Notes on Induction, Algebras and Fixed Points

Wesleyan University

Fall 2014

1 The induction schemes

We begin by reviewing the principle of mathematical induction in various forms. We first consider induction on the natural numbers. We will need to discuss *properties* $P(x)$ of natural numbers x. For example

$$P(x) \stackrel{\text{def}}{\equiv} \quad x \text{ is prime}\,.$$

For the time being we will not make precise what we mean by a property. Once we introduce formal logic, a property will be a formula in predicate logic. Properties of natural numbers are closely related to sets[1] of natural numbers: if S is a subset of $\mathbb{N}$ say the set of prime numbers, then a statement of membership in S

$$x \in S$$

is a way of saying "x is prime." The set of numbers with property P is written

$$\{x \in \mathbb{N} | P(x)\}.$$

Definition 1 *Let P be a property of natural numbers. Then the following formula is called the* **induction axiom** *for P*

$$Ind_P: \quad [\ \underbrace{P(0)}_{\text{if 0 has property } P} \quad \underbrace{\&}_{\text{and}} \quad \underbrace{\forall x}_{\text{for every } x} \quad \underbrace{(\underbrace{P(x) \to P(x+1)}_{P(x) \text{ implies } P(x+1)})}_{\ } \ ] \underbrace{\to}_{\text{then}} \quad \underbrace{\forall x P(x).}_{P \text{ holds for every } x.}$$

Expressed informally, the axiom says: **if** we establish that

- $P(0)$ is true, and
- whenever $P(x)$ is true then $P(x+1)$ is true.

then we have shown that $P(x)$ **holds for every natural number x.** We distinguish between the induction **axiom** Ind_P and the induction **scheme** (Ind) which is the (infinite) set of axioms Ind_P, one for every property P.

Now we look at alternative formulations of induction that will prove useful.

[1] which brings up the question of whether every set of numbers is in fact given by a property expressed as a formula. One needs to nail down just what a property is and just what a set is. But, in general, the answer is no. There are many more subsets of $\mathbb{N}$ than there are definable ones. More on this later.

Definition 2 *We define so-called* **course-of-values** *induction for the property P to be the axiom*

$$COV_P: \qquad \forall x[(\forall y < x P(y)) \to P(x)] \ \to \ \forall x P(x) \tag{1}$$

i.e. if we can show that P is a property satisfying the condition:

whenever it holds for every $y < x$ it must also hold for x

then P is true of all x.

Note that it is not necessary to establish $P(0)$ since this actually follows from the definition[2].

Definition 3 *Let P be a property of natural numbers. The* **least number principle** *for P is the axiom: if there is any number x for which P holds then there is a smallest one. Written in the rather dry style of first-order logic:*

$$LN_P \quad \exists x(P(x)) \to \exists x[P(x) \,\&\, \forall y(P(y) \to x \leq y)]. \tag{2}$$

Equivalently, LN_P says: every nonempty subset of $\mathbb{N}$ has a least element.

As with Ind we can also define the COV- **scheme** to be the collection of axioms COV_P for every P and the LN-**scheme** to be the set of axioms LN_P.

Theorem 4 *The following are equivalent* **as schemes**, *by which we mean if all P-instances of any one of them is true than all P-instances of the others are:*

1. *Ind*
2. *COV*
3. *LN*

proof: Exercise! □

.

We can generalize the least number principle to a condition on any strict order (of any size) so as to guarantee that a suitable rephrasing of the COV scheme will continue to hold.

Definition 5 *A strict order $\mathcal{A} = \langle A, <_A \rangle$ is said to be* **well-founded** *if every nonempty subset S of A has an $<_A$-minimal element, that is to say, there is an element $a \in S$ such that for no other $x \in S$ do we have $x <_A a$.*

Theorem 6 (transfinite induction) *Let $\langle A, <_A \rangle$ be a well-founded strict order. Then for any property P*

$$(\forall x \in A)[(\forall y <_A x P(y)) \ \to \ P(x)] \ \to \ (\forall x \in A)\, P(x)$$

proof: Exercise. □

[2]Does it really? Well since there is no y smaller than 0, $y < 0$ is always false, so $\forall y < 0 P(y)$ is said to be *vacuously true* according to conventional logical formalisms. Thus, since we have assumed $\forall x[(\forall y < x P(y)) \to P(x)]$, substituting 0 for x yields $P(0)$.

.

Problem 1 *A* **relation** R *on a set* A *is said to be* **well-founded** *if every nonempty subset* S *of* A *has an* R*-minimal member. Show that this condition is equivalent to saying that* A *has no infinite descending* R*-chain, i.e. for any countable sequence* $a_1, \ldots, a_n, \ldots$, *the assumption*

$$a_2 R a_1 \ \text{ and } \ a_3 R a_2 \ \text{ and } \ \cdots$$

leads to a contradiction.

2 Inductively defined structures and term algebras.

We define a **signature** Σ to be a triple

$$\Sigma = \langle \mathcal{K}_\Sigma, \mathcal{F}_\Sigma, \alpha \rangle$$

consisting of sequences[3] of constant symbols $\mathcal{K}_\Sigma = \langle c_1, c_2, \cdots \rangle$ and of function symbols $\mathcal{F}_\Sigma = \langle f_1, f_2, \cdots \rangle$ each of which has an associated natural number $\alpha(c), \alpha(f)$ called its *arity*. Arities are often not displayed, but when we want to do so we will use exponent-notation, as in $\langle a^0, b^0, c^1, f^3, g^4 \rangle$, where arity 0 identifies constant symbols[4] A signature often captures the essential algebraic structure of some area of mathematics under study, e.g. for arithmetic, $\Sigma = \langle 0, 1, +^2, \times^2 \rangle$. In logic programming, signatures are created by the user through the text of the logic program. In other programming languages, user defined data constructors play a similar role.

In this course we will usually only consider finite or countably infinite signatures. This is tacitly assumed in all relevant theorems unless otherwise stated.

Definition 7 *Let* $\Sigma = \{c_1, c_2, \cdots, f_1, f_2, \cdots\}$ *be a signature. A* Σ**-algebra**

$$\mathfrak{A} = \langle A, c_1^{\mathfrak{A}}, c_2^{\mathfrak{A}}, \cdots, f_1^{\mathfrak{A}}, f_2^{\mathfrak{A}}, \cdots \rangle$$

is a set A *(sometimes written* $| \mathfrak{A} |$ *and called the* **carrier** *set or underlying set of* $\mathfrak{A}$*), together with the following family of functions and constants:*

- *For each constant symbol* c *in* Σ*, a constant (i.e. a member)* $c^{\mathfrak{A}}$ *of* A*.*
- *For each function symbol* f *of arity* n *in* Σ*, a function* $f^{\mathfrak{A}} : A^n \to A$*.*

Let $\mathfrak{A}$,$\mathfrak{B}$ *be two* Σ*-algebras. A* Σ*-algebra* **morphism** $\varphi : \mathfrak{A} \to \mathfrak{B}$ *is a function from* $| \mathfrak{A} |$ *to* $| \mathfrak{B} |$ *which "respects the* Σ*-structure", that is to say, satisfying*

[3] sometimes –without warning– we will treat $\mathcal{K}_\Sigma$ and $\mathcal{F}_\Sigma$ as *sets* of symbols, and forget their ordering

[4] In fact a constant can be thought of as a function of arity 0, meaning a function whose domain is any singleton set $\{*\}$.

1. *For each constant c in Σ, $\varphi(c^{\mathfrak{A}}) = c^{\mathfrak{B}}$,*
2. *For each function symbol f in Σ of arity n and any $a_1, \ldots, a_n \in A$,*

$$\varphi(f^{\mathfrak{A}}(a_1, \ldots, a_n)) = f^{\mathfrak{B}}(\varphi(a_1), \ldots, \varphi(a_n))$$

If a morphism is surjective (onto) it is called an epi-*morphism, if injective (one-to-one) a* mono-*morphism, and if both, an isomorphism.*

The second property above is often expressed by saying that the following diagram *commutes*.

$$\begin{array}{ccc} A^n & \xrightarrow{f^{\mathfrak{A}}} & A \\ \downarrow{\scriptstyle \varphi^n} & & \downarrow{\scriptstyle \varphi} \\ B^n & \xrightarrow{f^{\mathfrak{B}}} & B \end{array} \tag{3}$$

where $\varphi^n : A^n \longrightarrow B^n$ is the function that maps n-tuples $(a_1, \ldots, a_n)$ of members of A to the n-tuple $(\varphi(a_1), \ldots, \varphi(a_n))$ of members of B.

We say a diagram *commutes* if all routes, in this case, from the NW corner to the SE corner, yield the same function, which is exactly what condition 2 said.

Before looking at examples we will need to define the set $T_\Sigma(X)$ of Σ-terms.

Definition 8 *Let Σ be a signature, and X a set of variables (a set of symbols disjoint from the signature Σ). The set of* **open Σ-terms** *over X is given by the following inductive definition.*

1. *If c is a constant in Σ then c is a term.*
2. *If x is a variable, x is a term.*
3. *If $t_1, \ldots, t_n$ are terms and f is a function symbol in Σ of arity n then $ft_1 \cdots t_n$ is a term (sometimes also written $f(t_1, \ldots, t_n)$).*
4. *Nothing else is a term.*

If a term has no variables it is called a **ground term**. *We use the notation T_Σ to denote the set of of ground Σ-terms, and $T_\Sigma(X)$ to denote the set of open terms over the set of variables X.*

The terms $t_1, \ldots, t_n$ are called immediate subterms *of $ft_1 \cdots t_n$.*

The set of terms (open or ground) is inductively defined. The main significance of this in practice is that we can prove properties of terms by induction on this definition, so-called *structural induction*.

Definition 9 (Structural Induction) *Suppose P is a property of terms such that*

1. *$P(c)$ is true for every constant.*
2. *$P(x)$ is true for every variable.*
3. *If f is a function symbol of arity n and $t_1, \ldots, t_n$ are terms, and $P(t_1), \ldots, P(t_n)$ are true, then $P(ft_1 \cdots t_n)$ is also true. Said differently: if all immediate subterms of a term have the property P then so does the term.*

Then every term has the property P.

Suitably formulated, this principle is a consequence of ordinary induction on the natural numbers. Observe that if we set

$$\begin{aligned} \mathcal{T}_\Sigma^0(X) &= \mathcal{K}_\Sigma \cup X \\ \mathcal{T}_\Sigma^{n+1}(X) &= \mathcal{T}_\Sigma^n \cup \{ ft_1 \cdots t_n : t_j \in \mathcal{T}_\Sigma^n \ \& \ f \in \mathcal{F}_\Sigma \} \end{aligned}$$

then

$$\mathcal{T}_\Sigma(X) = \bigcup \mathcal{T}_\Sigma^n(X).$$

We can then establish structural induction by showing, by induction on the natural numbers, that if the premises 1, 2 and 3 in the definition of structural induction hold, then $P(t)$ is true for every member of $\mathcal{T}_\Sigma^n(X)$ for every n. This is true for $\mathcal{T}_\Sigma^0(X)$ by 1 and 2, and if P holds for every term in $\mathcal{T}_\Sigma^n(X)$ it must hold for every term in $\mathcal{T}_\Sigma^{n+1}(X)$ by premise 3.

Now we need some examples of Σ-algebras. Let's pick a familiar signature, namely that of arithmetic: $\Sigma = \langle \mathsf{0}, \mathsf{1}, +^2, \times^2 \rangle$. It will be important in this example to carefully distinguish the constant *symbol* $\mathsf{0}$, which has no *a priori* meaning, from the natural number 0. We consider two Σ-algebras.

1. Let $\mathfrak{N} = \langle \mathbb{N}, \mathsf{0}^{\mathfrak{N}}, \mathsf{1}^{\mathfrak{N}}, +^{\mathfrak{N}}, \times^{\mathfrak{N}} \rangle$ be the so-called "standard model", with carrier set the natural numbers $\mathbb{N}$, and with the usual interpretations: $\mathsf{0}^{\mathfrak{N}} = 0, \mathsf{1}^{\mathfrak{N}} = 1$ and $+^{\mathfrak{N}}, \times^{\mathfrak{N}}$ ordinary addition and multiplication.
2. Now we consider the so-called **term algebra** $\mathcal{T}_\Sigma$, given by:

   $$\mathcal{T}_\Sigma = \langle T_\Sigma, \mathsf{0}^{\mathcal{T}_\Sigma}, \mathsf{1}^{\mathcal{T}_\Sigma}, \oplus, \otimes \rangle$$

   where T_Σ is the set of ground terms over Σ, and $\mathsf{0}^{\mathcal{T}_\Sigma} = \mathsf{0}$, and $\mathsf{1}^{\mathcal{T}_\Sigma} = \mathsf{1}$ (i.e. $\mathsf{0}$ and $\mathsf{1}$ are interpreted as *themselves* viewed as atomic terms) and

   $$\begin{aligned} \oplus(t_1, t_2) &= +t_1 t_2 \\ \otimes(t_1, t_2) &= \times t_1 t_2 \end{aligned}$$

We now give the definition of (open) term algebra for arbitrary signatures.

Definition 10 *Let $\Sigma = \langle c_1, c_2, \ldots; f_1, f_2, \ldots\rangle$ be a signature and X a set of variables. We define the Σ-algebra*

$$\mathcal{T}_\Sigma(X) = \langle U\mathcal{T}(X); c_1^{\mathcal{T}_\Sigma(X)}, c_2^{\mathcal{T}_\Sigma(X)}, \ldots; f_1^{\mathcal{T}_\Sigma(X)}, f_2^{\mathcal{T}_\Sigma(X)}, \ldots\rangle$$

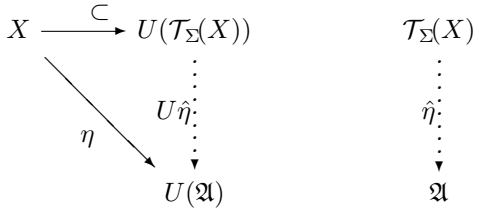
by:

$$\begin{aligned} c_j^{\mathcal{T}_\Sigma(X)} &= c_j \\ f_j^{\mathcal{T}_\Sigma(X)}(t_1, \ldots, t_{n_j}) &= f t_1 \cdots t_{n_j} \end{aligned}$$

where n_j is assumed to be the arity of f_j. Note that if we let $X = \varnothing$ this gives the definition of the algebra of ground terms.

Theorem 11 *For any signature Σ, and any Σ-algebra $\mathfrak{A}$, there is a unique Σ-morphism $\iota_{\mathfrak{A}}$ from $\mathcal{T}_\Sigma$ to $\mathfrak{A}$.*

If X is a set of variables and $\eta : X \to |\mathfrak{A}|$ an arbitrary function (called an $\mathfrak{A}$-environment for X) then there is a unique Σ-morphism $\mathcal{T}_\Sigma(X) \xrightarrow{\hat{\eta}} \mathfrak{A}$ such that for every x in X, $\hat{\eta}(x) = \eta(x)$. In diagram form:



(4)

Notice that the triangle on the left, including the vertical dotted map, is a diagram of sets *and functions between sets, whereas the right hand diagram shows that the map $\hat{\eta}$ is actually a Σ-morphism*[5].

This property of $\mathcal{T}_\Sigma(X)$ is often stated thus: $\mathcal{T}_\Sigma(X)$ is a **free** Σ-algebra over X, or an **initial** Σ-algebra over X.
proof: Exercise □

.

The word *free* here refers to the fact that the least number of assumptions possible are used to construct this Σ-algebra. There are no gratuitous relations between the elements of the algebra. For example, in the $\langle 0, 1; +, \times\rangle$-algebra of the natural numbers, different-looking terms formed with $+$ and $\times$, such as $(1+1)\times(1+1)$ and $1+1+1+1$, actually coincide. That is a "gratuitous" relation that the corresponding terms in the free algebra for this signature would *not* satisfy.

[5] We use U applied to a morphism to "forget" the additional algebraic properties, and just treat it as a function on sets, just the way we use $U(\mathfrak{A})$ or $|\mathfrak{A}|$ to "forget" the algebraic structure and just refer to the underlying (hence the U) set.

The word *initial* is just making reference to the property illustrated in the preceding diagram, namely that given any other algebra $\mathfrak{A}$ with a map into it from X, there is a unique arrow starting at $\mathcal{T}_\Sigma(X)$ and going into $\mathfrak{A}$. All paths, so to speak, initiate at $\mathcal{T}_\Sigma(X)$, and lead to any other algebra.

Yet another way to state the freeness property of $\mathcal{T}_\Sigma(X)$ is as follows:

For every map of sets $X \xrightarrow{\eta} U(\mathfrak{A})$*, where* $U(\mathfrak{A})$ *is the underlying set of* $\mathfrak{A}$*, there is a unique* Σ*-morphism* $\mathcal{T}_\Sigma(X) \xrightarrow{\hat{\eta}} \mathfrak{A}$ *and conversely.*

This information is displayed thus:

$$\frac{X \xrightarrow{\eta} U(\mathfrak{A})}{\mathcal{T}_\Sigma(X) \xrightarrow{\hat{\eta}} \mathfrak{A}}.$$

This (together with some other conditions we will not mention now) is called an *adjoint situation* and the operator $\mathcal{T}_\Sigma$ is said to be a *left adjoint* of the operator U.

2.1 Monoids

Definition 12 *A monoid* $\mathcal{M} = (M, \otimes, \mathbf{1}_M)$ *is a set* M *with a distinguished member* $\mathbf{1}$ *(called a* unit*) and a binary operation*

$$\otimes : M \times M \to M$$

which is

- *associative: for all* $m_1, m_2, m_3 \in M$ *we have* $m_1 \otimes (m_2 \otimes m_3) = (m_1 \otimes m_2) \otimes m_3$
- *unitary: for each* m *in* M*,* $m \otimes \mathbf{1} = m = \mathbf{1} \otimes m$.

It should be clear that a monoid is just a Σ-algebra over the signature $\Sigma = \{\mathbf{1}; \otimes^2\}$ subject to the additional condition that the equation $x \otimes (y \otimes z) = (x \otimes y) \otimes z$ holds in M for all values of its variables, as well as the equation defining the unit condition cited above.

A class of structures, such as monoids, consisting of all algebras satisfying a set of equations is called a *variety*.

A nice example of a monoid is $(\mathbb{N}, +, 0)$, the natural numbers with addition, or $(\mathbb{R}, +, 0)$, with $\mathbb{R}$ the real numbers. Yet another is $(\mathbb{N}^+, \cdot, 1)$, the *positive* natural numbers with multiplication, or $(\mathbb{R}^+, \cdot, 1)$, with $\mathbb{R}^+$ the positive reals.

The reader is invited to find a (famous) Σ-morphism (also known as a monoid homomorphism) from $(\mathbb{R}^+, \cdot, 1)$ to $(\mathbb{R}, +, 0)$.

A natural question to ask here is what is the *free* monoid, X^* over a set X, if it exists, i.e. the analogue of the term algebra for monoids, satisfying the condition given by diagram 4 above. It can't be the free $\{\mathbf{1}, \otimes\}$-algebra, consisting of all terms built up from $\mathbf{1}$ and X using $\otimes$, because this structure

does not satisfy the associative law, or the unit law, $m \otimes 1$ and m are just not the same terms.

It is easy to construct. Let X^* be the set of all *words* (or sequences, or strings) over X, with **1** taken to be the empty sequence $\langle\rangle$, often written "" by computer scientists, and with $\otimes^{M(X)}$ defined by *concatenation*:

$$\otimes(x_1 \cdots x_n, y_1 \cdots y_k) = x_1 \cdots x_n y_1 \cdots y_k.$$

The reader should check that it's a monoid and that it's free: *every monoid is the image of a free monoid*, meaning that, for every monoid M there is a set X and an onto morphism η from X^* to M. Check that $(\mathbb{N}, +, 0)$ is essentially, i.e. isomorphic to, the free monoid on a single generator, i.e. on a singleton set $X = \{x\}$.

3 Closure

Let S be a set with some operation defined on it (thus, some kind of algebra). A sub**set** A of S is said to be closed under the operation if it can be applied to any members of A and produce an output in A. Sometimes sets are not closed under some natural operation, and we must construct a minimal extension that will be closed, called a closure.

Here are the definitions.

Definition 13 *Let S be a set, A a subset of S and f a k-ary function on S. Then we say A is* **closed under** *f if for every k-tuple $a_1, \ldots, a_k$ of elements from A, we have $f(a_1, \ldots, a_k) \in A$.*

Some examples: the subset $\{1, 2, 3\}$ of $\mathbb{N}$ is not closed under addition: $2 + 3$ is not in the set, we have to go outside it for answers. If the set were our universe of discourse we would have to call $+$ a partial or incomplete operation. On the other hand, the set $\{-1, 0, 1\}$ is closed under multiplication.

Suppose we started with $\{2, 4, 6\}$ and wanted to add only the numbers required to make it closed under addition. We would have to add $2 + 2, 2 + 2 + 2, 6 + 6 + 4, 4 + 4$, etc. Would we have to add all the natural numbers?

Definition 14 *Let S be a set, A a subset, and $\mathcal{F}$ a set of functions on S. We call a subset $\hat{A}$ of S the* **closure** *of A under $\mathcal{F}$ if it satisfies:*

1. *$A \subseteq \hat{A}$.*
2. *$\hat{A}$ is closed under every function in $\mathcal{F}$.*
3. *$\hat{A}$ is the smallest such set: if B contains A and is closed under all functions in $\mathcal{F}$ then $\hat{A} \subseteq B$.*

How do we know such a set always exists? You can construct it, from below, or from above. First from above.

Theorem 15 *Let S be a set, A a subset, and $\mathcal{F}$ a set of functions on S. Then $\hat{A}$ is the intersection of all closed subsets of S containing A.*

Problem 2 *Prove the preceding theorem, i.e. that the set defined by intersection has the three required properties. (1 and 3 are obvious, 2 is the interesting one).*

Let $S, A, \mathcal{F}$ be as in the theorem. Define

$$\begin{aligned} A_0 &= A && (5)\\ A_{n+1} &= A_n \cup \{f(a_1,\ldots,a_k) : f \in \mathcal{F} \text{ and } a_1,\ldots,a_k \in A_n\} && (6)\end{aligned}$$

then we claim:

Theorem 16 $\hat{A} = \bigcup_0^\infty A_n$.

Problem 3 *Prove the preceding theorem. To establish $\hat{A} \subseteq \bigcup_0^\infty A_n$ show that $\bigcup_0^\infty A_n$ is a closed subset of S. Then since $\hat{A}$ is the intersection of all such, it must be contained in it. To show the opposite containment, prove, by induction on n, that each $A_n \subseteq \hat{A}$. Then show why this forces the union to be contained in $\hat{A}$ as well.*

These notions can be stated in terms of algebras.

Definition 17 *Let $\mathfrak{A}$ be a Σ-algebra, and $E \subseteq |\mathfrak{A}|$. Then the subalgebra $\mathfrak{A}(E)$ of $\mathfrak{A}$* **generated by** *E is the smallest subalgebra of $\mathfrak{A}$ containing E.*

It is easily seen that the algebra generated by E exists: it is the intersection of all subalgebras of $\mathfrak{A}$ containing E. Actually, to be more precise, its carrier set is the intersection of the carriers of all the algebras containing E, and one actually has to show that it contains the $\mathfrak{A}$-interpretations $c^{\mathfrak{A}}$ of all the constants in Σ and is closed under the functions of $\mathfrak{A}$ that interpret the function symbols in Σ and is therefore a Σ-algebra.

If we denote by $\mathfrak{A}_K$ and $\mathfrak{A}_F$ the sets of constants $c^{\mathfrak{A}}$ and functions $f^{\mathfrak{A}}$ of $\mathfrak{A}$ corresponding to the constant and function symbols in Σ, it is precisely the closure of $E \cup \mathfrak{A}_K$ in $|\mathfrak{A}|$ under $\mathfrak{A}_F$.

We can also give a bottom-up description of $\mathfrak{A}(E)$, using the approximations

$$\begin{aligned} \mathfrak{A}^0(E) &= E \cup \mathfrak{A}_K\\ \mathfrak{A}^{n+1}(E) &= \mathfrak{A}^n(E) \cup \{f^{\mathfrak{A}}(x_1,\ldots,x_m) : x_i \in \mathfrak{A}^n(E) \;\&\; f \in \Sigma, m = \text{arity of } f\}.\end{aligned}$$

Lemma 18 *Let $\mathfrak{A}$ be a Σ-algebra, and $E \subseteq |\mathfrak{A}|$.*

$$\mathfrak{A}(E) = \bigcup \mathfrak{A}^n(E).$$

This is shown by the same arguments given above. It should be remarked that there is some abuse of language in the statement of the lemma. The right hand side is a set, whereas the left-hand side is an algebra. What is meant is that the underlying set of the algebra on the left is the same set as the one at right.

We conclude this section with a discussion of generating sets.

Definition 19 *Let $\mathfrak{A}$ be a Σ-algebra, and $E \subseteq |\mathfrak{A}|$. Then E is said to* **generate** *$\mathfrak{A}$ if*

$$\mathfrak{A}(E) = \mathfrak{A}.$$

Observe that generating sets always exist: $\mathfrak{A}$ is generated by $|\mathfrak{A}|$. If we think of $|\mathfrak{A}|$ itself (or any generating set G) as a set of variables (or "fresh constants"), then the identity map of sets $Id : |\mathfrak{A}| \to |\mathfrak{A}|$ (or the inclusion $G \subseteq \mathfrak{A}$) induces a unique Σ-morphism

$$\mathcal{T}_\Sigma(|\mathfrak{A}|) \xrightarrow{\widehat{Id}} \mathfrak{A}$$

(or $\mathcal{T}_\Sigma(G) \xrightarrow{\widehat{\subseteq}} \mathfrak{A}$), which is easily seen surjective. Thus:

Theorem 20 *Every Σ-algebra is the image of a free algebra on some set.*

4 Lattices, Continuity and Fixed Points

Definition 21 *A lattice $L = \langle S, \leq \rangle$ is a partially ordered set in which every pair of members has a least upper bound (lub, or $\bigvee$) and a greatest lower bound (glb, or $\bigwedge$). A lattice is* **complete** *if any subset of L has a $\bigvee$ and a $\bigwedge$. A subset X of L is* **directed** *if every finite subset of X has an upper bound in X. A function*

$$f : L \to L$$

is **monotone** *if for every x, with $x \leq y$ we have $f(x) \leq f(y)$. It is* **continuous** *if for every directed subset $X \subseteq L$*

$$f(\bigvee X) = \bigvee(f(X)).$$

Note that a complete lattice always has a least ($\bot$) and greatest element ($\top$).

Theorem 22 (Tarski-Knaster) *Let L be a complete lattice, $\bot$ its least element. and $T : L \to L$.*

If T is continuous then it has a least fixed point $\mathsf{lfp}(\mathsf{T})$ and

$$\mathsf{lfp}(\mathsf{T}) = \bigcup_{\mathsf{n} \in \omega} \mathsf{T}^{\mathsf{n}}(\bot)$$

where $T^{n+1}(X)$ means $T(T^n(X))$ and $T^0(X) = X$.

proof: Exercise. □

.

Observe that the powerset of any set X is a complete lattice with the order relation given by $\subseteq$, $\bigvee$ given by $\cup$, $\bigwedge$ by $\cap$, greatest element by X, and least element by $\varnothing$.

Now we apply these ideas to algebras. First observe that if $\mathfrak{A}$ is a Σ-algebra and $E \subset \mathfrak{A}$ then $Sub(\mathfrak{A}, E)$, the collection of subalgebras of $\mathfrak{A}$ containing E, is a complete lattice, with order given by the *subalgebra* relation, minimal element $\mathfrak{A}(E)$, maximal element $\mathfrak{A}$, glb given by intersection, and lub by **closure** of unions, i.e. by the subalgebra generated by the union. Also the set $\wp(\mathfrak{A}, E \cup \mathfrak{A}_K)$ of *subsets* of $\mathfrak{A}$ containing $E \cup \mathfrak{A}_K$ is a complete lattice with the containment order.

Lemma 23 *Let $\mathfrak{A}$ be a Σ-algebra and $E \subset \mathfrak{A}$. Then the operator*

$$S_{\mathfrak{A}} : \wp(\mathfrak{A}, E) \to \wp(\mathfrak{A}, E)$$

given by

$$S_{\mathfrak{A}}(X) = X \cup \{f^{\mathfrak{A}}(x_1, \ldots, x_m) : x_i \in X \ \& \ f \in \Sigma, m = \textit{arity of } f\}.$$

is continuous.

We then have the following consequence of the Tarski-Knaster theorem and of lemma 18:

Theorem 24 *Let $\mathfrak{A}$ be a Σ-algebra and $E \subset \mathfrak{A}$. Then*

$$\mathfrak{A}(E) = \mathsf{lfp}(\mathsf{S}_{\mathfrak{A}}) = \bigcup \mathsf{S}^{\mathsf{n}}_{\mathfrak{A}}(\varnothing).$$

proof: Exercise. □

.

The characterization of least fixed points as *unions* of sets from below, in the case of continuous operators, is sometimes called a *bottom-up* description of the set in question. A description of a set as an intersection, or least member of a class is sometimes called top-down[6].

We have essentially shown that every closure of a generating subset (such as the set of terms or the subalgebra generated by some set) is the least fixed point of some continuous operator and hence an inductively defined set (e.g. the bottom-up description of lemma 18).

[6]There is a deeper distinction than just "up" and "down" in these two approaches, one pointed out by Poincaré almost a century ago, and of interest to many computer scientists. A definition of a set A as an intersection of all sets in a class is disturbing –as a definition, not as an equation– because the intersection is being taken over a class *that already includes* A, an apparent circularity. This is known as an *impredicative* definition, and some logicians and computer scientists only allow them if there is an alternative predicative description of the set in question.

If we allow that a term is really a string over some alphabet, that happens to be particularly well-formed, then the set of terms in $\mathcal{T}_\Sigma(X)$is a subset of Γ^*, the set (in fact, monoid) of strings over $\Gamma = X \cup \mathcal{F}_\Sigma \cup \mathcal{K}_\Sigma \cup \{(,)\}$. Can we view it as some sort of closure, say the closure of $\mathcal{K}_\Sigma \cup X$ under a suitably defined set of functions (corresponding to the symbols in $\mathcal{F}_\Sigma$), from Γ^* to itself?

Problem 4 *Describe the class of functions with respect to which $\mathcal{T}_\Sigma(X)$ is the closure of $\mathcal{K}_\Sigma \cup X$ in Γ^*. Describe the continuous operator on $\wp(\Gamma^*, \mathcal{K}_\Sigma \cup X)$ whose least fixed point is $\mathcal{T}_\Sigma(X)$.*

You may use the parenthesis-free formulations of terms discussed in class if you wish, and take a smaller alphabet.

Appendix

Some Proofs of Theorems above

Solution to problem 1
Suppose R is a well-founded binary relation in a set A but there is an infinite descending sequence

$$\cdots a_n R a_{n-1} \cdots a_2 R a_1.$$

Let $S = \{a_i : i \in \mathbb{N}\}$. S must have an R-minimal element. So for some n the element a_n has no R predecessor. But by assumption $a_{n+1} R a_n$, a contradiction. No such infinite descending sequence exists.

Conversely, suppose no infinite descending R sequences exist in A and suppose that S is a nonempty subset of A with no R-minimal element. That means every element of S has an R predecessor in S. Define a function $f : \mathbb{N} \to S$ by letting $f(0)$ be an arbitrary element a of S. Since a is not R-minimal there is an a' in S with $a'Ra$. Let $f(1)$ be a member of $\{a' \in S : a'Ra\}$. Let $f(n+1)$ be some member of $\{a' \in S : a'Rf(n)\}$. Thus we define an infinite descending sequence

$$\cdots f(n) R f(n-1) \cdots f(2) R f(1),$$

contradicting our hypothesis.
Proof of Theorem 4
$\underline{Ind \Rightarrow Cov}$:
Assume all instances of the induction scheme hold, that is to say, that Ind_P holds for every P. Assume, for every x that $(\forall y < xp(y)) \to p(x)$. Call this assumption (*).

Let $r(x)$ be the assertion $\forall y < xp(y)$. Then observe that $r(0)$ holds trivially, since there are no y below 0. Now suppose $r(n)$ holds. Then $\forall y < np(y)$ holds. But by assumption (*) $p(n)$ holds, so $r(n+1)$ holds. By Ind we have $\forall x r(x)$. But that means that for every x we have $\forall y < xp(y)$. So by (*) again, we have $p(x)$ for every x. So we have shown that assumption (*) implies $\forall x p(x)$. That is Cov.

$\underline{Cov \Rightarrow Ind}$:
Suppose $p(0)$ and $\forall n p(n) \to p(n+1)$. Further suppose, for $n > 0$ that $\forall y < np(y)$. Then $p(n-1)$ holds, so $p(n)$ holds. We have shown that $\forall y < np(y)$ implies $p(n)$. By Cov we have $\forall n p(n)$.

$\underline{LNP \Rightarrow Cov}$:
Suppose $\forall y < xp(y)$ implies $p(x)$. Call that assumption (**). Let $B = \{z | p(z)$ does not hold $\}$ and assume (for the sake of a contradiction) that B is not empty. Then it has a least element z_0. But then $\forall y < z_0 (y \notin B)$, which gives $z_0 \notin B$, a contradiction. So B must be empty and $\forall z p(z)$. This followed from assumption (**). So Cov holds.

$\underline{Cov \Rightarrow LNP}$:
Suppose B is a nonempty set of natural numbers that has no least element.

Now assume $\forall y < zy \notin B$. If z were in B it would be the least element, so we must have $z \notin B$. Thus $\forall y < zy \notin B \Rightarrow z \notin B$ By Cov we have $\forall zz \notin B$, i.e. that B is empty, a contradiction. So B must have a least element. $\square$