm{rnk}(\pi_1)$ we obtain:

$$|\mathrm{Fr}(\rho_1)| = |\mathrm{Fr}(\pi_1)| = \mathrm{rnk}(\pi_1) = |\mathrm{Var}(\rho_1)|$$

from which we see that $\mathrm{Var}(\rho_1) = \mathrm{Fr}(\rho_1)$ and consequently it follows that $x \notin \mathrm{Fr}(\pi_1) = \mathrm{Fr}(\rho_1) = \mathrm{Var}(\rho_1)$. Hence we see that:

$$\mathrm{rnk}(\pi_1) \leq |\mathrm{Var}(\rho_1)|$$

$$\begin{array}{rcl} x \notin \mathrm{Var}(\rho_1) \ \rightarrow & < & |\{x\} \cup \mathrm{Var}(\rho_1)| \\ & = & |\mathrm{Var}(\nabla x \rho_1)| \\ & = & |\mathrm{Var}(\rho)| \end{array}$$

So we now assume that $\mathrm{rnk}(\pi_1) < |\mathrm{Var}(\rho_1)|$, in which case we obtain:

$$\begin{array}{rcl} \mathrm{rnk}(\pi_1) & < & |\mathrm{Var}(\rho_1)| \\ & \leq & |\{x\} \cup \mathrm{Var}(\rho_1)| \\ & = & |\mathrm{Var}(\nabla x \rho_1)| \\ & = & |\mathrm{Var}(\rho)| \end{array}$$

We now consider the case when $\rho = \nabla y \rho_1$ where $\rho_1 \sim \pi_1[y:x]$, $x \neq y$ and $y \notin \mathrm{Fr}(\pi_1)$. Once again, defining $\rho_1^* = \rho_1[y:x]$ and $\rho^* = \nabla x \rho_1^*$ we obtain the equivalence $\rho_1^* \sim \pi_1$ and $|\mathrm{Var}(\rho^*)| = |\mathrm{Var}(\rho)|$. So we need to prove that $\mathrm{rnk}(\pi_1) < |\mathrm{Var}(\rho^*)|$ knowing that $\rho_1^* \sim \pi_1$ which follows from our initial case. .

As already discussed at the start of this section, the existence of essential substitutions crucially relies on the inequality $\mathrm{rnk}(\bar{\sigma} \circ \mathcal{M}(\pi)) \leq |W|$. The following proposition allows us to write $\mathrm{rnk}(\bar{\sigma} \circ \mathcal{M}(\pi)) \leq \mathrm{rnk}(\mathcal{M}(\pi))$. Since we know from proposition (283) that $\mathrm{rnk}(\mathcal{M}(\pi)) = \mathrm{rnk}(\pi)$ we finally obtain $\mathrm{rnk}(\bar{\sigma} \circ \mathcal{M}(\pi)) \leq \mathrm{rnk}(\pi)$, which gives us the sufficient condition $\mathrm{rnk}(\pi) \leq |W|$. Note that the result makes no use of the fact that $\bar{\sigma}$ is valid for $\mathcal{M}(\pi)$, and the inequality $\mathrm{rnk}(\sigma(\pi)) \leq \mathrm{rnk}(\pi)$ is always true, regardless of whether σ is valid for π. The following proposition is the counterpart of proposition (110) :

Proposition 287 *Let V, W be sets and $\sigma : V \rightarrow W$ be a map. Let $\pi \in \mathbf{\Pi}(V)$:*

$$\mathrm{rnk}(\sigma(\pi)) \leq \mathrm{rnk}(\pi)$$

where $\sigma : \mathbf{\Pi}(V) \rightarrow \mathbf{\Pi}(W)$ is the associated proof substitution mapping.

Proof
We shall prove $\mathrm{rnk}(\sigma(\pi)) \leq \mathrm{rnk}(\pi)$ by structural induction using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then the inequality follows from proposition (110). We now assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. Then using proposition (110) once more together with proposition (279) :

$$\begin{array}{rcl} \mathrm{rnk}(\sigma(\pi)) & = & \mathrm{rnk}(\sigma(\partial\phi)) \\ & = & \mathrm{rnk}(\partial\sigma(\phi)) \\ \text{prop. (279)} \ \rightarrow & = & \mathrm{rnk}(\sigma(\phi)) \\ \text{prop. (110)} \ \rightarrow & \leq & \mathrm{rnk}(\phi) \\ \text{prop. (279)} \ \rightarrow & = & \mathrm{rnk}(\partial\phi) \\ & = & \mathrm{rnk}(\pi) \end{array}$$

So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ satisfy our property:

$$\begin{array}{rcl} \mathrm{rnk}(\sigma(\pi)) & = & \mathrm{rnk}(\sigma(\pi_1 \oplus \pi_2)) \\ & = & \mathrm{rnk}(\sigma(\pi_1) \oplus \sigma(\pi_2)) \\ \text{prop. (285)} \ \rightarrow & = & \max(\,|\,\mathrm{Fr}(\sigma(\pi))\,|\,,\, \mathrm{rnk}(\sigma(\pi_1))\,,\, \mathrm{rnk}(\sigma(\pi_2))\,) \\ & \leq & \max(\,|\,\mathrm{Fr}(\sigma(\pi))\,|\,,\, \mathrm{rnk}(\pi_1)\,,\, \mathrm{rnk}(\pi_2)\,) \\ \text{prop. (209)} \ \rightarrow & \leq & \max(\,|\,\sigma(\mathrm{Fr}(\pi))\,|\,,\, \mathrm{rnk}(\pi_1)\,,\, \mathrm{rnk}(\pi_2)\,) \\ & \leq & \max(\,|\mathrm{Fr}(\pi)|\,,\, \mathrm{rnk}(\pi_1)\,,\, \mathrm{rnk}(\pi_2)\,) \\ \text{prop. (285)} \ \rightarrow & = & \mathrm{rnk}(\pi) \end{array}$$

Finally we assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ satisfies our induction property. Then $\sigma(\pi) = \nabla \sigma(x) \sigma(\pi_1)$. Let $\epsilon = \mathrm{rnk}(\pi) - \mathrm{rnk}(\pi_1)$ and let $\eta = \mathrm{rnk}(\sigma(\pi)) - \mathrm{rnk}(\sigma(\pi_1))$. From proposition (286) we know that $\epsilon, \eta \in 2$. We shall distinguish two cases: first we assume that $\eta = 0$. Then we have:

$$\mathrm{rnk}(\sigma(\pi)) = \mathrm{rnk}(\sigma(\pi_1)) \leq \mathrm{rnk}(\pi_1) \leq \mathrm{rnk}(\pi)$$

Next we assume that $\eta = 1$. We shall distinguish two further cases: if $\epsilon = 1$:

$$\mathrm{rnk}(\sigma(\pi)) = 1 + \mathrm{rnk}(\sigma(\pi_1)) \leq 1 + \mathrm{rnk}(\pi_1) = \mathrm{rnk}(\pi)$$

So it remains to deal with the last possibility when $\eta = 1$ and $\epsilon = 0$. Using proposition (286), from $\epsilon = 0$ we see that $x \in \mathrm{Fr}(\pi_1)$ or $|\mathrm{Fr}(\pi_1)| < \mathrm{rnk}(\pi_1)$. So we shall distinguish two further cases. These cases may not be exclusive of one another but we don't need them to be. So first we assume $x \in \mathrm{Fr}(\pi_1)$. Using proposition (286) again, from $\eta = 1$ we obtain $|\mathrm{Fr}(\sigma(\pi_1))| = \mathrm{rnk}(\sigma(\pi_1))$ and furthermore $\sigma(x) \notin \mathrm{Fr}(\sigma(\pi_1))$. Having assumed that $x \in \mathrm{Fr}(\pi_1)$ it follows that $\sigma(x)$ is an element of $\sigma(\mathrm{Fr}(\pi_1))$ but not an element of $\mathrm{Fr}(\sigma(\pi_1))$. Hence, we see that the inclusion $\mathrm{Fr}(\sigma(\pi_1)) \subseteq \sigma(\mathrm{Fr}(\pi_1))$ which we know is true from proposition (209) is in fact a strict inclusion. So we have a strict inequality between the finite cardinals $|\mathrm{Fr}(\sigma(\pi_1))| < |\sigma(\mathrm{Fr}(\pi_1))|$. Thus:

$$\begin{array}{rcl} \mathrm{rnk}(\sigma(\pi)) & = & 1 + \mathrm{rnk}(\sigma(\pi_1)) \\ |\mathrm{Fr}(\sigma(\pi_1))| = \mathrm{rnk}(\sigma(\pi_1)) \ \rightarrow & = & 1 + |\mathrm{Fr}(\sigma(\pi_1))| \\ |\mathrm{Fr}(\sigma(\pi_1))| < |\sigma(\mathrm{Fr}(\pi_1))| \ \rightarrow & \leq & |\sigma(\mathrm{Fr}(\pi_1))| \\ & \leq & |\mathrm{Fr}(\pi_1)| \\ \text{prop. (280)} \ \rightarrow & \leq & \mathrm{rnk}(\pi_1) \\ \epsilon = 0 \ \rightarrow & = & \mathrm{rnk}(\pi) \end{array}$$

So we now assume that $|\mathrm{Fr}(\pi_1)| < \mathrm{rnk}(\pi_1)$. In this case we have:

$$\begin{array}{rcl} \mathrm{rnk}(\sigma(\pi)) & = & 1 + \mathrm{rnk}(\sigma(\pi_1)) \\ |\mathrm{Fr}(\sigma(\pi_1))| = \mathrm{rnk}(\sigma(\pi_1)) \ \rightarrow & = & 1 + |\mathrm{Fr}(\sigma(\pi_1))| \\ \text{prop. (209)} \ \rightarrow & \leq & 1 + |\sigma(\mathrm{Fr}(\pi_1))| \\ & \leq & 1 + |\mathrm{Fr}(\pi_1)| \\ |\mathrm{Fr}(\pi_1)| < \mathrm{rnk}(\pi_1) \ \rightarrow & \leq & \mathrm{rnk}(\pi_1) \\ \epsilon = 0 \ \rightarrow & = & \mathrm{rnk}(\pi) \end{array}$$

.

This completes our study of substitution ranks for proofs. We are now ready to prove the existence of essential substitutions $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ associated with $\sigma : V \to W$. This will be done in the following section.

3.5.2 Existence of Essential Substitution

An essential substitution $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ associated with a map $\sigma : V \to W$ is the sharpest tool so far created in these notes. First order logic is plagued with the annoying glitch of variable capture. Most texts in mathematical logic will simply ignore the problem and ask the reader to accept that every mathematical argument involving variable substitution is sound and preserves α-equivalence. There are two issues with this approach: on the one hand, the reader cannot formally check the arguments presented to him and must instead resort to some form of informal mathematical intuition to accept the proof presented to him in good faith, thinking 'yes, this is probably correct, modulo α-equivalence'. On the other hand, as discussed prior to definition (62), the informal approach of implicitly renaming variables where needed, or simply rejecting substitutions which are not capture-avoiding cannot work in the context of first order logic with finitely many variables. Our purpose is to study the language $\mathcal{L} = \{\in\}$ which is the language of **ZF** without equality, and to do so with a set of variables V of arbitrary cardinality. We are of course sceptical that a cardinality beyond $\aleph_0$ will bring anything interesting, but we certainly think that fragments of first order logic with finitely many variables are worthy of attention. In any case, we are looking for a unified approach in our study of the free algebra $\mathbf{P}(V)$, that is an approach which makes no assumption on the cardinality of V. In this context, the ability to substitute variables while avoiding capture is tantamount and the introduction of essential substitutions $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ in definition (42) has proved invaluable. In particular, it has allowed us to present an axiomatization of first order logic with specialization axioms $\forall x \phi_1 \to \phi_1[y/x]$ which have no caveats on variable capture. As discussed prior to definition (62) this is a key fact to ensure completeness of the system with finitely many variables.

The ability to substitute variables in proofs while avoiding capture will also be very useful. In fact, a first application of essential substitutions for proofs will be given in theorem (30) of page 388 allowing us to carry over sequents from $\Gamma \vdash \phi$ into $\sigma(\Gamma) \vdash \sigma(\phi)$ for every essential substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ and no other assumption. In this section, we shall prove the existence of essential substitutions $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ associated with a map $\sigma : V \to W$ with the usual conditions on the cardinals $|V|$ and $|W|$ as can be seen from theorem (29) of page 375 below. We shall literally follow the steps which were used prior to theorem (18) of page 174. As we have said on a few occasions before, it is rather shameful to *cut-and-paste* existing proofs with no effort to bring about a unified abstract approach. On the positive side, this allowed us to get the result quickly and safely, and we can move on to worry about other things.

Definition 94 *Let V, W be sets and $\sigma : V \to W$ be a map. We call* essential proof substitution mapping *associated with σ, a map $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ with:*

$$\mathcal{M} \circ \sigma^* = \bar{\sigma} \circ \mathcal{M} \tag{3.53}$$

where $\bar{\sigma} : \bar{V} \to \bar{W}$ is the minimal extension and $\mathcal{M}$ is the minimal transform.

Suppose $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ is an essential substitution associated to the map $\sigma : V \to W$. Since $\mathbf{P}(V) \subseteq \mathbf{\Pi}(V)$, it is meaningful to consider the restriction $(\sigma^*)_{|\mathbf{P}(V)}$ with domain $\mathbf{P}(V)$. Since the equality $\mathcal{M} \circ \sigma^*(\pi) = \bar{\sigma} \circ \mathcal{M}(\pi)$ holds for all $\pi \in \mathbf{\Pi}(V)$, in particular we have $\mathcal{M} \circ \sigma^*(\phi) = \bar{\sigma} \circ \mathcal{M}(\phi)$ for all $\phi \in \mathbf{P}(V)$. So it is very tempting to conclude that the restriction $(\sigma^*)_{|\mathbf{P}(V)}$ is an essential substitution associated with $\sigma : V \to W$ in the sense of definition (42). This conclusion is correct. However, it is not completely obvious that $\sigma^*(\phi)$ should be an element of $\mathbf{P}(W)$ for all $\phi \in \mathbf{P}(V)$. The following proposition checks this is indeed the case, so $(\sigma^*)_{|\mathbf{P}(V)} : \mathbf{P}(V) \to \mathbf{P}(W)$ is essential.

Proposition 288 *Let V, W be sets and $\sigma : V \to W$ be a map. We assume that $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ is an essential proof substitution associated with σ. Then the restriction $(\sigma^*)_{|\mathbf{P}(V)}$ is an essential substitution associated with σ.*

Proof
We assume that $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ is a map which satisfies the equality $\mathcal{M} \circ \sigma^*(\pi) = \bar{\sigma} \circ \mathcal{M}(\pi)$ for all $\pi \in \mathbf{\Pi}(V)$. Then in particular for all $\phi \in \mathbf{P}(V)$ we have $\mathcal{M} \circ \sigma^*(\phi) = \bar{\sigma} \circ \mathcal{M}(\phi)$. So it remains to check that the restriction $(\sigma^*)_{|\mathbf{P}(V)}$ is indeed a map $(\sigma^*)_{|\mathbf{P}(V)} : \mathbf{P}(V) \to \mathbf{P}(W)$. So we need to show that $\sigma^*(\phi) \in \mathbf{P}(W)$ for all $\phi \in \mathbf{P}(V)$. However we have $\mathcal{M} \circ \sigma^*(\phi) \in \mathbf{P}(\bar{W})$. Furthermore, we know from theorem (2) of page 21 that the proof $\sigma^*(\phi)$ can only be of four types, namely $\sigma^*(\phi) = \psi$ for some $\psi \in \mathbf{P}(W)$ or $\sigma^*(\phi) = \partial\psi$ or $\sigma^*(\phi) = \rho_1 \oplus \rho_2$ or $\sigma^*(\phi) = \nabla u \rho_1$. Looking at definition (87) the minimal transform $\mathcal{M} \circ \sigma^*(\phi)$ has essentially the same type as $\sigma^*(\phi)$. Thus from $\mathcal{M} \circ \sigma^*(\phi) \in \mathbf{P}(\bar{W})$ and the uniqueness property of theorem (2) we conclude that $\sigma^*(\phi)$ must be of the form $\sigma^*(\phi) = \psi$ for some $\psi \in \mathbf{P}(W)$. **.**

We shall now follow the trail of what was done for formulas. The following definition is the counterpart of definition (43), prior to which the reader may find some motivating comments and a description of the proof strategy. Note that the maps $p : \bar{\bar{V}} \to \bar{V}$ of definition (43) and definition (94) below are actually the same. Furthermore given $\phi \in \mathbf{P}(\bar{V})$, since $\mathbf{P}(\bar{V}) \subseteq \mathbf{\Pi}(\bar{V})$ the notation $\mathcal{N}(\phi)$ is potentially ambiguous as it may refer to the weak transform of definition (43), or to this new weak transform for proofs of definition (94) below. Luckily, the two notions coincide as they do for minimal transforms.

Definition 95 *Let V be a set. We call* weak transform *on $\mathbf{\Pi}(\bar{V})$ the map $\mathcal{N} : \mathbf{\Pi}(\bar{V}) \to \mathbf{\Pi}(\bar{V})$ defined by $\mathcal{N} = p \circ \bar{\mathcal{M}}$ where $\bar{\mathcal{M}} : \mathbf{\Pi}(\bar{V}) \to \mathbf{\Pi}(\bar{\bar{V}})$ is the minimal transform mapping and $p : \bar{\bar{V}} \to \bar{V}$ is defined by:*

$$\forall u \in \bar{\bar{V}} \ , \ p\,(u) = \begin{cases} u & \text{if} \quad u \in \bar{V} \\ n & \text{if} \quad u = \bar{n} \in \bar{\mathbf{N}} \end{cases}$$

The following lemma is the counterpart of lemma (12). It shows that the minimal transform can be defined from the weak transform and the inclusion map $i : V \to \bar{V}$ with $\mathcal{M} = \mathcal{N} \circ i = p \circ \bar{\mathcal{M}} \circ i$. For example, suppose π is the proof (formula) $\pi = \forall y(x \in y)$. Then $i(\pi) = \forall y(x \in y)$ now viewed as an element of $\mathbf{\Pi}(\bar{V})$. It follows that $\bar{\mathcal{M}} \circ i(\pi) = \forall\, \bar{0}(x \in \bar{0})$ and $p \circ \bar{\mathcal{M}} \circ i(\pi) = \forall\, 0(x \in 0)$ which is indeed the minimal transform of π. So let us quote:

Lemma 25 *Let V be a set and $\mathcal{N} : \mathbf{\Pi}(\bar{V}) \to \mathbf{\Pi}(\bar{V})$ be the weak transform on $\mathbf{\Pi}(\bar{V})$. Let $i : V \to \bar{V}$ be the inclusion map. Then we have:*

$$\mathcal{M} = \mathcal{N} \circ i$$

where $\mathcal{M} : \mathbf{\Pi}(V) \to \mathbf{\Pi}(\bar{V})$ is the minimal transform mapping.

Proof
Let $\bar{\mathcal{M}} : \mathbf{\Pi}(\bar{V}) \to \mathbf{\Pi}(\bar{\bar{V}})$ be the minimal transform mapping and $p : \bar{\bar{V}} \to \bar{V}$ be the map of definition (94). Given $\pi \in \mathbf{\Pi}(V)$, since $i : V \to \bar{V}$ is an injective map, in particular it is valid for π. Hence we have:

$$\begin{aligned} \mathcal{N} \circ i(\pi) &= p \circ \bar{\mathcal{M}} \circ i(\pi) \\ \text{theorem (23)} \ \to \ &= p \circ \bar{i} \circ \mathcal{M}(\pi) \\ \text{A: to be proved} \ \to \ &= \mathcal{M}(\pi) \end{aligned}$$

So it remains to show that $p \circ \bar{i}(u) = u$ for all $u \in \bar{V}$, where $\bar{i} : \bar{V} \to \bar{\bar{V}}$ is the minimal extension of i. So let $u \in \bar{V}$. We shall distinguish two cases: first we assume that $u \in V$. Then $\bar{i}(u) = i(u) = u$ and consequently $p \circ \bar{i}(u) = p\,(u) = u$ as requested. Next we assume that $u \in \mathbf{N}$. Then $\bar{i}(u) = \bar{u}$ and it follows that $p \circ \bar{i}(u) = p\,(\bar{u}) = u$, which completes our proof. Please refer to the proof of lemma (12) for a more detailed discussion on the step $\bar{i}(u) = \bar{u}$. **.**

The following lemma is the counterpart of lemma (13). It shows that the weak transform $\mathcal{N}$ has no effect when acting on $\bar{\sigma} \circ \mathcal{M}$. For example, suppose $\pi = \forall y(x \in y)$ and $\sigma = [y/x]$. Then $\bar{\sigma} \circ \mathcal{M}(\pi) = \forall\, 0(y \in 0)$. Taking the minimal transform $\bar{\mathcal{M}}$ we obtain $\bar{\mathcal{M}} \circ \bar{\sigma} \circ \mathcal{M}(\pi) = \forall\, \bar{0}(y \in \bar{0})$. Composing by p we conclude that $\mathcal{N} \circ \bar{\sigma} \circ \mathcal{M}(\pi) = \forall\, 0(y \in 0) = \bar{\sigma} \circ \mathcal{M}(\pi)$. More generally:

Lemma 26 *Let V, W be sets and $\sigma : V \to W$ be a map. Then:*

$$\mathcal{N} \circ \bar{\sigma} \circ \mathcal{M} = \bar{\sigma} \circ \mathcal{M}$$

where $\mathcal{N} : \mathbf{\Pi}(\bar{W}) \to \mathbf{\Pi}(\bar{W})$ is the weak transform on $\mathbf{\Pi}(\bar{W})$.

Proof
For once we shall be able to prove the formula without resorting to a structural induction argument. In the interest of lighter notations, we shall keep the same notations $\mathcal{M}, \bar{\mathcal{M}}, \mathcal{N}$ and p in relation to the sets V and W. So let $\pi \in \mathbf{\Pi}(V)$:

$$\mathcal{N} \circ \bar{\sigma} \circ \mathcal{M}(\pi) \quad = \quad p \circ \bar{\mathcal{M}} \circ \bar{\sigma} \circ \mathcal{M}(\pi)$$

$$\begin{aligned}
\text{theorem (23) of p. 327} \ \rightarrow \ &= \ p \circ \bar{\bar{\sigma}} \circ \bar{\mathcal{M}} \circ \mathcal{M}(\pi) \\
\text{prop. (274)} \ \rightarrow \ &= \ p \circ \bar{\bar{\sigma}} \circ \bar{\mathcal{M}} \circ i(\pi) \\
\text{A: to be proved} \ \rightarrow \ &= \ \bar{\sigma} \circ p \circ \bar{\mathcal{M}} \circ i(\pi) \\
&= \ \bar{\sigma} \circ \mathcal{N} \circ i(\pi) \\
\text{lemma (25)} \ \rightarrow \ &= \ \bar{\sigma} \circ \mathcal{M}(\pi)
\end{aligned}$$

So it remains to show that $p \circ \bar{\bar{\sigma}}(u) = \bar{\sigma} \circ p\,(u)$ for all $u \in \bar{\bar{V}}$. So let $u \in \bar{\bar{V}}$. Since $\bar{\bar{V}}$ is the disjoint union of $\bar{V}$ and $\bar{\mathbf{N}}$, we shall distinguish two cases: first we assume that $u \in \bar{V}$. Then $\bar{\bar{\sigma}}(u) = \bar{\sigma}(u) \in \bar{W}$ and consequently $p \circ \bar{\bar{\sigma}}(u) = \bar{\sigma}(u)$. So the equality $p \circ \bar{\bar{\sigma}}(u) = \bar{\sigma} \circ p\,(u)$ is satisfied since $p\,(u) = u$ for $u \in \bar{V}$. Next we assume that $u \in \bar{\mathbf{N}}$ i.e. that $u = \bar{n}$ for some $n \in \mathbf{N}$. Then $\bar{\bar{\sigma}}(u) = u = \bar{n}$ and consequently $p \circ \bar{\bar{\sigma}}(u) = n = \bar{\sigma} \circ p\,(u)$. **.**

The following proposition is the counterpart of proposition (112). It is not directly related to our objective of proving theorem (28) below, but it is a very useful proposition allowing us to establish an equality $\mathcal{M}(\pi) = \mathcal{M}(\rho)$ simply from an α-equivalence $\mathcal{M}(\pi) \sim \mathcal{M}(\rho)$. Now is a good time to prove this:

Proposition 289 *Let V be a set and $\pi, \rho \in \mathbf{\Pi}(V)$. Then we have:*

$$\mathcal{M}(\pi) \sim \mathcal{M}(\rho) \ \Rightarrow \ \mathcal{M}(\pi) = \mathcal{M}(\rho)$$

where the relation $\sim$ denotes the substitution congruence on $\mathbf{\Pi}(\bar{V})$.

Proof
We assume that $\mathcal{M}(\pi) \sim \mathcal{M}(\rho)$. We need to show that $\mathcal{M}(\pi) = \mathcal{M}(\rho)$. However, from theorem (26) of page 348 we obtain $\bar{\mathcal{M}} \circ \mathcal{M}(\pi) = \bar{\mathcal{M}} \circ \mathcal{M}(\rho)$, where $\bar{\mathcal{M}} : \mathbf{\Pi}(\bar{V}) \rightarrow \mathbf{\Pi}(\bar{\bar{V}})$ is the minimal transform mapping. Hence, from definition (94), we see that $\mathcal{N} \circ \mathcal{M}(\pi) = \mathcal{N} \circ \mathcal{M}(\rho)$. Applying lemma (26) to $W = V$ and the identity mapping $\sigma : V \rightarrow V$ we conclude that $\mathcal{M}(\pi) = \mathcal{M}(\rho)$. **.**

The following lemma is the counterpart of lemma (14). It is also not related to theorem (28) below, but will be very useful in the future.

Lemma 27 *Let V be a set and $p : \bar{\bar{V}} \rightarrow \bar{V}$ be the map of* definition (94)*. Then for all $\pi \in \mathbf{\Pi}(V)$, the substitution p is valid for the proof $\bar{\mathcal{M}} \circ \mathcal{M}(\pi)$.*

Proof
Using proposition (224) it is sufficient to show that p is injective on the set $\mathrm{Var}(\bar{\mathcal{M}} \circ \mathcal{M}(\pi))$. First we shall show that p is injective on $V \cup \bar{\mathbf{N}}$: we already did this in the course of proving lemma (14). We repeat the argument here for the reader's convenience: so suppose $u, v \in V \cup \bar{\mathbf{N}}$ are such that $p\,(u) = p\,(v)$. We need to show that $u = v$. We shall distinguish four cases: first we assume that $u, v \in V \subseteq \bar{V}$. Then $u = v$ follows immediately from definition (94). Next we assume that $u, v \in \bar{\mathbf{N}}$. Then $u = \bar{n}$ and $v = \bar{m}$ for some $n, m \in \mathbf{N}$. From $p\,(u) = p\,(v)$ we obtain $n = m$ and consequently $u = v$. Next we assume that $u \in V$ and $v \in \bar{\mathbf{N}}$. Then $v = \bar{m}$ for some $m \in \mathbf{N}$ and from the equality

$p(u) = p(v)$ we obtain $u = n$ which contradicts the fact that $V \cap \mathbf{N} = \emptyset$. So this case is in fact impossible. The case $u \in \bar{\mathbf{N}}$ and $v \in V$ is likewise impossible and we have proved that p is injective on $V \cup \bar{\mathbf{N}}$. So it remains to show that $\mathrm{Var}(\bar{\mathcal{M}} \circ \mathcal{M}(\pi)) \subseteq V \cup \bar{\mathbf{N}}$. Let $u \in \mathrm{Var}(\bar{\mathcal{M}} \circ \mathcal{M}(\pi))$. We need to show that $u \in V \cup \bar{\mathbf{N}}$. Since $\bar{V} = \bar{V} \uplus \bar{\mathbf{N}}$, we shall distinguish two cases: first we assume that $u \in \bar{V}$. Then using proposition (252) we obtain:

$$u \in \mathrm{Var}(\bar{\mathcal{M}} \circ \mathcal{M}(\pi)) \cap \bar{V} = \mathrm{Fr}(\mathcal{M}(\pi)) = \mathrm{Fr}(\pi) \subseteq V \subseteq V \cup \bar{\mathbf{N}}$$

Next we assume that $u \in \bar{\mathbf{N}}$. Then it is clear that $u \in V \cup \bar{\mathbf{N}}$. **.**

We are now ready to quote the main theorem of this section which is the counterpart of theorem (17) of page 172. This theorem shows that the condition $\mathrm{rnk}(\,\bar{\sigma} \circ \mathcal{M}(\pi)\,) \leq |W|$ is indeed sufficient for the proof $\bar{\sigma} \circ \mathcal{M}(\pi)$ to be *squeezed* into the space $\mathbf{\Pi}(W)$. Specifically, it is sufficient to ensure the existence of $\rho \in \mathbf{\Pi}(W)$ such that $\bar{\sigma} \circ \mathcal{M}(\pi) = \mathcal{M}(\rho)$. This will crucially allow us to prove the existence of essential proof substitutions in theorem (29) below. Note that theorem (28) has nothing magical and fundamentally consists in a simple application of proposition (281), allowing us to move variables around provided they are bound, and provided the substitution rank meets the right condition.

Theorem 28 *Let V, W be sets and $\sigma : V \to W$ be a map. Let $\pi \in \mathbf{\Pi}(V)$ with:*

$$\mathrm{rnk}(\,\bar{\sigma} \circ \mathcal{M}(\pi)\,) \leq |W|$$

where $\bar{\sigma} : \bar{V} \to \bar{W}$ is the minimal extension of σ and $\mathcal{M}(\pi)$ is the minimal transform of π. Then, there exists $\rho \in \mathbf{\Pi}(W)$ such that $\bar{\sigma} \circ \mathcal{M}(\pi) = \mathcal{M}(\rho)$.

Proof
Our first step is to find $\rho_1 \in \mathbf{\Pi}(\bar{W})$ such that $\bar{\sigma} \circ \mathcal{M}(\pi) \sim \rho_1$ and $\mathrm{Var}(\rho_1) \subseteq W$, where $\sim$ denotes the substitution congruence on $\mathbf{\Pi}(\bar{W})$. We shall do so using proposition (281) applied to the set $\bar{W}$ and the proof $\bar{\sigma} \circ \mathcal{M}(\pi) \in \mathbf{\Pi}(\bar{W})$. Suppose for now that we have proved the inclusion $\mathrm{Fr}(\bar{\sigma} \circ \mathcal{M}(\pi)) \subseteq W$. Then from the assumption $\mathrm{rnk}(\,\bar{\sigma} \circ \mathcal{M}(\pi)\,) \leq |W|$ and proposition (281) we obtain the existence of $\rho_1 \in \mathbf{\Pi}(\bar{W})$ such that $\bar{\sigma} \circ \mathcal{M}(\pi) \sim \rho_1$ and $\mathrm{Var}(\rho_1) \subseteq W$. In fact, proposition (281) allows to assume that $|\mathrm{Var}(\rho_1)| = \mathrm{rnk}(\,\bar{\sigma} \circ \mathcal{M}(\pi)\,)$ but we shall not be using this property. So we need to prove that $\mathrm{Fr}(\bar{\sigma} \circ \mathcal{M}(\pi)) \subseteq W$:

$$\begin{array}{rcl}
\mathrm{Fr}(\bar{\sigma} \circ \mathcal{M}(\pi)) & = & \mathrm{Fr}(\,\bar{\sigma}(\mathcal{M}(\pi))\,) \\
\text{prop. (209)} \;\to & \subseteq & \bar{\sigma}(\,\mathrm{Fr}(\mathcal{M}(\pi))\,) \\
\text{prop. (252)} \;\to & = & \bar{\sigma}(\mathrm{Fr}(\pi)) \\
\pi \in \mathbf{\Pi}(V) \;\to & \subseteq & \bar{\sigma}(V) \\
\text{def. (39)} \;\to & = & \sigma(V) \\
& \subseteq & W
\end{array}$$

So the existence of $\rho_1 \in \mathbf{\Pi}(\bar{W})$ such that $\bar{\sigma} \circ \mathcal{M}(\pi) \sim \rho_1$ and $\mathrm{Var}(\rho_1) \subseteq W$ is now established. Next we want to project ρ_1 onto $\mathbf{\Pi}(W)$ by defining $\rho = q(\rho_1)$

where $q : \bar{W} \to W$ is a substitution such that $q(u) = u$ for all $u \in W$. To be rigorous, we need to define $q(n)$ for $n \in \mathbf{N}$ which we cannot do when $W = \emptyset$. So in the case when $W \neq \emptyset$, let $u^* \in W$ and define $q : \bar{W} \to W$ as follows:

$$\forall u \in \bar{W}\ ,\ q(u) = \begin{cases} u & \text{if} \quad u \in W \\ u^* & \text{if} \quad u \in \mathbf{N} \end{cases}$$

and consider the associated proof substitution mapping $q : \mathbf{\Pi}(\bar{W}) \to \mathbf{\Pi}(W)$. In the case when $W = \emptyset$, there exists no substitution $q : \bar{W} \to W$ but we can define an operator $q : \mathbf{P}(\bar{W}) \to \mathbf{P}(W)$ with the following structural recursion:

$$q(\chi) = \begin{cases} \bot & \text{if} \quad \chi = (u \in v) \\ \bot & \text{if} \quad \chi = \bot \\ q(\chi_1) \to q(\chi_2) & \text{if} \quad \chi = \chi_1 \to \chi_2 \\ \bot & \text{if} \quad \chi = \forall u \chi_1 \end{cases} \tag{3.54}$$

and we can extend this operator as $q : \mathbf{\Pi}(\bar{W}) \to \mathbf{\Pi}(W)$ with the recursion:

$$q(\kappa) = \begin{cases} q(\chi) & \text{if} \quad \kappa = \chi \in \mathbf{P}(\bar{W}) \\ \partial q(\chi) & \text{if} \quad \kappa = \partial \chi \\ q(\kappa_1) \oplus q(\kappa_2) & \text{if} \quad \kappa = \kappa_1 \oplus \kappa_2 \\ \bot & \text{if} \quad \kappa = \nabla u \kappa_1 \end{cases} \tag{3.55}$$

We do not really care how $q(\kappa)$ is defined when $\kappa = \nabla u \kappa_1$, so we are simply setting $q(\kappa) = \bot$ which is the proof with hypothesis $\bot$ and conclusion $\bot$. Whether $W = \emptyset$ or not, we have an operator $q : \mathbf{\Pi}(\bar{W}) \to \mathbf{\Pi}(W)$ and we set $\rho = q(\rho_1) \in \mathbf{\Pi}(W)$. We shall complete the proof of the theorem by proving the equality $\bar{\sigma} \circ \mathcal{M}(\pi) = \mathcal{M}(\rho)$. Using lemma (26) we have:

$$\begin{array}{rcl} \bar{\sigma} \circ \mathcal{M}(\pi) & = & \mathcal{N} \circ \bar{\sigma} \circ \mathcal{M}(\pi) \\ \text{def. (94)} \ \to & = & p \circ \bar{\mathcal{M}} \circ \bar{\sigma} \circ \mathcal{M}(\pi) \\ \text{theorem (26) and } \bar{\sigma} \circ \mathcal{M}(\pi) \sim \rho_1 \ \to & = & p \circ \bar{\mathcal{M}}(\rho_1) \\ & = & \mathcal{N}(\rho_1) \\ \text{A: to be proved} \ \to & = & \mathcal{N} \circ i \circ q(\rho_1) \\ \rho = q(\rho_1) \ \to & = & \mathcal{N} \circ i(\rho) \\ \text{lemma (25)} \ \to & = & \mathcal{M}(\rho) \end{array}$$

So it remains to show that $i \circ q(\rho_1) = \rho_1$ where $i : W \to \bar{W}$ is the inclusion map. As before, we shall distinguish two cases: first we assume that $W \neq \emptyset$. Then q arises from the substitution $q : \bar{W} \to W$ and from proposition (202) it is sufficient to prove that $i \circ q(u) = u$ for all $u \in \mathrm{Var}(\rho_1)$. Since $\mathrm{Var}(\rho_1) \subseteq W$ the equality is clear. Next we assume that $W = \emptyset$. From the inclusion $\mathrm{Var}(\rho_1) \subseteq W$ it follows that $\mathrm{Var}(\rho_1) = \emptyset$ and it is therefore sufficient to prove the property:

$$\mathrm{Var}(\kappa) = \emptyset \ \Rightarrow\ i \circ q(\kappa) = \kappa$$

for all $\kappa \in \mathbf{\Pi}(\bar{W})$. We shall first prove the property is true for $\kappa = \chi \in \mathbf{P}(\bar{W})$ with a structural induction argument on $\mathbf{P}(\bar{W})$. Note that when $W = \emptyset$, the inclusion map $i : W \to \bar{W}$ is simply the map with empty domain, namely the empty set. First we assume that $\chi = (u \in v)$ for some $u, v \in \bar{W}$. Then the above implication is vacuously true. Next we assume that $\chi = \bot$. Then $i \circ q(\chi) = \chi$ is clear. So we now assume that $\chi = \chi_1 \to \chi_2$ where χ_1, χ_2 satisfy the above implication. We need to show the same is true of χ. So we assume that $\mathrm{Var}(\chi) = \emptyset$. We need to show that $i \circ q(\chi) = \chi$. However, from $\mathrm{Var}(\chi) = \emptyset$ we obtain $\mathrm{Var}(\chi_1) = \emptyset$ and $\mathrm{Var}(\chi_2) = \emptyset$. Having assumed χ_1 and χ_2 satisfy the implication, we obtain the equalities $i \circ q(\chi_1) = \chi_1$ and $i \circ q(\chi_2) = \chi_2$ from which $i \circ q(\chi) = \chi$ follows immediately. So it remains to check the case when $\chi = \forall u \chi_1$ for which the above implication is also vacuously true. We now show the above property with an induction argument on $\mathbf{\Pi}(\bar{W})$: first we assume that $\kappa = \chi \in \mathbf{P}(\bar{W})$. Then the above implication has been established. Next we assume that $\kappa = \partial\chi$ for some $\chi \in \mathbf{P}(\bar{W})$. We need to show the implication is true for κ. So we assume that $\mathrm{Var}(\kappa) = \emptyset$ and we have:

$$\begin{array}{rcl} i \circ q(\kappa) & = & i \circ q(\partial\chi) \\ & = & \partial\, i \circ q(\chi) \\ \mathrm{Var}(\chi) = \emptyset \ \to & = & \partial\chi \\ & = & \kappa \end{array}$$

Next we assume that $\kappa = \kappa_1 \oplus \kappa_2$ for some $\kappa_1, \kappa_2 \in \mathbf{\Pi}(\bar{W})$ satisfying our implication. We need to show the same is true of κ. So we assume that $\mathrm{Var}(\kappa) = \emptyset$:

$$\begin{array}{rcl} i \circ q(\kappa) & = & i \circ q(\kappa_1 \oplus \kappa_2) \\ & = & i(\, q(\kappa_1) \oplus q(\kappa_2)\,) \\ & = & i \circ q(\kappa_1) \oplus i \circ q(\kappa_2) \\ \mathrm{Var}(\kappa_1) = \emptyset,\ \mathrm{Var}(\kappa_2) = \emptyset \ \to & = & \kappa_1 \oplus \kappa_2 \\ & = & \kappa \end{array}$$

Finally we assume that $\kappa = \nabla u \kappa_1$ in which case the property is vacuously true.
.

The following theorem is the counterpart of theorem (18) of page 174.

Theorem 29 *Let V, W be sets and $\sigma : V \to W$ be a map. Then, there exists an essential proof substitution mapping $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ associated with σ, if and only if $|W|$ is an infinite cardinal or the inequality $|V| \leq |W|$ holds.*

Proof
First we prove the 'if' part: so we assume that $|W|$ is an infinite cardinal, or that it is finite with $|V| \leq |W|$. We need to prove the existence of an essential substitution mapping $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ associated with σ. Let $c : \mathcal{P}(\mathbf{\Pi}(W)) \setminus \{\emptyset\} \to \mathbf{\Pi}(W)$ be a choice function whose existence follows from the axiom of choice. Let us accept for now that for all $\pi \in \mathbf{\Pi}(V)$, there exists

some $\rho \in \mathbf{\Pi}(W)$ such that $\bar{\sigma} \circ \mathcal{M}(\pi) = \mathcal{M}(\rho)$. Given $\rho \in \mathbf{\Pi}(W)$, let $[\rho]$ denote the congruence class of ρ modulo the substitution congruence, which is a non-empty subset of $\mathbf{\Pi}(W)$. Define $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ by setting $\sigma^*(\pi) = c([\rho])$, where ρ is an arbitrary proof of $\mathbf{\Pi}(W)$ such that $\bar{\sigma} \circ \mathcal{M}(\pi) = \mathcal{M}(\rho)$. We need to check that σ^* is well defined, namely that $\sigma^*(\pi)$ is independent of the particular choice of ρ. But if ρ' is such that $\bar{\sigma} \circ \mathcal{M}(\pi) = \mathcal{M}(\rho')$ then $\mathcal{M}(\rho) = \mathcal{M}(\rho')$ and it follows from theorem (26) of page 348 that $[\rho] = [\rho']$. So it remains to show the existence of ρ such that $\bar{\sigma} \circ \mathcal{M}(\pi) = \mathcal{M}(\rho)$ for all $\pi \in \mathbf{\Pi}(V)$. So let $\pi \in \mathbf{\Pi}(V)$. Using theorem (28) of page 373 it is sufficient to prove that $\mathrm{rnk}(\,\bar{\sigma} \circ \mathcal{M}(\pi)\,) \leq |W|$. The substitution rank of a proof being always finite, this is clearly true if $|W|$ is infinite. Otherwise, using proposition (287):

$$\begin{array}{rcl} \mathrm{rnk}(\,\bar{\sigma} \circ \mathcal{M}(\pi)\,) & \leq & \mathrm{rnk}(\mathcal{M}(\pi)) \\ \text{prop. (283)} \;\to & = & \mathrm{rnk}(\pi) \\ & \leq & |\mathrm{Var}(\pi)| \\ & \leq & |V| \\ |V| \leq |W| \;\to & \leq & |W| \end{array}$$

We now prove the 'only if' part: So we assume there exists $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ essential substitution associated with σ. We need to show that $|W|$ is an infinite cardinal, or that it is finite with $|V| \leq |W|$. However, from proposition (288) the restriction $\sigma^*_{|\mathbf{P}(V)} : \mathbf{P}(V) \to \mathbf{P}(W)$ is an essential substitution and the conclusion follows from theorem (18) of page 174. **.**

3.5.3 Properties of Essential Substitution

Just as we did for formulas, we shall now investigate some of the basic properties of essential substitutions for proofs. The following definition is very similar to definition (93). In effect, we are simply defining an *essential substitution* as any map $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ for which there exists a map $\sigma : V \to W$ such that σ^* is associated to σ as per definition (93). As soon as we show that such σ is unique, we shall drop the '$*$' and refer to σ and σ^* with the same symbol. Indeed, if we start with a map $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$, we can safely and unambiguously refer to the map $\sigma : V \to W$. However, one should be a little cautious about notations: if we start from $\sigma : V \to W$, then there are potentially more than one map $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ which qualifies as an essential substitution associated to σ. Furthermore, the notation $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ could also refer to the usual proof substitution as per definition (74). There will be situations when we shall want to speak about both the non-essential $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ of definition (74), and some essential representative $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$. When this happens, we shall use a different symbol σ^* to single out one of them.

Definition 96 *Let V, W be sets. We say that a map $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ is an* essential proof substitution *if and only if there exists $\sigma : V \to W$ such that:*

$$\mathcal{M} \circ \sigma^* = \bar{\sigma} \circ \mathcal{M}$$

where $\bar{\sigma} : \bar{V} \to \bar{W}$ is the minimal extension and $\mathcal{M}$ is the minimal transform.

Proposition 290 *Let V, W be sets and $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ be an essential proof substitution. Then the map $\sigma : V \to W$ associated with σ^* is unique.*

Proof
Suppose $\sigma_0, \sigma_1 : V \to W$ are two maps which are associated with an essential proof substitution $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$. Then using proposition (288), the restriction $\sigma^*_{|\mathbf{P}(V)} : \mathbf{P}(V) \to \mathbf{P}(W)$ is an essential substitution associated with σ_0 and σ_1. From the uniqueness property of proposition (113), we have $\sigma_0 = \sigma_1$. .

An essential proof substitution $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ can be redefined arbitrarily modulo α-equivalence, without affecting it status of *essential substitution associated to σ*. The following is the counterpart of proposition (114).

Proposition 291 *Let V, W be sets and $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ be an essential proof substitution. Let $\tau : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ be a map such that $\sigma(\pi) \sim \tau(\pi)$ for all $\pi \in \mathbf{\Pi}(V)$ where $\sim$ is the substitution congruence on $\mathbf{\Pi}(W)$. Then τ is itself an essential substitution with associated map $\tau : V \to W$ identical to σ.*

Proof
Since σ is essential we have $\mathcal{M} \circ \sigma(\pi) = \bar{\sigma} \circ \mathcal{M}(\pi)$ for all $\pi \in \mathbf{\Pi}(V)$. Having assumed that $\sigma(\pi) \sim \tau(\pi)$ for all $\pi \in \mathbf{\Pi}(V)$, from theorem (26) of page 348 we have $\mathcal{M} \circ \sigma(\pi) = \mathcal{M} \circ \tau(\pi)$. It follows that $\mathcal{M} \circ \tau(\pi) = \bar{\sigma} \circ \mathcal{M}(\pi)$ and we conclude that τ is itself essential with associated map $\sigma : V \to W$. .

The following proposition has no counterpart for formulas. We know from proposition (288) that restricting an essential substitution $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ to $\mathbf{P}(V)$ leads to an essential substitution $\sigma_{|\mathbf{P}(V)} : \mathbf{P}(V) \to \mathbf{P}(W)$. In fact, every essential substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is obtained that way. In other words, every essential substitution for formulas is the restriction of an essential substitution for proofs, associated with the same underlying map $\sigma : V \to W$. This proposition will prove very useful when attempting to prove the substitution theorem (30) of page 388. Starting from an essential substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ and a true sequent $\Gamma \vdash \phi$ with underlying proof $\pi \in \mathbf{\Pi}(V)$, we shall extend σ to an essential substitution $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ which will give us the proof $\sigma(\pi)$, allowing us to establish the sequent $\sigma(\Gamma) \vdash \sigma(\phi)$. This is true magic.

Proposition 292 *Let V, W be sets and $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ be an essential substitution. Then the map σ can be extended to an essential proof substitution $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ associated with the same underlying $\sigma : V \to W$.*

Proof
We assume that $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is an essential substitution associated with $\sigma : V \to W$ as per definition (44). We need to show the existence of an essential proof substitution $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ associated with $\sigma : V \to W$ such that $\sigma^*_{|\mathbf{P}(V)} = \sigma$. However, from the existence of $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ using theorem (18) of page 174 it follows that $|W|$ is an infinite cardinal, or that it is finite

with $|V| \leq |W|$. We can therefore apply theorem (29) of page 375 from which we deduce the existence of an essential substitution $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ associated with $\sigma : V \to W$. Using proposition (288), the restriction $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ is an essential substitution associated with $\sigma : V \to W$. Hence we must have $\sigma(\phi) \sim \sigma^*(\phi)$ for all $\phi \in \mathbf{P}(V)$, where $\sim$ is the substitution congruence on $\mathbf{P}(W)$. In fact, from proposition (270) this equivalence remains true if $\sim$ is regarded as the substitution congruence on $\mathbf{\Pi}(W)$. From proposition (291) we can therefore redefine σ^* on $\mathbf{P}(V)$ by setting $\sigma^*(\phi) = \sigma(\phi)$ so as to obtain an essential proof substitution $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ associated with $\sigma : V \to W$ which coincides with σ on $\mathbf{P}(V)$. This completes our proof. **.**

Our initial idea of variable substitution for proofs is to blindly substitute variables and create $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ as per definition (74). This does not work very well, unless the substitution $\sigma : V \to W$ is valid for the proof π. So we introduced essential substitutions $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ to eliminate the problem of variable capture. We should check that the solution provided is a good solution, namely that $\sigma(\pi)$ and $\sigma^*(\pi)$ are in fact the same proofs modulo α-equivalence, whenever σ is valid for π. See also proposition (115).

Proposition 293 *Let V, W be sets and $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ be an essential substitution. Then if σ is valid for $\pi \in \mathbf{\Pi}(V)$, we have the substitution equivalence:*

$$\sigma(\pi) \sim \sigma^*(\pi)$$

where $\sigma^* : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ is the associated substitution as per definition (74)*.*

Proof
We assume that σ is valid for π. We need to show that $\sigma(\pi) \sim \sigma^*(\pi)$, that is $\mathcal{M} \circ \sigma(\pi) = \mathcal{M} \circ \sigma^*(\pi)$. However, having assumed σ is valid for π, from theorem (23) of page 327 we have $\mathcal{M} \circ \sigma^*(\pi) = \bar{\sigma} \circ \mathcal{M}(\pi)$. Since σ is an essential proof substitution we also have $\mathcal{M} \circ \sigma(\pi) = \bar{\sigma} \circ \mathcal{M}(\pi)$. So the result follows. **.**

The following proposition is the counterpart of proposition (116) :

Proposition 294 *Let V, W be sets and $\sigma : V \to W$ be an injective map. Then the associated map $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ is essential with associated map σ itself.*

Proof
Let $\sigma : V \to W$ be an injective map. Let $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ be the associated substitution mapping as per definition (74). The fact that both mappings are called 'σ' is standard practice at this stage for us. We need to prove that $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ is an essential substitution mapping, with associated map $\sigma : V \to W$. In other words, we need to prove that $\mathcal{M} \circ \sigma(\pi) = \bar{\sigma} \circ \mathcal{M}(\pi)$ for all $\pi \in \mathbf{\Pi}(V)$. Using theorem (23) of page 327 it is sufficient to show that σ is valid for π which follows from proposition (224) and the injectivity of $\sigma : V \to W$. **.**

If we consider the inclusion map $i : V \to \bar{V}$, there are two ways to *essentially* substitute variables in accordance to i. One way to is to consider the associated $i : \mathbf{\Pi}(V) \to \mathbf{\Pi}(\bar{V})$. The other and possibly unexpected way is to consider the minimal transform $\mathcal{M} : \mathbf{\Pi}(V) \to \mathbf{\Pi}(\bar{V})$. See also proposition (117).

Proposition 295 *Let V be a set. The minimal transform $\mathcal{M} : \mathbf{\Pi}(V) \to \mathbf{\Pi}(\bar{V})$ is an essential substitution with associated map the inclusion $i : V \to \bar{V}$.*

Proof
Let $\bar{\mathcal{M}} : \mathbf{\Pi}(\bar{V}) \to \mathbf{\Pi}(\bar{\bar{V}})$ denote the minimal transform on $\mathbf{\Pi}(\bar{V})$. We need to show that $\bar{\mathcal{M}} \circ \mathcal{M}(\pi) = \bar{i} \circ \mathcal{M}(\pi)$ for all $\pi \in \mathbf{\Pi}(V)$. However, since i is injective, from proposition (224) it is valid for π and it follows from theorem (23) of page 327 that $\bar{\mathcal{M}} \circ i(\pi) = \bar{i} \circ \mathcal{M}(\pi)$. Hence we need to show that $\bar{\mathcal{M}} \circ \mathcal{M}(\pi) = \bar{\mathcal{M}} \circ i(\pi)$. Using theorem (26) of page 348 we need to show $\mathcal{M}(\pi) \sim i(\pi)$ where $\sim$ is the substitution congruence on $\mathbf{\Pi}(\bar{V})$, which we know is true from proposition (274) and which completes our proof. **.**

The following proposition is the counterpart of proposition (118) :

Proposition 296 *Let V be a set and $\sim$ be the substitution congruence on $\mathbf{\Pi}(V)$. Then for all $\pi, \rho \in \mathbf{\Pi}(V)$ we have $\pi \sim \rho$ if and only if $\rho = \sigma(\pi)$ for some essential substitution $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(V)$ such that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\pi)$.*

Proof
First we show the 'if' part: so suppose $\rho = \sigma(\pi)$ for some essential substitution $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(V)$ such that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\pi)$. We need to show that $\pi \sim \rho$. From theorem (26) of page 348 it is sufficient to prove that $\mathcal{M}(\pi) = \mathcal{M}(\rho)$. Having assumed that $\rho = \sigma(\pi)$ we need to show that $\mathcal{M}(\pi) = \mathcal{M} \circ \sigma(\pi)$. However, since σ is essential we have $\mathcal{M} \circ \sigma(\pi) = \bar{\sigma} \circ \mathcal{M}(\pi)$. Hence we need to show that $\mathcal{M}(\pi) = \bar{\sigma} \circ \mathcal{M}(\pi)$. Using proposition (202) it is sufficient to prove that $\bar{\sigma}(u) = u$ for all $u \in \mathrm{Var}(\mathcal{M}(\pi))$. So let $u \in \mathrm{Var}(\mathcal{M}(\pi))$. Since $\bar{V} = V \uplus \mathbf{N}$ we shall distinguish two cases: first we assume that $u \in \mathbf{N}$. Then $\bar{\sigma}(u) = u$ is clear from definition (39). Next we assume that $u \in V$. Then from proposition (252) we obtain $u \in \mathrm{Fr}(\pi)$ and it follows that $\bar{\sigma}(u) = \sigma(u) = u$. We now prove the 'only if' part: so suppose $\pi \sim \rho$. We need to show that $\rho = \sigma(\pi)$ for some essential substitution $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(V)$ such that $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\pi)$. Let $i : \mathbf{\Pi}(V) \to \mathbf{\Pi}(V)$ be the identity mapping. From proposition (294), i is an essential substitution associated with the identity $i : V \to V$. Let $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(V)$ be defined by $\sigma(\kappa) = i(\kappa)$ whenever $\kappa \neq \pi$ and $\sigma(\pi) = \rho$. Having assumed that $\pi \sim \rho$ we have $\sigma(\kappa) \sim i(\kappa)$ for all $\kappa \in \mathbf{\Pi}(V)$. It follows from proposition (291) that σ is an essential substitution whose associated map $\sigma : V \to V$ is the identity. In particular, we have $\sigma(u) = u$ for all $u \in \mathrm{Fr}(\pi)$. **.**

The following proposition is the counterpart of proposition (119) :

Proposition 297 *Let U, V and W be sets while the maps $\tau : \mathbf{\Pi}(U) \to \mathbf{\Pi}(V)$ and $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ are essential substitutions. Then $\sigma \circ \tau : \mathbf{\Pi}(U) \to \mathbf{\Pi}(W)$ is itself an essential proof substitution with associated map $\sigma \circ \tau : U \to W$.*

Proof
We need to show that $\mathcal{M} \circ (\sigma \circ \tau) = \overline{(\sigma \circ \tau)} \circ \mathcal{M}$. However from definition (39), it is clear that the minimal extension $\overline{(\sigma \circ \tau)} : \bar{U} \to \bar{W}$ is equal to the composition

of the minimal extensions $\bar{\sigma} \circ \bar{\tau}$. Hence we have:

$$\begin{aligned} \mathcal{M} \circ (\sigma \circ \tau) &= \bar{\sigma} \circ \mathcal{M} \circ \tau \\ &= \bar{\sigma} \circ \bar{\tau} \circ \mathcal{M} \\ &= \overline{(\sigma \circ \tau)} \circ \mathcal{M} \end{aligned}$$

.

The following proposition is the counterpart of proposition (120):

Proposition 298 *Let V, W be sets and $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ be an essential proof substitution. Then for all $\pi \in \mathbf{\Pi}(V)$ we have the equality:*

$$\mathrm{Fr}(\sigma(\pi)) = \sigma(\mathrm{Fr}(\pi))$$

Proof
Using proposition (252) we obtain the following:

$$\begin{aligned} \mathrm{Fr}(\sigma(\pi)) &= \mathrm{Fr}(\, \mathcal{M} \circ \sigma(\pi)\,) \\ &= \mathrm{Fr}(\, \bar{\sigma} \circ \mathcal{M}(\pi)\,) \\ \bar{\sigma} \text{ valid for } \mathcal{M}(\pi) \;\to\; &= \bar{\sigma}(\, \mathrm{Fr}(\mathcal{M}(\pi))\,) \\ \text{prop. (252)} \;\to\; &= \bar{\sigma}(\mathrm{Fr}(\pi)) \\ \mathrm{Fr}(\pi) \subseteq V \;\to\; &= \sigma(\mathrm{Fr}(\pi)) \end{aligned}$$

.

The following proposition is the counterpart of proposition (121):

Proposition 299 *Let V, W be sets and $\sigma, \tau : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ be two essential proof substitutions. Then for all $\pi \in \mathbf{\Pi}(V)$ we have the equivalence:*

$$\sigma_{|\mathrm{Fr}(\pi)} = \tau_{|\mathrm{Fr}(\pi)} \quad \Leftrightarrow \quad \sigma(\pi) \sim \tau(\pi)$$

where $\sim$ denotes the substitution congruence on the algebra $\mathbf{\Pi}(W)$.

Proof
From theorem (26) of page 348, $\sigma(\pi) \sim \tau(\pi)$ is equivalent to the equality $\mathcal{M} \circ \sigma(\pi) = \mathcal{M} \circ \tau(\pi)$. Having assumed σ and τ are essential, this is in turn equivalent to $\bar{\sigma} \circ \mathcal{M}(\pi) = \bar{\tau} \circ \mathcal{M}(\pi)$. Using proposition (202), this last equality is equivalent to $\bar{\sigma}(u) = \bar{\tau}(u)$ for all $u \in \mathrm{Var}(\mathcal{M}(\pi))$. Hence we need to show that this last statement is equivalent to $\sigma(u) = \tau(u)$ for all $u \in \mathrm{Fr}(\pi)$. First we show $\Rightarrow$: so suppose $\bar{\sigma}(u) = \bar{\tau}(u)$ for all $u \in \mathrm{Var}(\mathcal{M}(\pi))$ and let $u \in \mathrm{Fr}(\pi)$. We need to show that $\sigma(u) = \tau(u)$. From proposition (252) we have $\mathrm{Var}(\mathcal{M}(\pi)) \cap V = \mathrm{Fr}(\pi)$. It follows that $u \in \mathrm{Var}(\mathcal{M}(\pi)) \cap V$ and consequently we have $\sigma(u) = \bar{\sigma}(u) = \bar{\tau}(u) = \tau(u)$ as requested. So we now prove $\Leftarrow$: So we assume that $\sigma(u) = \tau(u)$ for all $u \in \mathrm{Fr}(\pi)$ and consider $u \in \mathrm{Var}(\mathcal{M}(\pi))$. We need to show that $\bar{\sigma}(u) = \bar{\tau}(u)$. Since $\bar{V} = V \uplus \mathbf{N}$ we shall distinguish two cases: first we

assume that $u \in \mathbf{N}$. Then $\bar{\sigma}(u) = u = \bar{\tau}(u)$. Next we assume that $u \in V$. Then $u \in \mathrm{Var}(\mathcal{M}(\pi)) \cap V = \mathrm{Fr}(\pi)$ and $\bar{\sigma}(u) = \sigma(u) = \tau(u) = \bar{\tau}(u)$. .

The fact that α-equivalence is preserved by certain maps $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ has already been seen on a few occasions. We have the case of $\sigma : V \to W$ injective of proposition (260). We have the case of $\sigma : V \to W$ valid for both π and ρ of theorem (27) of page 350. We now have the case of $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ essential. The following is the counterpart of proposition (122) :

Proposition 300 *Let V, W be sets and $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ be an essential proof substitution. Then for all proofs $\pi, \rho \in \mathbf{\Pi}(V)$ we have the implication:*

$$\pi \sim \rho \;\Rightarrow\; \sigma(\pi) \sim \sigma(\rho)$$

where $\sim$ denotes the substitution congruence on $\mathbf{\Pi}(V)$ and $\mathbf{\Pi}(W)$.

Proof
So we assume that $\pi \sim \rho$. We need to show that $\sigma(\pi) \sim \sigma(\rho)$. Using theorem (26) of page 348 it is sufficient to show that $\mathcal{M} \circ \sigma(\pi) = \mathcal{M} \circ \sigma(\rho)$. Having assumed that σ is essential, it is sufficient to show that $\bar{\sigma} \circ \mathcal{M}(\pi) = \bar{\sigma} \circ \mathcal{M}(\rho)$ which follows immediately from $\mathcal{M}(\pi) = \mathcal{M}(\rho)$, itself a consequence of $\pi \sim \rho$. .

The following proposition is the counterpart of proposition (123) :

Proposition 301 *Let V, W be sets and $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ be an essential proof substitution. Let $\pi \in \mathbf{\Pi}(V)$ such that $\sigma_{|\mathrm{Fr}(\pi)}$ is an injective map. Then:*

$$\mathrm{rnk}(\sigma(\pi)) = \mathrm{rnk}(\pi)$$

where rnk( ) *refers to the substitution rank as per* definition (92)*.*

Proof
Using proposition (283) we obtain the following:

$$\begin{aligned} \mathrm{rnk}(\sigma(\pi)) &= \mathrm{rnk}(\mathcal{M} \circ \sigma(\pi)) \\ \sigma \text{ essential } \to &= \mathrm{rnk}(\bar{\sigma} \circ \mathcal{M}(\pi)) \\ \text{A: to be proved } \to &= \mathrm{rnk}(\mathcal{M}(\pi)) \\ \text{prop. (283) } \to &= \mathrm{rnk}(\pi) \end{aligned}$$

So it remains to show that $\mathrm{rnk}(\bar{\sigma} \circ \mathcal{M}(\pi)) = \mathrm{rnk}(\mathcal{M}(\pi))$. Using proposition (284) it is sufficient to show that $\bar{\sigma}$ is valid for $\mathcal{M}(\pi)$ and furthermore that it is injective on $\mathrm{Fr}(\mathcal{M}(\pi))$. We know that $\bar{\sigma}$ is valid for $\mathcal{M}(\pi)$ from proposition (256). We also know that $\mathrm{Fr}(\mathcal{M}(\pi)) = \mathrm{Fr}(\pi)$ from proposition (252). So it remains to show that $\bar{\sigma}$ is injective on $\mathrm{Fr}(\pi) \subseteq V$ which is clearly the case since $\bar{\sigma}$ coincide with σ on V and σ is by assumption injective on $\mathrm{Fr}(\pi)$. .

The following proposition is the counterpart of proposition (124) :

Proposition 302 *Let V, W be sets and $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ be an essential proof substitution. Then for all proof $\pi \in \mathbf{P}(V)$ we have the inequality:*

$$\mathrm{rnk}(\sigma(\pi)) \leq \mathrm{rnk}(\pi)$$

where rnk( ) *refers to the substitution rank as per* definition (92)*.*

Proof
Using proposition (283) we obtain the following:

$$\begin{array}{rcl} \mathrm{rnk}(\sigma(\pi)) & = & \mathrm{rnk}(\mathcal{M}\circ\sigma(\pi)) \\ \sigma \text{ essential } \rightarrow & = & \mathrm{rnk}(\bar{\sigma}\circ\mathcal{M}(\pi)) \\ \text{prop. (287)} \rightarrow & \leq & \mathrm{rnk}(\mathcal{M}(\pi)) \\ \text{prop. (283)} \rightarrow & = & \mathrm{rnk}(\pi) \end{array}$$

.

Essential substitutions provide a huge benefit as they avoid variable capture. However, they come with a price. It is no longer possible to write something like $\sigma(\pi_1 \oplus \pi_1) = \sigma(\pi_1) \oplus \sigma(\pi_2)$ which we could do if σ was a naive substitution as per definition (74). Instead, we have to settle for the substitution equivalence $\sigma(\pi_1 \oplus \pi_1) \sim \sigma(\pi_1) \oplus \sigma(\pi_2)$. Note that we cannot even write $\sigma(\nabla x \pi_1) \sim \nabla \sigma(x) \sigma(\pi_1)$ in general. Indeed, if the α-equivalence was always true, then $\sigma(x)$ could never be a free variable of $\sigma(\pi)$ where $\pi = \nabla x \pi_1$. This is the whole point of essential substitutions: we want to allow some $u \in \mathrm{Fr}(\pi)$ to be such that $\sigma(u) = \sigma(x)$, while making sure $\sigma(\pi)$ is still meaningful. So we certainly want $\sigma(x)$ to be a free variable of $\sigma(\pi)$ on occasions. When this happens, the essential substitution σ will automatically redefine the bound variable so to speak, and avoid capture. This is what most texts in mathematical logic implicitly assume. Essential substitutions provide the tool to do this formally. The following proposition is the counterpart of proposition (125) :

Proposition 303 *Let V, W be sets and $\sigma : \mathbf{\Pi}(V) \rightarrow \mathbf{\Pi}(W)$ be an essential proof substitution. Let $\sim$ be the substitution congruence on $\mathbf{\Pi}(W)$. Then:*

$$\forall \pi \in \mathbf{\Pi}(V) \ , \ \sigma(\pi) \sim \begin{cases} \sigma(\phi) & \text{if} \quad \pi = \phi \in \mathbf{P}(V) \\ \partial\sigma(\phi) & \text{if} \quad \pi = \partial\phi \\ \sigma(\pi_1) \oplus \sigma(\pi_2) & \text{if} \quad \pi = \pi_1 \oplus \pi_2 \\ \nabla\sigma(x)\sigma(\pi_1) & \text{if} \quad \pi = \nabla x \pi_1 \ , \ \sigma(x) \notin \mathrm{Fr}(\sigma(\pi)) \end{cases}$$

Proof
First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then $\sigma(\pi) = \sigma(\phi)$ and we are not saying much by claiming $\sigma(\pi) \sim \sigma(\phi)$ which is clear. Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. We need to show that $\sigma(\pi) \sim \partial\sigma(\phi)$. Using theorem (26) of page 348, we simply compute the minimal transforms:

$$\begin{array}{rcl} \mathcal{M}\circ\sigma(\pi) & = & \bar{\sigma}\circ\mathcal{M}(\pi) \\ & = & \bar{\sigma}\circ\mathcal{M}(\partial\phi) \\ & = & \bar{\sigma}(\,\partial\mathcal{M}(\phi)\,) \\ & = & \partial\,\bar{\sigma}\circ\mathcal{M}(\phi) \\ & = & \partial\,\mathcal{M}\circ\sigma(\phi) \\ & = & \mathcal{M}(\,\partial\sigma(\phi)\,) \end{array}$$

So we now assume that $\pi = \pi_1 \oplus \pi_2$ for some $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$. We need to show $\sigma(\pi) \sim \sigma(\pi_1) \oplus \sigma(\pi_2)$. Once again, we simply compute the minimal transforms:

$$\begin{aligned}
\mathcal{M} \circ \sigma(\pi) &= \bar{\sigma} \circ \mathcal{M}(\pi) \\
&= \bar{\sigma} \circ \mathcal{M}(\pi_1 \oplus \pi_2) \\
&= \bar{\sigma}(\, \mathcal{M}(\pi_1) \oplus \mathcal{M}(\pi_2)\,) \\
&= \bar{\sigma} \circ \mathcal{M}(\pi_1) \oplus \bar{\sigma} \circ \mathcal{M}(\pi_2) \\
&= \mathcal{M} \circ \sigma(\pi_1) \oplus \mathcal{M} \circ \sigma(\pi_2) \\
&= \mathcal{M}(\, \sigma(\pi_1) \oplus \sigma(\pi_2)\,)
\end{aligned}$$

So we now assume that $\pi = \nabla x \pi_1$ and $\sigma(x) \notin \mathrm{Fr}(\sigma(\pi))$. We need to show that $\sigma(\pi) \sim \nabla \sigma(x) \sigma(\pi_1)$. Likewise, we shall compute minimal transforms:

$$\begin{aligned}
\mathcal{M} \circ \sigma(\pi) &= \bar{\sigma} \circ \mathcal{M}(\pi) \\
&= \bar{\sigma} \circ \mathcal{M}(\nabla x \pi_1) \\
n = \min\{k : [k/x] \text{ valid for } \mathcal{M}(\pi_1)\} \;\rightarrow\; &= \bar{\sigma}(\, \nabla n \mathcal{M}(\pi_1)[n/x]\,) \\
&= \nabla \bar{\sigma}(n) \bar{\sigma}(\, \mathcal{M}(\pi_1)[n/x]\,) \\
&= \nabla n\, \bar{\sigma} \circ [n/x] \circ \mathcal{M}(\pi_1) \\
\text{A: to be proved} \;\rightarrow\; &= \nabla n\, [n/\sigma(x)] \circ \bar{\sigma} \circ \mathcal{M}(\pi_1) \\
&= \nabla n\, [n/\sigma(x)] \circ \mathcal{M} \circ \sigma(\pi_1) \\
&= \nabla n\, \mathcal{M}[\sigma(\pi_1)][n/\sigma(x)] \\
\text{B: to be proved} \;\rightarrow\; &= \nabla m\, \mathcal{M}[\sigma(\pi_1)][m/\sigma(x)] \\
m = \min\{k : [k/\sigma(x)] \text{ valid for } \mathcal{M}[\sigma(\pi_1)]\} \;\rightarrow\; &= \mathcal{M}(\nabla \sigma(x) \sigma(\pi_1))
\end{aligned}$$

So it remains to justify point A and B. First we deal with point A: it is sufficient to prove the equality $\bar{\sigma} \circ [n/x] \circ \mathcal{M}(\pi_1) = [n/\sigma(x)] \circ \bar{\sigma} \circ \mathcal{M}(\pi_1)$, which follows from lemma (22) and $\sigma(x) \notin \sigma(\mathrm{Fr}(\pi))$, itself a consequence of $\sigma(x) \notin \mathrm{Fr}(\sigma(\pi))$ and proposition (298). We now deal with point B: it is sufficient to prove the equivalence $[k/x]$ valid for $\mathcal{M}(\pi_1) \;\Leftrightarrow\; [k/\sigma(x)]$ valid for $\bar{\sigma} \circ \mathcal{M}(\pi_1)$ which follows from lemma (23) and the fact that $\sigma(x) \notin \sigma(\mathrm{Fr}(\pi))$. .

As we have discussed prior to proposition (303) we cannot write the equivalence $\sigma(\pi) \sim \nabla \sigma(x) \sigma(\pi_1)$ in general when $\pi = \nabla x \pi_1$ and σ is an essential substitution. However, we can write $\sigma(\pi) \sim \nabla \tau(x) \tau(\pi_1)$ whenever τ is an essential substitution which coincides with σ on $V \setminus \{x\}$ and is such that $\tau(x) \notin \mathrm{Fr}(\sigma(\pi))$. This is very useful, and even more so knowing that such an essential substitution τ always exists. The following is the counterpart of proposition (126) :

Proposition 304 *Let V, W be sets and $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ be an essential proof substitution. Let $\pi = \nabla x \pi_1$ where $x \in V$, $\pi_1 \in \mathbf{\Pi}(V)$. There exists an essential substitution $\tau : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ such that $\tau = \sigma$ on $V \setminus \{x\}$ and $\tau(x) \notin \mathrm{Fr}(\sigma(\pi))$. Furthermore, for any such τ we have the substitution equivalence:*

$$\sigma(\pi) \sim \nabla \tau(x) \tau(\pi_1)$$

Proof
We shall first prove the substitution equivalence. So let $\tau : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ be an essential proof substitution which coincide with σ on $V \setminus \{x\}$ and such that $\tau(x) \notin \mathrm{Fr}(\sigma(\pi))$. We need to show that $\sigma(\pi) \sim \nabla\tau(x)\tau(\pi_1)$ where $\sim$ denotes the substitution congruence on $\mathbf{\Pi}(W)$. However, since $\mathrm{Fr}(\pi) \subseteq V \setminus \{x\}$ we see that σ and τ are essential substitutions which coincide on $\mathrm{Fr}(\pi)$. It follows from proposition (299) that $\sigma(\pi) \sim \tau(\pi)$. Hence it is sufficient to prove that $\tau(\pi) \sim \nabla\tau(x)\tau(\pi_1)$. Applying proposition (303) it is sufficient to show that $\tau(x) \notin \mathrm{Fr}(\tau(\pi))$. However, by assumption we have $\tau(x) \notin \mathrm{Fr}(\sigma(\pi))$ and so:

$$\tau(x) \notin \mathrm{Fr}(\sigma(\pi)) = \sigma(\mathrm{Fr}(\pi)) = \tau(\mathrm{Fr}(\pi)) = \mathrm{Fr}(\tau(\pi))$$

where we have used proposition (298). It remains to show that such an essential substitution $\tau : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ exists. Suppose we have proved that $\mathrm{Fr}(\sigma(\pi))$ is a proper subset of W. Then there exists $y^* \in W$ such that $y^* \notin \mathrm{Fr}(\sigma(\pi))$. Consider the map $\tau : V \to W$ defined by:

$$\forall u \in V \ , \ \tau(u) = \begin{cases} \sigma(u) & \text{if} \quad u \in V \setminus \{x\} \\ y^* & \text{if} \quad u = x \end{cases}$$

Then it is clear that τ coincides with σ on $V \setminus \{x\}$ and $\tau(x) \notin \mathrm{Fr}(\sigma(\pi))$. In order to show the existence of $\tau : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ it is sufficient to show the existence of an essential substitution associated with $\tau : V \to W$. From theorem (29) of page 375 it is sufficient to show that $|W|$ is an infinite cardinal, or that it is finite with $|V| \leq |W|$. However, this follows immediately from the existence of the essential substitution $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ and theorem (29). So it remains to show that $\mathrm{Fr}(\sigma(\pi))$ is a proper subset of W. This is clearly true if $|W|$ is an infinite cardinal. So we may assume that $|W|$ if finite, in which case we have $|V| \leq |W|$. In particular, $|V|$ is also a finite cardinal and since $x \notin \mathrm{Fr}(\pi)$ we have $|\mathrm{Fr}(\pi)| < |V|$. Hence we have the following inequalities:

$$|\mathrm{Fr}(\sigma(\pi))| = |\sigma(\mathrm{Fr}(\pi))| \leq |\mathrm{Fr}(\pi)| < |V| \leq |W|$$

So $\mathrm{Fr}(\sigma(\pi))$ is indeed a proper subset of W, as requested. **.**

3.5.4 Essential Substitution of Clean Proof

It is all very nice to have constructed essential substitutions $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ associated with $\sigma : V \to W$. So we have a tool substituting variables in proofs while avoiding capture. However, given $\pi \in \mathbf{\Pi}(V)$ we need to check that the conclusion and hypothesis of $\sigma(\pi)$ are what we expect. This is the purpose of the present section. With regards to the conclusion, we cannot hope to say much about the valuation $\mathrm{Val} \circ \sigma(\pi)$, but we certainly should be able to prove that $\mathrm{Val}^+ \circ \sigma(\pi) \sim \sigma \circ \mathrm{Val}^+(\pi)$ where $\sim$ is the substitution congruence on $\mathbf{P}(W)$. Note that the 'σ' appearing in $\sigma \circ \mathrm{Val}^+(\pi)$ refers to the restriction of the essential proof substitution $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ to $\mathbf{P}(V)$, and not to the brute force substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ of definition (24). It would not

make sense otherwise: we have no assumption about the validity of σ for π or the validity of σ for $\mathrm{Val}^+(\pi)$. The context gives us an essential substitution $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ which can equally act on formulas since $\mathbf{P}(V) \subseteq \mathbf{\Pi}(V)$. So it is clear from the context that the only sensible interpretation of $\sigma \circ \mathrm{Val}^+(\pi)$ is to regard σ as essential. This is in contrast with similar results we previously obtained in these notes: for π totally clean and σ valid for π, we obtained $\mathrm{Val} \circ \sigma(\pi) = \sigma \circ \mathrm{Val}(\pi)$ in proposition (229). For π clean and σ valid for π we obtained $\mathrm{Val}^+ \circ \sigma(\pi) = \sigma \circ \mathrm{Val}^+(\pi)$ in proposition (248). In both cases, the right-hand-side 'σ' was the naive substitution of definition (24). One question we may ask is whether we should hope to have $\mathrm{Val}^+ \circ \sigma(\pi) = \sigma \circ \mathrm{Val}^+(\pi)$ rather than a mere α-equivalence. The answer is no. By virtue of proposition (291), an essential proof substitution $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ can be redefined modulo the substitution congruence, and still qualify as an essential substitution associated to the same $\sigma : V \to W$. So if $\mathrm{Val}^+ \circ \sigma(\pi) = \sigma \circ \mathrm{Val}^+(\pi)$ happened to be true, we could redefine σ on $\mathbf{P}(V)$ alone, without changing $\sigma(\pi)$.

Proposition 305 *Let V, W be sets and $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ be an essential proof substitution. Let $\pi \in \mathbf{\Pi}(V)$ be a clean proof. Then $\sigma(\pi)$ is clean and:*

$$\mathrm{Val}^+ \circ \sigma(\pi) \sim \sigma \circ \mathrm{Val}^+(\pi) \tag{3.56}$$

where $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is the restriction and $\sim$ is the substitution congruence.

Proof
Before we start, it should be noted that the map $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ on the right-hand-side of (3.56) is simply the restriction of $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ and not the substitution associated with $\sigma : V \to W$ as per definition (24). We know from proposition (288) that $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is an essential substitution associated with the same $\sigma : V \to W$ as is $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$. We now assume that π is a clean proof. First we show that $\sigma(\pi)$ is clean. From proposition (275) it is sufficient to show that $\mathcal{M} \circ \sigma(\pi)$ is clean. Having assumed $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ is an essential proof substitution, we have $\mathcal{M} \circ \sigma(\pi) = \bar{\sigma} \circ \mathcal{M}(\pi)$. So we need to show that $\bar{\sigma} \circ \mathcal{M}(\pi)$ is clean. However, from proposition (275) we know that $\mathcal{M}(\pi)$ is clean, while from proposition (256) the minimal extension $\bar{\sigma} : \bar{V} \to \bar{W}$ is valid for $\mathcal{M}(\pi)$. It follows from proposition (248) that $\bar{\sigma} \circ \mathcal{M}(\pi)$ is clean as requested. It remains to prove the equivalence $\mathrm{Val}^+ \circ \sigma(\pi) \sim \sigma \circ \mathrm{Val}^+(\pi)$. Using theorem (14) of page 149 it is sufficient to prove the equality between minimal transforms $\mathcal{M} \circ \mathrm{Val}^+ \circ \sigma(\pi) = \mathcal{M} \circ \sigma \circ \mathrm{Val}^+(\pi)$. In fact, from proposition (112) we simply need to show the equivalence $\mathcal{M} \circ \mathrm{Val}^+ \circ \sigma(\pi) \sim \mathcal{M} \circ \sigma \circ \mathrm{Val}^+(\pi)$ where $\sim$ denotes the substitution congruence on $\mathbf{P}(\bar{W})$. Having established that $\sigma(\pi)$ is clean, using proposition (254) we obtain the following:

$$\begin{array}{rcl}
\mathcal{M} \circ \mathrm{Val}^+ \circ \sigma(\pi) & \sim & \mathrm{Val}^+ \circ \mathcal{M} \circ \sigma(\pi) \\
\sigma \text{ essential } \to & = & \mathrm{Val}^+ \circ \bar{\sigma} \circ \mathcal{M}(\pi) \\
\text{prop. (248) } \to & = & \bar{\sigma} \circ \mathrm{Val}^+ \circ \mathcal{M}(\pi) \\
\text{A: to be proved } \to & \sim & \bar{\sigma} \circ \mathcal{M} \circ \mathrm{Val}^+(\pi)
\end{array}$$

$$\sigma \text{ essential } \rightarrow \quad = \quad \mathcal{M} \circ \sigma \circ \text{Val}^+(\pi)$$

So it remains to prove the equivalence $\bar{\sigma} \circ \text{Val}^+ \circ \mathcal{M}(\pi) \sim \bar{\sigma} \circ \mathcal{M} \circ \text{Val}^+(\pi)$. Using theorem (15) of page 152, it is sufficient to show $\text{Val}^+ \circ \mathcal{M}(\pi) \sim \mathcal{M} \circ \text{Val}^+(\pi)$ and furthermore that $\bar{\sigma}$ is valid for both formulas. The equivalence follows from π being clean and proposition (254). The fact that $\bar{\sigma}$ is valid for $\mathcal{M} \circ \text{Val}^+(\pi)$ follows from proposition (100). The fact that $\bar{\sigma}$ is valid for $\text{Val}^+ \circ \mathcal{M}(\pi)$ follows from proposition (237) and the validity of $\bar{\sigma}$ for $\mathcal{M}(\pi)$, which is itself a consequence of proposition (256) and which completes our proof. **.**

We shall now check that $\text{Hyp}(\sigma(\pi))$ is also what we expect, namely the image $\sigma(\text{Hyp}(\pi)) = \{\sigma(\phi) : \phi \in \text{Hyp}(\pi)\}$. Once again, the '$\sigma$' involved in this last expression can only be the essential σ, not the substitution $\sigma : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$ of definition (24). Since σ can be arbitrarily redefined modulo the substitution congruence, we cannot hope to have an exact equality $\text{Hyp}(\sigma(\pi)) = \sigma(\text{Hyp}(\pi))$. The best we can hope for is that every element of $\text{Hyp}(\sigma(\pi))$ be α-equivalent to an element of $\sigma(\text{Hyp}(\pi))$ and conversely. We should also remember that no sensible result can be obtained unless π is a clean proof. For example, consider $V = \{x, y\}$ with $x \neq y$, $\pi = \nabla x(x \in x)$ and $\sigma : \mathbf{\Pi}(V) \rightarrow \mathbf{\Pi}(V)$ an an essential substitution associated with the identity mapping $i : V \rightarrow V$. Since $\pi \sim \rho$ where $\rho = \nabla y(y \in y)$, we can redefine σ so as to have $\sigma(\pi) = \rho$. It is clear the equality modulo $\text{Hyp}(\sigma(\pi)) \sim \sigma(\text{Hyp}(\pi))$ is false in this case.

Proposition 306 *Let V, W be sets and $\sigma : \mathbf{\Pi}(V) \rightarrow \mathbf{\Pi}(W)$ be an essential proof substitution. Let $\pi \in \mathbf{\Pi}(V)$ be a clean proof. Then we have:*

$$\text{Hyp}(\sigma(\pi)) \sim \sigma(\text{Hyp}(\pi)) \tag{3.57}$$

where $\sim$ is the equality modulo the substitution congruence as per definition (85)*.*

Proof
Before we start, it should be noted that the map $\sigma : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$ on the right-hand-side of (3.57) is simply the restriction of $\sigma : \mathbf{\Pi}(V) \rightarrow \mathbf{\Pi}(W)$ and not the substitution associated with $\sigma : V \rightarrow W$ as per definition (24). We know from proposition (288) that the map $\sigma : \mathbf{P}(V) \rightarrow \mathbf{P}(W)$ is an essential substitution associated with the same $\sigma : V \rightarrow W$ as is $\sigma : \mathbf{\Pi}(V) \rightarrow \mathbf{\Pi}(W)$. We now assume that π is a clean proof. We need to show that any formula of $\text{Hyp}(\sigma(\pi))$ is substitution equivalent to a formula of $\sigma(\text{Hyp}(\pi))$ and conversely that any formula of $\sigma(\text{Hyp}(\pi))$ is substitution equivalent to a formula of $\text{Hyp}(\sigma(\pi))$. Using theorem (14) of page 149 it is therefore sufficient to prove $\mathcal{M}(\text{Hyp}(\sigma(\pi))) = \mathcal{M}(\sigma(\text{Hyp}(\pi)))$. Using proposition (305), the proof $\sigma(\pi)$ is clean and consequently from proposition (251) we obtain:

$$\begin{array}{rcl} \mathcal{M}(\text{Hyp}(\sigma(\pi))) & = & \text{Hyp}(\mathcal{M} \circ \sigma(\pi)) \\ \sigma \text{ essential } \rightarrow & = & \text{Hyp}(\bar{\sigma} \circ \mathcal{M}(\pi)) \\ \text{prop. (193)} \rightarrow & = & \bar{\sigma}(\,\text{Hyp}(\mathcal{M}(\pi))\,) \end{array}$$

$$\begin{array}{rcl} \text{prop. (251), } \pi \text{ clean } \rightarrow & = & \bar{\sigma}(\,\mathcal{M}(\mathrm{Hyp}(\pi))\,) \\ & = & \bar{\sigma} \circ \mathcal{M}(\mathrm{Hyp}(\pi)) \\ \sigma \text{ essential } \rightarrow & = & \mathcal{M} \circ \sigma(\mathrm{Hyp}(\pi)) \\ & = & \mathcal{M}(\sigma(\mathrm{Hyp}(\pi))) \end{array}$$

.

3.5.5 The Substitution Theorem

We have now reached the end of a long journey, as we are about to prove what appears to us as a delicate point of mathematical logic: the substitution theorem. Everything we did in this long chapter, all the details and the pedantry over the free algebra $\mathbf{\Pi}(V)$ was directed at this single result. We did what we could to arrive at it with the shortest possible route, developing along the way some key notions of valuation modulo, minimal transform, substitution congruence, substitution rank and essential substitution. It is ironic that most texts in mathematical logic will not take more than half a page to prove the result. Some will simply use one line to point out that substituting variables in a proof gives you another proof etc. . . So we must be doing something wrong. To be fair, these texts always assume that V is countably infinite. So it is possible to carry out substitutions of variables which rely on freshness and are injective. Proving a substitution theorem in the injective case is of course a lot simpler, as can be seen from proposition (230). Our substitution theorem is stated for essential substitutions, a notion which does not exist in mathematical textbooks as far as we can tell. We believe essential substitutions are a key notion in formal languages with variable binding. If we knew enough about category theory and decided to design a category whose objects are the spaces $\mathbf{P}(V)$, the morphisms should be essential substitutions $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ or something approaching, depending on the exact identification we wish to perform on $\mathbf{P}(V)$. Of course we are not completely convinced about this, as we are troubled by the fact that no essential substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ exists whenever W is a finite set which is smaller than V. This can be seen from theorem (18) of page 174.

Now what is the big fuss about the substitution theorem, why do we care so much? A sequent $\Gamma \vdash \phi$ can be carried over into the sequent $\sigma(\Gamma) \vdash \sigma(\phi)$: this is rather obvious and nowhere near as interesting as determining for example whether the sequent $\mathbf{ZF} \vdash \mathtt{Cons}(\mathbf{ZF})$ is true or not. Yes, Gödel's second incompleteness theorem is far more interesting, we cannot argue about that. We are doing what we can. We need to walk before we can run. In the big scheme of things, the substitution theorem is just a small step. It has given us the opportunity to derive some valuable insight on the free algebra $\mathbf{\Pi}(V)$ and more generally on Hilbert-style deduction systems. More fundamentally, the substitution theorem is a prerequisite to a milestone of mathematical logic: Gödel's completeness theorem. We have no hope of proving the completeness theorem unless we can prove that consistency is preserved through embeddings. Specifi-

cally, if $i : V \to W$ is an injective map and Γ is a consistent subset of V, then $i(\Gamma)$ should be a consistent subset of W. As can be seen from definition (99), proving the consistency of $i(\Gamma)$ from the consistency of Γ involves carrying over the sequent $i(\Gamma) \vdash \bot$ into $\Gamma \vdash \bot$. Without thinking very hard about this, it is clear we need some form of substitution theorem before anything else.

Unfortunately, despite the successful delivery of theorem (30) below, our initial question remains open: in order to carry over the sequent $i(\Gamma) \vdash \bot$ into $\Gamma \vdash \bot$, we need an essential substitution $\sigma : \mathbf{P}(W) \to \mathbf{P}(V)$ associated with a left inverse $\sigma : W \to V$ of the embedding $i : V \to W$. Such essential substitution does not exist when V is finite and strictly smaller than W. So we still do not know whether consistency is preserved through embedding in our axiomatization of first order logic with finitely many variables.

Theorem 30 (Substitution Theorem) *Let $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ where V, W are sets be an essential substitution. Let $\Gamma \subseteq \mathbf{P}(V)$ and $\phi \in \mathbf{P}(V)$. Then:*

$$\Gamma \vdash \phi \quad \Rightarrow \quad \sigma(\Gamma) \vdash \sigma(\phi)$$

Proof
We assume the sequent $\Gamma \vdash \phi$ is true. There exists a proof $\pi \in \mathbf{\Pi}(V)$ such that $\mathrm{Val}(\pi) = \phi$ and $\mathrm{Hyp}(\pi) \subseteq \Gamma$. From proposition (185) we may assume without loss of generality that π is totally clean. In particular from proposition (238) the proof π is clean. Furthermore from proposition (232) we have the equality $\mathrm{Val}^+(\pi) = \mathrm{Val}(\pi)$. From proposition (292) there exists an essential proof substitution $\sigma : \mathbf{\Pi}(V) \to \mathbf{\Pi}(W)$ which is an extension of σ. Consider the proof $\sigma(\pi) \in \mathbf{\Pi}(W)$. In order to show that $\sigma(\Gamma) \vdash \sigma(\phi)$ is true, from theorem (22) of page 293 it is sufficient to prove $\mathrm{Val}^+(\sigma(\pi)) \sim \sigma(\phi)$ and $\mathrm{Hyp}(\sigma(\pi)) \precsim \sigma(\Gamma)$, where $\sim$ is the substitution congruence on $\mathbf{P}(W)$ and $\precsim$ is the inclusion modulo. Since π is a clean proof, from proposition (305) we have the following:

$$\mathrm{Val}^+(\sigma(\pi)) \sim \sigma \circ \mathrm{Val}^+(\pi) = \sigma \circ \mathrm{Val}(\pi) = \sigma(\phi)$$

Furthermore from proposition (306) since π is clean we obtain:

$$\mathrm{Hyp}(\sigma(\pi)) \sim \sigma(\mathrm{Hyp}(\pi)) \subseteq \sigma(\Gamma)$$

From which we conclude $\mathrm{Hyp}(\sigma(\pi)) \precsim \sigma(\Gamma)$ as requested. **.**

Most people are presumably not familiar with essential substitutions. However, the idea of capture-avoiding substitutions is quite common. We shall now provide a corollary of theorem (30) dealing with naive substitutions in the sense of definition (24). Given a true sequent $\Gamma \vdash \phi$, it is a natural question to ask whether $\sigma(\Gamma) \vdash \sigma(\phi)$ whenever $\sigma : V \to W$ avoids capture on ϕ and every element of Γ. We are able to answer this question in the case when $|W|$ is an infinite cardinal or $|V| \leq |W|$: we simply invoke the existence of an associated essential substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ and use theorem (30) to conclude. Needless to say that having to keep conditions on the cardinals $|V|$ and $|W|$ is highly unsatisfactory. We would like to claim that $\sigma(\Gamma) \vdash \sigma(\phi)$ in all cases when σ avoids capture. We currently do not know whether this is true.

Proposition 307 *Let V, W be sets such that $|W|$ is an infinite cardinal or $|V| \leq |W|$. Let $\sigma : V \to W$ be a map. Let $\Gamma \subseteq \mathbf{P}(V)$ and $\phi \in \mathbf{P}(V)$. We assume that σ is valid for ϕ and every element of Γ. Then we have:*

$$\Gamma \vdash \phi \quad \Rightarrow \quad \sigma(\Gamma) \vdash \sigma(\phi)$$

where $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is the associated substitution as per definition (24).

Proof
Since $|W|$ is an infinite cardinal or $|V| \leq |W|$, from theorem (18) of page 174 there exists an essential substitution $\sigma^* : \mathbf{P}(V) \to \mathbf{P}(W)$ associated with σ. Hence if we assume that $\Gamma \vdash \phi$, from theorem (30) we obtain $\sigma^*(\Gamma) \vdash \sigma^*(\phi)$. Using theorem (22) of page 293 there exists a proof $\pi^* \in \mathbf{\Pi}(W)$ such that $\mathrm{Val}^+(\pi^*) \sim \sigma^*(\phi)$ and $\mathrm{Hyp}(\pi^*) \precsim \sigma^*(\Gamma)$, where $\sim$ is the substitution congruence on $\mathbf{P}(W)$ and $\precsim$ is the associated inclusion modulo. We need to show that $\sigma(\Gamma) \vdash \sigma(\phi)$. In order to do so, applying theorem (22) once more it is sufficient to prove that $\mathrm{Val}^+(\pi^*) \sim \sigma(\phi)$ and $\mathrm{Hyp}(\pi^*) \precsim \sigma(\Gamma)$. First we show that $\mathrm{Val}^+(\pi^*) \sim \sigma(\phi)$: it is sufficient to prove that $\sigma^*(\phi) \sim \sigma(\phi)$ which follows immediately from proposition (115) and the validity of σ for ϕ. Next we show that $\mathrm{Hyp}(\pi^*) \precsim \sigma(\Gamma)$. So let $\chi \in \mathrm{Hyp}(\pi^*)$. We need to show the existence of $\psi \in \Gamma$ such that $\chi \sim \sigma(\psi)$. However, from the inclusion modulo $\mathrm{Hyp}(\pi^*) \precsim \sigma^*(\Gamma)$ there exists $\psi \in \Gamma$ such that $\chi \sim \sigma^*(\psi)$. It is therefore sufficient to prove that $\sigma^*(\psi) \sim \sigma(\psi)$. Having assumed that $\sigma : V \to W$ is valid for every element of Γ, in particular it is valid for ψ. Hence the equivalence $\sigma^*(\psi) \sim \sigma(\psi)$ follows once again from proposition (115), which completes our proof. **.**

Chapter 4

Semantics and Dual Space

4.1 Valuation and Semantics

4.1.1 Preliminaries

One of the fascinating aspects of mathematical logic, at least for us, is a sense of renewal: we are starting all over again, rebuilding mathematics from scratch, from the solid ground of axiomatic set theory. Most living mathematicians have studied set theory from a naive point of view, where formal reasoning is muddled up with intuition. The dream is to eliminate the old intuitive knowledge and to replace it with a new set of completely formal deductions. We are of course still relying on the old school: everything we have done so far is tainted with the doubt and suspicion which surrounds inappropriate foundations. But we console ourselves by labeling the work as *meta-mathematics*. It is the lesser kind of mathematics, the one for which it is ok to be unsure. The *true* mathematics will come later. It will be almighty and powerful, or so we hope.

In the pursuit of complete certainty, the purely syntactic approach of spelling out a formal language $\mathbf{P}(V)$, a set of axioms $\mathbf{A}(V)$ and a deductive system $\mathbf{\Pi}(V)$, appears to be the way forward. Why should we need anything more? Why bother with semantics and in particular model theory? Surely the last thing we want is to mix up axiomatic set theory with semantic arguments. These cannot be trusted. So why? There is an immediate answer to this: we simply love it. We may look down on meta-mathematics for its lack of appropriate foundations, but we are still compelled to push it further. Although we claim otherwise, we believe in it. In fact, we are pretty sure our heuristic meta-mathematical arguments can be formalized, once the proper framework is in place. The sequent $\Gamma \vdash \phi$ will become a formula $\mathbf{Prf}(\Gamma, \ulcorner\phi\urcorner)$. We may even be able to design our own proof of Gödel's incompleteness theorem following Peter Smith [56]. There are many fascinating results of mathematical logic, which we hope one day to understand: **AC** is independent of **ZF** and **GCH** is independent of **ZFC**. Clearly we cannot stop just yet.

However, there is an even greater purpose to semantics: it is all very nice to

spell out a set of axioms and a deductive system. But how do we know it makes any sense? An axiomatization of first order logic relies on many choices. What do we have to validate these choices? Yes, the *modus ponens* rule of inference seems pretty reasonable, and the deduction theorem holds in full generality. But what about our choice of axioms? For all we know, these axioms could be inconsistent. We have no way to tell. Or there could be too few of them, which would prevent us from formalizing standard mathematical arguments. Somehow we need a form of validation, and this is where model theory comes in: a *good* axiomatization of first order logic should be *sound* and *complete*. This is the least we can ask for. So we shall put it to the test. We are not claiming that *soundness* and *completeness* are enough. We certainly believe the deduction theorem should also be true while many authors disagree (e.g. [18], [30], [32], [39], [44], [45], [62]). If we are completely honest, what constitutes a *good* axiomatization of first order logic is still an open question.

So we need semantics and model theory. For those who remain unconvinced, here is the final blow: semantics is arguably about the concept of *truth*. We give birth to special maps $v : \mathbf{P}(V) \to 2$ which we call *valuations*. Whenever $v(\phi) = 1$ we say that a formula ϕ is *true*. Otherwise if $v(\phi) = 0$, we say that a formula ϕ is false. After waiting for so long, we seem to have reached an answer to one of the most fascinating questions of all: *what is the nature of mathematical truth*? This is magical. It feels like we are playing God, looking at mathematics *from above*. Assuming we are right and $\mathbf{P}(V)$ is rich enough to code the Riemann hypothesis as a formula ϕ, here we are wondering whether $v(\phi) = 1$. For so many years, the concept of *truth* has eluded us. We remember the words of André Lichnerowicz telling us "*I do not know what a true proposition is, which is not provable*"[1], and somehow we agreed with him. We still do, despite learning about Gödel. But things have become messy. As children, we believed in absolute truth: mathematics was its guardian. Everything was either true or false. Physicists could gloat as much as they want about the *real world*. They had no handle on the *truth*. Everything they did was mere *modeling*. How sad. Things are no longer so simple: the pre-eminence of euclidian geometry is gone and the continuum hypothesis is neither true nor false. André Lichnerowicz is right and so is Kurt Gödel: we need to get smarter. The physicists were right all along.

4.1.2 Valuation and Dual Space

As far as we can tell, every textbook in mathematical logic introduces semantics via model theory. We shall not do so. We believe there are many good reasons to postpone the study of model theory to a later stage. So here they are: first of all, the approach we shall take will turn out to be equivalent to the standard approach anyway. This is hardly a reason to be different, but it may alleviate some of the irritation from the reader, and generate some degree of acceptance. We are interested in the concept of truth: so we shall define the notion of *valuation* which are maps $v : \mathbf{P}(V) \to 2$ with the obvious properties

[1] Je ne sais pas ce qu'est une proposition vraie non démontrable.

and in particular the *soundness* property $\vdash \phi \;\Rightarrow\; v(\phi) = 1$. As it turns out, every model and variables assignment will give rise to a *valuation*. This is hardly surprising and is commonly known under the slogan *first order logic is sound*. What is less obvious and somehow linked to the completeness theorem, is the fact that every valuation arises from a model and variables assignment. So although we shall consider the notion of semantic entailment in terms of valuations and not models, since *every valuation has a model* the two approaches are equivalent. This is our first point. Another reason for postponing the introduction of model theory is this: the set of valuations $v : \mathbf{P}(V) \to 2$ which we shall denote $\mathbf{P}^*(V)$ and call the *dual space* is of enormous interest in its own right. Rushing into model theory is a wasted opportunity as we fail to pay due attention to what we believe is a fundamental object. We are pretty sure this object has connections with existing works such as P.T. Johnstone [33], Henrik Forssell [19] and Murdoch J. Gabbay [21] which we have yet to investigate. Furthermore, the dual space $\mathbf{P}^*(V)$ is a set and not a proper class. Defining semantic entailments in terms of a class of models seems to be madness when we can simply and equivalently do so in terms of a set. Another reason for postponing model theory is *decoupling*: most of us have experience in coding where our projects should adopt a modular design with decoupled functionality. The same is true in mathematics: the proof of Gödel's completeness theorem involves a fair amount of work on maximal consistent sets which have nothing to do with models. In fact as will appear later, a maximal consistent set is nothing but a valuation. In other words, the dual space $\mathbf{P}^*(V)$ is exactly the set of maximal consistent sets. The crunch of the completeness theorem is to show that *every valuation has a model*, and this is the way we intend to present it. Finally, we feel there is another good reason to define *semantic entailment* in terms of valuations rather than models: it offers a scope for further generalization. As pointed out by W.J. Blok and D. Pigozzi [6], the *Lindenbaum-Tarski process* is somehow general: we start with a consequence relation $\vdash$. We obtain a congruence from it, which in turn gives us a quotient algebra. The consequence relation $\vdash$ also gives us a dual space $\mathbf{P}^*(V)$. In fact as will appear later, this dual space can be defined directly in terms of the congruence, without reference to the consequence relation, and the quotient algebra is isomorphic to an algebra of subsets of the dual. We feel we are only scratching the surface and there is a lot more to the story. This story belongs to *abstract algebraic logic* and has little to do with model theory as far as we can tell. It is a story which is most likely expounded in the references [33], [19] and [21] which we hope to investigate further in due course.

Definition 97 *Let V be a set. A map $v : \mathbf{P}(V) \to 2$ is called a* valuation *on $\mathbf{P}(V)$ if and only if it satisfies the following properties. Given $\phi_1, \phi_2, \phi \in \mathbf{P}(V)$:*

$$\begin{array}{ll} (i) & v(\bot) = 0 \\ (ii) & v(\phi_1 \to \phi_2) = v(\phi_1) \to v(\phi_2) \\ (iii) & \vdash \phi \;\Rightarrow\; v(\phi) = 1 \end{array}$$

The set of valuations on $\mathbf{P}(V)$ is called the dual space *and denoted $\mathbf{P}^*(V)$.*

Looking at definition (56), a *valuation* is therefore a propositional valuation which satisfies the implication $\vdash \phi \Rightarrow v(\phi) = 1$. We could call this the *soundness* property. So a *valuation* is a propositional valuation which is *sound*. Note that we are not yet in a position to say whether there exists any valuation at all. We do not know whether our deductive system is consistent. If the sequent $\vdash \bot$ were to be true, then the dual space $\mathbf{P}^*(V)$ would be the empty set. Luckily this will not be the case, but we shall need to wait for some model theory and the soundness theorem (37) of page 426 to be sure.

So the dual space $\mathbf{P}^*(V)$ is not empty. But how many elements does it have? We have no idea at this stage. Let us assume for now that set theory can be coded in the language of $\mathbf{P}(V)$. Does there exist a valuation $v : \mathbf{P}(V) \to 2$ which satisfies **ZFC**? Obviously we do not have a precise understanding of this question at this point. But we understand it well enough to be interested. So suppose we have defined a subset $\Gamma \subseteq \mathbf{P}(V)$ representing all the axioms of **ZFC**. Does there exist a valuation $v \in \mathbf{P}^*(V)$ such that $v(\phi) = 1$ for all $\phi \in \Gamma$? Is such valuation unique? If it is not unique, can we add a few reasonable axioms to **ZFC** so we end up with a unique valuation? We remember the phrase of Albert Einstein: "*God doesn't play dice*". So if there is some form of *mathematical God* presiding over the realm of *absolute truth*, we should expect a particular valuation $v^* : \mathbf{P}(V) \to 2$ to stand out: the official word from above. Given a formula $\phi \in \mathbf{P}(V)$, we may not be able to evaluate $v^*(\phi)$ ever. But $v^*(\phi)$ is there: it is either 1 or 0. It is for us humans to decipher the divine truth. As David Hilbert once said: "*We must know - we will know!*".[2]

Unfortunately, the ideal of an immutable God-sent *mathematical truth* has become very hard to justify: there is no unique valuation $v^* : \mathbf{P}(V) \to 2$ which satisfies the axioms of **ZFC**. In fact, we cannot even be sure there is any valuation at all satisfying these axioms. So let us see why this is: in 1940 Kurt Gödel established that the *continuum hypothesis* **CH** could not be disproved from the axioms of **ZFC**. In 1963 Paul Cohen showed that $\neg$**CH** could not be disproved either. In other words, if we assume **ZFC** is consistent, then both **ZFC** + **CH** and **ZFC** + $\neg$**CH** are also consistent. As we shall soon discover in theorem (31) of page 405, consistent subsets are satisfiable and vice-versa. So if there exists a valuation $v \in \mathbf{P}^*(V)$ which satisfies **ZFC**, then there are at least two such valuations, one which satisfies **CH** and one which doesn't. So we can forget about uniqueness. The best we can hope for is to design a reasonable extension of **ZFC**. But this will not work either: assuming we had a good reason to accept or reject the continuum hypothesis, we are told from Gödel's first incompleteness theorem that no *reasonable* extension Δ of **ZFC** will ever be *complete*: there will always be a formula $\phi \in \mathbf{P}(V)$ which can neither be disproved nor be proved from Δ, i.e. for which the sequents $\Delta \vdash (\phi \to \bot)$ and $\Delta \vdash \phi$ are false. As we shall see from proposition (314), this would mean that both $\Delta \cup \{\phi\}$ and $\Delta \cup \{\phi \to \bot\}$ are consistent hence satisfiable, and we cannot have a unique valuation satisfying Δ. Of course we do not know what a *reasonable* extension of **ZFC** is. The set of axioms Δ would need to

[2] Wir müssen wissen wir werden wissen!

be *recursively enumerable* (as well as consistent) and we have not yet studied any computability theory in these pages. This is for later: we certainly intend to push these notes further, until we fully understand the work of Kurt Gödel, and indeed Paul Cohen. In the meantime, we shall accept that the only way to obtain a unique valuation $v^* : \mathbf{P}(V) \to 2$ would be to adopt a set of axioms $\Delta \supseteq \mathbf{ZFC}$ which no computer program could ever enumerate, let alone decide.

We now consider the question of existence: is there a valuation $v : \mathbf{P}(V) \to 2$ satisfying **ZFC**? By virtue of theorem (31) of page 405, this question amounts to asking whether **ZFC** is consistent. Once, again the answer is highly disappointing: if **ZFC** happens to be consistent, it would seem from Gödel's second incompleteness theorem that we shall never be able to prove it. Broadly speaking, Gödel second incompleteness theorem states that no consistent and *effectively generated* theory can prove its own consistency. In particular, **ZFC** cannot be consistent and prove its own consistency. So assume once again that $\Gamma \subseteq \mathbf{P}(V)$ represents all the axioms of **ZFC**. Then we cannot ever hope to prove that Γ is a consistent subset of $\mathbf{P}(V)$. Why not? Well suppose we are able to prove the mathematical statement "Γ *is consistent*". Saying that **ZFC** is *effectively generated* is the same as saying that Γ is a *recursively enumerable* set. In other words, there exists some computer program which generates all the elements of Γ. A computer program is nothing but a big formula in some formal language. So it is easy to believe that if Γ is recursively enumerable, then the mathematical statement "Γ *is consistent*" can be coded as some formula of first order logic $\phi \in \mathbf{P}(V)$. For the purpose of the present discussion, we may denote this formula ϕ as $\ulcorner \Gamma$ is consistent$\urcorner$. Now remember that everything we do in these notes relies on **ZFC**. The foundation of our meta-mathematics is naive set theory based on the axioms of **ZFC**. So if we are able to prove the mathematical statement "Γ *is consistent*", then by carefully following every step of the proof we should be able to design a formal proof $\pi \in \mathbf{\Pi}(V)$ whose conclusion is the formula $\mathrm{Val}(\pi) = \phi = \ulcorner \Gamma$ is consistent$\urcorner$, using premises which are axioms of **ZFC**, i.e. such that $\mathrm{Hyp}(\pi) \subseteq \Gamma$. In other words, if we are able to prove "Γ *is consistent*", then the sequent $\Gamma \vdash \ulcorner \Gamma$ is consistent$\urcorner$ should be true. According to Gödel's second incompleteness theorem, this cannot be the case, unless Γ is inconsistent. Note that we are not claiming any part of the preceding argument is anything but informal gibberish, which an expert reader will scorn. There is only so much we understand at this stage. We simply hope to convince the less informed reader that the consistency of **ZFC** is probably beyond our reach and furthermore, that fully understanding Gödel will require serious work. A recent textbook on Gödel is Peter Smith [56].

So we shall never prove that **ZFC** is consistent. Even if we are successful in using the algebra $\mathbf{P}(V)$ as the basis of a formal language for axiomatic set theory, even if we manage to properly define a subset $\Gamma \subseteq \mathbf{P}(V)$ representing all the axioms of **ZFC**, we shall never be able to prove the existence of a valuation $v \in \mathbf{P}^*(V)$ which satisfies Γ. As long as our meta-mathematics is based on **ZFC**, we shall never know. However, the history of human thoughts has seen many changes and **ZFC** is not cast in stone. There is nothing excluding the possibility of a stronger system emerging at some time in the future. This

formal system may be represented as a wider set of axioms $\Delta \supseteq \mathbf{ZFC}$. When this happens, the newly accepted set of axioms Δ may be strong enough for us to show that **ZFC** is consistent. There is light at the end of the tunnel. After all, we could argue this type of scenario has already occurred: once upon a time, the human race believed in Peano Arithmetic **PA**. In those days, no one could prove that **PA** was consistent. Yet one day, **ZFC** appeared and we now know that **PA** is consistent. Regardless of how frivolous the story is, it is unfortunate that the consistency of **PA** is no longer what matters: what we care about is **ZFC**. So when the time comes and the mathematical community finally adopts a stronger axiomatic system $\Delta \supseteq \mathbf{ZFC}$, the odds are we shall care about Δ. This is the curse of Gödel's second incompleteness theorem: Δ cannot prove the consistency of Δ. So whichever way we look at it, we shall never be content.

At this point most of us will cry. Yet, it is precisely at the height of gloom and disappointment that some twisted miracle happens: this miracle is the realization that knowing the consistency of **ZFC** is in fact worthless. As we shall see from proposition (313), if Γ is an inconsistent subset of $\mathbf{P}(V)$ then the sequent $\Gamma \vdash \phi$ is true for all $\phi \in \mathbf{P}(V)$. In other words, it is possible to prove anything from an inconsistent theory. So suppose Gödel was wrong and we could somehow prove the consistency of **ZFC** from **ZFC**. This could be for two reasons: the first reason is that **ZFC** is indeed consistent. The second reason is that **ZFC** is simply inconsistent. Proving the consistency of **ZFC** wouldn't prove anything. In fact, in light of Gödel's second incompleteness theorem, proving the consistency of **ZFC** would actually prove something: it would constitute a contradiction and show that **ZFC** is inconsistent.

Proposition 308 *Let V be a set and $\leq$ be the Hilbert deductive preorder on $\mathbf{P}(V)$. Then for all $\phi, \psi \in \mathbf{P}(V)$ and valuation $v \in \mathbf{P}^*(V)$ we have:*

$$\phi \leq \psi \;\Rightarrow\; v(\phi) \leq v(\psi)$$

Proof
Suppose $\phi \leq \psi$. Then we have $\vdash (\phi \to \psi)$ and since $v : \mathbf{P}(V) \to 2$ is a valuation we obtain $1 = v(\phi \to \psi) = v(\phi) \to v(\psi)$. It follows that $v(\phi) \leq v(\psi)$. .

The next proposition is elementary but very important: let $\sigma : V \to W$ be a map which has an associated essential substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$. Then we know that such essential substitution is not unique. However it is uniquely determined modulo the substitution congruence. So if $v : \mathbf{P}(W) \to 2$ is a valuation and $\phi \in \mathbf{P}(V)$, then $v(\sigma(\phi))$ is uniquely determined. For example in the case when $V = W$, the formula $\phi = \forall x \phi_1 \to \phi_1[y/x]$ is an axiom provided $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ refers to an essential substitution of y in place of x. So the details of the formula $\phi_1[y/x]$ may be unclear, but $v(\phi_1[y/x])$ is unambiguous.

Proposition 309 *Let V be a set and $\sim$ be a congruence which is stronger than the Hilbert deductive congruence. Then for all $\phi, \psi \in \mathbf{P}(V)$ and $v \in \mathbf{P}^*(V)$:*

$$\phi \sim \psi \;\Rightarrow\; v(\phi) = v(\psi)$$

Proof
So we assume that $v : \mathbf{P}(V) \to 2$ is a valuation and $\phi \sim \psi$. We need to show that $v(\phi) = v(\psi)$. Having assumed that $\sim$ is stronger than the Hilbert deductive congruence $\equiv$, in particular we have $\phi \equiv \psi$. Using $\phi \leq \psi$, from proposition (308) we obtain $v(\phi) \leq v(\psi)$. Likewise, from $\psi \leq \phi$ we obtain $v(\psi) \leq v(\phi)$. **.**

4.1.3 Semantic Entailment and Valid Formula

As explained in the previous section, we shall define the notion of semantic entailment in terms of valuation rather than model. In line with this convention, the following definition introduces the notion of *truth* and *satisfaction* also in terms of valuation. Hence we shall introduce obvious notations such as $v \vDash \phi$ and $v \vDash \Gamma$, which should be read as "v *satisfies* ϕ" and "v *satisfies* Γ".

Definition 98 *Let V be a set and $v : \mathbf{P}(V) \to 2$ be a valuation on $\mathbf{P}(V)$. We say that $\phi \in \mathbf{P}(V)$ is* true *for v or that v* satisfies *ϕ and we write:*

$$v \vDash \phi$$

if and only if $v(\phi) = 1$. Given $\Gamma \subseteq \mathbf{P}(V)$, we say that v satisfies *Γ and we write:*

$$v \vDash \Gamma$$

if and only if $v \vDash \psi$ for all $\psi \in \Gamma$. We say Γ is satisfiable *if $v \vDash \Gamma$ for some v.*

Note that the notations $v \vDash \phi$ and $v \vDash \{\phi\}$ have equivalent meaning. It is also clear that if v satisfies Δ and $\Delta \supseteq \Gamma$ then v also satisfies Γ. Finally, any valuation v vacuously satisfies the empty set $\emptyset$. This does not mean the empty set is satisfiable, until we know for a fact that $\mathbf{P}^*(V)$ is not empty. In definition (70) we introduced a relation $\vdash \subseteq \mathcal{P}(\mathbf{P}(V)) \times \mathbf{P}(V)$, which is often referred to as the relation of *syntactic entailment*. We shall now define a similar relation $\vDash$ which is that of *semantic entailment*. Given $\Gamma \subseteq \mathbf{P}(V)$ and $\phi \in \mathbf{P}(V)$, the statement $\Gamma \vDash \phi$ expresses the fact that for every valuation $v \in \mathbf{P}^*(V)$:

$$v \text{ satisfies } \Gamma \;\Rightarrow\; v \text{ satisfies } \phi$$

At this stage of the discussion, we still cannot be sure that the dual space $\mathbf{P}^*(V)$ is not empty. If this was the case, then $\Gamma \vDash \phi$ would be vacuously true.

Definition 99 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. Let $\phi \in \mathbf{P}(V)$. We say that ϕ is a semantic consequence of Γ, or that Γ* semantically entails *ϕ and we write:*

$$\Gamma \vDash \phi$$

if and only if for every valuation $v : \mathbf{P}(V) \to 2$ we have the implication:

$$v \vDash \Gamma \;\Rightarrow\; v \vDash \phi$$

Furthermore, we say that ϕ is valid *and we write $\vDash \phi$ if and only if $\emptyset \vDash \phi$.*

We defined a valid formula as any formula ϕ which satisfies the semantic entailment $\emptyset \vDash \phi$. However, a valuation $v : \mathbf{P}(V) \to 2$ always satisfies the empty set. Hence, a valid formula is simply a formula which is true for every valuation.

Proposition 310 *Let V be a set and $\phi \in \mathbf{P}(V)$. Then we have the equivalence:*

$$\vDash \phi \;\Leftrightarrow\; (\forall v \in \mathbf{P}^*(V)\;,\; v \vDash \phi)$$

In other words, a formula is valid if and only if it is true for every valuation.

Proof
First we show $\Rightarrow$: so we assume that ϕ is valid, i.e. $\vDash \phi$. Let $v \in \mathbf{P}^*(V)$ be a valuation. We need to show that $v \vDash \phi$. However from $\vDash \phi$ which is $\emptyset \vDash \phi$, we have the implication $v \vDash \emptyset \;\Rightarrow\; v \vDash \phi$. It is therefore sufficient to prove that $v \vDash \emptyset$, i.e. that v satisfies the empty set $\emptyset$. But this last statement is equivalent to $v \vDash \psi$ for all $\psi \in \emptyset$ which is vacuously true. So we now prove $\Leftarrow$: we assume that $v \vDash \phi$ for all $v \in \mathbf{P}^*(V)$. We need to show that $\vDash \phi$. So let v be a valuation. We need to show the implication $v \vDash \emptyset \;\Rightarrow\; v \vDash \phi$. However, $v \vDash \emptyset$ is vacuously true. So we simply need to show that $v \vDash \phi$ which is true by assumption. **.**

The relation $\vDash \subseteq \mathcal{P}(\mathbf{P}(V)) \times \mathbf{P}(V)$ will be seen to coincide with $\vdash$ after we prove theorem (33) of page 406. In particular, both relations satisfy the same properties. So rather than spend too much time investigating the relation $\vDash$, we shall focus on establishing the equality $\vDash = \vdash$. However, we now need to show:

Proposition 311 *Let V be a set and $\Gamma, \Delta \subseteq \mathbf{P}(V)$. Then for all $\phi \in \mathbf{P}(V)$:*

$$(\Gamma \supseteq \Delta) \wedge (\Delta \vDash \phi) \;\Rightarrow\; \Gamma \vDash \phi$$

Proof
We assume that $\Gamma \supseteq \Delta$ and $\Delta \vDash \phi$. We need to show that $\Gamma \vDash \phi$. So let v be a valuation which satisfies Γ, i.e. such that $v \vDash \Gamma$. We need to show that ϕ is true for v, i.e. that $v \vDash \phi$. However, from $v \vDash \Gamma$ we have $v \vDash \psi$ for all $\psi \in \Gamma$. Having assumed that $\Gamma \supseteq \Delta$, it follows that $v \vDash \psi$ for all $\psi \in \Delta$. Hence we see that v satisfies Δ i.e. that $v \vDash \Delta$. From $\Delta \vDash \phi$, we conclude that $v \vDash \phi$. **.**

We shall now establish one side of the equivalence between syntactic and semantic entailments. The full result will be obtained in theorem (33) of page 406. The proof of the following proposition is similar in spirit to that of the transitivity of $\vdash$ in proposition (169) which relies on a induction on the cardinal $|\Gamma|$. The deduction theorem (21) of page 226 effectively allows us to focus on proving the implication $\vdash \phi \;\Rightarrow \vDash \phi$ which is true from the very definition of a valuation.

Proposition 312 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. Then for all $\phi \in \mathbf{P}(V)$:*

$$\Gamma \vdash \phi \;\Rightarrow\; \Gamma \vDash \phi \tag{4.1}$$

Proof
Without loss of generality, we may assume that Γ is a finite set. Indeed, suppose the proposition has been proved for Γ finite. We need to show it is also true in

the general case. So suppose $\Gamma \vdash \phi$. We need to show that $\Gamma \vDash \phi$. However, there exists Γ_0 finite such that $\Gamma_0 \subseteq \Gamma$ and $\Gamma_0 \vdash \phi$. Having assumed the proposition is true in the finite case, we obtain $\Gamma_0 \vDash \phi$ and $\Gamma \vDash \phi$ follows from $\Gamma_0 \subseteq \Gamma$ and proposition (311). So without loss of generality, we assume that Γ is a finite set. We shall prove the implication (4.1) for all $\phi \in \mathbf{P}(V)$ using an induction argument on the cardinal $|\Gamma|$ of the set Γ. So first we assume that $|\Gamma| = 0$. Then $\Gamma = \emptyset$ and given $\phi \in \mathbf{P}(V)$ we need to prove that $\vdash \phi \ \Rightarrow \vDash \phi$. So we assume that $\vdash \phi$ and we need to show that $\vDash \phi$. So let $v \in \mathbf{P}^*(V)$ be a valuation. Using proposition (310) we need to show that $v \vDash \phi$, i.e. $v(\phi) = 1$ which is true since v is a valuation and $\vdash \phi$. So given $n \in \mathbf{N}$, we now assume that (4.1) is true for all $\phi \in \mathbf{P}(V)$ whenever we have $|\Gamma| = n$. We need to show the same applies when $|\Gamma| = n + 1$. So we assume that $|\Gamma| = n + 1$, and given $\phi \in \mathbf{P}(V)$ we assume that $\Gamma \vdash \phi$. We need to show that $\Gamma \vDash \phi$. So let $v \in \mathbf{P}^*(V)$ be a valuation satisfying Γ i.e. such that $v \vDash \Gamma$. We need to show that ϕ is true for v which is $v \vDash \phi$. However, from $|\Gamma| = n + 1$ we see that Γ is not empty. So let $\psi^* \in \Gamma$ and define $\Gamma^* = \Gamma \setminus \{\psi^*\}$. Then $|\Gamma^*| = n$ and $\Gamma = \Gamma^* \cup \{\psi^*\}$. From our assumption $\Gamma \vdash \phi$ we obtain $\Gamma^* \cup \{\psi^*\} \vdash \phi$. Using the deduction theorem (21) of page 226 it follows that $\Gamma^* \vdash (\psi^* \to \phi)$. Having assumed that (4.1) is true for all $\phi \in \mathbf{P}(V)$ whenever $|\Gamma| = n$, in particular it is true for $\psi^* \to \phi$ and Γ^*. Hence from $\Gamma^* \vdash (\psi^* \to \phi)$ we obtain $\Gamma^* \vDash (\psi^* \to \phi)$. Furthermore, from the inclusion $\Gamma^* \subseteq \Gamma$ and the assumption that v satisfies Γ, we see that v also satisfies Γ^* i.e. $v \vDash \Gamma^*$. So from $\Gamma^* \vDash (\psi^* \to \phi)$ we see that $v \vDash (\psi^* \to \phi)$, which is $1 = v(\psi^* \to \phi) = v(\psi^*) \to v(\phi)$. So we see that $v(\psi^*) \leq v(\phi)$. In order to show that $v \vDash \phi$ which is $v(\phi) = 1$, it is therefore sufficient to prove that $v(\psi^*) = 1$. However, $\psi^* \in \Gamma$ and by assumption v satisfies Γ. It follows that ψ^* is true for v, i.e. $v(\psi^*) = 1$, which completes our induction argument. .

4.1.4 Maximal Consistent Subset

In this section we introduce the notion of *consistency* and define *maximal consistent subsets* leading up to Lindenbaum's lemma (30) in the following section.

Definition 100 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. We say that Γ is* consistent *if and only if there exists no proof of $\perp$ from Γ, i.e. the sequent $\Gamma \vdash \perp$ is false.*

It is clear that any subset Δ which is larger than an inconsistent subset Γ is itself inconsistent. At this point in time, we do not know of any subset Γ which is consistent. Since we have not yet proved that the sequent $\vdash \perp$ is false, it may be that the empty set itself is inconsistent. If this were the case, then any sequent $\Gamma \vdash \phi$ would be true, as the following proposition shows:

Proposition 313 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$ be an inconsistent subset:*

$$\forall \phi \in \mathbf{P}(V) \ , \ \Gamma \vdash \phi$$

In other words, every formula can be proved from an inconsistent subset.

Proof
We assume that Γ is inconsistent, i.e. $\Gamma \vdash \bot$. Given $\phi \in \mathbf{P}(V)$, we need to show that $\Gamma \vdash \phi$. However, using the simplification property of proposition (163) we obtain $\Gamma \vdash [(\phi \to \bot) \to \bot]$. Hence we see from the transposition property of proposition (165) that $\Gamma \vdash \phi$ as requested. **.**

If a statement ϕ cannot be proven from a set of premises Γ, then in particular Γ must be consistent by virtue of proposition (313). In fact, we can add the negation of ϕ to the set Γ and still obtain a consistent set. In short, if something is not provable, adding its negation to a set of premises is consistent.

Proposition 314 *Let V be a set. Then for all $\phi \in \mathbf{P}(V)$ and $\Gamma \subseteq \mathbf{P}(V)$:*

$$\Gamma \vdash \phi \text{ is false } \Leftrightarrow \Gamma \cup \{\phi \to \bot\} \text{ is consistent}$$

Proof
First we show $\Rightarrow$: so suppose the sequent $\Gamma \vdash \phi$ is false. We need to show that $\Gamma \cup \{\phi \to \bot\}$ is consistent. Suppose to the contrary that $\Gamma \cup \{\phi \to \bot\}$ is not consistent. Then we can deduce a contradiction from it, i.e. we have $\Gamma \cup \{\phi \to \bot\} \vdash \bot$. Using the deduction theorem (21) of page 226 we obtain $\Gamma \vdash (\phi \to \bot) \to \bot$ and consequently, from the transposition property of proposition (165) we conclude that $\Gamma \vdash \phi$ which is a contradiction. We now prove $\Leftarrow$: so we assume that $\Gamma \cup \{\phi \to \bot\}$ is consistent. We need to show that $\Gamma \vdash \phi$ is false. So suppose to the contrary that $\Gamma \vdash \phi$ is true. Then in particular we have $\Gamma \cup \{\phi \to \bot\} \vdash \phi$. However, it is clear that $\Gamma \cup \{\phi \to \bot\} \vdash (\phi \to \bot)$. Using the modus ponens property of proposition (161) we obtain $\Gamma \cup \{\phi \to \bot\} \vdash \bot$, which contradicts our assumption that $\Gamma \cup \{\phi \to \bot\}$ is consistent. **.**

As we shall see in theorem (31) of page 405, the notions of *consistent* and *satisfiable* subsets are in fact equivalent. This will allow us to derive the compactness theorem (32) of page 405. We can now prove one side of the equivalence:

Proposition 315 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. Then we have the implication:*

$$\Gamma \text{ is satisfiable } \Rightarrow \Gamma \text{ is consistent}$$

Proof
We assume that Γ is satisfiable. So there exists a valuation $v \in \mathbf{P}^*(V)$ which satisfies Γ, i.e. such that $v \vDash \Gamma$. We need to show that Γ is consistent. So suppose to the contrary that Γ is not consistent. Then the sequent $\Gamma \vdash \bot$ is true. Using proposition (312) it follows that $\Gamma \vDash \bot$. Since the valuation v satisfies Γ we conclude that it also satisfies $\bot$, i.e. $v \vDash \bot$. Hence we obtain $v(\bot) = 1$ which contradicts definition (96) of v being a valuation on $\mathbf{P}(V)$. **.**

The subsets $\Gamma \subseteq \mathbf{P}(V)$ which are consistent form a subset X of the power set $\mathcal{P}(\mathbf{P}(V))$. In other words, they form a set of subsets of $\mathbf{P}(V)$. This set X can be partially ordered by inclusion. A maximal consistent set Γ is an element of X which is a maximal element with respect to this partial order. Recall that given a partially ordered set $(X, \leq)$, an element $a \in X$ is said to be *maximal* if and only if for all $b \in X$ we have the implication:

$$a \leq b \Rightarrow a = b$$

We shall need to remember this when stating Zorn's lemma in the next section.

Definition 101 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. We say that Γ is* maximal consistent *if and only if it is consistent and for all $\Delta \subseteq \mathbf{P}(V)$ we have:*

$$(\Gamma \subseteq \Delta) \wedge (\Delta \textit{ consistent}) \Rightarrow \Gamma = \Delta$$

Maximal consistent subsets have many interesting properties. In particular, they are *closed under syntactic entailment*. In other words, anything which can be proven from a maximal consistent subset, actually belongs to that subset.

Proposition 316 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$ be maximal consistent. Then:*

$$\forall \phi \in \mathbf{P}(V) \ , \ (\Gamma \vdash \phi \ \Rightarrow \ \phi \in \Gamma)$$

Proof
We assume that $\Gamma \subseteq \mathbf{P}(V)$ is maximal consistent. Let $\phi \in \mathbf{P}(V)$ be such that $\Gamma \vdash \phi$. We need to show that $\phi \in \Gamma$. So suppose to the contrary that $\phi \notin \Gamma$. Then $\Delta = \Gamma \cup \{\phi\}$ is a set which is strictly larger than Γ. Having assumed that Γ is maximal consistent, Δ cannot be consistent. It follows that $\Delta \vdash \bot$ which is $\Gamma \cup \{\phi\} \vdash \bot$. Using the deduction theorem (21) of page 226 we obtain $\Gamma \vdash (\phi \rightarrow \bot)$. However, by assumption $\Gamma \vdash \phi$. Using the modus ponens property of proposition (161) we see that $\Gamma \vdash \bot$, contradicting the consistency of Γ. **.**

Another interesting property of maximal consistent subsets is the fact they always contain a formula ϕ or its negation $\phi \rightarrow \bot$, for all $\phi \in \mathbf{P}(V)$. Obviously they cannot contain both without being inconsistent. Hence we have:

Proposition 317 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$ be maximal consistent. Then for all $\phi \in \mathbf{P}(V)$ we have $\phi \in \Gamma$ or $(\phi \rightarrow \bot) \in \Gamma$, and these are exclusive.*

Proof
If Γ is consistent, it is clear we cannot have both $\phi \in \Gamma$ and $(\phi \rightarrow \bot) \in \Gamma$, as otherwise the sequents $\Gamma \vdash \phi$ and $\Gamma \vdash (\phi \rightarrow \bot)$ would both be true, and using the modus ponens property of proposition (161), this would imply $\Gamma \vdash \bot$ contradicting the consistency of Γ. So we assume that $\Gamma \subseteq \mathbf{P}(V)$ is maximal consistent and given $\phi \in \mathbf{P}(V)$, we need to show that $\phi \in \Gamma$ or $(\phi \rightarrow \bot) \in \Gamma$. So we assume that $(\phi \rightarrow \bot) \notin \Gamma$. We need to show that $\phi \in \Gamma$. However, having assumed $(\phi \rightarrow \bot) \notin \Gamma$, the set $\Delta = \Gamma \cup \{\phi \rightarrow \bot\}$ is a set which is strictly larger than Γ. Having assumed Γ is maximal consistent, it follows that Δ cannot be consistent. So $\Gamma \cup \{\phi \rightarrow \bot\}$ is not consistent and consequently from proposition (314) we see that the sequent $\Gamma \vdash \phi$ is true. Since Γ is maximal consistent, using proposition (316) we conclude that $\phi \in \Gamma$ as requested. **.**

A maximal consistent subset can be thought of as the set of *true* formulas of a valuation $v \in \mathbf{P}^*(V)$. This fact will be made precise after we show the following proposition, which expresses the familiar idea that an implication $\phi_1 \rightarrow \phi_2$ is *true*, if and only if ϕ_1 is *false* or ϕ_2 is *true*. More precisely, we have:

Proposition 318 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$ be a maximal consistent subset. Then for all formulas $\phi_1, \phi_2 \in \mathbf{P}(V)$ we have the equivalence:*

$$(\phi_1 \to \phi_2) \in \Gamma \;\Leftrightarrow\; (\phi_1 \notin \Gamma) \vee (\phi_2 \in \Gamma)$$

Proof
First we prove $\Rightarrow$: so we assume that $(\phi_1 \to \phi_2) \in \Gamma$. We need to show that $\phi_1 \notin \Gamma$ or $\phi_2 \in \Gamma$. So suppose $\phi_1 \in \Gamma$. We need to show that $\phi_2 \in \Gamma$. However, we obviously have $\Gamma \vdash (\phi_1 \to \phi_2)$ and $\Gamma \vdash \phi_1$. Using the modus ponens property of proposition (161) we obtain $\Gamma \vdash \phi_2$. Having assumed Γ is maximal consistent, it follows from proposition (316) that $\phi_2 \in \Gamma$ as requested. We now prove $\Leftarrow$: so we assume that $\phi_1 \notin \Gamma$ or $\phi_2 \in \Gamma$. We need to show that $(\phi_1 \to \phi_2) \in \Gamma$. Using proposition (316) once more, it is sufficient to prove that $\Gamma \vdash (\phi_1 \to \phi_2)$. From the deduction theorem (21) of page 226, it is therefore sufficient to show that $\Gamma \cup \{\phi_1\} \vdash \phi_2$. This is clearly true if $\phi_2 \in \Gamma$, so we may assume that $\phi_2 \notin \Gamma$. However by assumption, this implies that $\phi_1 \notin \Gamma$. Having assumed Γ is maximal consistent, from proposition (317) it follows that $(\phi_1 \to \bot) \in \Gamma$ and in particular we have $\Gamma \vdash (\phi_1 \to \bot)$. Using the deduction theorem once more, we see that $\Gamma \cup \{\phi_1\} \vdash \bot$. So the subset $\Gamma \cup \{\phi_1\}$ is inconsistent and the required sequent $\Gamma \cup \{\phi_1\} \vdash \phi_2$ follows from proposition (313). **.**

The following proposition establishes a bijection between the dual space $\mathbf{P}^*(V)$ and the set of maximal consistent subsets of $\mathbf{P}(V)$. This gives us valuable insight, and allows us to view any valuation $v : \mathbf{P}(V) \to 2$ as a maximal consistent subset, or to regard any maximal consistent subset as a valuation. This result will be particularly interesting once we show that $\mathbf{P}^*(V) \neq \emptyset$.

Proposition 319 *Let V be a set and $v : \mathbf{P}(V) \to 2$ be a valuation. Consider:*

$$\Gamma_v = \{\phi \in \mathbf{P}(V) : v(\phi) = 1\}$$

Then Γ_v is maximal consistent. Conversely, let Γ be maximal consistent and:

$$\forall \phi \in \mathbf{P}(V)\ ,\ 1_\Gamma(\phi) = \begin{cases} 1 & \text{if} \quad \phi \in \Gamma \\ 0 & \text{if} \quad \phi \notin \Gamma \end{cases}$$

Then the characteristic function $1_\Gamma : \mathbf{P}(V) \to 2$ is a valuation. Furthermore, the maps $v \to \Gamma_v$ and $\Gamma \to 1_\Gamma$ are bijections which are inverse of each other, between the dual space $\mathbf{P}^*(V)$ and the set of maximal consistent subsets of $\mathbf{P}(V)$.

Proof
We first consider a valuation $v : \mathbf{P}(V) \to 2$ and $\Gamma_v = \{\phi \in \mathbf{P}(V) : v(\phi) = 1\}$. We need to show that Γ_v is maximal consistent. First we show that Γ_v is consistent. So suppose to the contrary that Γ_v is not consistent. Then we have $\Gamma_v \vdash \bot$. It follows from proposition (312) that $\Gamma_v \vDash \bot$. However, for all $\phi \in \Gamma_v$ we have $v(\phi) = 1$. So v satisfies Γ_v, i.e. we have $v \vDash \Gamma_v$. From $\Gamma_v \vDash \bot$ we therefore conclude that $v \vDash \bot$ which is $v(\bot) = 1$ and contradicts definition (96) of v being a valuation on $\mathbf{P}(V)$. So we now show that Γ_v is in fact maximal consistent. So suppose $\Delta \subseteq \mathbf{P}(V)$ is a set which is strictly larger than Γ_v. We

need to show that Δ is not consistent, i.e. that $\Delta \vdash \bot$. However by assumption the set $\Delta \setminus \Gamma_v$ is not empty. So let $\phi \in \Delta \setminus \Gamma_v$. From $\phi \notin \Gamma_v$ we obtain $v(\phi) = 0$ and consequently $v(\phi \to \bot) = v(\phi) \to v(\bot) = v(\phi) \to 0 = 1$. It follows that $(\phi \to \bot) \in \Gamma_v$. However, from $\Gamma_v \subseteq \Delta$ we also have $(\phi \to \bot) \in \Delta$. Furthermore, by assumption $\phi \in \Delta$. Hence we see that $\Delta \vdash \phi$ and $\Delta \vdash (\phi \to \bot)$ are both true and using the modus ponens property of proposition (161) we obtain $\Delta \vdash \bot$ as requested. So we have proved that Γ_v is maximal consistent. We now assume that $\Gamma \subseteq \mathbf{P}(V)$ is maximal consistent and we need to show that its characteristic function $1_\Gamma : \mathbf{P}(V) \to 2$ is a valuation. First we show that $1_\Gamma(\bot) = 0$: we need to prove that $\bot \notin \Gamma$. This is clearly the case since $\bot \in \Gamma$ implies $\Gamma \vdash \bot$ which would contradict the consistency of Γ. Next we show that $1_\Gamma(\phi_1 \to \phi_2) = 1_\Gamma(\phi_1) \to 1_\Gamma(\phi_2)$ for all $\phi_1, \phi_2 \in \mathbf{P}(V)$. This goes as follows:

$$\begin{array}{rcl} 1_\Gamma(\phi_1 \to \phi_2) = 1 & \Leftrightarrow & (\phi_1 \to \phi_2) \in \Gamma \\ \text{prop. (318)} \ \to & \Leftrightarrow & (\phi_1 \notin \Gamma) \vee (\phi_2 \in \Gamma) \\ & \Leftrightarrow & (1_\Gamma(\phi_1) = 0) \vee (1_\Gamma(\phi_2) = 1) \\ & \Leftrightarrow & 1_\Gamma(\phi_1) \to 1_\Gamma(\phi_2) = 1 \end{array}$$

Finally given $\phi \in \mathbf{P}(V)$, we need to show the implication $\vdash \phi \ \Rightarrow \ 1_\Gamma(\phi) = 1$. So we assume that $\vdash \phi$. We need to show that $1_\Gamma(\phi) = 1$, i.e. that $\phi \in \Gamma$. However, from $\vdash \phi$ we have in particular $\Gamma \vdash \phi$. Having assumed Γ is maximal consistent, using proposition (316) we obtain $\phi \in \Gamma$ as requested. So we have proved that $1_\Gamma : \mathbf{P}(V) \to 2$ is a valuation on $\mathbf{P}(V)$. It remains to show that the maps $v \to \Gamma_v$ and $\Gamma \to 1_\Gamma$ are bijections which are inverse of one another, from $\mathbf{P}^*(V)$ to the set of maximal consistent subsets of $\mathbf{P}(V)$. Let us denote $\mathcal{C}(V)$ the set of maximal consistent subsets of $\mathbf{P}(V)$, and define $f : \mathbf{P}^*(V) \to \mathcal{C}(V)$ by $f(v) = \Gamma_v$ and $g : \mathcal{C}(V) \to \mathbf{P}^*(V)$ by $g(\Gamma) = 1_\Gamma$. Until now we have proved that the range of f is indeed a subset of $\mathcal{C}(V)$ while the range of g is indeed a subset of $\mathbf{P}^*(V)$. We need to show that f and g are bijective and inverse of one another. First we show that $g \circ f(v) = v$ for all $v \in \mathbf{P}^*(V)$. This will show that f is injective and g is surjective. We need to show that $1_{\Gamma_v} = v$. Let $\phi \in \mathbf{P}(V)$:

$$1_{\Gamma_v}(\phi) = 1 \ \Leftrightarrow \ \phi \in \Gamma_v \ \Leftrightarrow \ v(\phi) = 1$$

We now show that $f \circ g(\Gamma) = \Gamma$ for all $\Gamma \in \mathcal{C}(V)$. This will show that g is injective and f is surjective. We need to show that $\Gamma_{1_\Gamma} = \Gamma$. Let $\phi \in \mathbf{P}(V)$:

$$\phi \in \Gamma_{1_\Gamma} \ \Leftrightarrow \ 1_\Gamma(\phi) = 1 \ \Leftrightarrow \ \phi \in \Gamma$$

.

4.1.5 Lindenbaum's Lemma

In this section we prove Lindenbaum's lemma from which follow many interesting and deeper results such as theorem (33) of page 406 establishing the equivalence between syntactic and semantic entailments. Our proof relies on Zorn's lemma and therefore on the axiom of choice. It is usually possible to

provide a proof of Lindenbaum's lemma which does not rely on the axiom of choice. However our set V being arbitrary, we do not have this option when dealing with the general case. We shall provide a statement of Zorn's lemma below, but are not able to spell out a proof, as this would take us too long. Zorn's lemma is a monster of usefulness and we certainly hope to design a proof of it, once we are able to deal with proper axiomatic set theory. Recall that a *partially ordered set* is an ordered pair $(X \ \leq)$ where $\leq$ is a *partial order* on X, namely a relation on X which is reflexive, anti-symmetric and transitive on X. We have already studied a case of partial order when defining the *sub-formula relation* $\preceq$ of definition (19), where X is a free universal algebra. If $(X, \leq)$ is a partially ordered set and $Y \subseteq X$, there is an obvious relation on Y namely:

$$R_Y = \{(x, y) \in Y \times Y \ : \ x \leq y\}$$

It is easy to check that R_Y is a partial order on Y which we also denote $\leq$. So $(Y, \leq)$ becomes a partially ordered set. We say that Y is a *totally ordered subset* of X if and only if the partially ordered set $(Y, \leq)$ is *totally ordered*. A partially ordered set $(X, \leq)$ is said to be *totally ordered*, if and only if for all $x, y \in X$ we have $x \leq y$ or $y \leq x$. We say that $Y \subseteq X$ *has an upper-bound in* X, if and only if there exists $a \in X$ such that $y \leq a$ for all $y \in Y$. Zorn's lemma says that if $(X, \leq)$ is a partially ordered set for which every totally ordered subset $Y \subseteq X$ has an upper-bound in X, then X has a maximal element. Note that it is not necessary to assume $X \neq \emptyset$ in the statement of Zorn's lemma. Indeed $Y = \emptyset$ is a subset of X which is vacuously totally ordered. Any element $a \in X$ is vacuously an upper-bound of $Y = \emptyset$. So if we assume that every totally ordered subset of X has an upper-bound in X, then in particular $Y = \emptyset$ has an upper-bound in X and consequently X cannot be empty. We are now ready to state:

Lemma 28 (Zorn's Lemma) *Let $(X, \leq)$ be a partially ordered set for which every totally ordered subset has an upper-bound in X. Then X has a maximal element, i.e. there exists $x_0 \in X$ satisfying the property:*

$$\forall x \in X \ , \ (x_0 \leq x \ \Rightarrow \ x_0 = x)$$

Proof
See for example Walter Rudin [51]. **.**

Lindenbaum's lemma states that every consistent subset of $\mathbf{P}(V)$ can be extended to a maximal consistent subset. Its proof relies on Zorn's lemma by considering the set X of all consistent extensions Γ of a given consistent set Γ_0, partially ordered by inclusion. In order to successfully apply Zorn's lemma, we need to show that every totally ordered subset Y of X has an upper-bound in X. An upper-bound candidate will naturally be the union $\Gamma = \cup Y$, which we shall need to check is indeed a consistent extension of Γ_0. The following lemma will allow us to do that. Note that we are assuming Y to be non-empty in the following statement. If $Y = \emptyset$, then $\Gamma = \cup Y$ is also the empty set which is consistent but we cannot yet prove that. So removing the assumption $Y \neq \emptyset$ in the following lemma would yield a true conclusion, but with the wrong proof.

Lemma 29 *Let V be a set and Y be a set of consistent subsets of $\mathbf{P}(V)$ which is non-empty and totally ordered by inclusion. Then $\Gamma = \cup Y$ is consistent.*

Proof
We have $\Gamma = \cup Y = \{\, \phi \in \mathbf{P}(V) \ : \ \exists \Delta \in Y \ , \ \phi \in \Delta \,\}$. Suppose Γ is not consistent. Then we have $\Gamma \vdash \bot$. So there exists Γ_0 finite such that $\Gamma_0 \subseteq \Gamma$ and $\Gamma_0 \vdash \bot$. Note that Γ_0 cannot be the empty set, as otherwise from $\vdash \bot$ we would have $\Delta \vdash \bot$ for every $\Delta \subseteq \mathbf{P}(V)$, and no subset of $\mathbf{P}(V)$ would be consistent, contradicting the fact that Y is non-empty. Let $n = |\Gamma_0|$ be the cardinal of Γ_0. Then there exists a bijection $\psi : n \to \Gamma_0$. For all $k \in n$ we have $\psi(k) \in \Gamma_0$ and in particular $\psi(k) \in \Gamma$. Hence, there exists $\Delta(k) \in Y$ such that $\psi(k) \in \Delta(k)$. Since $\Gamma_0 \neq \emptyset$ we have $n \geq 1$ and the set $\{\Delta(k) \ : k \in n\}$ is therefore a non-empty subset of Y. Having assumed Y is totally ordered by inclusion, this set has a maximum. So there exists $k^* \in n$ such that $\Delta(k) \subseteq \Delta(k^*)$ for all $k \in n$. It follows that $\psi(k) \in \Delta(k^*)$ for all $k \in n$. The map $\psi : n \to \Gamma_0$ being a surjection, we see that $\Gamma_0 \subseteq \Delta(k^*)$. So from $\Gamma_0 \vdash \bot$ we have $\Delta(k^*) \vdash \bot$. It follows that $\Delta(k^*)$ is not consistent, contradicting the fact that $\Delta(k^*) \in Y$. **.**

As already mentioned on prior occasions, we still do not know for a fact that consistent subsets do exist, as we haven't proved the sequent $\vdash \bot$ is false. If there was no consistent set at all, the statement of Lindenbaum's lemma which follows would be vacuously true. Luckily, consistent subsets will be seen to exist.

Lemma 30 (Lindenbaum) *Let V be a set and $\Gamma_0 \subseteq \mathbf{P}(V)$ be a consistent subset. Then there exists $\Gamma \subseteq \mathbf{P}(V)$ maximal consistent subset such that $\Gamma_0 \subseteq \Gamma$.*

Proof
Consider the partially ordered set $(X, \subseteq)$ defined by the following:

$$X = \{\, \Gamma \subseteq \mathbf{P}(V) \ : \ \Gamma_0 \subseteq \Gamma \ , \ \Gamma \text{ consistent} \,\}$$

where $\subseteq$ denotes the standard inclusion on $\mathcal{P}(\mathbf{P}(V))$. We wish to apply Zorn's lemma to $(X, \subseteq)$. Let us accept the conclusion of Zorn's lemma for now, i.e. that X has a maximal element Γ. Then in particular we have $\Gamma \in X$. So Γ is consistent and $\Gamma_0 \subseteq \Gamma$. It remains to prove that Γ is in fact maximal consistent. So suppose $\Delta \subseteq \mathbf{P}(V)$ is consistent with $\Gamma \subseteq \Delta$. We need to show that $\Gamma = \Delta$. So it is sufficient to show that $\Delta \in X$ as the equality $\Gamma = \Delta$ will then follow from the maximality of Γ in X and $\Gamma \subseteq \Delta$. However, we have $\Gamma_0 \subseteq \Gamma$ and $\Gamma \subseteq \Delta$. It follows that $\Gamma_0 \subseteq \Delta$. Having assumed Δ is consistent, we see that Δ is indeed an element of X, and the proposition is proved. So it remains to show that X has a maximal element. Using Zorn's lemma (28), we need to show that if $Y \subseteq X$ is a totally ordered subset of X, then Y has an upper-bound in X. So let $Y \subseteq X$ be totally ordered. We shall distinguish two cases: first we assume that $Y = \emptyset$. Then any element of X is vacuously an upper-bound of Y. So it is sufficient to show that $X \neq \emptyset$ which is clearly the case since Γ_0 is consistent and consequently $\Gamma_0 \in X$. So we assume $Y \neq \emptyset$. Let $\Gamma = \cup Y$, i.e.:

$$\Gamma = \{\, \phi \in \mathbf{P}(V) \ : \ \exists \Delta \in Y \ , \ \phi \in \Delta \,\}$$

It is sufficient to show that Γ is an upper-bound of Y in X, namely that $\Gamma \in X$ and $\Delta \subseteq \Gamma$ for all $\Delta \in Y$. First we show that $\Delta \subseteq \Gamma$ for all $\Delta \in Y$. So let $\Delta \in Y$ and consider $\phi \in \Delta$. Then it is clear that $\phi \in \Gamma$ and the inclusion $\Delta \subseteq \Gamma$ follows. So we now prove that $\Gamma \in X$. We need to show that $\Gamma_0 \subseteq \Gamma$ and Γ is consistent. First we show that $\Gamma_0 \subseteq \Gamma$. So let $\phi \in \Gamma_0$. We need to show that $\phi \in \Gamma$. However, since $Y \neq \emptyset$, there exists $\Delta \in Y \subseteq X$. So in particular, we have $\Delta \in X$ and consequently $\Gamma_0 \subseteq \Delta$. It follows that $\phi \in \Delta$ and from $\Delta \in Y$ we see that $\phi \in \Gamma$ as requested. It remains to show that Γ is consistent. However, we have $\Gamma = \cup Y$ where Y is a set of consistent subsets of $\mathbf{P}(V)$ which is non-empty and totally ordered by inclusion. The fact that Γ is consistent follows immediately from lemma (29). **.**

4.1.6 The Compactness Theorem

Lindenbaum's lemma (30) has many applications. We shall start by showing that the notions of *satisfiable* and *consistent* subsets are in fact equivalent. Recall from definition (97) that being *satisfiable* is defined in terms of valuation and not model. This is contrary to standard practice and the reader is invited to refer to our discussion preceding definition (96). As we shall see, *every valuation has a model* so definition (97) is in fact equivalent to the standard notion of *satisfiable* set. We should also remember that $\mathbf{P}^*(V) \neq \emptyset$ has not been proved at this stage of the document. A consequence of the dual space being empty would be that no subset of $\mathbf{P}(V)$ is either satisfiable or consistent, not even $\emptyset$.

Theorem 31 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. Then we have the equivalence:*

$$\Gamma \textit{ is satisfiable } \Leftrightarrow \Gamma \textit{ is consistent}$$

Proof
The implication $\Rightarrow$ follows from proposition (315). So we now prove $\Leftarrow$: we assume that Γ is consistent. We need to show it is satisfiable. Using Lindenbaum's lemma (30), there exists Δ maximal consistent subset such that $\Gamma \subseteq \Delta$. From proposition (319) the characteristic function $1_\Delta : \mathbf{P}(V) \to 2$ is a valuation. Furthermore, for all $\phi \in \Gamma$ we have $\phi \in \Delta$ and consequently $1_\Delta(\phi) = 1$. It follows that 1_Δ satisfies Γ and we have proved that Γ is satisfiable. **.**

The compactness theorem which follows is a consequence of theorem (31) and therefore also a consequence of Lindenbaum's lemma (30). The same warning applies as for theorem (31): our version of the compactness theorem is not exactly the standard version found in the literature, because we have defined a *satisfiable* set in terms of valuation and not model. It is however equivalent to the standard version, since *every valuation has a model*, as we shall see.

Theorem 32 (Compactness) *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. Then Γ is satisfiable, if and only if every finite subset $\Gamma_0 \subseteq \Gamma$ is satisfiable.*

Proof
First we prove the 'only if' part: so we assume that Γ is satisfiable. Then clearly

all subsets of Γ are satisfiable, including the finite subsets. So we now show the 'if' part: we assume that every finite subset of Γ is satisfiable. We need to show that Γ is itself satisfiable. Using theorem (31), it is sufficient to show that Γ is consistent. So suppose to the contrary that Γ is inconsistent. Then we have $\Gamma \vdash \bot$ and consequently there exists Γ_0 finite such that $\Gamma_0 \subseteq \Gamma$ and $\Gamma_0 \vdash \bot$. Hence, Γ_0 is a finite subset of Γ which is not consistent. Using theorem (31), Γ_0 is a finite subset of Γ which is not satisfiable, contradicting the hypothesis. .

4.1.7 Equivalence of Syntax and Semantics

The equivalence between syntactic and semantic entailments is a consequence of theorem (31) and therefore a consequence of Lindenbaum's lemma (30). The implication $\Rightarrow$ of theorem (33) below was stated as proposition (312). The other implication $\Leftarrow$ will be proved now and is often referred to as the *strong completeness property*. The implication $\vdash \phi \;\; \Leftarrow \models \phi$ is normally known as Gödel's completeness theorem and referred to as the *weak completeness property*. However, it would be wrong for us to use the word *completeness* when referring to theorem (33). As already explained in the discussion preceding definition (96), our notion of semantic entailment is defined solely in terms of the dual space $\mathbf{P}^*(V)$ without reference to any model theory. We have many good reasons to do this and one of these reasons is precisely to show that results such as theorem (33) below can be obtained independently of any model theory, opening the way for possible generalization to axiomatic systems which may not be complete. The notion of completeness expresses the idea that a proof system is rich enough to prove any formula which is true in every model. If we remove axioms or replace them by weaker axioms, there are fewer formulas which can be proven from our deductive system, which has become weaker and may no longer be complete. In terms of the deductive congruence which stems from the preorder $\vdash (\phi \to \psi)$, a weaker deductive system leads to fewer pairs (ϕ, ψ) of *logically equivalent* formulas, so the congruence is stronger, assuming it is still a congruence, depending on the exact nature of the deductive system. From the point of view of the dual space $\mathbf{P}^*(V)$ which is defined by the soundness property $\vdash \phi \;\; \Rightarrow \;\; v(\phi) = 1$, a weaker deductive system leads to a larger dual space and therefore fewer *valid* formulas, in the sense of definition (98). So although we may have a weaker deductive system which is no longer complete, since there are fewer provable formulas *as well as* fewer valid formulas, it is conceivable that the equivalence between syntactic and semantic entailment still holds. This is worth investigating and we may do so at a later stage. This is one of the key reason for us to decouple semantics from model theory: we wanted to present an argument leading to theorem (33) below, which is specific to the Hilbert deductive congruence, and yet can probably be made to work for other cases of congruence. For us, the notion of completeness expresses the idea that the Hilbert deductive proof system is rich enough, so its associated dual space $\mathbf{P}^*(V)$ is small enough so that *every valuation has a model*. Note that theorem (33) below is established prior to proving $\mathbf{P}^*(V) \neq \emptyset$.

Theorem 33 *Let V be a set and $\Gamma \subseteq \mathbf{P}(V)$. Then for all $\phi \in \mathbf{P}(V)$:*

$$\Gamma \vdash \phi \;\Leftrightarrow\; \Gamma \vDash \phi \tag{4.2}$$

Proof
The implication $\Rightarrow$ follows from proposition (312). So we now prove $\Leftarrow$: we assume that $\Gamma \subseteq \mathbf{P}(V)$ and $\phi \in \mathbf{P}(V)$ are such that $\Gamma \vDash \phi$. We need to show that $\Gamma \vdash \phi$. Suppose this is not the case. Using proposition (314) we see that $\Gamma \cup \{\phi \to \bot\}$ is consistent. Using theorem (31), it is therefore satisfiable. So there exists $v \in \mathbf{P}^*(V)$ which satisfies $\Gamma \cup \{\phi \to \bot\}$. It follows that $v \vDash \Gamma$ and $v \vDash (\phi \to \bot)$. However, from $v \vDash \Gamma$ and $\Gamma \vDash \phi$ we obtain $v \vDash \phi$, i.e. $v(\phi) = 1$. From $v \vDash (\phi \to \bot)$ we obtain $1 = v(\phi \to \bot) = v(\phi) \to v(\bot) = v(\phi) \to 0$ and consequently $v(\phi) = 0$ which is our desired contradiction. .

4.1.8 Dual Characterization of the Deductive Congruence

The theorem which follows is yet another indirect consequence of Lindenbaum's lemma (30). It provides us with a characterization of the Hilbert deductive congruence in terms of the dual space $\mathbf{P}^*(V)$. The result has nothing to do with model theory: We started from a consequence relation $\vdash \subseteq \mathcal{P}(\mathbf{P}(V)) \times \mathbf{P}(V)$ from which both a congruence and a dual space were defined. This congruence turns out to be fully characterized by this dual space. Obviously the question should be asked: is the result specific to the Hilbert deductive congruence, or are there other congruences on $\mathbf{P}(V)$ for which a *natural consequence relation and dual space* can be defined, leading up to the following characterization?

Theorem 34 *Let V be a set and $\equiv$ be the Hilbert deductive congruence on $\mathbf{P}(V)$. Then for all formulas $\phi, \psi \in \mathbf{P}(V)$ we have the equivalence:*

$$\phi \equiv \psi \;\Leftrightarrow\; \forall v \in \mathbf{P}^*(V)\ ,\ v(\phi) = v(\psi)$$

Proof
The implication $\Rightarrow$ follows from proposition (309). So we now prove $\Leftarrow$: let $\phi, \psi \in \mathbf{P}(V)$ such that $v(\phi) = v(\psi)$ for all $v \in \mathbf{P}^*(V)$. We need to show that $\phi \equiv \psi$. By symmetry, it is sufficient to show that $\phi \leq \psi$ i.e. that we have $\vdash (\phi \to \psi)$. Using theorem (33) it is therefore sufficient to prove that $\vDash (\phi \to \psi)$. In other words, from proposition (310) it is sufficient to show that $v(\phi \to \psi) = 1$ for all $v \in \mathbf{P}^*(V)$. However, given $v \in \mathbf{P}^*(V)$ we have:

$$v(\phi \to \psi) = v(\phi) \to v(\psi) = v(\phi) \to v(\phi) = 1$$

.

From theorem (33) of page 406 we have the equivalence $\vdash \phi \;\Leftrightarrow \vDash \phi$. In other words, a formula is provable if and only if it is valid. In fact as we shall now see, a formula is provable if and only if it is logically equivalent to $\bot \to \bot$.

Proposition 320 *Let V be a set. For all $\phi \in \mathbf{P}(V)$ we have the equivalence:*

$$\vdash \phi \;\Leftrightarrow\; \phi \equiv (\bot \to \bot)$$

where $\equiv$ is the Hilbert deductive congruence on $\mathbf{P}(V)$.

Proof
Using theorem (34), the statement $\phi \equiv (\bot \to \bot)$ is equivalent to $v(\phi) = 1$ for all $v \in \mathbf{P}^*(V)$. Using proposition (310), this is in turn equivalent to $\vDash \phi$, which is itself equivalent to $\vdash \phi$ by virtue of theorem (33). **.**

In definition (96), we defined the dual space $\mathbf{P}^*(V)$ in terms of the consequence relation $\vdash$ by imposing the *soundness* property $\vdash \phi \;\Rightarrow\; v(\phi) = 1$. The following theorem shows that $\mathbf{P}^*(V)$ could equally have been defined directly in terms of the Hilbert deductive congruence $\equiv$, induced by the consequence relation $\vdash$. In other words, we do not need to have a consequence relation in order to define a dual space: given a congruence $\sim$ on $\mathbf{P}(V)$, we can define an associated dual space $\mathbf{P}^*(V)$ as the set of all propositional valuations v which are compatible with the congruence $\sim$, i.e. for which given $\phi, \psi \in \mathbf{P}(V)$:

$$\phi \sim \psi \;\Rightarrow\; v(\phi) = v(\psi)$$

We can then investigate whether this dual space $\mathbf{P}^*(V)$ gives rise to a characterization of the congruence $\sim$ which is similar to that of theorem (34).

Theorem 35 *Let V be a set and $v : \mathbf{P}(V) \to 2$ be a map. Then v is a valuation if and only if it is a propositional valuation such that for all $\phi, \psi \in \mathbf{P}(V)$:*

$$\phi \equiv \psi \;\Rightarrow\; v(\phi) = v(\psi)$$

i.e. such that v is compatible with the Hilbert deductive congruence $\equiv$ on $\mathbf{P}(V)$.

Proof
First we show the 'only if' part: so we assume that $v : \mathbf{P}(V) \to 2$ is a valuation. From definition (96) we see that $v(\bot) = 0$ and $v(\phi_1 \to \phi_2) = v(\phi_1) \to v(\phi_2)$ for all $\phi_1, \phi_2 \in \mathbf{P}(V)$. Comparing with definition (56) it follows that v is indeed a propositional valuation. Furthermore, if $\phi, \psi \in \mathbf{P}(V)$ are such that $\phi \equiv \psi$, it is clear from theorem (34) that $v(\phi) = v(\psi)$. So we now prove the 'if' part: we assume that $v : \mathbf{P}(V) \to 2$ is a propositional valuation which is compatible with the Hilbert deductive congruence, i.e. such that $v(\phi) = v(\psi)$ whenever we have $\phi \equiv \psi$. We need to show that v is a valuation. Being a propositional valuation, we already know that $v(\bot) = 0$ and $v(\phi_1 \to \phi_2) = v(\phi_1) \to v(\phi_2)$ for all $\phi_1, \phi_2 \in \mathbf{P}(V)$. It remains to show the implication $\vdash \phi \;\Rightarrow\; v(\phi) = 1$. So we assume that $\phi \in \mathbf{P}(V)$ is such that $\vdash \phi$. We need to show that $v(\phi) = 1$. However, from $\vdash \phi$ and proposition (320) we obtain $\phi \equiv (\bot \to \bot)$. By assumption, it follows that $v(\phi) = v(\bot \to \bot) = v(\bot) \to v(\bot) = 0 \to 0 = 1$ as requested. **.**

4.2 Elements of Classical Model Theory

4.2.1 Model and Variables Assignment

We have two compelling reasons to deal with model theory: one of them is to establish Gödel's completeness theorem which we need to do in order to validate our deductive system. Another reason is that model theory is the simplest way

to prove that valuations $v : \mathbf{P}(V) \to 2$ actually do exist. So the dual space $\mathbf{P}^*(V)$ is not empty, the sequent $\vdash \bot$ is false, the empty set is consistent and satisfiable. This is not much but it has to be done: a deductive system for which the sequent $\vdash \bot$ is true is pretty worthless. A semantic entailment $\vDash$ defined in terms of an empty dual space $\mathbf{P}^*(V)$ as per definition (98) is also pointless.

So we shall start by defining the notion of *model*, also known as *structure*. Since our language $\mathbf{P}(V)$ has no equality, no constant or function symbol, and is effectively limited to a single binary relation symbol '$\in$', the corresponding notion of *model* is restricted to an ordered pair (M, r) where M is a set and r is a binary relation on M. This is obviously a significant restriction compared to the general setting, for which the reader should consult David Marker [41]. At this point in time, our aim is simply to study the free universal algebra $\mathbf{P}(V)$, describe various natural congruences on it, and see whether axiomatic set theory can be coded with it. The language $\mathbf{P}(V)$ is similar to untyped λ-calculus: it is limited to the bare minimum, and we aim to show this minimum is enough.

Definition 102 *Let V be a set. We call* model *of $\mathbf{P}(V)$ any ordered pair (M, r) where M is a set and r is a binary relation on M, i.e. a subset of $M \times M$.*

Note that $(M, r) = (\emptyset, \emptyset)$ is a model of $\mathbf{P}(V)$ for any set V. Furthermore, if (M, r) is a model of $\mathbf{P}(V)$, then it is also a model of $\mathbf{P}(W)$ for any set W. Whenever the context is clear, we shall refer to a model (M, r) simply by 'M'. Most textbook references will exclude the empty set as a possible model. We see no reason to do that, and will follow P.T. Johnstone [32] and Wilfrid Hodges [29] in allowing the empty structure. As already pointed out, there is nothing deep or interesting about the empty set. It is often no more than a limiting case which feels like an annoying glitch. It is however a good discipline to confront our fear of the empty set, and we would hate to exclude it unless we find compelling reasons to do so. Thus we shall accept the empty set as a model, and carefully describe the implications of this choice as we go along. The next definition introduces the notion of *variables assignment* which are simply maps $a : V \to M$ where M is a model. If M is the empty model, then such variable assignments do not exist, unless of course V is itself empty, in which case there is a unique variables assignment, namely the empty map. Let us assume for now that $V \neq \emptyset$. In definition (104) below, we introduce the standard notion of *truth* of a formula $\phi \in \mathbf{P}(V)$ relative to a model M and assignment $a : V \to M$. The property of being *true* is denoted $M \vDash \phi[a]$. It is a standard practice to say that a formula ϕ is *true* in the model M which we denote $M \vDash \phi$, if and only if it is true relative to every assignment $a : V \to M$. Whenever M is the empty model and $V \neq \emptyset$, there exists no variables assignment $a : V \to M$ and the property $M \vDash \phi$ is vacuously true for every $\phi \in \mathbf{P}(V)$. This is probably why most authors wish to exclude the empty set as a possible structure: it is highly uncomfortable to claim that *everything is true in the empty model*. This is even more problematic when an author wishes to define a *satisfiable set* $\Gamma \subseteq \mathbf{P}(V)$ as a set *which has a model*, i.e. for which there exists a model M such that $M \vDash \phi$ for all $\phi \in \Gamma$. If we allow the empty model, then every set $\Gamma \subseteq \mathbf{P}(V)$

is *satisfiable* which is a huge problem. However, this problem is easily resolved: we just need to be careful about what it means for a formula ϕ to *have a model*, or a subset $\Gamma \subseteq \mathbf{P}(V)$ to be *satisfiable*: there should exist a model M *as well as* an assignment $a : V \to M$ such that $M \vDash \phi[a]$, or such that $M \vDash \phi[a]$ for all $\phi \in \Gamma$. With this in mind, it is clear the empty model is no longer a problem, as there is no pair (M, a) with $M = \emptyset$ which *satisfies* anything in the case when $V \neq \emptyset$. As it turns out, we defined a *satisfiable* subset $\Gamma \subseteq \mathbf{P}(V)$ in terms of valuations $v : \mathbf{P}(V) \to 2$ as per definition (97). As we shall see, every valuation $v \in \mathbf{P}^*(V)$ *has a model*, which is the essence of Gödel's completeness theorem. Once again we should be clear as to what v *having a model* means: there should exist a model M *as well as* an assignment $a : V \to M$ such that $v = \beta(\,\cdot\,)(a)$, where β is the model valuation function of M, as per definition (103) below.

Definition 103 *Let V be a set and M be a model of $\mathbf{P}(V)$. Any arbitrary map $a : V \to M$ is called an* assignment of variables *relative to the model M.*

4.2.2 Model Valuation Function

Let V be a set and (M, r) be a model. In definition (97) we defined the notion of *truth* of a formula $\phi \in \mathbf{P}(V)$ with respect to a valuation $v \in \mathbf{P}^*(V)$. We now want to formally define what it means for a formula $\phi \in \mathbf{P}(V)$ to be *true in the model M*. So suppose $\phi = (x \in y)$ for some $x, y \in V$. We want to assign a truth value to the formula ϕ in relation to the model M. The relation r on M is our interpretation of '$\in$'. Asking whether $\phi = (x \in y)$ is *true in M* is asking whether x and y satisfy the relation r. However, x and y are not elements of M, and it makes little sense to ask whether $(x, y) \in r$. We need some interpretation of x and y as elements of M. So let $a : V \to M$ be a variables assignment. We now have a natural interpretation of x and y as $a(x)$ and $a(y)$. So it is meaningful to ask whether $a(x)$ and $a(y)$ satisfy the relation r. Hence, although we cannot say what it is for $\phi = (x \in y)$ to be *true in M*, we can naturally define what it is for ϕ to be *true in M under the assignment a*. So let us focus on the latter: we shall say that $\phi = (x \in y)$ is *true in M under the assignment* $a : V \to M$ if and only if $(a(x), a(y)) \in r$. We now want to extend this definition to every $\phi \in \mathbf{P}(V)$. In order to do so, we need to rely on some form of structural recursion definition and it is therefore convenient to think in terms of *truth value* $\beta(\phi)(a)$. So we want to define a map $\beta : \mathbf{P}(V) \to [M^V \to 2]$ so that for all $\phi \in \mathbf{P}(V)$ we have a map $\beta(\phi) : M^V \to 2$ which determines whether ϕ is *true in M under the assignment* $a : V \to M$ by evaluating $\beta(\phi)$ at a i.e. by considering the value $\beta(\phi)(a)$. If $\beta(\phi)(a) = 1$ we shall say that ϕ is *true in M under the assignment* $a : V \to M$ and otherwise, if $\beta(\phi)(a) = 0$ we shall say that ϕ is false. So in the case when $\phi = (x \in y)$ the map $\beta(\phi) : M^V \to 2$ is defined as $\beta(\phi)(a) = 1_r(a(x), a(y))$ where $1_r : M \times M \to 2$ is the characteristic function of the relation $r \subseteq M \times M$. At this point, a natural question arises: the truth value of the formula ϕ under a given assignment $a \in M^V$ is a function of both ϕ and a. Why are we choosing β to be a map $\beta : \mathbf{P}(V) \to [M^V \to 2]$ i.e. with domain $\mathbf{P}(V)$ and range the set of maps $f : M^V \to 2$? Why not regard β

simply as a map $\beta : \mathbf{P}(V) \times M^V \to 2$? The answer is *structural recursion*: we need to define β by structural recursion on $\mathbf{P}(V)$, using either theorem (4) of page 42 or theorem (5) of page 44. The object we want to define needs to be a function with domain $\mathbf{P}(V)$ and nothing else. But then why not define β as a function $\beta : M^V \to [\mathbf{P}(V) \to 2]$? Given an assignment $a \in M^V$ the evaluation of β at a would yield a map $\beta(a) : \mathbf{P}(V) \to 2$ with domain $\mathbf{P}(V)$ and $\beta(a)$ could simply be defined by structural recursion. This is arguably more natural and simpler than considering a map $\beta : \mathbf{P}(V) \to [M^V \to 2]$. The answer is once again *structural recursion*: consider the formula $\phi = \forall x \phi_1$ for some $x \in V$ and $\phi_1 \in \mathbf{P}(V)$. Suppose we had to define the truth value $\beta(a)(\phi)$ of the formula ϕ under a. We would need to define what it means to be *true* for $\forall x \phi_1$. Roughly speaking, it would mean that ϕ_1 is *true under* a regardless of how the variable x is interpreted in M. In other words, it would mean that $\beta(b)(\phi_1) = 1$ whenever $b \in M^V$ is an assignment which coincides with a on V, except possibly for the value x. So our definition of $\beta(a)(\phi)$ would become:

$$\beta(a)(\phi) = \min \{ \beta(b)(\phi_1) \ : \ b = a \text{ on } V \setminus \{x\} \}$$

Unfortunately, this doesn't work. We are claiming to define $\beta(a) : \mathbf{P}(V) \to 2$ by structural recursion, but our definition has dependencies to some other functions $\beta(b) : \mathbf{P}(V) \to 2$. There is no way we can apply theorem (4) or theorem (5) with this sort of set up. We need to regard β as a map $\beta : \mathbf{P}(V) \to [M^V \to 2]$ with:

$$\beta(\phi)(a) = \min \{ \beta(\phi_1)(b) \ : \ b = a \text{ on } V \setminus \{x\} \}$$

In doing so, we are defining the map $\beta(\phi) : M^V \to 2$ simply in terms of the various values of the map $\beta(\phi_1) : M^V \to 2$. In effect, our structural recursion is defining all the maps $\beta(a) : \mathbf{P}(V) \to 2$ for $a \in M^V$ at the same time. This is done in a way which allows a successful application of theorem (4) of page 42. So the question is settled and we have put forward a formula to define $\beta(\phi)(a)$ in the case when $\phi = \forall x \phi_1$. It is clear that $\beta(\phi)(a)$ should be defined as 0 when $\phi = \bot$ which represents the *absurd* or *contradiction* and cannot be regarded as *true* under any assignment. It remains to define $\beta(\phi)(a)$ in the case when $\phi = \phi_1 \to \phi_2$ for some $\phi_1, \phi_2 \in \mathbf{P}(V)$. In line with mathematical practice, the formula $\phi = \phi_1 \to \phi_2$ should be regarded as *true* if and only if ϕ_1 is *false* or ϕ_2 is *true*. In other words, $\beta(\phi)(a) = 1$ if and only if $\beta(\phi_1)(a) = 0$ or $\beta(\phi_2)(a) = 1$:

$$\beta(\phi)(a) = \beta(\phi_1)(a) \to \beta(\phi_2)(a)$$

where $\to : 2^2 \to 2$ denotes the usual boolean operator defined by the table:

$$\begin{aligned} 0 \to 0 &= 1 \\ 0 \to 1 &= 1 \\ 1 \to 0 &= 0 \\ 1 \to 1 &= 1 \end{aligned}$$

The following definition if often known as *Tarski's definition of truth*. For the sake of lighter notations, we denote the set $V \setminus \{x\}$ simply by V_x. We also

identify the set of all maps $f : M^V \to 2$ with the power set $\mathcal{P}(M^V)$. There is an obvious bijection between the two, as any map $f : M^V \to 2$ can be regarded as the subset $A_f = \{a \in M^V : f(a) = 1\}$ and any subset $A \subseteq M^V$ can be viewed as its characteristic function $1_A : M^V \to 2$. With this in mind, the function $\beta : \mathbf{P}(V) \to [M^V \to 2]$ can be denoted $\beta : \mathbf{P}(V) \to \mathcal{P}(M^V)$, and given $\phi \in \mathbf{P}(V)$ the evaluation $\beta(\phi)$ can be viewed as the map $\beta(\phi) : M^V \to 2$, or equally as the set of all assignments $a : V \to M$ under which the formula ϕ is *true*. This latter point of view is the one adopted in Ferenczi and Szőts [18].

Definition 104 *Let V be a set and (M, r) be a model of $\mathbf{P}(V)$. We call* model valuation function *associated with M the map $\beta : \mathbf{P}(V) \to \mathcal{P}(M^V)$ defined by the following recursion: for all $\phi \in \mathbf{P}(V)$ and assignment $a : V \to M$:*

$$\beta(\phi)(a) = \begin{cases} 1_r(\, a(x), a(y)\,) & \text{if} \quad \phi = (x \in y) \\ 0 & \text{if} \quad \phi = \bot \\ \beta(\phi_1)(a) \to \beta(\phi_2)(a) & \text{if} \quad \phi = \phi_1 \to \phi_2 \\ \min\{\, \beta(\phi_1)(b) \;:\; b = a \text{ on } V_x \,\} & \text{if} \quad \phi = \forall x \phi_1 \end{cases}$$

where 1_r denotes the characteristic function of r on $M \times M$ and $V_x = V \setminus \{x\}$.

Proposition 321 *The structural recursion of* definition (103) *is legitimate.*

Proof
We need to show the existence and uniqueness of a map $\beta : \mathbf{P}(V) \to \mathcal{P}(M^V)$ which satisfies the four equations of definition (103). More, precisely, after we remove the abuse of language resulting from the identification of $\mathcal{P}(M^V)$ with the set of all maps $f : M^V \to 2$, we want $\beta : \mathbf{P}(V) \to A$ where $A = [M^V \to 2]$. One of the key decisions to make, is whether to use theorem (4) of page 42 or theorem (5) of page 44: given $\phi = \forall x \phi_1$, the question is whether $\beta(\phi)$ is a function of $\beta(\phi_1)$ alone, or whether it is functionally linked to both $\beta(\phi_1)$ and ϕ_1 itself. Looking at definition (103), it is clear the map $\beta(\phi) : M^V \to 2$ is simply a function of the map $\beta(\phi_1) : M^V \to 2$. So we shall use theorem (4). So we want to prove the existence and uniqueness of the map $\beta : \mathbf{P}(V) \to A$ satisfying the four equations of definition (103). First we need to provide a map $g_0 : \mathbf{P}_0(V) \to A$ so that the first equation is met. Given $x, y \in V$ we define $g_0(x \in y) : M^V \to 2$ by setting $g_0(x \in y)(a) = 1_r(a(x), a(y))$. Next we need to provide a map $h(\bot) : A^0 \to A$ so the second equation is met. So we define the map $h(\bot)(0) : M^V \to 2$ by setting $h(\bot)(0)(a) = 0$. Next we need to provide a map $h(\to) : A^2 \to A$ so as to meet the third equation. Given $f_1, f_2 : M^V \to 2$ we define $h(\to)(f_1, f_2) : M^V \to 2$ by setting $h(\to)(f_1, f_2)(a) = f_1(a) \to f_2(a)$. Finally, given $x \in V$ we need to provide a map $h(\forall x) : A^1 \to A$ so as to meet the fourth equation. So given $f_1 : M^V \to 2$ let $h(\forall x)(f_1) : M^V \to 2$ be defined by setting $h(\forall x)(f_1)(a) = \min\{\, f_1(b) \;:\; b = a \text{ on } V_x \,\}$. In other words, $h(\forall x)(f_1)(a)$ is defined as the minimum of the graph of the map f_1, restricted to the set of assignments $b : V \to M$ which coincide with the assignment a on $V_x = V \setminus \{x\}$. Let us check formally that the fourth equation is indeed

satisfied: from theorem (4) there exists a unique map $\beta : \mathbf{P}(V) \to A$ satisfying four equations defined by our data, and in particular when $\phi = \forall x \phi_1$ we have:

$$\beta(\phi)(a) = h(\forall x)(\beta(\phi_1))(a) = \min\{\, \beta(\phi_1)(b) \;:\; b = a \text{ on } V_x \,\}$$

.

Having defined the model valuation function $\beta : \mathbf{P}(V) \to [M^V \to 2]$ of a model (M, r), we should pause a few seconds to reflect on the case when $M = \emptyset$. We shall distinguish two cases: first we assume that $V \neq \emptyset$. Then $M^V = \emptyset$ and $[M^V \to 2] = 2^0 = 1 = \{0\}$. So β is the unique map $\beta : \mathbf{P}(V) \to \{0\}$. It should be noted that this map does not contradict the details of definition (103). Indeed, the set of variables assignments M^V being empty, the map β vacuously satisfies the recursion property of definition (103). We now consider the case when $V = \emptyset$. Then $M^V = 0^0 = 1 = \{0\}$ and $[M^V \to 2] = 2^1$. It follows that β is the map $\beta : \mathbf{P}(V) \to 2^1$ defined by the recursion property:

$$\beta(\phi)(0) = \begin{cases} 0 & \text{if} \quad \phi = \bot \\ \beta(\phi_1)(0) \to \beta(\phi_2)(0) & \text{if} \quad \phi = \phi_1 \to \phi_2 \end{cases}$$

Of course, there is no need to distinguish between the sets 2^1 and 2 and we can regard β simply as the map $\beta : \mathbf{P}(V) \to 2$ satisfying the recursion property:

$$\beta(\phi) = \begin{cases} 0 & \text{if} \quad \phi = \bot \\ \beta(\phi_1) \to \beta(\phi_2) & \text{if} \quad \phi = \phi_1 \to \phi_2 \end{cases}$$

This case is in fact applicable whenever $V = \emptyset$, regardless of whether $M = \emptyset$.

Definition 105 *Let V be a set and M be a model of $\mathbf{P}(V)$. We say that a formula $\phi \in \mathbf{P}(V)$ is* true *in the model M under the assignment $a : V \to M$, if and only if $\beta(\phi)(a) = 1$ where β is the model valuation function, and we write:*

$$M \vDash \phi[a]$$

In definition (97) we defined the notion of *truth* of a formula $\phi \in \mathbf{P}(V)$ with respect to a valuation $v \in \mathbf{P}^*(V)$ which we denoted $v \vDash \phi$. So definition (104) introduces what appears to be a new notion of *truth*, this time relative to a model M and assignment $a : V \to M$. In fact, as we shall see from theorem (38) of page 427, the map $\beta(\,.\,)(a) : \mathbf{P}(V) \to 2$ is itself a valuation. So definition (104) is in fact a particular case of definition (97) and the statement $M \vDash \phi[a]$ is equivalent to $\beta(\,.\,)(a) \vDash \phi$. However, the notion of dual space $\mathbf{P}^*(V)$ and the notation $v \vDash \phi$ are not commonly found in mathematical textbooks whereas $M \vDash \phi[a]$ is a well established standard. So it is important for us to quote definition (104). Note that this new notion of *truth* is not only relative to a model M, but also to an assignment $a : V \to M$. We do not wish to introduce the notation $M \vDash \phi$ in the case when $M \vDash \phi[a]$ is true for all $a \in M^V$. If we did that, as we have already discussed the statement $M \vDash \phi$ would be vacuously true in the case when M is the empty model and $V \neq \emptyset$.

4.2.3 The Relevance Lemma

Looking back at definition (103), if M is a model of $\mathbf{P}(V)$ with model valuation function $\beta : \mathbf{P}(V) \to \mathcal{P}(M^V)$, given a variables assignment $a : V \to M$ we have:

$$\beta(\forall x \phi_1)(a) = \min \{ \beta(\phi_1)(b) \ : \ b = a \text{ on } V_x \}$$

So the truth value of $\phi = \forall x \phi_1$ under the assignment $a : V \to M$ is determined by the set of all assignments $b : V \to M$ which coincide with a on the set $V \setminus \{x\}$. In particular, the value $a(x)$ i.e. the interpretation of the variable x under the assignment a is not relevant. More generally, it is easy to believe that unless $x \in V$ is a free variable of the formula $\phi \in \mathbf{P}(V)$, the truth value $\beta(\phi)(a)$ is not impacted by the value $a(x)$. In other words, we expect $\beta(\phi)(a)$ to solely depend on the restriction $a_{|\mathrm{Fr}(\phi)}$. The following proposition establishes that fact. We chose to entitle this section *The Relevance Lemma* following lecture 26 of the online course of Prof. Arindama Singh [55] which offers a proof of the result on the YouTube link `http://nptel.iitm.ac.in/courses/111106052/26`.

Proposition 322 *Let V be a set and M be a model of $\mathbf{P}(V)$ with model valuation function $\beta : \mathbf{P}(V) \to \mathcal{P}(M^V)$. Then for all $\phi \in \mathbf{P}(V)$ and $a, b : V \to M$:*

$$a_{|\mathrm{Fr}(\phi)} = b_{|\mathrm{Fr}(\phi)} \ \Rightarrow \ \beta(\phi)(a) = \beta(\phi)(b) \tag{4.3}$$

Proof
For all $\phi \in \mathbf{P}(V)$ we need to show that for all assignments $a, b : V \to M$, the implication (4.3) is true. We shall do so by structural induction, using theorem (3) of page 31. First we assume that $\phi = (x \in y)$ where $x, y \in V$. Let $a, b : V \to M$ be two assignments such that $a = b$ on $\mathrm{Fr}(\phi)$. Then in particular we have $a(x) = b(x)$ and $a(y) = b(y)$. We need to show that $\beta(\phi)(a) = \beta(\phi)(b)$, which goes as follows, denoting $r \subseteq M \times M$ the relation on M:

$$\begin{aligned} \beta(\phi)(a) &= \beta(x \in y)(a) \\ &= 1_r(a(x), a(y)) \\ &= 1_r(b(x), b(y)) \\ &= \beta(x \in y)(b) \\ &= \beta(\phi)(b) \end{aligned}$$

Next we assume that $\phi = \bot$. Let $a, b : V \to M$ be two assignments. Then a and b vacuously coincide on $\mathrm{Fr}(\phi)$. In any case we have $\beta(\bot)(a) = 0 = \beta(\bot)(b)$. So we now assume that $\phi = \phi_1 \to \phi_2$ where $\phi_1, \phi_2 \in \mathbf{P}(V)$ are such that the implication (4.3) is true for all $a, b : V \to M$. We need to show the same is true of ϕ. So let $a, b : V \to M$ be two assignments such that $a = b$ on $\mathrm{Fr}(\phi) = \mathrm{Fr}(\phi_1) \cup \mathrm{Fr}(\phi_2)$. We need to show that $\beta(\phi)(a) = \beta(\phi)(b)$:

$$\beta(\phi)(a) \quad = \quad \beta(\phi_1 \to \phi_2)(a)$$

$$
\begin{array}{rcl}
 & = & \beta(\phi_1)(a) \to \beta(\phi_2)(a) \\
a = b \text{ on } \mathrm{Fr}(\phi_1) \ \to & = & \beta(\phi_1)(b) \to \beta(\phi_2)(a) \\
a = b \text{ on } \mathrm{Fr}(\phi_2) \ \to & = & \beta(\phi_1)(b) \to \beta(\phi_2)(b) \\
 & = & \beta(\phi_1 \to \phi_2)(b) \\
 & = & \beta(\phi)(b)
\end{array}
$$

Finally we assume that $\phi = \forall x \phi_1$ where $x \in V$ and $\phi_1 \in \mathbf{P}(V)$ is such that the implication (4.3) is true for all $a, b : V \to M$. We need to show the same is true of ϕ. So let $a, b : V \to M$ be two assignments such that $a = b$ on $\mathrm{Fr}(\phi)$. We need to show that $\beta(\phi)(a) = \beta(\phi)(b)$ which goes as follows:

$$
\begin{array}{rcl}
\beta(\phi)(a) & = & \beta(\forall x \phi_1)(a) \\
 & = & \min \{ \, \beta(\phi_1)(c) \ : \ c = a \text{ on } V_x \, \} \\
\text{A: to be proved } \to & = & \min \{ \, \beta(\phi_1)(d) \ : \ d = b \text{ on } V_x \, \} \\
 & = & \beta(\forall x \phi_1)(b) \\
 & = & \beta(\phi)(b)
\end{array}
$$

So it remains to prove point A, for which it is sufficient to show the set equality:

$$
X = \{ \, \beta(\phi_1)(c) \ : \ c = a \text{ on } V_x \, \} = \{ \, \beta(\phi_1)(d) \ : \ d = b \text{ on } V_x \, \} = Y
$$

First we show that $X \subseteq Y$: so let $\epsilon \in X$. There exists an assignment $c : V \to M$ such that $c = a$ on $V \setminus \{x\}$ and $\epsilon = \beta(\phi_1)(c)$. Define the assignment $d : V \to M$ by setting $d = b$ on $V \setminus \{x\}$ and $d(x) = c(x)$. In order to show that $\epsilon \in Y$, it is sufficient to prove that $\epsilon = \beta(\phi_1)(d)$. So we need to prove that $\beta(\phi_1)(c) = \beta(\phi_1)(d)$. Having assumed the implication (4.3) is true for ϕ_1 and all assignments a, b, it is sufficient to show that c and d coincide on $\mathrm{Fr}(\phi_1)$. So let $u \in \mathrm{Fr}(\phi_1)$. We need to show that $c(u) = d(u)$. We shall distinguish two cases: first we assume that $u = x$. Then $c(x) = d(x)$ is true by definition of d. Next we assume that $u \neq x$. Then $u \in \mathrm{Fr}(\phi_1) \setminus \{x\} = \mathrm{Fr}(\phi)$. Having assumed a and b coincide on $\mathrm{Fr}(\phi)$, we obtain $a(u) = b(u)$. Furthermore, since $u \neq x$ and $c = a$ and $V \setminus \{x\}$ we have $c(u) = a(u)$. By definition, $d = b$ on $V \setminus \{x\}$ and consequently $d(u) = b(u)$. We conclude that $c(u) = d(u)$ as requested, and we have proved that $X \subseteq Y$. By symmetry, we show similarly that $Y \subseteq X$. **.**

4.2.4 The Substitution Lemma

Let M be a model and $\sigma : V \to W$ be a map. For each variables assignment $a : W \to M$ we obtain map $a \circ \sigma : V \to M$ which is also a variables assignment. Given $\phi \in \mathbf{P}(V)$, it is therefore meaningful to ask whether the formula ϕ is true in the model M under the assignment $a \circ \sigma$. Denoting β the model valuation function of M on $\mathbf{P}(V)$, this amounts to asking whether $\beta(\phi)(a \circ \sigma) = 1$. Now consider the formula $\sigma(\phi) \in \mathbf{P}(W)$. It is also meaningful to ask wether the formula $\sigma(\phi)$ is true in the model M under the assignment a. Again denoting

β the model valuation function of M on $\mathbf{P}(W)$ this amounts to asking whether $\beta(\sigma(\phi))(a) = 1$. However, the formula $\sigma(\phi)$ is roughly speaking identical to the formula ϕ, after all variables have been interpreted in W according to the *assignment* $\sigma : V \to W$. It follows that interpreting the variables of $\sigma(\phi)$ in M according to the assignment $a : W \to M$ seemingly amounts to interpreting the variables of ϕ in M according to the assignment $a \circ \sigma : V \to M$. So if the formula $\sigma(\phi)$ is true under the assignment a, we should expect the formula ϕ to be true under the assignment $a \circ \sigma$ and conversely. In other words we expect:

$$\beta(\sigma(\phi))(a) = \beta(\phi)(\, a \circ \sigma\,) \tag{4.4}$$

Of course things are slightly more complicated and we are now well aware that things usually go wrong when σ is not a valid substitution for ϕ. So let us find a simple counterexample: Consider $V = \{x, y\}$ with $x \neq y$ and $W = \{u\}$. Let σ be the unique map $\sigma : V \to W$ defined by $\sigma(x) = \sigma(y) = u$. Let $\phi = \forall y(x \in y)$. Then we have $\sigma(\phi) = \forall u(u \in u)$ and σ is clearly not valid for ϕ. It should not be difficult to find a model (M, r) together with an assignment $a : W \to M$ for which the equation (4.4) fails. We cannot use the empty model $M = \emptyset$ as there exists no assignment $a : W \to M$ in this case. So let us try a model with a single element, namely $M = 1 = \{0\}$. In this case, there exists a unique assignment $a : W \to M$ defined by $a(u) = 0$. It follows that $a \circ \sigma : V \to M$ is given by $a \circ \sigma(x) = a \circ \sigma(y) = 0$. So every variable of $\phi = \forall y(x \in y)$ or $\sigma(\phi) = \forall u(u \in u)$ is interpreted as 0 in M. Now we need to choose a binary relation r on M. Since $M \times M = 1 \times 1 = \{(0, 0)\}$, we have two possible choices, namely $r = \emptyset$ or $r = M \times M$. First we assume that $r = \emptyset$. Then we have:

$$\begin{aligned}
\beta(\sigma(\phi))(a) &= \beta(\,\forall u(u \in u)\,)(a) \\
&= \min\{\beta(u \in u)(b) \;:\; b = a \text{ on } W_u\} \\
&= \min\{1_r(b(u), b(u)) \;:\; b = a \text{ on } W_u\} \\
r = \emptyset \;\to\; &= \min\{0 \;:\; b = a \text{ on } W_u\} \\
&= 0
\end{aligned}$$

So the formula $\sigma(\phi) = \forall u(u \in u)$ is false in M under the assignment a in the case when $r = \emptyset$, a fact which we could have guessed from our intuition. Now:

$$\begin{aligned}
\beta(\phi)(a \circ \sigma) &= \beta(\,\forall y(x \in y)\,)(a \circ \sigma) \\
&= \min\{\beta(x \in y)(c) \;:\; c = a \circ \sigma \text{ on } V_y\} \\
&= \min\{1_r(c(x), c(y)) \;:\; c = a \circ \sigma \text{ on } V_y\} \\
r = \emptyset \;\to\; &= \min\{0 \;:\; c = a \circ \sigma \text{ on } V_y\} \\
&= 0
\end{aligned}$$

So the formula $\phi = \forall y(x \in y)$ is also false in M under the assignment $a \circ \sigma$, and the case $r = \emptyset$ fails to provide us with a counterexample. So we now assume that $r = M \times M$. Then $1_r = 1$ and going through the same calculations as above, we obtain $\beta(\sigma(\phi))(a) = 1 = \beta(\phi)(a \circ \sigma)$. So once again, we fail to obtain

our desired counterexample. So we now consider a more complicated model with two elements namely $M = 2 = \{0, 1\}$. There are two possible assignments $a : W \to M$ depending on whether $a(u) = 0$ or $a(u) = 1$. Since we have not yet chosen any relation $r \subseteq M \times M$, it is easy to believe that choosing the assignment $a(u) = 0$ bears no loss of generality. Now we want to find a relation r on M so that $\forall y(x \in y)$ and $\forall u(u \in u)$ have different truth value in (M, r). For example, we want $\forall y(x \in y)$ to be true and $\forall u(u \in u)$ to be false. Loosely speaking, since $a \circ \sigma(x) = 0$ we want $\forall y(0 \in y)$ to be true while $\forall u(u \in u)$ is false. So let us pick $r = \{(0, 0), (0, 1)\}$. Then we have:

$$\begin{array}{rcl}
\beta(\sigma(\phi))(a) & = & \beta(\,\forall u(u \in u)\,)(a) \\
 & = & \min\{\beta(u \in u)(b) \;:\; b = a \text{ on } W_u\} \\
\text{for any } b : W \to M \;\to & \leq & \beta(u \in u)(b) \\
 & = & 1_r(b(u), b(u)) \\
\text{choosing } b(u) = 1 \;\to & = & 1_r(1, 1) \\
(1, 1) \notin r \;\to & = & 0
\end{array}$$

and:

$$\begin{array}{rcl}
\beta(\phi)(a \circ \sigma) & = & \beta(\,\forall y(x \in y)\,)(a \circ \sigma) \\
 & = & \min\{\beta(x \in y)(c) \;:\; c = a \circ \sigma \text{ on } V_y\} \\
c_1(y) = 0 \text{ while } c_2(y) = 1 \;\to & = & \beta(x \in y)(c_1) \wedge \beta(x \in y)(c_2) \\
 & = & 1_r(c_1(x), c_1(y)) \wedge 1_r(c_2(x), c_2(y)) \\
 & = & 1_r(c_1(x), 0) \wedge 1_r(c_2(x), 1) \\
x \in V_y \;\to & = & 1_r(a \circ \sigma(x), 0) \wedge 1_r(a \circ \sigma(x), 1) \\
 & = & 1_r(0, 0) \wedge 1_r(0, 1) \\
 & = & 1 \wedge 1 \\
 & = & 1
\end{array}$$

So we have found a counterexample to equation (4.4) in the case when σ is not a valid substitution for $\phi \in \mathbf{P}(V)$. We shall now establish the positive result:

Proposition 323 *Let V, W be sets and $\sigma : V \to W$ be a map. Let M be a model of $\mathbf{P}(V)$ and $\mathbf{P}(W)$ with associated model valuation functions denoted β. Then for all $\phi \in \mathbf{P}(V)$ and assignment $a : W \to M$, if σ is valid for ϕ we have:*

$$\beta(\sigma(\phi))(a) = \beta(\phi)(\,a \circ \sigma\,)$$

where $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ also denotes the associated substitution mapping.

Proof
Note that the 'β' appearing on the left-hand-side is the model valuation function $\beta : \mathbf{P}(W) \to \mathcal{P}(M^W)$ while the 'β' appearing on the right-hand-side is the model valuation function $\beta : \mathbf{P}(V) \to \mathcal{P}(M^V)$. Recall that $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$

is the associated substitution mapping as per definition (24) and consequently $\sigma(\phi) \in \mathbf{P}(W)$ whenever $\phi \in \mathbf{P}(V)$. Finally, if $a : W \to M$ is an assignment, then $a \circ \sigma : V \to M$ is also an assignment. So everything makes sense. Given M and $\sigma : V \to W$, for all $\phi \in \mathbf{P}(V)$ we need to prove that for all $a : W \to M$:

$$(\sigma \text{ valid for } \phi) \;\Rightarrow\; \beta(\sigma(\phi))(a) = \beta(\phi)(\, a \circ \sigma\,)$$

We shall do so by a structural induction argument, using theorem (3) of page 31. First we assume that $\phi = (x \in y)$ where $x, y \in V$. Let $a : W \to M$. Then σ is always valid for ϕ and denoting $r \subseteq M \times M$ the relation on M we have:

$$\begin{aligned}
\beta(\sigma(\phi))(a) &= \beta(\sigma(x \in y))(a) \\
&= \beta(\, \sigma(x) \in \sigma(y)\,)(a) \\
&= 1_r(\, a(\sigma(x))\,,\, a(\sigma(y))\,) \\
&= 1_r(\, a \circ \sigma(x)\,,\, a \circ \sigma(y)\,) \\
&= \beta(x \in y)(a \circ \sigma) \\
&= \beta(\phi)(a \circ \sigma)
\end{aligned}$$

We now assume that $\phi = \bot$. Then given $a : W \to M$ we have:

$$\beta(\sigma(\bot))(a) = \beta(\bot)(a) = 0 = \beta(\bot)(a \circ \sigma)$$

So we now assume that $\phi = \phi_1 \to \phi_2$ where $\phi_1, \phi_2 \in \mathbf{P}(V)$ satisfy our property. We need to show the same is true of ϕ. So let $a : W \to M$ be an assignment and suppose σ is valid for ϕ. We need to show $\beta(\sigma(\phi))(a) = \beta(\phi)(\, a \circ \sigma\,)$. However, using proposition (54), σ is valid for both ϕ_1 and ϕ_2. Hence the equation is true both for ϕ_1 and ϕ_2 and consequently we have:

$$\begin{aligned}
\beta(\sigma(\phi))(a) &= \beta(\sigma(\phi_1 \to \phi_2))(a) \\
&= \beta(\, \sigma(\phi_1) \to \sigma(\phi_2)\,)(a) \\
&= \beta(\sigma(\phi_1))(a) \to \beta(\sigma(\phi_2))(a) \\
&= \beta(\phi_1)(a \circ \sigma) \to \beta(\phi_2)(a \circ \sigma) \\
&= \beta(\phi_1 \to \phi_2)(a \circ \sigma) \\
&= \beta(\phi)(a \circ \sigma)
\end{aligned}$$

So we now assume that $\phi = \forall x \phi_1$ where $x \in V$ and $\phi_1 \in \mathbf{P}(V)$ satisfy our property. We need to show the same is true for ϕ. So let $a : W \to M$ be an assignment and suppose σ is valid for ϕ. We want $\beta(\sigma(\phi))(a) = \beta(\phi)(\, a \circ \sigma\,)$. However, from proposition (55), σ is also valid for ϕ_1. Hence, the equation is true for ϕ_1 and any assignment $b : W \to M$. It follows that:

$$\begin{aligned}
\beta(\sigma(\phi))(a) &= \beta(\sigma(\forall x \phi_1))(a) \\
&= \beta(\, \forall \sigma(x) \sigma(\phi_1)\,)(a)
\end{aligned}$$

$$
\begin{array}{rcl}
 & = & \min\{\,\beta(\sigma(\phi_1))(b)\ :\ b = a \text{ on } W_{\sigma(x)}\,\} \\
 & = & \min\{\,\beta(\phi_1)(b\circ\sigma)\ :\ b = a \text{ on } W_{\sigma(x)}\,\} \\
\text{A: to be proved } \rightarrow & = & \min\{\,\beta(\phi_1)(k)\ :\ k = a\circ\sigma \text{ on } V_x\,\} \\
 & = & \beta(\forall x\phi_1)(a\circ\sigma) \\
 & = & \beta(\phi)(a\circ\sigma)
\end{array}
$$

So it remains to prove point A, for which it is sufficient to show the set equality:

$$X = \{\,\beta(\phi_1)(b\circ\sigma)\ :\ b = a \text{ on } W_{\sigma(x)}\,\} = \{\,\beta(\phi_1)(k)\ :\ k = a\circ\sigma \text{ on } V_x\,\} = Y$$

First we show that $X \subseteq Y$. So let $\epsilon \in X$. There exists an assignment $b : W \to M$ which coincides with a on $W \setminus \{\sigma(x)\}$ such that $\epsilon = \beta(\phi_1)(b\circ\sigma)$. We need to show that $\epsilon \in Y$. Define the assignment $k : V \to M$ by setting $k = a\circ\sigma$ on $V \setminus \{x\}$ and $k(x) = b\circ\sigma(x)$. In order to show that $\epsilon \in Y$ it is sufficient to show that $\epsilon = \beta(\phi_1)(k)$. So we need to show that $\beta(\phi_1)(b\circ\sigma) = \beta(\phi_1)(k)$. Using proposition (322), it is sufficient to prove that $b\circ\sigma$ and k coincide on $\mathrm{Fr}(\phi_1)$. So let $u \in \mathrm{Fr}(\phi_1)$. We need to show that $b\circ\sigma(u) = k(u)$. We shall distinguish two cases: first we assume that $u = x$. Then $b\circ\sigma(x) = k(x)$ is true by definition of k. Next we assume that $u \neq x$. Then $u \in \mathrm{Fr}(\phi_1) \setminus \{x\} = \mathrm{Fr}(\phi)$. From the validity of σ for ϕ and proposition (55) we obtain $\sigma(u) \neq \sigma(x)$. It follows that a and b coincide on $\sigma(u)$ i.e. $a\circ\sigma(u) = b\circ\sigma(u)$. However by definition, the assignment k coincides with $a\circ\sigma$ on $V \setminus \{x\}$. Since $u \neq x$ we obtain $k(u) = a\circ\sigma(u)$ and it follows that $b\circ\sigma(u) = k(u)$ as requested. So we now show that $Y \subseteq X$: let $\epsilon \in Y$. There exists an assignment $k : V \to M$ which coincides with $a\circ\sigma$ on $V \setminus \{x\}$ such that $\epsilon = \beta(\phi_1)(k)$. We need to show that $\epsilon \in X$. Define the assignment $b : W \to M$ by setting $b = a$ on $W \setminus \{\sigma(x)\}$ and $b(\sigma(x)) = k(x)$. In order to show that $\epsilon \in X$ it is sufficient to prove that $\epsilon = \beta(\phi_1)(b\circ\sigma)$. So we need to show that $\beta(\phi_1)(b\circ\sigma) = \beta(\phi_1)(k)$, for which we shall pretty much repeat our previous argument: using proposition (322), it is sufficient to prove that $b\circ\sigma$ and k coincide on $\mathrm{Fr}(\phi_1)$. So let $u \in \mathrm{Fr}(\phi_1)$. We need to show that $b\circ\sigma(u) = k(u)$. We shall distinguish two cases: first we assume that $u = x$. Then $b\circ\sigma(x) = k(x)$ is true by definition of b. Next we assume that $u \neq x$. Then $u \in \mathrm{Fr}(\phi_1) \setminus \{x\} = \mathrm{Fr}(\phi)$. From the validity of σ for ϕ and proposition (55) we obtain $\sigma(u) \neq \sigma(x)$. However by definition, the assignment b coincides with a on $W \setminus \{\sigma(x)\}$. Since $\sigma(u) \neq \sigma(x)$ we obtain $b\circ\sigma(u) = a\circ\sigma(u)$. Furthermore, since the assignment k coincide with $a\circ\sigma$ on $V \setminus \{x\}$ and $u \neq x$ we have $a\circ\sigma(u) = k(u)$ and it follows that $b\circ\sigma(u) = k(u)$. .

So we know that $\beta(\sigma(\phi))(a) = \beta(\phi)(\,a\circ\sigma\,)$ whenever $\sigma : V \to W$ is valid for $\phi \in \mathbf{P}(V)$ and $a : W \to M$ is an arbitrary assignment. As we have done on several occasions before, we would like to extend this formula from valid substitutions to essential substitutions of definition (44). So we need to say something about minimal transforms of definition (38). So let V be a set with minimal extension $\bar{V}$. Given $\phi \in \mathbf{P}(V)$ with minimal transform the formula $\mathcal{M}(\phi) \in \mathbf{P}(\bar{V})$, we know that ϕ and $\mathcal{M}(\phi)$ are essentially the same formula

where the bound variables of ϕ have been replaced with elements of $\mathbf{N}$. So we would expect the *truth* of the formula ϕ in a model M under an assignment $a : V \to M$ to be equivalent to the *truth* of $\mathcal{M}(\phi)$ under the same assignment. More precisely, whichever way we decide to extend the assignment $a : V \to M$ into an assignment $a^* : \bar{V} \to M$, since every $n \in \mathbf{N}$ cannot be a free variable of the minimal transform $\mathcal{M}(\phi)$, we know from the relevance lemma of proposition (322) that $\beta(\mathcal{M}(\phi))(a^*)$ will essentially depend on a and not on the specifics of the extension a^*. In fact, we expect $\beta(\mathcal{M}(\phi))(a^*) = \beta(\phi)(a)$:

Proposition 324 *Let V be a set with minimal extension $\bar{V}$. Let M be a model of $\mathbf{P}(V)$ and $\mathbf{P}(\bar{V})$ with associated model valuation functions denoted β. Let $a : V \to M$ and $a^* : \bar{V} \to M$ be an arbitrary extension of a. For all $\phi \in \mathbf{P}(V)$:*

$$\beta(\mathcal{M}(\phi))(a^*) = \beta(\phi)(a) \tag{4.5}$$

where $\mathcal{M}(\phi) \in \mathbf{P}(\bar{V})$ is the minimal transform of ϕ as per definition (38)*.*

Proof
Given $\phi \in \mathbf{P}(V)$ we need to show that for any assignment $a : V \to M$ and any extension $a^* : \bar{V} \to M$, the equality (4.5) holds. We shall do so by structural induction, using theorem (3) of page 31. First we assume that $\phi = (x \in y)$ where $x, y \in V$. Let $a : V \to M$ and $a^* : \bar{V} \to M$ be an extension of a. Then, denoting $r \subseteq M \times M$ the relation on M, we have:

$$\begin{array}{rcl} \beta(\mathcal{M}(\phi))(a^*) & = & \beta(\mathcal{M}(x \in y))(a^*) \\ & = & \beta(x \in y)(a^*) \\ & = & 1_r(a^*(x), a^*(y)) \\ a^*_{|V} = a \ \to & = & 1_r(a(x), a(y)) \\ & = & \beta(x \in y)(a) \\ & = & \beta(\phi)(a) \end{array}$$

Next we assume that $\phi = \bot$. Given $a : V \to M$ and extension $a^* : \bar{V} \to M$:

$$\beta(\mathcal{M}(\bot))(a^*) = \beta(\bot)(a^*) = 0 = \beta(\bot)(a)$$

So we now assume that $\phi = \phi_1 \to \phi_2$ where $\phi_1, \phi_2 \in \mathbf{P}(V)$ are such that for all $a : V \to M$ and extension $a^* : \bar{V} \to M$, the equality (4.5) holds. We need to show the same is true of ϕ. So let $a : V \to M$ with extension $a^* : \bar{V} \to M$:

$$\begin{array}{rcl} \beta(\mathcal{M}(\phi))(a^*) & = & \beta(\mathcal{M}(\phi_1 \to \phi_2))(a^*) \\ & = & \beta(\, \mathcal{M}(\phi_1) \to \mathcal{M}(\phi_2) \,)(a^*) \\ & = & \beta(\mathcal{M}(\phi_1))(a^*) \to \beta(\mathcal{M}(\phi_2))(a^*) \\ & = & \beta(\phi_1)(a) \to \beta(\phi_2)(a) \\ & = & \beta(\phi_1 \to \phi_2)(a) \\ & = & \beta(\phi)(a) \end{array}$$

Finally, we assume that $\phi = \forall x \phi_1$ where $x \in V$ and $\phi_1 \in \mathbf{P}(V)$ is such that for all $a : V \to M$ and extension $a^* : \bar{V} \to M$, the equality (4.5) holds. We need to show the same is true of ϕ. So let $a : V \to M$ with extension $a^* : \bar{V} \to M$:

$$\begin{array}{rcl}
\beta(\mathcal{M}(\phi))(a^*) & = & \beta(\mathcal{M}(\forall x \phi_1))(a^*) \\
[n/x] \text{ valid for } \mathcal{M}(\phi_1) \ \rightarrow & = & \beta(\ \forall n \mathcal{M}(\phi_1)[n/x]\ )(a^*) \\
& = & \min\left\{\beta(\ [n/x] \circ \mathcal{M}(\phi_1)\ )(b^*) : b^* = a^* \text{ on } \bar{V}_n\right\} \\
\text{prop. (323)} \ \rightarrow & = & \min\left\{\beta(\mathcal{M}(\phi_1))(\ b^* \circ [n/x]\ ) : b^* = a^* \text{ on } \bar{V}_n\right\} \\
& = & \min\left\{\beta(\phi_1)(\ (b^* \circ [n/x])_{|V}\ ) : b^* = a^* \text{ on } \bar{V}_n\right\} \\
\text{A: to be proved} \ \rightarrow & = & \min\{\beta(\phi_1)(b) \ : \ b = a \text{ on } V_x\} \\
& = & \beta(\forall x \phi_1)(a) \\
& = & \beta(\phi)(a)
\end{array}$$

So it remains to prove point A, for which it is sufficient to show the set equality:

$$X = \left\{\beta(\phi_1)(\ (b^* \circ [n/x])_{|V}\ ) : b^* = a^* \text{ on } \bar{V}_n\right\} = \{\beta(\phi_1)(b) \ : \ b = a \text{ on } V_x\} = Y$$

First we show that $X \subseteq Y$: so let $\epsilon \in X$. There exists an assignment $b^* : \bar{V} \to M$ such that $b^* = a^*$ on $\bar{V} \setminus \{n\}$ and $\epsilon = \beta(\phi_1)(\ (b^* \circ [n/x])_{|V}\ )$. We need to show that $\epsilon \in Y$. Define the assignment $b : V \to M$ by setting $b = a$ on $V \setminus \{x\}$ and $b(x) = b^*(n)$. In order to show that $\epsilon \in Y$, it is sufficient to prove that $\epsilon = \beta(\phi_1)(b)$. So we need to show that $\beta(\phi_1)(\ (b^* \circ [n/x])_{|V}\ ) = \beta(\phi_1)(b)$. Using proposition (322), it is sufficient to prove that $(b^* \circ [n/x])_{|V}$ and b coincide on $\mathrm{Fr}(\phi_1)$. So let $u \in \mathrm{Fr}(\phi_1)$. We need to prove that $b^* \circ [n/x](u) = b(u)$. We shall distinguish two cases: first we assume that $u = x$. Then we need to show that $b^*(n) = b(x)$ which is true by definition of b. Next we assume that $u \neq x$. Then we need to show that $b^*(u) = b(u)$. However, since $b^* = a^*$ on $\bar{V} \setminus \{n\}$ and $u \in V$, we have $u \neq n$ and consequently $b^*(u) = a^*(u)$. Furthermore, a^* is an extension of a so $a^*(u) = a(u)$. So we need to show that $a(u) = b(u)$ which is true by definition of b and $u \neq x$. We now show that $Y \subseteq X$: so let $\epsilon \in Y$. There exists an assignment $b : V \to M$ such that $b = a$ on $V \setminus \{x\}$ and $\epsilon = \beta(\phi_1)(b)$. We need to show that $\epsilon \in X$. Define the assignment $b^* : \bar{V} \to M$ by setting $b^* = a^*$ on $\bar{V} \setminus \{n\}$ and $b^*(n) = b(x)$. In order to show that $\epsilon \in X$ it is sufficient to prove that $\epsilon = \beta(\phi_1)(\ (b^* \circ [n/x])_{|V}\ )$. Hence we need to show the equality $\beta(\phi_1)(\ (b^* \circ [n/x])_{|V}\ ) = \beta(\phi_1)(b)$. Using proposition (322), it is sufficient to prove that $(b^* \circ [n/x])_{|V}$ and b coincide on $\mathrm{Fr}(\phi_1)$. So let $u \in \mathrm{Fr}(\phi_1)$. We need to prove that $b^* \circ [n/x](u) = b(u)$. We shall distinguish two cases: first we assume that $u = x$. Then we need to show that $b^*(n) = b(x)$ which is true by definition of b^*. Next we assume that $u \neq x$. Then we need to show that $b^*(u) = b(u)$. However, since $b^* = a^*$ on $\bar{V} \setminus \{n\}$ and $u \in V$, we have $u \neq n$ and consequently $b^*(u) = a^*(u)$. Furthermore, a^* is an extension of a so $a^*(u) = a(u)$. So we need to show that $a(u) = b(u)$ which follows from $u \neq x$. .

Having established proposition (324) we are able to link the notions of minimal transform $\mathcal{M}(\phi)$ and that of model valuation function β. So we can now

hope to prove the formula $\beta(\sigma(\phi))(a) = \beta(\phi)(\,a \circ \sigma\,)$ in the general case when $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is an essential substitution as per definition (44). However before we do so, we need to check the formula makes sense in principle. So let $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ be an essential substitution. Then σ is associated to a unique map $\sigma : V \to W$ (also denoted σ) and for every map $a : W \to M$, we have a meaningful assignment $a \circ \sigma : V \to M$. Hence the expression $\beta(\phi)(\,a \circ \sigma\,)$ makes perfect sense for all $\phi \in \mathbf{P}(V)$. However, we know from proposition (114) that any essential substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ can be redefined arbitrarily modulo the substitution congruence, without changing its associated map $\sigma : V \to W$. So the formula $\beta(\sigma(\phi))(a) = \beta(\phi)(\,a \circ \sigma\,)$ cannot be true unless $\beta(\,\cdot\,)(a)$ is invariant with respect to a particular choice of formula modulo substitution. The following proposition ensures this is the case. As we shall soon discover from theorem (38) of page 427, $\beta(\,\cdot\,)(a)$ is in fact a valuation and proposition (325) below is therefore a particular case of proposition (309).

Proposition 325 *Let V be a set and M be a model of $\mathbf{P}(V)$ with model valuation function β. Then for all $\phi, \psi \in \mathbf{P}(V)$ and assignment $a : V \to M$:*

$$\phi \sim \psi \;\Rightarrow\; \beta(\phi)(a) = \beta(\psi)(a)$$

where $\sim$ denotes the substitution congruence on $\mathbf{P}(V)$.

Proof
Let $\phi, \psi \in \mathbf{P}(V)$ such that $\phi \sim \psi$ and let $a : V \to M$ be an assignment. We need to show that $\beta(\phi)(a) = \beta(\psi)(a)$. We shall distinguish two cases: first we assume that there exists an assignment $a^* : \bar{V} \to M$ which is an extension of a. Then using proposition (324) we obtain the following equalities:

$$\beta(\phi)(a) = \beta(\mathcal{M}(\phi))(a^*) = \beta(\mathcal{M}(\psi))(a^*) = \beta(\psi)(a)$$

where we have used the fact that $\mathcal{M}(\phi) = \mathcal{M}(\psi)$, itself a consequence of $\phi \sim \psi$ and theorem (14) of page 149. Next we assume that there exists no extension $a^* : \bar{V} \to M$. This can only be the case when $M = \emptyset$. Otherwise, pick an arbitrary $m^* \in M$ and define $a^*(n) = m^*$ for all $n \in \mathbf{N}$. Now if $M = \emptyset$, the only possible assignment $a : V \to M$ is the map with empty domain, i.e. $a = \emptyset$. It follows that $V = \emptyset$ and consequently from definition (35), the substitution congruence on $\mathbf{P}(V)$ is generated by the empty set. Hence from the equivalence $\phi \sim \psi$ we obtain $\phi = \psi$ and the equality $\beta(\phi)(a) = \beta(\psi)(a)$ follows. **.**

We are now ready to prove our next theorem which extends proposition (323) to essential substitutions and is commonly known as the *Substitution Lemma*.

Theorem 36 *Let V, W be sets and $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ be an essential substitution. Let M be a model of $\mathbf{P}(V)$ and $\mathbf{P}(W)$ with model valuation functions β. Then for all $\phi \in \mathbf{P}(V)$ and assignment $a : W \to M$, we have the equality:*

$$\beta(\sigma(\phi))(a) = \beta(\phi)(a \circ \sigma) \tag{4.6}$$

Proof
Note that the 'σ' appearing on the right-hand-side of equation (4.6) is the map

$\sigma : V \to W$ associated with the essential substitution $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$, i.e. the unique map σ such that $\mathcal{M} \circ \sigma = \bar{\sigma} \circ \mathcal{M}$ as per definition (44). So if $a : W \to M$ is an assignment then $a \circ \sigma : V \to M$ is also an assignment. Now given $\phi \in \mathbf{P}(V)$ and an assignment $a : W \to M$, we need to prove equation (4.6). We shall distinguish two cases: first we assume there exists an extension $a^* : \bar{W} \to M$ of the assignment a. Then using proposition (324) we obtain:

$$\begin{array}{rcl} \beta(\sigma(\phi))(a) & = & \beta(\,\mathcal{M} \circ \sigma(\phi)\,)(a^*) \\ \text{def. (44)} \;\to & = & \beta(\,\bar{\sigma} \circ \mathcal{M}(\phi)\,)(a^*) \\ \text{prop. (323), } \bar{\sigma} \text{ valid for } \mathcal{M}(\phi) \;\to & = & \beta(\mathcal{M}(\phi))(\,a^* \circ \bar{\sigma}\,) \\ \text{prop. (324)} \;\to & = & \beta(\phi)(\,(a^* \circ \bar{\sigma})_{|V}\,) \\ \bar{\sigma}_{|V} = \sigma,\; a^*_{|W} = a \;\to & = & \beta(\phi)(a \circ \sigma) \end{array}$$

We now assume that there exists no extension $a^* : \bar{W} \to M$. This can only be the case when $M = \emptyset$. Otherwise, pick an arbitrary $m^* \in M$ and define $a^*(n) = m^*$ for all $n \in \mathbf{N}$. Now if $M = \emptyset$, the only possible assignment $a : W \to M$ is the map with empty domain, i.e. $a = \emptyset$. It follows that $W = \emptyset$. However, since $\sigma : \mathbf{P}(V) \to \mathbf{P}(W)$ is an essential substitution, using theorem (18) of page 174 we see that $V = \emptyset = W$. From definition (35) the substitution congruence on $\mathbf{P}(V)$ is generated by the empty set and therefore coincides with the equality. Using proposition (125) it follows that $\sigma(\phi_1 \to \phi_2) = \sigma(\phi_1) \to \sigma(\phi_2)$ for all $\phi_1, \phi_2 \in \mathbf{P}(V)$, and $\sigma(\bot) = \bot$. A simple induction argument shows that $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$ coincides with the identity mapping, which is associated to the empty mapping $\sigma : V \to V$ as per definition (44) since $\mathcal{M} \circ \sigma = \bar{\emptyset} \circ \mathcal{M}$, as the minimal extension $\bar{\emptyset} : \bar{V} \to \bar{V}$ is simply the identity on $\mathbf{N}$. So $a \circ \sigma$ is the empty assignment and the equality (4.6) follows. **.**

4.2.5 The Soundness Theorem

In this section we prove the soundness theorem, which can be expressed as:

$$\vdash \phi \;\Rightarrow\; M \vDash \phi[a]$$

In other words, any provable formula ϕ is true in any model M under any assignment $a : V \to M$. If $\beta : \mathbf{P}(V) \to \mathcal{P}(M^V)$ denotes the model valuation function of M, the soundness theorem becomes $\vdash \phi \;\Rightarrow\; \beta(\phi)(a) = 1$. This is hugely important for us: we already know from definition (103) that $\beta(\bot)(a) = 0$ and $\beta(\phi_1 \to \phi_2)(a) = \beta(\phi_1)(a) \to \beta(\phi_2)(a)$. So the map $\beta(\,\cdot\,)(a) : \mathbf{P}(V) \to 2$ is a propositional valuation as per definition (56). Knowing furthermore that the implication $\vdash \phi \;\Rightarrow\; \beta(\phi)(a) = 1$ holds allows us to claim that $\beta(\,\cdot\,)(a)$ is in fact a valuation as per definition (96). So the dual space $\mathbf{P}^*(V)$ is not empty: take any set M together with a binary relation r, take any assignment $a : V \to M$ and you obtain a corresponding element $\beta(\,\cdot\,)(a)$ of the dual space $\mathbf{P}^*(V)$. This means our relation $\vDash$ of semantic entailment as per definition (98) is not trivial. It also means the sequent $\vdash \bot$ is false as otherwise the dual space

$\mathbf{P}^*(V)$ would clearly be empty. Our deductive system is therefore consistent which is an important validation. The soundness theorem will be quoted as theorem (37) of page 426 below. We start with a small lemma which establishes the truth of any axiom of first order logic under any model and assignment:

Lemma 31 *Let V be a set. Let M be a model of $\mathbf{P}(V)$ and $a : V \to M$ be an arbitrary variables assignment. Then for all $\phi \in \mathbf{A}(V)$ we have:*

$$M \vDash \phi[a]$$

i.e. an axiom of first order logic is true under any model and assignment.

Proof
Let $\beta : \mathbf{P}(V) \to \mathcal{P}(M^V)$ be the model valuation function associated with the model M. Given an assignment $a : V \to M$, we need to show that $\beta(\phi)(a) = 1$ for every $\phi \in \mathbf{A}(V)$. We shall consider the five possible cases of axioms individually. First we assume that ϕ is a simplification axiom. From definition (58), there exist $\phi_1, \phi_2 \in \mathbf{P}(V)$ such that $\phi = \phi_1 \to (\phi_2 \to \phi_1)$. We need to show that $\beta(\phi)(a) = 1$. However, defining $v_1 = \beta(\phi_1)(a)$ and $v_2 = \beta(\phi_2)(a)$:

$$\beta(\phi)(a) = v_1 \to (v_2 \to v_1)$$

where we have used definition (103). So suppose $\beta(\phi)(a) = 0$. Then $v_1 = 1$ while $v_2 \to v_1 = 0$. From this last equality we see that $v_2 = 1$ while $v_1 = 0$, which is a contradiction. So $\beta(\phi)(a) = 1$ is proved. We now assume that ϕ is a Frege axiom. From definition (59) there exist $\phi_1, \phi_2, \phi_3 \in \mathbf{P}(V)$ such that $\phi = [\phi_1 \to (\phi_2 \to \phi_3)] \to [(\phi_1 \to \phi_2) \to (\phi_1 \to \phi_3)]$. Defining $v_1 = \beta(\phi_1)(a)$, $v_2 = \beta(\phi_2)(a)$ and $v_3 = \beta(\phi_3)(a)$ we obtain from definition (103) :

$$\beta(\phi)(a) = [v_1 \to (v_2 \to v_3)] \to [(v_1 \to v_2) \to (v_1 \to v_3)]$$

We need to show that $\beta(\phi)(a) = 1$. So suppose to the contrary that $\beta(\phi)(a) = 0$. Then we have $v_1 \to (v_2 \to v_3) = 1$ while $(v_1 \to v_2) \to (v_1 \to v_3) = 0$. From this last equality we see that $v_1 \to v_2 = 1$ while $v_1 \to v_3 = 0$, which in turn implies that $v_1 = 1$ while $v_3 = 0$. However, from $v_1 = 1$ and $v_1 \to v_2 = 1$ we obtain $v_2 = 1$. So we have proved that $(v_1, v_2, v_3) = (1, 1, 0)$ and consequently:

$$v_1 \to (v_2 \to v_3) = 1 \to (1 \to 0) = 1 \to 0 = 0$$

which is a contradiction. So we now assume that ϕ is a transposition axiom. From definition (60) we have $\phi = [(\phi_1 \to \bot) \to \bot] \to \phi_1$ for some $\phi_1 \in \mathbf{P}(V)$. Defining $v_1 = \beta(\phi_1)(a)$ from definition (103) we obtain the equality:

$$\beta(\phi)(a) = [(v_1 \to 0) \to 0] \to v_1$$

We need to show that $\beta(\phi)(a) = 1$. So suppose to the contrary that $\beta(\phi)(a) = 0$. Then $(v_1 \to 0) \to 0 = 1$ while $v_1 = 0$. It follows that:

$$(v_1 \to 0) \to 0 = (0 \to 0) \to 0 = 1 \to 0 = 0$$

which is a contradiction. So we now assume that ϕ is a quantification axiom. From definition (61), there exist $\phi_1, \phi_2 \in \mathbf{P}(V)$ and $x \in V$ with $x \notin \mathrm{Fr}(\phi_1)$ and $\phi = \forall x(\phi_1 \to \phi_2) \to (\phi_1 \to \forall x\phi_2)$. Defining $v_1 = \beta(\phi_1)(a)$, $v_2 = \beta(\forall x\phi_2)(a)$ and $v_3 = \beta(\forall x(\phi_1 \to \phi_2))(a)$ we obtain the equality:

$$\beta(\phi)(a) = v_3 \to (v_1 \to v_2)$$

We need to show that $\beta(\phi)(a) = 1$. So suppose to the contrary that $\beta(\phi)(a) = 0$. Then we have $v_3 = 1$ while $v_1 \to v_2 = 0$ which in turn implies that $v_1 = 1$ while $v_2 = 0$. Using definition (103) we therefore obtain:

$$0 = v_2 = \beta(\forall x\phi_2)(a) = \min\{\beta(\phi_2)(b) \ : \ b = a \text{ on } V_x\}$$

Hence, we see that there exists an assignment $b^* : V \to M$ such that $b^* = a$ on $V \setminus \{x\}$ and $\beta(\phi_2)(b^*) = 0$. It follows that we have:

$$\begin{array}{rcl} v_3 & = & \beta(\forall x(\phi_1 \to \phi_2))(a) \\ & = & \min\{\beta(\phi_1 \to \phi_2)(b) \ : \ b = a \text{ on } V_x\} \\ & \leq & \beta(\phi_1 \to \phi_2)(b^*) \\ & = & \beta(\phi_1)(b^*) \to \beta(\phi_2)(b^*) \\ & = & \beta(\phi_1)(b^*) \to 0 \\ \text{A: to be proved } \to & = & \beta(\phi_1)(a) \to 0 \\ & = & v_1 \to 0 \\ & = & 1 \to 0 \\ & = & 0 \end{array}$$

which contradicts $v_3 = 1$. So it remains to show that $\beta(\phi_1)(b^*) = \beta(\phi_1)(a)$. Using proposition (322) it is sufficient to show that $b^* = a$ on $\mathrm{Fr}(\phi_1)$, which follows from $\mathrm{Fr}(\phi_1) \subseteq V \setminus \{x\}$, itself a consequence of the assumption $x \notin \mathrm{Fr}(\phi_1)$. So we now assume that ϕ is a specialization axiom. From definition (62) there exist $\phi_1 \in \mathbf{P}(V)$ and $x, y \in V$ such that $\phi = \forall x\phi_1 \to \phi_1[y/x]$ where $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ denotes an essential substitution of y in place of x, i.e. an essential substitution associated with the map $[y/x] : V \to V$. Defining $v_1 = \beta(\forall x\phi_1)(a)$ and $v_2 = \beta(\phi_1[y/x])(a)$ we obtain $\beta(\phi)(a) = v_1 \to v_2$ and we need to show that $\beta(\phi)(a) = 1$. So suppose to the contrary that $\beta(\phi)(a) = 0$. Then we have $v_1 = 1$ while $v_2 = 0$ and consequently we obtain:

$$\begin{array}{rcl} v_1 & = & \beta(\forall x\phi_1)(a) \\ & = & \min\{\beta(\phi_1)(b) \ : \ b = a \text{ on } V_x\} \\ a \circ [y/x] = a \text{ on } V_x \ \to & \leq & \beta(\phi_1)(\, a \circ [y/x]\,) \\ \text{theorem (36), p. 422} \ \to & = & \beta(\,[y/x](\phi_1)\,)(a) \\ & = & \beta(\phi_1[y/x])(a) \\ & = & v_2 \\ & = & 0 \end{array}$$

which contradicts the equality $v_1 = 1$ and completes our proof. .

The proof of the soundness theorem which follows relies on a structural induction argument based on our free universal algebra of proofs $\mathbf{\Pi}(V)$.

Theorem 37 (Soundness) *Let V be a set and M be a model of $\mathbf{P}(V)$. Then for every assignment $a : V \to M$ and any formula $\phi \in \mathbf{P}(V)$ we have:*

$$\vdash \phi \;\Rightarrow\; M \vDash \phi[a]$$

In other words, a provable formula is true under any model and assignment.

Proof
Let $\beta : \mathbf{P}(V) \to \mathcal{P}(M^V)$ denote the model valuation function of the model M. Given a provable formula $\phi \in \mathbf{P}(V)$ we need to show that $\beta(\phi)(a) = 1$ for every assignment $a : V \to M$. It is therefore sufficient to prove that for every proof $\pi \in \mathbf{\Pi}(V)$ and every assignment $a : V \to M$, we have the implication:

$$\mathrm{Hyp}(\pi) = \emptyset \;\Rightarrow\; \beta(\mathrm{Val}(\pi))(a) = 1 \tag{4.7}$$

Indeed, suppose this property has been established and let $\phi \in \mathbf{P}(V)$ be such that $\vdash \phi$. Then there exists a proof $\pi \in \mathbf{\Pi}(V)$ such that $\mathrm{Val}(\pi) = \phi$ and $\mathrm{Hyp}(\pi) = \emptyset$. Using (4.7) we obtain $\beta(\phi)(a) = 1$ for all $a : V \to M$. So we shall now prove that (4.7) is true for every assignment and every proof $\pi \in \mathbf{\Pi}(V)$. We shall do so by structural induction, using theorem (3) of page 31. First we assume that $\pi = \phi$ for some $\phi \in \mathbf{P}(V)$. Then $\mathrm{Hyp}(\pi) = \{\phi\} \neq \emptyset$ and (4.7) is vacuously true. Next we assume that $\pi = \partial\phi$ for some $\phi \in \mathbf{P}(V)$. We shall distinguish two cases: first we assume that $\phi \notin \mathbf{A}(V)$. Then $\mathrm{Hyp}(\pi) = \emptyset$ and $\mathrm{Val}(\pi) = \bot \to \bot$. So we need to show that $\beta(\bot \to \bot)(a) = 1$ for every assignment, which follows immediately from definition (103). Next we assume that $\phi \in \mathbf{A}(V)$. Then $\mathrm{Hyp}(\pi) = \emptyset$ and $\mathrm{Val}(\pi) = \phi$. So we need to show that $\beta(\phi)(a) = 1$ for every assignment, which follows immediately from lemma (31). So we now assume that $\pi = \pi_1 \oplus \pi_2$ where $\pi_1, \pi_2 \in \mathbf{\Pi}(V)$ are such that (4.7) is true for every assignment. We need to show the same is true of π. So let $a : V \to M$ be an assignment and suppose $\mathrm{Hyp}(\pi) = \emptyset$. We need to show that $\beta(\mathrm{Val}(\pi))(a) = 1$. We shall distinguish two cases: first we assume that $\mathrm{Val}(\pi_2)$ cannot be expressed as $\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \to \phi$ for any $\phi \in \mathbf{P}(V)$. Then we have $\mathrm{Val}(\pi) = M(\mathrm{Val}(\pi_1), \mathrm{Val}(\pi_2)) = \bot \to \bot$ where $M : \mathbf{P}(V)^2 \to \mathbf{P}(V)$ is the modus ponens mapping of definition (68). Hence we have:

$$\begin{aligned}
\beta(\mathrm{Val}(\pi))(a) &= \beta(\bot \to \bot)(a) \\
&= \beta(\bot)(a) \to \beta(\bot)(a) \\
&= 0 \to 0 \\
&= 1
\end{aligned}$$

So we now assume that $\mathrm{Val}(\pi_2) = \mathrm{Val}(\pi_1) \to \phi$ for some $\phi \in \mathbf{P}(V)$. In this case we have $\mathrm{Val}(\pi) = M(\mathrm{Val}(\pi_1), \mathrm{Val}(\pi_2)) = \phi$ and we need to show that $\beta(\phi)(a) = 1$. However, from $\emptyset = \mathrm{Hyp}(\pi) = \mathrm{Hyp}(\pi_1) \cup \mathrm{Hyp}(\pi_2)$ we see that both

$\mathrm{Hyp}(\pi_1)$ and $\mathrm{Hyp}(\pi_2)$ are the empty set. Having assumed the implication (4.7) is true for π_1 and π_2 it follows that $\beta(\mathrm{Val}(\pi_1))(a) = 1$ and furthermore:

$$\begin{aligned} 1 &= \beta(\mathrm{Val}(\pi_2))(a) \\ &= \beta(\,\mathrm{Val}(\pi_1) \to \phi\,)(a) \\ &= \beta(\mathrm{Val}(\pi_1))(a) \to \beta(\phi)(a) \\ &= 1 \to \beta(\phi)(a) \end{aligned}$$

So we conclude that $\beta(\phi)(a) = 1$ as requested. We now assume that $\pi = \nabla x \pi_1$ where $x \in V$ and $\pi_1 \in \mathbf{\Pi}(V)$ is such that (4.7) is true for every assignment. We need to show the same if true of π. So let $a : V \to M$ be an assignment and suppose $\mathrm{Hyp}(\pi) = \emptyset$. We need to show that $\beta(\mathrm{Val}(\pi))(a) = 1$. Since we have $\mathrm{Hyp}(\pi_1) = \mathrm{Hyp}(\pi) = \emptyset$ we see that $x \notin \mathrm{Fr}(\pi_1)$. So $\mathrm{Val}(\pi) = \forall x \phi_1$ with $\phi_1 = \mathrm{Val}(\pi_1)$ and we need to show that $\beta(\forall x \phi_1)(a) = 1$. However from $\mathrm{Hyp}(\pi_1) = \emptyset$, having assumed the implication (4.7) is true for π_1 and every assignment, we have $\beta(\phi_1)(b) = 1$ for every assignment $b : V \to M$. It follows that $\beta(\forall x \phi_1)(a) = \min\{\beta(\phi_1)(b) : b = a \text{ on } V_x\} = 1$ as requested. **.**

Theorem 38 *Let V be a set and M be a model of $\mathbf{P}(V)$ with model valuation function β. For every $a : V \to M$ the map $\beta(\,.\,)(a) : \mathbf{P}(V) \to 2$ is a valuation.*

Proof
Let $a : V \to M$ be an assignment and define $v_a : \mathbf{P}(V) \to 2$ by setting $v_a(\phi) = \beta(\phi)(a)$. We need to show that v_a is a valuation. The fact that $v_a(\bot) = 0$ and $v_a(\phi_1 \to \phi_2) = v_a(\phi_1) \to v_a(\phi_2)$ for all $\phi_1, \phi_2 \in \mathbf{P}(V)$ follows immediately from definition (103). Furthermore, the implication $\vdash \phi \;\Rightarrow\; v_a(\phi) = 1$ follows from theorem (37). By virtue of definition (96), v_a is a valuation. **.**

4.2.6 Regular Valuation

We want to prove Gödel's completeness theorem. Our strategy to do so will be to show that *every valuation has a model*, namely that for all $v : \mathbf{P}(V) \to 2$ element of the dual space $\mathbf{P}^*(V)$ of definition (96), there exists a model (M, r) together with an assignment $a : V \to M$ such that $v = \beta(\,\cdot\,)(a)$, where β denotes the associated model valuation function of definition (103). This strategy is clearly sufficient: Gödel's completeness theorem is usually known as the statement that a valid formula must be provable. However, the word *valid* is usually understood as *being true under every model and assignment* which does not correspond to definition (98) where we defined a *valid* formula in terms of valuations and not models. So for us Gödel's completeness theorem is the statement that if a formula is true under any model and assignment, then it must be provable. Now suppose we have proved that every valuation has a model. Then if $\phi \in \mathbf{P}(V)$ is a formula which is true under any model and assignment, then it is also true under any valuation. Indeed, let $v \in \mathbf{P}^*(V)$. Then v has a model, i.e. $v = \beta(\,\cdot\,)(a)$ for some model (M, r) and assignment $a : V \to M$. By assumption we have

$M \vDash \phi[a]$ which is $\beta(\phi)(a) = 1$ and consequently $v(\phi) = 1$, i.e. $v \vDash \phi$. Having proved that ϕ is true under any valuation, we conclude from theorem (33) of page 406 that ϕ is provable, and Gödel's completeness theorem is true.

In this section, we shall study the notion of *regular valuation* which will allow us to follow the spirit of Leon Henkin's proof of Gödel's completeness theorem, by considering maximal consistent sets in which every existential statement has a *Henkin witness*. A regular valuation $v : \mathbf{P}(V) \to 2$ is a valuation for which:

$$v(\forall x \phi_1) = \min \{v(\phi_1[y/x]) \ : \ y \in V\} \tag{4.8}$$

Since $\phi = \forall x \phi_1 \to \phi_1[y/x]$ is an axiom of first order logic, it is a provable formula and consequently $v(\phi) = 1$ which is $v(\forall x \phi_1) \leq v(\phi_1[y/x])$ for all $v \in \mathbf{P}^*(V)$. So the interpretation of equation (4.8) can be thought of as follows: whenever a valuation v is regular, if a statement $\forall x \phi_1$ is false then there must exist some $y \in V$ for which the statement $\phi_1[y/x]$ is also false. We already know from proposition (319) that a valuation can be identified with a maximal consistent set. We are also familiar with the duality $\forall x \leftrightarrow \neg \exists x \neg$. Hence another way to think of equation (4.8) is as follows: whenever a maximal consistent set is regular, if it contains a statement $\exists x \phi_1$ then it must also contain $\phi_1[y/x]$ for some $y \in V$. In other words, every true statement $\exists x \phi_1$ has a *Henkin witness*.

One interesting point to note is that equation (4.8) is in general very hard to write with full mathematical rigor, since the substitution $[y/x]$ is usually not valid for ϕ_1. Fortunately for us, the notation $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ refers to an essential substitution of y in place of x, which eliminates the issue altogether.

Definition 106 *Let V be a set and $v : \mathbf{P}(V) \to 2$ be a valuation on $\mathbf{P}(V)$. we say that v is* regular*, if and only if for all $\phi_1 \in \mathbf{P}(V)$ and $x \in V$ we have:*

$$v(\forall x \phi_1) = \min \{v(\phi_1[y/x]) \ : \ y \in V\}$$

where $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ denotes an essential substitution of y in place of x.

Regular valuations have the very appealing property of being induced by their *naive model*. In other words, if $v : \mathbf{P}(V) \to 2$ is a regular valuation then $v = \beta(\,\cdot\,)(i)$ where β is the model valuation function associated with the naive model of v and $i : V \to V$ is the identity assignment. The *naive model* of v is simply the model (M, r) where $M = V$ and $r = \{(x, y) \in V \times V \ : \ v(x \in y) = 1\}$.

Definition 107 *Let V be a set and $v : \mathbf{P}(V) \to 2$ be a valuation on $\mathbf{P}(V)$. We call* naive model *of v the ordered pair (M, r) defined by $M = V$ and:*

$$r = \{(x, y) \in V \times V \ : \ v(x \in y) = 1\}$$

In fact the converse is also true: if a valuation is induced by its naive model then it is regular, as we shall now see from the following theorem:

Theorem 39 *Let V be a set and $v \in \mathbf{P}^*(V)$. Then v is regular, if and only if it is induced by its naive model and the identity assignment $i : V \to V$, i.e. :*

$$\forall \phi \in \mathbf{P}(V) \ , \ v(\phi) = \beta(\phi)(i)$$

where β is the model valuation function associated with the naive model of v.

Proof
First we show the 'if' part: so we assume that $v : \mathbf{P}(V) \to 2$ is a valuation such that $v(\phi) = \beta(\phi)(i)$ for all $\phi \in \mathbf{P}(V)$, where β is the model valuation function associated with the naive model of v, and $i : V \to V$ is the identity. We need to show that v is regular. So let $\phi_1 \in \mathbf{P}(V)$ and $x \in V$. We have:

$$\begin{array}{rcl} v(\forall x \phi_1) & = & \beta(\forall x \phi_1)(i) \\ & = & \min\{\beta(\phi_1)(b) \ : \ b = i \text{ on } V_x\} \\ \text{A: to be proved } \to & = & \min\{\beta(\phi_1)([y/x]) \ : \ y \in V\} \\ & = & \min\{\beta(\phi_1)(\, i \circ [y/x]\,) \ : \ y \in V\} \\ \text{B: to be proved } \to & = & \min\{\beta(\,[y/x](\phi_1)\,)(i) \ : \ y \in V\} \\ & = & \min\{\beta(\phi_1[y/x])(i) \ : \ y \in V\} \\ & = & \min\{v(\phi_1[y/x]) \ : \ y \in V\} \end{array}$$

So it remains to justify points A and B. For point A, we need to show:

$$X = \{b : V \to V \ : \ b = i \text{ on } V_x\} = \{[y/x] : V \to V \ , \ y \in V\} = Y$$

First we show that $X \subseteq Y$: so suppose $b = i$ on $V \setminus \{x\}$. Define $y = b(x)$. In order to show that $b \in Y$ it is sufficient to prove that $b = [y/x]$. So suppose $u \in V$. If $u = x$, then $b(x) = [y/x](x)$ follows from our definition of y. If $u \neq x$ then we have $b(u) = i(u) = u = [y/x](u)$. So we now prove that $Y \subseteq X$: so let $b = [y/x]$ for some $y \in V$. Then it is clear that $b = i$ on $V \setminus \{x\}$. It remains to justify point B, which is an immediate consequence of theorem (36) of page 422 provided the map $[y/x] : \mathbf{P}(V) \to \mathbf{P}(V)$ is understood to be an arbitrary essential substitution associated with the map $[y/x] : V \to V$. Note that such an essential substitution always exists by virtue of theorem (18) of page 174. We now show the 'only if' part: so we assume that $v : \mathbf{P}(V) \to 2$ is a valuation which is regular. We need to show that $\beta(\phi)(i) = v(\phi)$ for all $\phi \in \mathbf{P}(V)$, where β is the model valuation function of the naive model of v and $i : V \to V$ is the identity. We shall prove the seemingly stronger result that $\beta(\phi)(\sigma) = v(\sigma(\phi))$ for all essential substitutions $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$. We shall do so by structural induction, using theorem (3) of page 31. Note that from proposition (116) the identity $i : \mathbf{P}(V) \to \mathbf{P}(V)$ being injective, is an essential substitution associated with the identity $i : V \to V$. So what we set out to prove is indeed sufficient. First we assume that $\phi = (x \in y)$ for some $x, y \in V$. Let $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$ be an arbitrary essential substitution:

$$\begin{array}{rcl} \beta(\phi)(\sigma) & = & \beta(x \in y)(\sigma) \\ & = & 1_r(\sigma(x), \sigma(y)) \\ \text{def. (106)} \ \to & = & v(\sigma(x) \in \sigma(y)) \\ \text{prop. (125)} \ \to & = & v(\sigma(\phi)) \end{array}$$

Next we assume that $\phi = \bot$. We have $\beta(\bot)(\sigma) = 0 = v(\bot) = v(\sigma(\bot))$, where $\bot = \sigma(\bot)$ follows from proposition (125). So we now assume that $\phi = \phi_1 \to \phi_2$ where $\phi_1, \phi_2 \in \mathbf{P}(V)$ satisfy our equality for any $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$ essential:

$$\begin{aligned}
\beta(\phi)(\sigma) &= \beta(\phi_1 \to \phi_2)(\sigma) \\
&= \beta(\phi_1)(\sigma) \to \beta(\phi_2)(\sigma) \\
&= v(\sigma(\phi_1)) \to v(\sigma(\phi_2)) \\
&= v(\,\sigma(\phi_1) \to \sigma(\phi_2)\,) \\
\text{A: to be proved } \to &= v(\sigma(\phi))
\end{aligned}$$

It remains to show that $v(\,\sigma(\phi_1) \to \sigma(\phi_2)\,) = v(\sigma(\phi))$. From proposition (125) we have $\sigma(\phi) \sim \sigma(\phi_1) \to \sigma(\phi_2)$ where $\sim$ is the substitution congruence. So our desired equality follows from proposition (309). We now assume that $\phi = \forall x \phi_1$ where $\phi_1 \in \mathbf{P}(V)$ satisfies our equality for all $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$ essential. We need to show the same is true of ϕ. So let $\sigma : \mathbf{P}(V) \to \mathbf{P}(V)$ be an essential substitution. Using proposition (126), let $\tau : \mathbf{P}(V) \to \mathbf{P}(V)$ be an essential substitution such that $\tau = \sigma$ on $V \setminus \{x\}$, and $\tau(x) \notin \mathrm{Fr}(\sigma(\phi))$. Note that we have the substitution equivalence $\sigma(\phi) \sim \forall \tau(x) \tau(\phi_1)$ and consequently:

$$\begin{aligned}
\beta(\phi)(\sigma) &= \beta(\forall x \phi_1)(\sigma) \\
&= \min\{\beta(\phi_1)(b) \;:\; b = \sigma \text{ on } V_x\} \\
\tau = \sigma \text{ on } V_x \;\to &= \min\{\beta(\phi_1)(b) \;:\; b = \tau \text{ on } V_x\} \\
\text{A: to be proved } \to &= \min\{\beta(\phi_1)(\,[y/\tau(x)] \circ \tau\,) \;:\; y \in V\} \\
\text{B: to be proved } \to &= \min\{v(\,[y/\tau(x)] \circ \tau(\phi_1)\,) \;:\; y \in V\} \\
&= \min\{v(\,\tau(\phi_1)[y/\tau(x)]\,) \;:\; y \in V\} \\
v \text{ is regular } \to &= v(\,\forall \tau(x) \tau(\phi_1)\,) \\
\text{prop. (309)} \to &= v(\sigma(\phi))
\end{aligned}$$

So it remains to prove points A and B. First we start with point B: we need to show the equality $\beta(\phi_1)(\,[y/\tau(x)] \circ \tau\,) = v(\,[y/\tau(x)] \circ \tau(\phi_1)\,)$ which is in fact simply our induction hypothesis, provided $[y/\tau(x)] \circ \tau : \mathbf{P}(V) \to \mathbf{P}(V)$ is an essential substitution. However, we already know that $\tau : \mathbf{P}(V) \to \mathbf{P}(V)$ is essential, and from theorem (18) of page 174 we can choose $[y/\tau(x)] : \mathbf{P}(V) \to \mathbf{P}(V)$ to be an essential map associated with $[y/\tau(x)] : V \to V$. From proposition (119), the composition $[y/\tau(x)] \circ \tau : \mathbf{P}(V) \to \mathbf{P}(V)$ is indeed an essential substitution, associated with $[y/\tau(x)] \circ \tau : V \to V$. So it remains to prove A, which is:

$$X = \{\beta(\phi_1)(b) \;:\; b = \tau \text{ on } V_x\} = \{\beta(\phi_1)(\,[y/\tau(x)] \circ \tau\,) \;:\; y \in V\} = Y$$

First we show that $X \subseteq Y$: so let $\epsilon \in X$. There exists an assignment $b : V \to V$ such that $b = \tau$ on $V \setminus \{x\}$ and $\epsilon = \beta(\phi_1)(b)$. We need to show that $\epsilon \in Y$. Let $y = b(x)$. In order to show that $\epsilon \in Y$, it is sufficient to show that $\epsilon = \beta(\phi_1)(\,[y/\tau(x)] \circ \tau\,)$. So we need to show $\beta(\phi_1)(b) = \beta(\phi_1)(\,[y/\tau(x)] \circ \tau\,)$.

Using proposition (322), it is sufficient to prove that b and $[y/\tau(x)] \circ \tau$ coincide on $\mathrm{Fr}(\phi_1)$. So let $u \in \mathrm{Fr}(\phi_1)$. We need to show that $b(u) = [y/\tau(x)] \circ \tau(u)$. We shall distinguish two cases: first we assume that $u = x$. Then we need to show that $b(x) = y$ which is true by definition of y. Next we assume that $u \neq x$. Then $u \in \mathrm{Fr}(\phi_1) \setminus \{x\} = \mathrm{Fr}(\phi)$. From proposition (120) we have $\mathrm{Fr}(\sigma(\phi)) = \sigma(\mathrm{Fr}(\phi))$. It follows that $\sigma(u) \in \mathrm{Fr}(\sigma(\phi))$. Furthermore, since $\tau = \sigma$ on $V \setminus \{x\}$ we have $\tau(u) = \sigma(u)$. So we see that $\tau(u) \in \mathrm{Fr}(\sigma(\phi))$. Having assumed that $\tau(x) \notin \mathrm{Fr}(\sigma(\phi))$ it follows that $\tau(u) \neq \tau(x)$. Hence, we see that $[y/\tau(x)] \circ \tau(u) = \tau(u)$, and the equality $b(u) = [y/\tau(x)] \circ \tau(u)$ follows from the fact that $b = \tau$ on $V \setminus \{x\}$. So we now prove that $Y \subseteq X$: let $\epsilon \in Y$. There exists $y \in V$ such that $\epsilon = \beta(\phi_1)(\,[y/\tau(x)] \circ \tau\,)$. We need to show that $\epsilon \in X$. Define the assignment $b : V \to V$ by setting $b = \tau$ on $V \setminus \{x\}$ and $b(x) = y$. In order to show that $\epsilon \in X$, it is sufficient to prove that $\epsilon = \beta(\phi_1)(b)$. So we need to show that $\beta(\phi_1)(b) = \beta(\phi_1)(\,[y/\tau(x)] \circ \tau\,)$. Using proposition (322), it is sufficient to prove that b and $[y/\tau(x)] \circ \tau$ coincide on $\mathrm{Fr}(\phi_1)$. So let $u \in \mathrm{Fr}(\phi_1)$. We need to show that $b(u) = [y/\tau(x)] \circ \tau(u)$. We shall distinguish two cases: first we assume that $u = x$. Then we need to show that $b(x) = y$ which is true by definition of b. Next we assume that $u \neq x$. Then using an identical argument as previously we obtain $\tau(u) \neq \tau(x)$ and we therefore need to show that $b(u) = \tau(u)$ which is true by definition of b. .

Bibliography

[1] Hajnal Andréka, István Németi, Ildikó Sain, (2013). Universal Algebraic Logic. Studies in Universal Logic

[2] H. Andréka, I. Németi, L. Henkin, J.D. Monk, A. Tarski (1981). Cylindric Set Algebras. Lecture Notes in Mathematics. Springer.

[3] Sanjeev Arora, Boaz Barak, (2009). Computational Complexity. Cambridge University Press.

[4] Donald W. Barnes, John M. Mack, (1975). An Algebraic Introduction to Mathematical Logic. Graduate texts in mathematics. Springer.

[5] John L. Bell, (2005). Set Theory. Oxford Logic Guides.

[6] Blok W.J., Pigozzi D., (1989), Algebraizable Logics, Memoirs of the American Mathematical Society, Vol. 77, No. 396
`http://orion.math.iastate.edu/dpigozzi/papers/aaldedth.pdf`

[7] George S. Boolos, John P. Burgess, Richard C. Jeffrey, (1974). Computability and Logic. Cambridge University Press.

[8] Egon Börger, Erich Grädel, Yuri Gurevich, (2001). The Classical Decision Problem. Universitext. Springer.

[9] Stanley Burris, H.P. Sankappanavar, (1980). A Course in Universal Alegbra. Springer.

[10] C.C. Chang, (1973). Model Theory. Studies in Logic and the Foundations of Mathematics. Vol 73.

[11] Cirulis J., (1988). An Algebraization of First-Order Logic With Terms, in Algebraic Logic (Proc. Conf. Budapest 1988), H. Andreka, J.D. Monk and I. Nemeti, Eds., Colloq. Math. Soc. J. Bolyai, North-Holland, Amsterdam 1991, pp. 125-146

[12] S. Barry Cooper, (2004). Computability Theory. Chapman & Hall.

[13] René Cori, Daniel Lascar, Donald Pelletier, (2000). Mathematical Logic, Part 1. Oxford Universty Press.

[14] René Cori, Daniel Lascar, Donald Pelletier, (2000). Mathematical Logic, Part 2. Oxford Universty Press.

[15] Nigel Cutland, (1980). Computability. Cambridge University Press.

[16] Gilles Dowek, (2011). Les Démonstrations et les Algorithmes. Introduction à la Logique et à la Calculabilité. Editions de l'Ecole Polytechnique.

[17] H.D. Ebbinghaus, J. Flum, W. Thomas, (1994). Mathematical Logic. Springer.

[18] Miklós Ferenczi, Miklós Szőts, (2011). Mathematical Logic for Applications. `http://tankonyvtar.ttk.bme.hu/pdf/22.pdf`

[19] Henrik Forssell, (2008). First-Order Logical Duality. PhD dissertation. `http://www.andrew.cmu.edu/user/awodey/students/forssell.pdf`

[20] Thomas Forster, (2003). Logic, Induction and Sets. London Mathematical Society Student Texts.

[21] Murdoch J. Gabbay, (2011). Stone Duality for first-order logic: a nominal approach to logic and topology. Howard Barringer Festschrift. `http://www.gabbay.org.uk/papers/stodfo.pdf`

[22] Murdoch J. Gabbay, (2009). A study of substitution, using nominal techniques and Fraenkel-Mostowski sets. Theoretical Computer Science, Volume 410, Issues 12-13, 17 March 2009, Pages 1159-1189. `http://www.gabbay.org.uk/papers/stusun.pdf`

[23] Murdoch J. Gabbay and Aad Mathijssen, (2008). Capture-avoiding Substitution as a Nominal Algebra. Formal Aspects of Computing, Volume 20, Numbers 4-5, July, 2008, Pages 451-479. `http://www.gabbay.org.uk/papers/capasn-jv.pdf`

[24] Jean H. Gallier, (1987). Logic for Computer Science. John Wiley & Sons.

[25] Mohan Ganesalingam, (2013). The Language of Mathematics. Springer.

[26] Jean-Yves Girard, (2006). Le Point Aveugle I. Cours de Logique. Hermann.

[27] Jean-Yves Girard, (2007). Le Point Aveugle II. Cours de Logique. Hermann.

[28] Paul R. Halmos, (1962). Algebraic Logic. Chelsea Publishing Company New York.

[29] Wilfrid Hodges, (1993). Model Theory. Cambridge University Press.

[30] Marc Hoyois, (2012). The Syntax of First Order Logic. Preprint. `http://math.northwestern.edu/~hoyois/papers/logic.pdf`

[31] Thomas Jech, (2003). Set Theory (3rd ed.). Springer.

[32] P.T. Johnstone, (1987). Notes on Logic and Set Theory. Cambridge Mathematical Textbooks. Cambridge University Press.

[33] P.T. Johnstone, (1986). Stone Spaces. Cambridge Studies in Advanced Mathematics.

[34] Akihiro Kanamori, (2009). The Higher Infinite (2nd ed.). Springer.

[35] Richard Kaye, (2007). The Mathematics of Logic. Cambridge University Press.

[36] Stephen Cole Kleene (2009). Introduction to Metamathematics. Ishi Press International.

[37] Ulrich Kohlenbach, (2008). Applied Proof Theory: Proof Interpretations and their Use in Mathematics. Springer.

[38] Jean-Louis Krivine, (2007). Théorie des Ensembles (2nd ed.). Nouvelle Bibliothèque Mathématique.

[39] Kenneth Kunen, (2009). The Foundations of Mathematics. Studies in Logic. Mathematical Logic and Foundations. Vol 19. College Publications.

[40] Kenneth Kunen, (2011). Set Theory. Studies in Logic. Mathematical Logic and Foundations. Vol 34. College Publications.

[41] David Marker, (2010). Model Theory: An Introduction. Graduate Texts in Mathematics. Springer.

[42] J.P. Mayberry (2012). First Order Logic via the Theory of Functional Forms. `http://www.bristol.ac.uk/philosophy/department/staff/jpm/logicalt.pdf`

[43] Elliott Mendelson (2009). Introduction to Mathematical Logic. CRC Press

[44] J. Donald Monk, (1976). Mathematical Logic. Springer.

[45] Norman Megill, Metamath, `http://www.metamath.org/`

[46] PlanetMath, (2012). Deduction theorem holds for first order logic. `http://planetmath.org/DeductionTheoremHoldsForFirstOrderLogic.html`

[47] Wolfram Pohlers, (2009). Proof Theory. Universitext. Springer.

[48] Bruno Poizat, (2000). A Course in Model Theory. Universitext. Springer.

[49] Wolfgang Rautenberg, (2006). A Concise Introduction to Mathematical Logic. Universitext. Springer.

[50] Umberto Rivieccio, (2012). What is Abstract Algebraic Logic? Preprint. `http://www.cs.bham.ac.uk/~rivieccu/pub/wha.pdf`

[51] Walter Rudin, (1987). Real and Complex Analysis, 3rd ed. McGraw-Hill.

[52] Ildikó Sain, (2000). On the Search for a Finitizable Algebraization of First Order Logic. Logic Journal of the IGPL 8(4):497-591.
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.23.2238

[53] Jacob T. Schwartz, Domenico Cantone, Eugenio G. Omodeo, (2011). Computational Logic and Set Theory. Springer.

[54] Stephen G. Simpson, (2009). Subsystems of Second Order Arithmetic. Perspective in Logic. Cambridge University Press.

[55] Arindama Singh, (2012). Mathematical Logic. Online Course. IIT Madras.
http://nptel.iitm.ac.in/courses/111106052/

[56] Peter Smith, (2007). An Introduction to Gödel's Theorems. Cambridge University Press.

[57] Peter Smith, (2003). Formal Logic. Cambridge University Press.

[58] Raymond M. Smullyan, Melvin Fitting, (1996). Set Theory and the Continuum Problem. Dover Publications, Inc.

[59] S.M. Srivastava, (2008). A course on mathematical logic. Springer.

[60] G. Takeuti, (1975). Proof Theory. Dover Publications, Inc.

[61] G. Takeuti, W.M. Zaring, (1973). Introduction to Axiomatic Set Theory. Springer.

[62] George Tourlakis, (2003). Lectures in Logic and Set Theory. Volume 1. Cambridge University Press.

[63] Dirk Van Dalen, (2004). Logic and Structure. Universitext. Springer.

[64] George Voutsadakis, (2004). On the Categorical Algebras of First Order Logic. Scientiae Mathematicae Japonicae Online, Vol. 10, 4754
http://www.voutsadakis.com/RESEARCH/PUBLISHED/cylindric.pdf