THE L.E.J. BROUWER CENTENARY SYMPOSIUM
A.S. Troelstra and D. van Dalen (editors)

THE TYPE THEORETIC INTERPRETATION OF CONSTRUCTIVE SET THEORY: CHOICE PRINCIPLES

Peter Aczel

Department of Mathematics
Manchester University
England

In an earlier paper I gave an interpretation of a system CZF of constructive set theory within an extension of Martin-Löf's intuitionistic theory of types. In this paper some additional axioms, each a consequence of the axiom of choice, are shown to hold in the interpretation. The mathematical deductions are presented in an informal, but I hope rigorous style.

INTRODUCTION

The axiom of choice does not have an unambiguous status in constructive mathematics. On the one hand it is said to be an immediate consequence of the constructive interpretation of the quantifiers. Any proof of $\forall x \in A\, \exists y \in B\, F(x,y)$ must yield a function $f \in A \to B$ such that $\forall x \in A\, F(x,f(x))$. This is certainly the case in Martin-Löf's intuitionistic theory of types. On the other hand, from the very earliest days, the axiom of choice has been criticised as an excessively non-constructive principle even for classical set theory. Moreover, in more recent years, it has been observed that the full axiom of choice cannot be added to systems of constructive set theory without yielding constructively unacceptable cases of excluded middle (see e.g. Diaconescu [1975]). In Myhill [1975] a system of constructive set theory was put forward as a suitable setting for the style of constructive mathematics pursued by Bishop and his school (see Bishop [1967] and Bridges [1979] and also this proceedings). Myhill argued informally that the axiom DC of dependent choices was constructively acceptable. Aczel [1978] contains an interpretation of a system CZF of constructive set theory that is closely related to Myhill's system. I claimed there, without proof, that DC was true in the interpretation. This will be shown in §5 of this paper. In §7 of Aczel [1978] I also put forward an axiom called the presentation axiom, which I thought to be a plausible addition to constructive set theory. But there I was unable to verify its truth in the interpretation. A fundamental aim of this paper is to show that the presentation axiom is indeed true in the interpretation. In fact a strengthening, ΠΣI-PA, of the presentation axiom will be verified in §7.

The interpretation of CZF given in Aczel [1978] was carried out within a natural extension of Martin-Löf's intuitionistic theory of types as presented in Martin-Löf [1975]. Type theory is intended to be a fundamental conceptual framework for the basic notions of constructive mathematics. For this reason I believe that the interpretation of constructive set theory in type theory can lay claim to give a good constructive meaning to the set theoretical notions. In view of this it is very natural to explore fully which set theoretical axioms are true in the interpretation. To do this I have found it convenient to develop a flexible informal style for presenting deductions in type theory. Moreover, if type theory is to be a practical vehicle for the presentation of mathematical deductions of constructive mathematics itself, such an informal style will be essential. So I have tried to write this paper relying only on the informal description of the type theoretic notions given in §1. There is the danger that I may be criticised for lack of rigour, as it may not be always transparent to the reader how each step could be formalised. But my primary aim has been to present the mathematical results stripped of excessive formalism. Of course, while writing this paper, I have had in mind a formal language for type theory such as that presented in Martin-Löf [1979], and the reader may find it helpful to refer to that paper both for the list of rules of the formal language and for the explanations of fundamental notions. Martin-Löf [1975] and [1979] give some information concerning the pre-history of the framework of type theory used here. The reader should also refer to Aczel [1978] for a more extensive discussion of CZF than will be given here. Apart from these topics the present paper is intended to be self-contained. In view of this, the paper starts with an informal description of type theory in §1, and in §2 and §3 goes on to present the interpretation of CZF in the framework described in §1. In contrast to the other sections the discussion in §4 takes place in an informal framework for constructive set theory. That discussion is concerned with formulating the axioms that will be verified in the remaining sections. Dependent choices is verified in §5, and this section also introduces some essential ideas to be used in the last two sections. The axioms ΠΣI-AC and ΠΣI-PA will be verified in §6 and §7 respectively. In the last section it turns out necessary to use a method not contemplated in Aczel [1978] or available in the formal languages of Martin-Löf [1975] and [1979], although the possibility of the method is mentioned in Martin-Löf [1975]. This method involves making explicit the conception of the type U of small types as a type inductively specified by a specific list of rules for forming small types. The method is to allow definitions of functions on U by a transfinite recursion following the inductive generation of the small types. The method is used to construct a suitable representation of each small type as an element of the type V of iterative sets. As pointed out in Aczel [1978] such a representation is what is needed to verify the presentation axiom.

As with any active research program the type theoretic approach to constructive mathematics has been under steady development over the years and the publications I have referred to only represent stages in that development. There have been some significant changes between the stages represented by Martin-Löf [1975] and Aczel [1978] and the more recent stages represented by Martin-Löf [1979] and this paper. A minor notational change has been that the symbols U and V have interchanged their meaning. A more significant change has been the introduction in Martin-Löf [1979] of the new form of type $(Wx \in A)B[x]$. With this new form the type V of iterative sets can be defined simply as $(Wx \in U)x$. But in this paper the new form will not be used, and its effect on the interpretation of constructive set theory will be left to another paper. In keeping with the above definition of V I have used the notation $\sup(A,b)$ or $(\sup x \in A)b(x)$ for the iterative set symbolised by $\{b(x) \mid x \in A\}$ in Aczel [1978]. Perhaps the most significant change has been that involving the treatment of equality. In Martin-Löf [1975] there is one relation of definitional equality which is defined to be the equivalence relation which is generated by the principles that a definiendum is always definitionally equal to its definiens and that definitional equality is preserved under substitution. In the present version of type theory each notion of object must carry with it an equality relation which is not necessarily to be understood as a definitional equality relation. So there is an equality relation for types, and also for each type A, a relation of equality for elements of type A. Martin-Löf writes

$$a = b \in A$$

to express the judgement that a and b are equal elements of type A. Each form of type has its own criteria for when such a judgement holds. So for example if f and g are elements of the type $A \to B$ of functions from A to B,

$$f = g \in A \to B$$

means that f and g are extensionally equal, i.e. $f(x) = g(x) \in B$ for $x \in A$. In practice when a judgement $a = b \in A$ is made it is usually either clear from the context that a and b are elements of type A or else it does not matter exactly what the type of a and b is. For this reason I propose to follow the standard convention of writing simply $a = b$. Whenever two expressions are definitionally equal, and in a given context one of them refers to an object of some sort then the other expression will refer to an equal object of that sort. For this reason it is safe to follow the standard convention, when making definitions, of simply writing equalities. This will be done here.

The mathematical results in this paper were obtained while preparing a series of talks on the type theoretic interpretation of constructive set theory given in Munich in October 1980. I am grateful to Prof. Schwichtenberg for his invitation which was the spur to a fresh look at the topic.

The contents of this paper do not exactly reflect the topic of my talk at the conference. I felt unable to write on that topic before having completed this paper, and I am grateful to the editors for accepting this substitute.

§1. AN INFORMAL DESCRIPTION OF TYPE THEORY

SOME NOTATION

If $b[x_1, \ldots, x_n]$ is an expression and $x_1, \ldots, x_n$ is a non-repeating list of variables then $(x_1, \ldots, x_n)\, b[x_1, \ldots, x_n]$ will denote the n-place function f having defining equation

$$f(x_1, \ldots, x_n) = b[x_1, \ldots, x_n].$$

So whenever $b[a_1, \ldots, a_n]$ refers to an object of some sort then $f(a_1, \ldots, a_n)$ will refer to an equal object of that sort and we can write

$$f(a_1, \ldots, a_n) = b[a_1, \ldots, a_n].$$

Here $b[a_1, \ldots, a_n]$ is the result of simultaneously substituting $a_1, \ldots, a_n$ for $x_1, \ldots, x_n$ in $b[x_1, \ldots, x_n]$, making suitable changes in the bound variables when necessary.

If c is the ordered pair (a, b) then $p(c)$ and $q(c)$ will be the two components a and b respectively.

TYPES AND THEIR ELEMENTS

1.1. The fundamental notions of type theory are

type

and if A is a type

element of A.

If a is an element of the type A then we shall write

$$a \in A.$$

1.2. We start our survey of the forms of type by considering the familiar forms

$$A \to B \quad A \times B \quad N.$$

$A \to B$ is the type of functions $(x)b[x]$ such that $b[x] \in B$ for $x \in A$, and $A \times B$ is the type of pairs (a, b) such that $a \in A$ and $b \in B$. N is the type of natural numbers and is inductively specified using the rules

$$0 \in N \qquad \frac{n \in N}{s(n) \in N}.$$

Associated with N is the method of definition by recursion over N. For example, given a type C, $a \in C$ and $f \in N \times C \to C$ we may define $h \in N \to C$ by recursion so that

$$\begin{aligned} h(0) &= a \\ h(s(n)) &= f(n, h(n)) \quad \text{for } n \in N. \end{aligned}$$

We shall write $R(n, a, f)$ for $h(n)$ if we wish to make the dependence of $h(n)$ on a and f explicit.

1.3. The notions we have introduced so far already suffice for the type structure of Gödel's primitive recursive functions of finite types. But here we wish to have a richer notion of type and in particular we wish to have types that are beyond the level of the finite types. For this reason it is useful to have types whose elements are themselves types. While a type of all types is unreasonable it is sensible to have a type U of types that reflects to a suitable extent the notion of type itself. Reflecting on the forms of type we have considered so far leads us to have $A \to B \in U$ and $A \times B \in U$ whenever $A, B \in U$ and also to have $N \in U$. Note that we do not wish to have $U \in U$. It is natural to call types in U small types and types such as U and $U \to U$ that are built up out of U are large types. Using the type U one may form by recursion functions such as $F \in N \to U$ where

$$\begin{aligned} F(0) &= N \\ F(s(n)) &= F(n) \to N \quad \text{for } n \in N. \end{aligned}$$

F is an example of a family of types. In general a family of types over a type A is a function F that assigns a type $F(a)$ to each $a \in A$.

1.4. We now consider the forms of type $\Pi(A, F)$ and $\Sigma(A, F)$ where F is a family of types over the type A. If F is $(x)B[x]$ then these types will also be written $(\Pi x \in A)B[x]$ and $(\Sigma x \in A)B[x]$ respectively. The cartesian product $\Pi(A, F)$ is the type of functions $(x)b[x]$ such that $b[x] \in F(x)$ for $x \in A$, and the disjoint union $\Sigma(A, F)$ is the type of pairs (a, b) such that $a \in A$

and $b \in F(a)$. The forms $A \to B$ and $A \times B$ are the special cases of these new forms when F is the function $(x)B$ having as constant value the type B, i.e.

$$A \to B = (\Pi x \in A)B,$$
$$A \times B = (\Sigma x \in A)B.$$

Let us consider more closely the elements of the new forms of type. If $f \in \Pi(A, F)$ then $f(x) \in F(x)$ for $x \in A$ and $f = (x)f(x)$. If $c \in \Sigma(A, F)$ then $p(c) \in A$, $q(c) \in F(p(c))$ and $c = (p(c), q(c))$. The method of definition by recursion on N applies in a slightly more general context than that previously considered. Previously $h \in N \to C$ was defined from $a \in C$ and $f \in N \times C \to C$ where C was a type. We may use the same equations to define $h \in \Pi(N, F)$ from $a \in F(0)$ and $f \in (\Pi z \in \Sigma(N, F))\, F(s(p(z)))$, where F is a family of types over N. The earlier formulation is now simply the special case when F has the constant value C.

Having introduced the new forms of type $\Pi(A, F)$ and $\Sigma(A, F)$ we should remember to reflect them in the type U. So we have that both these types are small whenever F is a family of small types over the small type A.

1.5. So far we have considered the primitive forms of type N, U, $\Pi(A, F)$ and $\Sigma(A, F)$, the last two having special instances $A \to B$ and $A \times B$. Our present survey of forms of type will be completed by considering the forms $I(A, a, b)$, $A + B$, N_0 and V.

1.6. $I(A, a, b)$ is a type provided that a and b are elements of the type A. It has an element r provided $a = b$. So $c = r$ and $a = b$ whenever $c \in I(A, a, b)$. The significance of this form will perhaps become clearer later. If A is small then so is $I(A, a, b)$.

1.7. If A and B are types then $A + B$ is a type called the <u>disjoint union</u> of the two types. It has an element $i(a)$ for each $a \in A$ and an element $j(b)$ for each $b \in B$. If $f \in (\Pi x \in A)\, C(i(x))$ and $g \in (\Pi y \in B)\, C(j(y))$ where C is a family of types over $A + B$ then we have a function $h \in \Pi(A + B, C)$ <u>defined by cases</u> so that

$$h(i(a)) = f(a) \quad \text{for} \quad a \in A$$
$$h(j(b)) = g(b) \quad \text{for} \quad b \in B$$

$h(c)$ will also be written $D(c, f, g)$ if we wish to make its dependence on f and g explicit. If A and B are small types then so is $A + B$.

1.8. N_0 is the <u>empty type</u>. Whenever C is a family of types over N_0 then $R_0 \in \Pi(N_0, C)$. For $k = 1, 2, 3, \ldots$ the k-element type N_k can be defined as follows

$$\begin{aligned} N_1 &= I(N, 0, 0) \\ N_2 &= N_1 + N_1 \\ N_3 &= N_2 + N_1 \\ &\text{etc. } \ldots \end{aligned}$$

The type N_k has elements $1_k, \ldots, k_k$ where

$$\begin{aligned} 1_1 &= r, \\ 1_2 &= i(1_1),\ 2_2 = j(r), \\ 1_3 &= i(1_2),\ 2_3 = i(2\ ),\ 3_3 = j(r), \\ &\text{etc. } \ldots \end{aligned}$$

If $a_1 \in C(1_k), \ldots, a_k \in C(k_k)$ where C is a family of types over N_k then $h \in \Pi(N_k, C)$ can be defined so that

$$\begin{aligned} h(1_k) &= a_1 \\ &\vdots \\ h(k_k) &= a_k. \end{aligned}$$

If we wish to make the dependence of $h(c)$ on $a_1, \ldots, a_k$ explicit then we write $R_k(c, a_1, \ldots, a_k)$ for $h(c)$. Each R_k can be defined as follows

$$\begin{aligned} R_1(c, a_1) &= a_1, \\ R_2(c, a_1, a_2) &= D(c, (x)a_1, (y)a_2), \\ R_3(c, a_1, a_2, a_3) &= D(c, (x)R_2(x, a_1, a_2), (y)a_3), \\ &\text{etc. } \ldots \end{aligned}$$

1.9. Finally we come to the type V of <u>(iterative) sets</u>. This type is inductively specified via the rule

$$\frac{A \in U \qquad b \in A \to V}{\sup(A, b) \in V}$$

We shall also write $(\sup x \in A)b[x]$ for $\sup(A, (x)b[x])$. Note that because $N_0 \in U$ and $R_0 \in N_0 \to V$ we certainly have the set $\sup(N_0, R_0)$, which we shall abbreviate ϕ. More generally, given sets $\alpha_1, \ldots, \alpha_k$ we may form the set

$(\sup x \in N_k)R_k(x, \alpha_1, \ldots, \alpha_k)$ which we shall abbreviate $\{\alpha_1, \ldots, \alpha_k\}$. In this way the hereditarily finite sets can be represented as elements of the type V. Associated with the rule inductively specifying the type V is the following method of definition by transfinite recursion on V. If d is a three place function such that $d(A, b, e) \in C(\sup(A, b))$ for all $A \in U$, $b \in A \to V$ and $e \in (\Pi x \in A)C(b(x))$, where C is a family of types over V, then we have $h \in \Pi(C, V)$ defined so that

$$h(\sup(A, b)) = d(A, b, (u)h(b(u))$$

for $A \in U$ and $b \in A \to V$. When we wish to make the dependence of $h(c)$ on d explicit it will be written $T(c, d)$. Note that V must be considered a large type as the rule used in specifying it makes explicit reference to U.

1.10. Let us review what we have said concerning the type U. It is a type whose elements are themselves types, called the small types. The following schemes express our rules for forming small types

$$N_0 \in U \qquad N \in U$$

$$\frac{A \in U \quad F \in A \to U}{\Pi(A, F) \in U} \qquad \frac{A \in U \quad F \in A \to U}{\Sigma(A, F) \in U}$$

$$\frac{A \in U \quad B \in U}{A + B \in U} \qquad \frac{A \in U \quad a, b \in A}{I(A, a, b) \in A}.$$

In this paper we shall need to consider these rules as giving an inductive specification of the type U. This means that we have the following method of definition by transfinite recursion on U. If C is a family of types over U the method allows us to form $h \in \Pi(U, C)$ such that for $A, B \in U$, $F \in A \to U$ and $a, b \in A$

$$\begin{aligned}
h(N_0) &= d_{N_0} \\
h(N) &= d_N \\
h(\Pi(A, F)) &= d_\Pi(A, F, h(A), (x)h(F(x))) \\
h(\Sigma(A, F)) &= d_\Sigma(A, F, h(A), (x)h(F(x))) \\
h(A + B) &= d_+(A, B, h(A), h(B)) \\
h(I(A, a, b)) &= d_I(A, h(A), a, b).
\end{aligned}$$

In these equations $d_{N_0} \in C(N\ )$, $d_N \in C(N)$ and d_Π, d_Σ, d_+ and d_I are four place functions such that if $A, B \in U$, $F \in A \to U$ and $a, b \in A$ then

$$d_\Pi(A, F, c, e) \in C(\Pi(A, F))$$
$$d_\Sigma(A, F, c, e) \in C(\Sigma(A, F))$$
$$d_+(A, B, c, d) \in C(A + B)$$
$$d_I(A, c, a, b) \in C(I(A, a, b))$$

for $c \in C(A)$, $d \in C(B)$ and $e \in (\Pi x \in A)C(F(x))$.

PROPOSITIONS AS TYPES

1.11. So far we have avoided explicit reference to the standard logical operations and how they are to be treated in type theory. The point of view to be adopted here is that the logical operations operate on propositions and propositions are types. Each proposition is the type of its proofs. So the logical operations are identified with the appropriate type forming operations in line with the constructive meaning of the logical operations. For example the constructive meaning of an implication $A \supset B$ is explained by saying that a proof of $A \supset B$ is a function that assigns to each proof of A a proof of B. Hence $A \supset B$ is the type $A \to B$. The following table gives a dictionary for translating the logical terminology into type theory. We shall freely use terminology from whichever side of the table seems most natural.

LOGICAL NOTION	TYPE THEORETIC EXPLICATION
proposition	type
proof of A	element of A
A is true	A has an element
$A \supset B$	$A \to B$
$A \& B$	$A \times B$
$A \vee B$	$A + B$
$A \equiv B$	$(A \to B) \times (B \to A)$
$\perp$	N_0
$\neg A$	$A \to N_0$
$a =_A b$	$I(A, a, b)$
$(\forall x \in A)B[x]$	$(\Pi x \in A)B[x]$
$(\exists x \in A)B[x]$	$(\Sigma x \in A)B[x]$

1.12. The following result is the fundamental fact of the 'propositions as types' treatment of logic.

FUNDAMENTAL THEOREM. For every instance in type theory of a natural deduction rule for intuitionistic predicate calculus with equality, if the premises are true then so is the conclusion.

Rather than give a detailed formulation and proof of this result I shall just examine a selection of the rules.

IMPLICATION INTRODUCTION

$$\frac{\begin{array}{c}[A]\\ B\end{array}}{A \supset B}$$

If B is true on the assumption that A is true then there is $b[x] \in B$ for $x \in A$ so that $(x)b[x] \in A \rightarrow B$ and hence the conclusion is true.

IMPLICATION ELIMINATION (i.e. modus poneus)

$$\frac{A \supset B \quad A}{B}$$

If the premises are true then there are $f \in A \rightarrow B$ and $a \in A$ so that $f(a) \in B$ and hence the conclusion is true.

UNIVERSAL QUANTIFICATION INTRODUCTION

$$\frac{\begin{array}{c}[x \in A]\\ B[x]\end{array}}{(\forall x \in A)B[x]}$$

If $B[x]$ is true for $x \in A$ then there is $b[x] \in B[x]$ for $x \in A$ so that $(x)b[x] \in (\Pi x \in A)B[x]$ and hence the conclusion is true.

EQUALITY ELIMINATION

$$\frac{a =_A b \quad B[a]}{B[b]}$$

If the first premise is true there is some element of $I(A, a, b)$ and hence $a = b$ so that $B[a] = B[b]$. If the second premise is also true then $B[a]$ has an element and hence so does $B[b]$ so that the conclusion is true.

1.13. In addition to the purely logical principles considered in the fundamental theorem there are a number of other principles that can be justified in type theory and will be needed in later sections of this paper. We list them below with an indication of why they are correct.

1.14. If F is a family of propositions (i.e. types) over the type A it is natural to call F a <u>species</u> over A.

N-INDUCTION. For every species F over N

$$\frac{F(0) \quad (\forall n \in N)(F(n) \supset F(s(n)))}{(\forall n \in N)F(n)}$$

V-INDUCTION. For every species F over V

$$\frac{(\forall A \in U)(\forall b \in A \to V)[(\forall x \in A)F(b(x)) \supset F(\sup(A, b))]}{(\forall \alpha \in V)F(\alpha)}$$

U-INDUCTION. For every species F over U

$$\frac{F(N_0) \quad F(N) \quad \Phi_\Pi \quad \Phi_\Sigma \quad \Phi_+ \quad \Phi_I}{(\forall A \in U)F(A)}$$

where Φ_Π is

$$(\forall A \in U)(\forall B \in A \to U)[F(A) \ \& \ (\forall x \in A)F(b(x)) \supset F(\Pi(A,B))],$$

Φ_Σ is like Φ_Π with Σ replacing Π and Φ_+ and Φ_I are

$$(\forall A \in U)(\forall B \in U)[F(A) \ \& \ F(B) \supset F(A+B)]$$

and

$$(\forall A \in U)(\forall a \in A)(\forall b \in B)[F(A) \supset F(I(A, a, b))].$$

These principles are justified by suitable definitions by recursion. Thus for N-induction, if the premises are true then there are $a \in F(0)$ and $b \in (\Pi n \in N)(F(n) \to F(s(n))$ so that

$$(n)R(n, a, (x, y)b(x)(y)) \in (\Pi n \in N)F(n)$$

and the conclusion is true. Similarly if d is an element of the premise of V-induction then $(\alpha)T(\alpha, (A, b, e)\ d(A)(b)(e))$ is an element of the conclusion.

1.15. If B is a family of types over the type A and F is a two place function such that $F(x, y)$ is a proposition for $x \in A$ and $y \in B(x)$ then

THE AXIOM OF CHOICE (AC)

$$\frac{(\forall x \in A)(\exists y \in B(x))F(x, y)}{(\exists z \in \Pi(A, B))(\forall x \in A)F(x, z(x))}$$

THE DEPENDENT CHOICES AXIOM (DC)

$$\frac{(\forall x \in A)[B(x) \supset (\exists y \in A)(B(y) \ \&\ F(x, y))]}{(\forall x \in A)[B(x) \supset (\exists z \in N \to A)G(x, z)]}$$

where $G(x, z)$ is

$$(z(0) =_A x) \ \&\ (\forall n \in N)[B(z(n)) \ \&\ F(z(n), z(s(n)))].$$

If f is an element of the premise of AC then let $g = (x)p(f(x))$ and $h = (x)q(f(x))$. Then $g \in \Pi(A, B)$ and $h \in (\forall x \in A)F(x, g(x))$ so that (g, h) is an element of the conclusion. So AC is correct.

If f is an element of the premise of DC then let

$$\begin{aligned} h &= (u)f(p(u))(q(u)), \\ g &= (u)(p(h(u)), p(q(h(u)))), \\ k &= (u)q(q(h(u))). \end{aligned}$$

Then $g \in C \to C$, where C is $\Sigma(A, B)$, and $k \in (\Pi u \in C)F(p(u), p(g(u)))$.

Now let $a \in A$ and $b \in B(a)$. Then by recursion over N we may define $e \in N \to C$ so that

$$\begin{aligned} e(0) &= (a, b) \\ e(s(n)) &= g(e(n)) \quad \text{for } n \in N. \end{aligned}$$

Then $(n)p(e(n)) \in N \to A$, $p(e(0) =_A a$ and $(n)(q(e(n)), k(e(n)))$ is an element of

$$(\forall n \in N)[B(p(e(n))) \ \&\ F(p(e(n)), p(e(s(n))))]$$

and hence

$$((n)p(e(n)), (r, (n)(q(e(n)), k(e(n)))))$$

is an element of $(\exists z \in N \to A)G(a, z)$. Thus given an element of A such that $B(a)$ has an element we have found an element of $(\exists z \in N \to A)G(a, z)$. In other words we have the conclusion of DC.

1.16. EXTENSIONALITY. If B is a family of types over the type A and $f, g \in \Pi(A, B)$ then

$$\frac{(\forall x \in A)(f(x) =_{B(x)} g(x))}{f =_{\Pi(A, B)} g}$$

If c is an element of the premise then $c(a) \in I(B(a), f(a), g(a))$ for $a \in A$ so that $f(a) = g(a)$ for $a \in A$ and hence $f = g$. As $f = g$ the type $I(\Pi(A, B), f, g)$ has the element r and hence the conclusion is true.

1.17. Let F be a species over the type C.

Σ-EXISTENCE. If C is $\Sigma(A, B)$ where B is a family of types over the type A then

$$(\exists z \in C)F(z) \equiv (\exists x \in A)(\exists y \in B(x))F((x, y))$$

$+$-EXISTENCE. If C is $A + B$ where A and B are types then

$$(\exists z \in C)F(z) \equiv (\exists x \in A)F(i(x)) \vee (\exists y \in B)F(j(y))$$

N_k-EXISTENCE. If C is N_k for $k = 0, 1, \ldots$ then

$$(\exists z \in C)F(z) \equiv F(1_k) \vee \ldots \vee F(k_k),$$

where in case $k = 0$ the right hand side is $\perp$.

In each of these equivalences the implication from right to left involves a simple direct application of the existence introduction rule. For the other direction let us just consider $+$-existence. If $a \in A$ then

$$(u)i((i(a), u)) \in F(i(a)) \to D$$

where D is the right hand side of the $+$-existence equivalence. Hence $(\Pi x \in A)(F(i(x)) \to D)$ has an element. Similarly $(\Pi y \in B)(F(j(y)) \to D)$ also has an element so that using definition by cases $(\Pi z \in A + B)(F(z) \to D)$ has an element. So $(\forall z \in A + B)(F(z) \supset D)$ is true, and using intuitionistic logic $(\exists z \in A + B)F(z) \supset D$ is true.

A WARNING

Of fundamental importance in understanding type theory is an awareness of the distinction between the notions of judgement and proposition. The distinction is critical and attempts to avoid it are liable to lead to confusion. Nevertheless, from the practical point of view it seems convenient to leave the distinction implicit in our informal deductions. Before doing so it may be worthwhile to give the distinction our explicit attention.

Examples of judgements are

$$N \text{ is a type},$$
$$0 \in N,$$
$$0 = 0 \in N,$$
$$s(x) \in N \quad \text{for} \quad x \in N.$$

Examples of propositions are

$$0 =_N 0,$$
$$0 =_N s(0),$$
$$(\forall x \in N)(x =_N 0 \vee (\exists y \in N)(y =_N s(x)).$$

Note that each proposition A is a type, which is true if it has an element and false if $A \to N_0$ has an element. Such a proposition is a meaningful object even when false. On the other hand judgements are necessarily correct as such, and an incorrectly formed judgement is meaningless.

Martin-Löf's formal language has a system of finitary rules for deriving judgements. This is in contrast to the standard formal systems (e.g. for HA or CZF) which involve finitary rules for deriving propositions. Nevertheless, as we have seen, the logical notions are represented in type theory and the standard rules for deriving propositions are also represented in type theory. So, conceptually, there are two distinct levels of derivation. There is the fundamental level where judgements are derived, and there is the secondary level concerned with the derivation of propositions. In our informal presentation the distinction between these levels will not always be explicit. For example, we have the notion of (iterative) set, and in later sections we shall make a lot of use of the notion of an injectively presented set. Now the statement that α is a set is simply the judgement $\alpha \in V$. On the other hand if $\alpha \in V$ then the statement that α is injectively presented is a proposition, which may be false. In following the arguments in this paper, which are presented in a combination of the English language and symbolic expressions, it is necessary to be aware of this distinction. In certain cases there is an easy interplay between the different levels. For example if a and b are elements of the type A then we may form the proposition $(a =_A b)$; i.e. the type $I(A, a, b)$. Now $a = b \in A$ may not be a correctly formed judgement. If it is then $r \in I(A, a, b)$ so that the proposition $a =_A b$ is true. Conversely if we know that $a =_A b$ is true, i.e. that the type $I(A, a, b)$ has an element, then the judgement $a = b \in A$ can be formed.

§2. V AS A TYPE OF EXTENSIONAL SETS

In this section we define the species on $V \times V$ of extensional equality, and extensional membership, and show that various set theoretical properties hold. An axiom system CZF for constructive set theory will be formulated in the next section and the work in this section shows the truth of those axioms. In this section and the next we are retracing the ground of §§4-6 of Aczel [1978], but now within the *informal setting of the previous section.*

2.1. THEOREM. There are one-place functions assigning $\bar{\alpha} \in U$ and $\tilde{\alpha} \in \bar{\alpha} \to V$ to $\alpha \in V$ such that if $\alpha = \sup(A, b)$ where $A \in U$ and $b \in A \to V$ then $\bar{\alpha} = A$ and $\tilde{\alpha} = b$. Moreover $\alpha = \sup(\bar{\alpha}, \tilde{\alpha})$ for $\alpha \in V$.

PROOF. Define $\tau \in V \to (\Sigma x \in U)(x \to V)$ by transfinite recursion on V so that for $A \in U$ and $b \in A \to V$

$$\tau(\sup(A, b)) = (A, b).$$

Now let $\bar{\alpha} = p(\tau(\alpha))$ and $\tilde{\alpha} = q(\tau(\alpha))$. Then clearly $\bar{\alpha} \in U$ and $\tilde{\alpha} \in \bar{\alpha} \to V$ for $\alpha \in V$. Also, if $\alpha = \sup(A, b)$ where $A \in U$ and $b \in A \to V$ then $\bar{\alpha} = A$ and $\tilde{\alpha} = b$. It remains to prove the final part of the theorem. Define $g = (x)\sup(\bar{x}, \tilde{x})$. Then $g \in V \to V$ and by the above $g(\alpha) = \alpha$ *whenever* $\alpha = \sup(A, b)$ *for some* $A \in U$ and $b \in A \to V$. To show that $g(\alpha) = \alpha$ for all $\alpha \in V$ we need to argue as follows. We know that $r \in I(V, g(\sup(A, b)), \sup(A, b))$ for all $A \in U$ and $b \in A \to V$. Hence, by transfinite recursion on V, $T(\alpha, (x, y, z)r) \in I(V, g(\alpha), \alpha)$ so that $g(\alpha) = \alpha$ for $\alpha \in V$.

If $B[x]$ is a proposition for $x \in V$ then define

$$(\forall x \in \alpha)B[x] = (\forall x \in \bar{\alpha})B[\tilde{\alpha}(x)]$$
$$(\exists x \in \alpha)B[x] = (\exists x \in \bar{\alpha})B[\tilde{\alpha}(x)].$$

2.2. THEOREM. If F is a species over V then

$$(\forall x \in V)[(\forall y \in x)F(y) \supset F(x)] \supset (\forall x \in V)F(x).$$

PROOF. This is an immediate application of V-induction from 1.2.

2.3. THEOREM. There is a species on $V \times V$ assigning a small proposition $(\alpha \doteq \beta)$ to $\alpha, \beta \in V$ such that

$$(\alpha \doteq \beta) = [\forall x \in \alpha \exists y \in \beta(x \doteq y)] \& [\forall y \in \beta \exists x \in \alpha(x \doteq y)].$$

PROOF. Define three-place functions G_1, G_2 and G_3 so that

$$G_1(u, v, w) = \forall x \in u \exists y \in v\, w(x)(y),$$
$$G_2(u, v, w) = \forall y \in v \exists x \in u\, w(x)(y),$$
$$G(u, z, w) = (v)(G_1(u, v, w) \,\&\, G_2(u, v, w)).$$

Then for $i = 1, 2$ $G_i(u, v, w)$ is a small type for $u \in U$, $v \in V$ and $w \in u \to (V \to U)$, so that $G(u, z, w) \in V \to U$ for $u \in U$, $z \in u \to V$ and $w \in u \to (V \to U)$.

It follows that $T(\alpha, G) \in V \to U$ for $\alpha \in V$ and

$$T(\sup(A, b), G) = G(A, b, (u)T(b(u), G)) \quad \text{for } A \in U,\ b \in A \to V.$$

Now define $(\alpha \doteq \beta) = T(\alpha, G)(\beta)$ for $\alpha, \beta \in V$. Then for $\alpha, \beta \in V$, $(\alpha \doteq \beta) \in U$ and if $f = (u)T(\tilde{\alpha}(u), G)$ then

$$\begin{aligned}(\alpha \doteq \beta) &= T(\sup(\bar{\alpha}, \tilde{\alpha}), G)(\beta)\\ &= G(\bar{\alpha}, \tilde{\alpha}, f)(\beta)\\ &= G_1(\bar{\alpha}, \beta, f) \,\&\, G_2(\bar{\alpha}, \beta, f)\end{aligned}$$

But
$$\begin{aligned}G_1(\bar{\alpha}, \beta, f) &= \forall x \in \bar{\alpha} \exists y \in \beta f(x)(y)\\ &= \forall x \in \bar{\alpha} \exists y \in \beta(\tilde{\alpha}(x) \doteq y)\\ &= \forall x \in \alpha \exists y \in \beta(x \doteq y),\end{aligned}$$

and similarly

$$G_2(\bar{\alpha}, \beta, f) = \forall y \in \beta \exists x \in \alpha(x \doteq y),$$

so that we get the desired result.

2.4. LEMMA. *For* $\alpha, \beta, \gamma \in V$

(i) $\alpha \doteq \alpha$,

(ii) $\alpha \doteq \beta \supset \beta \doteq \alpha$,

(iii) $\alpha \doteq \beta \,\&\, \beta \doteq \gamma \supset \alpha \doteq \gamma$.

PROOF. (i) *For* $\alpha \in V$

$$\begin{aligned}(\forall x \in \alpha)(x \doteq x) &\supset \forall x \in \bar{\alpha}(\tilde{\alpha}(x) \doteq \tilde{\alpha}(x))\\ &\supset \forall x \in \bar{\alpha}\exists y \in \bar{\alpha}(\tilde{\alpha}(x) \doteq \tilde{\alpha}(y))\\ &\supset \forall x \in \alpha\exists y \in \alpha(x \doteq y).\end{aligned}$$

Similarly

$$(\forall x \in \alpha)(x \doteq x) \supset \forall y \in \alpha\exists x \in \alpha(x \doteq y),$$

so that

$$(\forall x \in \alpha)(x \doteq x) \supset \alpha \doteq \alpha.$$

Hence by 2.2 we get $\alpha \doteq \alpha$ for all $\alpha \in V$.

(ii) Let $F = (x)(\forall y \in V)(x \doteq y \supset y \doteq x)$. Then F is a species over V. Let $\alpha \in V$ such that $(\forall x \in \alpha)F(x)$. Then if $\beta \in V$

$$\begin{aligned}\alpha \doteq \beta &\supset \forall x \in \bar{\alpha}\exists y \in \bar{\beta}(\tilde{\alpha}(x) \doteq \tilde{\beta}(y))\\ &\supset \forall x \in \bar{\alpha}\exists y \in \bar{\beta}(\tilde{\beta}(y) \doteq \tilde{\alpha}(x))\\ &\supset \forall x \in \alpha\exists y \in \beta(y \doteq x).\end{aligned}$$

Similarly $\alpha \doteq \beta \supset \forall y \in \beta\exists x \in \alpha(y \doteq x)$. It follows that $\alpha \doteq \beta \supset \beta \doteq \alpha$. So, we have proved that for $\alpha \in V$

$$(\forall x \in \alpha)F(x) \supset F(\alpha)$$

and hence by 2.2 we have $(\forall x \in V)F(x)$ as required.

(iii) Let $F = (x)(\forall y \in V)(\forall z \in V)(x \doteq y \;\&\; y \doteq z \supset x \doteq z)$. Then F is a species over V. Let $\alpha \in V$ such that $(\forall x \in \alpha)F(x)$. Then for $\beta, \gamma \in V$

$$\begin{aligned}\alpha \doteq \beta \;\&\; \beta \doteq \gamma &\supset \forall x \in \alpha\exists y \in \beta(x \doteq y) \;\&\; \forall y \in \beta\exists z \in \gamma(y \doteq z)\\ &\supset \forall x \in \bar{\alpha}\exists y \in \bar{\beta}(\tilde{\alpha}(x) \doteq \tilde{\beta}(y)) \;\&\; \forall y \in \bar{\beta}\exists z \in \bar{\gamma}(\tilde{\beta}(y) \doteq \tilde{\gamma}(z))\\ &\supset \forall x \in \bar{\alpha}\exists y \in \bar{\beta}\exists z \in \bar{\gamma}(\tilde{\alpha}(x) \doteq \tilde{\beta}(y) \;\&\; \tilde{\beta}(y) \doteq \tilde{\gamma}(z))\\ &\supset \forall x \in \bar{\alpha}\exists z \in \bar{\gamma}(\tilde{\alpha}(x) \doteq \tilde{\gamma}(z))\\ &\supset \forall x \in \alpha\exists z \in \gamma(x \doteq z).\end{aligned}$$

Similarly, $\alpha \doteq \beta \;\&\; \beta \doteq \gamma \supset \forall z \in \gamma\exists x \in \alpha(x \doteq z)$, so that $\alpha \doteq \beta \;\&\; \beta \doteq \gamma \supset \alpha \doteq \gamma$. So we have proved that for $\alpha \in V$

$$(\forall x \in \alpha)F(x) \supset F(\alpha)$$

and hence by 2.2 we have the desired result.

2.5. DEFINITION. For $\alpha, \beta \in V$ let

$$\alpha \,\varepsilon\, \beta = (\exists y \,\varepsilon\, \beta)(\alpha \doteq y)$$
$$\alpha \subseteq \beta = (\forall x \,\varepsilon\, \alpha)(x \,\varepsilon\, \beta).$$

Then both $\alpha \,\varepsilon\, \beta$ and $\alpha \subseteq \beta$ are small propositions for $\alpha, \beta \in V$.

A species F over V is <u>extensional</u> if

$$(\forall x \in V)(F(x) \supset (\forall y \in V)(y \doteq x \supset F(y))).$$

2.6. THEOREM. If F is an extensional species over V then for $\alpha \in V$

(i) $(\forall x \,\varepsilon\, \alpha)F(x) \equiv (\forall x \in V)(x \,\varepsilon\, \alpha \supset F(x))$
(ii) $(\exists x \,\varepsilon\, \alpha)F(x) \equiv (\exists x \in V)(x \,\varepsilon\, \alpha \,\&\, F(x))$

PROOF.

$$\begin{aligned}
\text{(i)}\quad (\forall x \in V)(x \,\varepsilon\, \alpha \supset F(x)) &\equiv (\forall x \in V)(\exists y \,\varepsilon\, \alpha(x \doteq y) \supset F(x)) \\
&\equiv (\forall x \in V)(\exists y \in \bar{\alpha})(x \doteq \tilde{\alpha}(y) \supset F(x)) \\
&\equiv (\forall y \in \bar{\alpha})(\forall x \in V)(x \doteq \tilde{\alpha}(y) \supset F(x)) \\
&\equiv (\forall y \in \bar{\alpha})F(\tilde{\alpha}(y)) \\
&\equiv (\forall x \,\varepsilon\, \alpha)F(x). \\
\text{(ii)}\quad (\exists x \in V)(x \,\varepsilon\, \alpha \,\&\, F(x)) &\equiv (\exists x \in V)(\exists y \,\varepsilon\, \alpha(x \doteq y) \,\&\, F(x)) \\
&\equiv (\exists x \in V)(\exists y \in \bar{\alpha})(x \doteq \tilde{\alpha}(y) \,\&\, F(x)) \\
&\equiv (\exists y \in \bar{\alpha})(\exists x \in V)(x \doteq \tilde{\alpha}(y) \,\&\, F(x)) \\
&\equiv (\exists y \in \bar{\alpha})F(\tilde{\alpha}(y)) \\
&\equiv (\exists x \,\varepsilon\, \alpha)F(x).
\end{aligned}$$

2.7. THEOREM. For $\alpha, \beta, \gamma \in V$

(i) $(\alpha \doteq \beta \,\&\, \beta \,\varepsilon\, \gamma) \supset \alpha \,\varepsilon\, \gamma$,
(ii) $\alpha \doteq \beta \equiv \forall x \in V(x \,\varepsilon\, \alpha \equiv x \,\varepsilon\, \beta)$.

PROOF. (i)
$$\begin{aligned}
(\alpha \doteq \beta \,\&\, \beta \,\varepsilon\, \gamma) &\supset (\alpha \doteq \beta \,\&\, \exists z \in \bar{\gamma}(\beta \doteq \tilde{\gamma}(z))) \\
&\supset \exists z \in \bar{\gamma}(\alpha \doteq \tilde{\gamma}(z)) \\
&\supset \alpha \,\varepsilon\, \gamma.
\end{aligned}$$

(ii) By (i) the species $(x)(x \,\varepsilon\, \alpha)$ is extensional so that by theorem 2.6

$$\alpha \subseteq \beta \equiv \forall x \,\varepsilon\, \alpha(x \,\varepsilon\, \beta)$$
$$\equiv \forall x \in V(x \,\varepsilon\, \alpha \supset x \,\varepsilon\, \beta).$$

Similarly, $$\beta \subseteq \alpha \equiv \forall x \in V(x \,\varepsilon\, \beta \supset x \,\varepsilon\, \alpha).$$

Hence, by 2.3 and 2.4 (ii)

$$\alpha \doteq \beta \equiv (\alpha \subseteq \beta \;\&\; \beta \subseteq \alpha)$$
$$\equiv \forall x \in V(x \,\varepsilon\, \alpha \equiv x \,\varepsilon\, \beta).$$

2.8. THEOREM.

(i) Unordered Pairs. If $\alpha, \beta \in V$ then there is $\gamma \in V$ such that for all $\eta \in V$

$$\eta \,\varepsilon\, \gamma \equiv (\eta \doteq \alpha \vee \eta \doteq \beta).$$

(ii) Union. If $\alpha \in V$ then there is $\gamma \in V$ such that for all $\eta \in V$

$$\eta \,\varepsilon\, \gamma \equiv \exists x \,\varepsilon\, \alpha \,(\eta \,\varepsilon\, x).$$

(iii) Small-Separation. If $\alpha \in V$ and $F \in V \to U$ then there is $\gamma \in V$ such that for all $\eta \in V$

$$\eta \,\varepsilon\, \gamma \equiv \exists x \,\varepsilon\, \alpha(F(x) \;\&\; \eta \doteq x).$$

PROOF. (i) Let $\alpha, \beta \in V$. Recall that $\{\alpha, \beta\} \in V$ where $\{\alpha, \beta\} = (\sup z \in N_2)R_2(z, \alpha, \beta)$. Let $\gamma = \{\alpha, \beta\}$. Then for $\eta \in V$

$$\eta \,\varepsilon\, \gamma \equiv \exists z \in N_2(\eta \doteq R_2(z, \alpha, \beta))$$
$$\equiv (\eta = \alpha \vee \eta \doteq \beta)$$

using the N_k-existence principle from 1.17.

(ii) Let $\alpha \in V$. Then $\gamma \in V$ where

$$\gamma = (\sup z \in (\Sigma x \in \bar{\alpha})\overline{\tilde{\alpha}(x)})(\tilde{\alpha}(p(z)))^{\sim}(q(z)).$$

Now, for $\eta \in V$, using the Σ-existence principle from 1.17,

$$\eta \,\varepsilon\, \gamma \equiv (\exists z \in (\Sigma x \in \bar{\alpha})\overline{\tilde{\alpha}(x)}(\eta \doteq (\tilde{\alpha}(p(z)))^{\sim}(q(z)))$$
$$\equiv (\exists x \in \bar{\alpha})(\exists y \in \overline{\tilde{\alpha}(x)})(\eta \doteq (\tilde{\alpha}(x))^{\sim}(y))$$
$$\equiv (\exists x \in \bar{\alpha})(\exists y \,\varepsilon\, \tilde{\alpha}(x))(\eta \doteq y)$$

$$\equiv (\exists x \in \alpha)(\exists y \in x)(\eta \doteq y)$$
$$\equiv \exists x \in \alpha\, (\eta \in x).$$

(iii) Let $\alpha \in V$ and $F \in V \to U$. Then $A \in U$, where $A = (\Sigma x \in \bar{\alpha})F(\tilde{\alpha}(x))$, so that $\gamma \in V$ where $\gamma = (\sup z \in A)\tilde{\alpha}(p(z))$. Now if $\eta \in V$

$$\begin{aligned}\eta \in \gamma &\equiv \exists z \in A\ (\eta \doteq \tilde{\alpha}(p(z)))\\ &\equiv \exists x \in \bar{\alpha}\ \exists y \in F(\tilde{\alpha}(x))\ (\eta \doteq \tilde{\alpha}(x))\\ &\equiv \exists x \in \bar{\alpha}(F(\tilde{\alpha}(x))\ \&\ \eta \doteq \tilde{\alpha}(x))\\ &\equiv \exists x \in \alpha(F(x)\ \&\ \eta \doteq x).\end{aligned}$$

2.9. THEOREM. If F is a species on $V \times V$ let F' be the species on $V \times V$ given by

$$F'(x, y) = \forall u \in x\ \exists v \in y\ F(u, v)\ \&\ \forall v \in y\ \exists u \in x\ F(u, v).$$

Then (i) If $\alpha, \beta \in V$ such that $\bar{\alpha} = \bar{\beta}$ then

$$(\forall x \in \bar{\alpha})\ F(\tilde{\alpha}(x), \tilde{\beta}(x)) \supset F'(\alpha, \beta).$$

(ii) Strong Collection. If $\alpha \in V$ then

$$(\forall x \in \alpha)(\exists y \in V)\ F(x, y) \supset \exists \beta \in V\ F'(\alpha, \beta).$$

(iii) Subset Collection. If $\alpha, \beta \in V$ then there is $\gamma \in V$, not depending on F, such that

$$(\forall x \in \alpha)(\exists y \in \beta)\ F(x, y) \supset \exists \delta \in \gamma\ F'(\alpha, \delta).$$

PROOF. (i) Let $\alpha, \beta \in V$ such that $\bar{\alpha} = \bar{\beta}$ and $\forall x \in \bar{\alpha}\ F(\tilde{\alpha}(x), \tilde{\beta}(x))$. Then $\forall x \in \bar{\alpha}\ \exists y \in \bar{\beta}\ F(\tilde{\alpha}(x), \tilde{\beta}(y))$ so that $\forall x \in \alpha\ \exists y \in \beta\ F(x, y)$. Similarly $\forall y \in \beta\ \exists x \in \alpha\ F(x, y)$. So $F'(\alpha, \beta)$.

(ii) Let $\alpha \in V$ such that $\forall x \in \alpha\ \exists y \in V\ F(x, y)$. Then $\forall x \in \bar{\alpha}\ \exists y \in V\ F(\tilde{\alpha}(x), y)$. Hence by AC in 1.15 there is $b \in \bar{\alpha} \to V$ such that $\forall x \in \bar{\alpha}\ F(\tilde{\alpha}(x), b(x))$. Then let $\beta = \sup(\bar{\alpha}, b)$. So $\beta \in V$, $\bar{\alpha} = \bar{\beta}$ and $\forall x \in \bar{\alpha}\ F(\tilde{\alpha}(x), \tilde{\beta}(x))$ so that by (i) $F'(\alpha, \beta)$.

(iii) Let $\alpha, \beta \in V$ and define

$$\gamma = (\sup z \in \bar{\alpha} \to \bar{\beta})(\sup x \in \bar{\alpha})\tilde{\beta}(z(x)).$$

It is easy to see that $\gamma \in V$ and is independent of F. Now assume that $\forall x \varepsilon \alpha\, \exists y \varepsilon \beta\, F(x, y)$. Then $\forall x \in \bar{\alpha}\, \exists y \in \bar{\beta}\, F(\tilde{\alpha}(x), \tilde{\beta}(y))$. Hence by AC in 1.15 there is $f \in \bar{\alpha} \to \bar{\beta}$ such that $\forall x \in \bar{\alpha}\, F(\tilde{\alpha}(x), \tilde{\beta}(f(x)))$. Let $\delta = (\sup x \in \bar{\alpha})\tilde{\beta}(f(x))$. Then $\delta \in V$ and $\delta \doteq \tilde{\gamma}(f)$ so that $\delta \varepsilon \gamma$. Also $\bar{\alpha} = \bar{\delta}$ and $\forall x \in \bar{\alpha}\, F(\tilde{\alpha}(x), \tilde{\delta}(x))$ so that by (i) $F'(\alpha, \delta)$.

2.10. THEOREM. Recall that $\phi = \sup(N_0, R_0)$ and for $\alpha \in V$ define $\alpha' = (\sup x \in \bar{\alpha} + N_1)D(x, \tilde{\alpha}, (y)\alpha)$. Then (i) $\phi \in V$ and for $\eta \in V$

$$\eta \varepsilon \phi \equiv \bot ,$$

(ii) for $\alpha \in V$, $\alpha' \in V$ and for $\eta \in V$

$$\eta \varepsilon \alpha' \equiv (\eta \varepsilon \alpha \vee \eta \doteq \alpha),$$

(iii) for $\alpha \in V$

$$\alpha' \doteq \phi \supset \bot ,$$

(iv) for $\alpha, \beta \in V$

$$\alpha' \doteq \beta' \supset \alpha \doteq \beta.$$

PROOF. (i) That $\phi \in V$ is clear. For $\eta \in V$

$$\begin{aligned} \eta \varepsilon \phi &\equiv (\exists x \in N_0)(\eta \doteq R_0(x)) \\ &\equiv \bot \end{aligned}$$

by N_0-existence in 1.17.

(ii) If $\alpha \in V$ then $\bar{\alpha} \in U$ so that $\bar{\alpha} + N_1 \in U$. Also $\tilde{\alpha}(x) \in V$ for $x \in \bar{\alpha}$ and $\alpha \in V$ for $y \in N_1$ so that $D(x, \tilde{\alpha}, (y)\alpha) \in V$ for $x \in \bar{\alpha} + N_1$. Hence $\alpha' \in V$. If $\eta \in V$ then, using 1.17

$$\begin{aligned} \eta \varepsilon \alpha' &\equiv (\exists x \in \bar{\alpha} + N_1)(\eta \doteq D(x, \tilde{\alpha}, (y)\alpha)) \\ &\ (\exists x \in \bar{\alpha})(\eta \doteq \tilde{\alpha}(x)) \vee (\exists y \in N_1)(\eta \doteq \alpha) \\ &\ (\eta \varepsilon \alpha \vee \eta \doteq \alpha). \end{aligned}$$

(iii) For $\alpha \in V$

$$\begin{aligned} \alpha' \doteq \phi &\supset \alpha \varepsilon \phi && \text{by (ii)} \\ &\supset \bot && \text{by (i)}. \end{aligned}$$

(iv) For $\alpha, \beta \in V$

$$\begin{aligned} \alpha' \doteq \beta' &\supset \alpha \varepsilon \beta' \ \&\ \beta \varepsilon \alpha', \quad \text{by (ii)} \\ &\supset (\alpha \varepsilon \beta \vee \alpha \doteq \beta) \ \&\ (\beta \varepsilon \alpha \vee \beta \doteq \alpha) \\ &\supset \alpha \doteq \beta. \end{aligned}$$

The last step uses $(\alpha \varepsilon \beta \ \&\ \beta \varepsilon \alpha) \supset \bot$ which can be proved using 2.2.

2.11. THEOREM. For $n \in N$ let

$$\Delta(n) = R(n, \phi, (x, y)y').$$

Then $\Delta(n) \in V$ for $n \in N$, so that $\omega \in V$ where

$$\omega = (\sup x \in N)\Delta(x),$$

and (i) $\phi \varepsilon \omega$,

(ii) $(\forall \alpha \varepsilon \omega)(\alpha' \varepsilon \omega)$,

(iii) for every species F on V

$$F(\phi) \ \&\ (\forall x \varepsilon \omega)(F(x) \supset F(x')) \supset (\forall x \varepsilon \omega)F(x).$$

PROOF. As $\phi \in V$ and $\alpha' \in V$ for $\alpha \in V$ it follows that $\Delta(n) \in V$ for $n \in N$. As $N \in U$, $\omega \in V$.

(i) As $\phi \doteq \Delta(0)$, $\phi \varepsilon \omega$.

(ii) As $(\Delta(n))' \doteq \Delta(s(n))$ for $n \in N$, it follows that $(\Delta(n))' \varepsilon \omega$ for $n \in N$ and hence $(\forall \alpha \varepsilon \omega)(\alpha' \varepsilon \omega)$.

(iii) Assume $F(\phi)$ and $(\forall x \varepsilon \omega)(F(x) \supset F(x'))$. Then $F(\Delta(0))$ and $(\forall n \in N)(F(\Delta(n)) \supset F(\Delta(s(n))))$ so that by N-induction from 1.14 we get $(\forall n \in N)\ F(\Delta(n))$, i.e. $(\forall x \varepsilon \omega)\ F(x)$.

§3. THE CZF AXIOM SYSTEM

3.1. In this section I review the language and axioms of the system CZF of constructive set theory. It will then be clear that the results of the previous section show that the type V, with extensional equality and membership, is a model of CZF.

The language of CZF is essentially a standard one for set theory. As the underlying logic is to be intuitionistic, all the logical operations $\bot$ & $\vee$ $\supset$ $(\forall x \in V)$ $(\exists x \in V)$ will be treated as primitive. Note that I use $(\forall x \in V)$ and $(\exists x \in V)$ rather than the more customary $(\forall x)$ and $(\exists x)$. As usual $\neg\phi$ and $\phi \equiv \psi$ will abbreviate $\phi \supset \bot$ and $(\phi \supset \psi)$ & $(\psi \supset \phi)$ respectively. Both $x \varepsilon y$ and $x \doteq y$ will be treated as primitive atomic formulae. In addition I shall take as primitive the restricted quantifiers $(\forall x \varepsilon y)$ and $(\exists x \varepsilon y)$. A formula is restricted if it has been built up without using the quantifiers $(\forall x \in V)$ and $(\exists x \in V)$.

CZF is axiomatised using a standard axiomatisation of intuitionistic predicate logic. The remaining axioms are presented below.

3.2. STRUCTURAL AXIOMS

Restricted Quantifier axioms

(i) $\Phi \supset [\forall x \varepsilon y\, \phi[x] \equiv \forall x \in V(x \varepsilon y \supset \phi[x])]$

(ii) $\Phi \supset [\exists x \varepsilon y\, \phi[x] \equiv \exists x \in V(x \varepsilon y \;\&\; \phi[x])]$

for every formula $\phi[x]$, where Φ is

$$\forall x \in V[\phi[x] \supset \forall z \in V(x \doteq z \supset \phi[z])].$$

Extensionality axioms

(i) $(x \doteq y \;\&\; x \varepsilon z) \supset y \varepsilon z$

(ii) $x \doteq y \equiv \forall z \in V\, (z \varepsilon x \equiv z \varepsilon y)$.

Set Induction

$$\forall x \in V(\forall y \varepsilon x\, \phi[y] \supset \phi[x]) \supset \forall x \in V \phi[x],$$

for every formula $\phi[x]$.

3.3. SET EXISTENCE AXIOMS

Pairing

$$\forall \alpha \in V\, \forall \beta \in V\, \exists \gamma \in V\, \forall \eta \in V\, (\eta \varepsilon \gamma \equiv (\eta \doteq \alpha \vee \eta \doteq \beta))$$

<u>Union</u>

$$\forall\alpha \in V\ \exists\gamma \in V\ \forall\eta \in V\ (\eta\ \varepsilon\ \gamma \equiv \exists x\ \varepsilon\ \alpha\ (\eta\ \varepsilon\ x)).$$

<u>Restricted Separation</u>

$$\forall\alpha \in V\ \exists\gamma \in V\ \forall\eta \in V\ (\eta\ \varepsilon\ \gamma \equiv \exists x\ \varepsilon\ \alpha\ (\phi[x]\ \&\ \eta \doteq x))$$

for every restricted formula $\phi[x]$.

<u>Strong Collection</u>

$$\forall\alpha \in V\ (\forall x\ \varepsilon\ \alpha\ \exists y \in V\ \phi[x, y] \supset \exists z \in V\ \phi'[\alpha, z])$$

for every formula $\phi[x, y]$, where $\phi'[\alpha, z]$ is

$$\forall x\ \varepsilon\ \alpha\ \exists y\ \varepsilon\ z\ \phi[x, y]\ \&\ \forall y\ \varepsilon\ z\ \exists x\ \varepsilon\ \alpha\ \phi[x, y].$$

<u>Subset Collection</u>

$$\forall\alpha \in V\ \forall\beta \in V\ \exists\gamma \in V\ \forall u \in V\ (\forall x\ \varepsilon\ \alpha\ \exists y\ \varepsilon\ \beta\ \phi[x, y] \supset \exists z\ \varepsilon\ \gamma\ \phi'[\alpha, z])$$

for every formula $\phi[x, y]$ (that may contain free occurrences of the variable u).

<u>Infinity</u>

$$\exists\gamma \in V\ (\exists x\ \varepsilon\ \gamma\ \forall y\ \varepsilon\ x\ \bot\ \&\ \forall x\ \varepsilon\ \gamma\ \exists y\ \varepsilon\ \gamma\ \mathrm{succ}(x, y)$$

where $\mathrm{succ}(x, y)$ is

$$x\ \varepsilon\ y\ \&\ \forall u\ \varepsilon\ x\ (u\ \varepsilon\ y)\ \&\ \forall u\ \varepsilon\ y\ (u\ \varepsilon\ x \vee u \doteq y).$$

3.4. If $\phi[x_1, \ldots, x_n]$ is a formula, all of whose free variables have been displayed then by interpreting the formula in type theory it yields an n-place function assigning a proposition $\phi[\alpha_1, \ldots, \alpha_n]$ to each n-tuple $\alpha_1, \ldots, \alpha_n$ of elements of the type V. Note that when $\phi[x_1, \ldots, x_n]$ is restricted the proposition $\phi[\alpha_1, \ldots, \alpha_n]$ will always be small. I say that the formula $\phi[x_1, \ldots, x_n]$ is <u>valid</u> if the proposition $(\forall x_1 \in V) \ldots (\forall x_n \in V)\ \phi[x_1, \ldots, x_n]$ is true.

The language and axioms that we have given for CZF have been chosen so that the following result has as direct a proof as possible.

THEOREM. Every theorem of CZF is valid.

PROOF. The correctness of intuitionistic predicate logic has already been discussed in §1. The validity of the structural axioms follows from theorems 2.6, 2.7 and 2.2. For the set existence axioms use theorems 2.8, 2.9, 2.10 and 2.11. The details are left to the reader.

3.5. REMARKS. In the restricted quantifier axioms the formula Φ expresses that the species over V defined by the formula $\phi[x]$ is extensional. A routine induction on the way that the formula $\phi[x]$ is built up suffices to prove Φ using only the restricted quantifier and extensionality axioms. It follows that the assumption Φ can be dropped from the restricted quantifier axioms without altering CZF, so that the restricted quantifiers can be treated in the standard way. Because of this the restricted separation axiom can be rephrased in the more familiar form using $(\eta \in \alpha \ \& \ \phi[\eta])$ instead of $\exists x \in \alpha \ (\phi[x] \ \& \ \eta \doteq x)$.

§4. CHOICE PRINCIPLES FOR CONSTRUCTIVE SET THEORY

4.1. In this section we shall work exclusively in an informal framework for CZF. The standard conventions and notations of classical set theory will be used. So ordered pairs are defined as usual. The cartesian product $A \times B$ of the sets A, B can be shown to exist as the set

$$\bigcup\{\{<x, y> \mid y \in B\} \mid x \in A\}$$

using replacement (which is a consequence of strong collection) and the union axiom. More generally we can define the disjoint union $\Sigma(A, B)$ of a family B of sets indexed by the set A as the set

$$\bigcup\{\{<x, y> \mid y \in B(x)\} \mid x \in A\}.$$

The disjoint union $A + B$ of sets A, B is defined to be the set

$$\{<\phi, x> \mid x \in A\} \cup \{<\{\phi\}, y> \mid y \in B\}.$$

As usual a relation R is a set of ordered pairs whose domain is the set of x such that $<x, y> \in R$ and whose range is the set of y such that $<x, y> \in R$. A function f is a single valued relation, i.e. one where $y \doteq z$ whenever $<x, y>, <x, z> \in f$. f is a function from A to B if f is a function with domain A and range a subset of B. Above we have used the notion of a family B of sets indexed by the set A. B is simply a function with domain A.

4.2. INDUCTIVE DEFINITIONS

We shall use the informal notion of class as in classical set theory. For any class Φ the class X is <u>Φ-closed</u> if $A \subseteq X$ implies $a \in X$ for every pair $\langle a, A\rangle \in \Phi$. The following result is useful.

THEOREM. For any class Φ there is a smallest Φ-closed class $I(\Phi)$, called the class of Φ-generated sets.

PROOF SKETCH. Call a relation g <u>good</u> if whenever $\langle x, y\rangle \in g$ there is a set A such that $\langle y, A\rangle \in \Phi$ and

$$\forall y' \in A\ \exists x' \in x \quad \langle x', y'\rangle \in g.$$

Call a set <u>Φ-generated</u> if it is in the range of some good relation. To see that the class $I(\Phi)$ of Φ-generated sets is Φ-closed let A be a set of Φ-generated sets, where $\langle a, A\rangle \in \Phi$. Then

$$\forall y \in A\ \exists g\ \ (g \text{ is good } \&\ \exists x \in V\ (\langle x, y\rangle \in g)).$$

By strong collection there is a set G of good sets such that

$$\forall y \in A\ \exists g \in G\ \exists x \in V \langle x, y\rangle \in g.$$

Now if $\bar{g} \doteq \bigcup G \cup \{\langle \bar{x}, a\rangle\}$ where $\bar{x} \doteq \{x \mid \exists y \in V \langle x, y\rangle \in \bigcup G\}$ then $\bar{g}$ is good and $\langle \bar{x}, a\rangle \in \bar{g}$ so that a is Φ-generated. Thus $I(\Phi)$ is Φ-closed. Now if X is a Φ-closed class and g is good then an easy proof by set induction on x will show that

$$\langle x, y\rangle \in g \supset y \in X,$$

so that $I(\Phi) \subseteq X$.

4.3. THE SET OF NATURAL NUMBERS

This may be characterised as the unique set ω such that for every set x

$$x \in \omega \equiv (x \doteq \phi \vee \exists y \in \omega (x \doteq y')),$$

where ϕ is the empty set and y' is the set of z such that $z \in y \vee z \doteq y$. The existence of such a set ω follows from the axiom of infinity using restricted separation. Its uniqueness can be proved by set induction, as can the scheme of mathematical induction for ω. Our first choice principle is the following.

4.4. DEPENDENT CHOICES (DC)

$$\forall x \in V\ (\theta[x] \supset \exists y \in V\ (\phi[x, y]\ \&\ \theta[y])) \supset \forall \alpha \in V\ \exists \gamma \in V\ \Phi[\alpha, \gamma]$$

for all formulae $\theta[x]$ and $\phi[x, y]$. Here $\Phi[\alpha, \gamma]$ expresses the conjunction of the following statements.

(i) γ is a function with domain ω.

(ii) $\langle\phi, \alpha\rangle \in \gamma$.

(iii) $(\langle n, x\rangle \in \gamma\ \&\ \langle n', y\rangle \in \gamma) \supset (\phi[x, y]\ \&\ \theta[x])$ for all $n \in \omega$ and all sets x, y.

The following specialised form of DC may be reduced to a single axiom using strong collection.

LIMITED DEPENDENT CHOICES (LDC)

$$\forall x \in \beta\ \exists y \in \beta\ \phi[x, y] \supset \forall \alpha \in \beta\ \exists \gamma \in V\ \Phi[\alpha, \gamma]$$

for all formulae $\phi[x, y]$, where $\Phi[\alpha,\gamma]$ is defined as before except that $x \in \beta$ replaces $\theta[x]$.

4.5. For the next choice principle we need the

DEFINITION. The set A is a <u>base</u> if every relation with domain A extends a function with domain A.

The following principle was introduced in Aczel [1978].

PRESENTATION AXIOM (PA). Every set has a presentation, where a presentation of a set A is a function with range A whose domain is a base.

In Aczel [1978] it was observed that $PA \supset LDC \supset CC$, where CC (the axiom of countable choice) expresses that ω is a base.

4.6. The remainder of this section will be taken up with the formulation of a strengthening of PA. First recall from Aczel [1978] that Myhill's exponentiation axiom is a consequence of subset collection. So for any sets A, B we may form the set B^A of functions from A to B. More generally we may form as a set the cartesian product $\Pi(A, B)$ of any family B of sets indexed by a set A. In fact $\Pi(A, B)$ is the set

$$\{f \in C^A \mid \forall x \in A\ (f(x) \in B(x))\}$$

where $C = \bigcup\{B(x) \mid x \in A\}$. In the next definition $I(a, b)$ is the set $\{z \in \{\phi\} \mid a \doteq b\}$ so that

$$z \in I(a, b) \equiv (z \doteq \phi \ \&\ a \doteq b).$$

DEFINITION. Let $\Pi\Sigma I$ be the class of pairs $\langle C, D\rangle$ such that either

(i) $C \doteq \omega$ and $D \doteq \phi$,

or (ii) $C \doteq \Pi(A, B)$ or $C \doteq \Sigma(A, B)$, and $D \doteq \{A\} \cup \{B(x) \mid x \in A\}$ for some family B of sets indexed by A,

or (iii) $C \doteq I(a, b)$ and $D \doteq \{A\}$ for some set A and some $a, b \in A$.

Then a class X is $\Pi\Sigma I$-closed if

(i) $\omega \in X$,

(ii) $\Pi(A, B), \Sigma(A, B) \in X$ for all families B of sets in X indexed by a set A in X,

and (iii) $I(a, b) \in X$ for all $a, b \in A$ and every set A in X.

Note that any $\Pi\Sigma I$-closed class X is easily seen to have the following additional closure properties

(iv) $\phi, \{\phi\} \in X$

(v) $B^A, A \times B, A + B \in X$ whenever $A, B \in X$.

4.7. We can now formulate our final choice principles.

THE $\Pi\Sigma I$-AXIOM OF CHOICE ($\Pi\Sigma I$-AC)

Every $\Pi\Sigma I$-generated set is a base.

THE $\Pi\Sigma I$-PRESENTATION AXIOM ($\Pi\Sigma I$-PA).

Every $\Pi\Sigma I$-generated set is a base and every set has a $\Pi\Sigma I$-presentation, i.e. there is a function whose range is the set and whose domain is a $\Pi\Sigma I$-generated base.

Note that $\Pi\Sigma I$-PA is a simultaneous strengthening of $\Pi\Sigma I$-AC and PA. Also note that $\Pi\Sigma I$-AC implies that sets such as $\omega, \omega^\omega, \omega^{(\omega^\omega)}, \ldots$ are bases. It follows that the system $HA^\omega + AC + ext$ of finite type arithmetic has a standard interpretation in CZF + ΠΣI-AC.

4.8. We end the section with an interesting characterisation of the notion of base when assuming ΠΣI-PA.

THEOREM. (assuming ΠΣI-PA). A set is a base if and only if it is in one-one correspondence with a ΠΣI-generated set.

PROOF. Clearly every set in one-one correspondence with a base is itself a base. So using ΠΣI-AC we get one direction. For the other direction let B be a base. By ΠΣI-PA there is a function f with range B whose domain is a ΠΣI-generated set B'. As B is a base there is a function g from B to B' such that $f(g(b)) \doteq b$ for all $b \in B$. Then g is a one-one correspondence between B and $\{x \in B' \mid g(f(x)) \doteq x\}$, and this latter set is clearly in one-one correspondence with the set $\Sigma(B', F)$ where

$$F(x) \doteq I(g(f(x)), x) \quad \text{for} \quad x \in B'.$$

As B' is ΠΣI-generated, so is $F(x)$ for each $x \in B'$ so that $\Sigma(B', F)$ is also ΠΣI-generated. Hence B is in one-one correspondence with the ΠΣI-generated set $\Sigma(B', F)$.

§5. DEPENDENT CHOICES

The aim of this section is to prove the validity of each instance of the set theoretical axiom scheme of dependent choices formulated in 4.4. Note that a type theoretical version was proved in 1.15 and in order to apply that version to the interpretation of set theory we shall need the notion of an injectively presented set. Although this is not an extensional notion of set theory it turns out to be closely related to the extensional notion of a base and will play an essential role in this and the later sections. We shall continue to work informally in type theory following the style of §2. We shall need the standard set theoretical notions, described in §4, as interpreted in type theory. So for example the iterative set $\alpha \in V$ is a relation if

$$\forall \beta \in \alpha\ \exists \gamma \in V\ \exists \delta \in V\ (\beta \doteq \langle \gamma\ \ \delta \rangle)$$

In our work with relations the following function will be useful. If $\alpha, \beta \in V$ such that $\bar{\alpha} = \bar{\beta}$ then let

$$S(\alpha, \beta) = (\sup x \in \bar{\alpha})\ \langle \tilde{\alpha}(x), \tilde{\beta}(x) \rangle.$$

Note that $\bar{\alpha} \in U$ and $\tilde{\alpha}(x)$, $\tilde{\beta}(x) \in V$ for $x \in \bar{\alpha}$, so that $<\tilde{\alpha}(x), \tilde{\beta}(x)> \in V$ for $x \in \bar{\alpha}$. Hence $S(\alpha, \beta) \in V$.

5.1. LEMMA.

(i) If $\alpha, \beta \in V$ with $\bar{\alpha} = \bar{\beta}$ then $S(\alpha, \beta)$ is a relation with domain α and range β.

(ii) If $\alpha, \gamma \in V$ such that γ is a relation with domain α then, for some $\beta \in V$ with $\bar{\alpha} = \bar{\beta}$, $S(\alpha, \beta) \subseteq \gamma$.

PROOF. Let $\alpha \in V$ and let $A = \bar{\alpha}$.

(i) Let $\beta \in V$ such that $\bar{\beta} = A$ and let $\gamma = S(\alpha, \beta)$. Then, by choosing $x = y = u$,

$$\forall u \in A\ \exists x \in A\ \exists y \in A\ (\tilde{\gamma}(u) \doteq <\tilde{\alpha}(x), \tilde{\beta}(y)>),$$

so that

$$\forall u \in \gamma\ \exists x \in \alpha\ \exists y \in \beta\ (u \doteq <x, y>).$$

Hence γ is a relation whose domain is a subset of α and whose range is a subset of β. Also, by choosing $u = y = x$, we get

$$\forall x \in \alpha\ \exists u \in \gamma\ \exists y \in \beta\ (u \doteq <x, y>),$$

so that α is a subset of the domain of γ, and hence γ has domain α. Similarly γ has range β.

(ii) Let $\gamma \in V$ be a relation with domain α. Then $\forall x \in A\ \exists z \in V\ (<\tilde{\alpha}(x), z> \in \gamma)$. By the AC in 1.15 there is $b \in A \to V$ such that $\forall x \in A\ (<\tilde{\alpha}(x), b(x)> \in \gamma)$, so that if $\beta = \sup(A, b)$ then $\beta \in V$ such that $\bar{\beta} = \bar{\alpha}$ and $\forall x \in S(\alpha, \beta)\ (x \in \gamma)$.

5.2. DEFINITION. $\alpha \in V$ is <u>injectively presented</u> if for all $x_1, x_2 \in \bar{\alpha}$

$$\tilde{\alpha}(x_1) \doteq \tilde{\alpha}(x_2) \supset x_1 =_{\alpha} x_2.$$

5.3. LEMMA. Let $\alpha \in V$ be injectively presented.

(i) If $\beta \in V$, such that $\bar{\beta} = \bar{\alpha}$ and $\delta \in V$ then for all $x \in \bar{\alpha}$

$$(<\tilde{\alpha}(x), \delta> \in S(\alpha, \beta)) \equiv (\delta \doteq \tilde{\beta}(x)).$$

(ii) If $\gamma \in V$ then γ is a function with domain α if and only if $\gamma \doteq S(\alpha, \beta)$ for some $\beta \in V$ such that $\bar{\beta} = \bar{\alpha}$.

(iii) If $\beta_1, \beta_2 \in V$ such that $\bar{\beta}_1 = \bar{\beta}_2 = \bar{\alpha}$ then

$$(S(\alpha, \beta_1) \doteq S(\alpha, \beta_2)) \equiv \forall x \in \bar{\alpha}(\tilde{\beta}_1(x) \doteq \tilde{\beta}_2(x)).$$

PROOF. Let $\alpha \in V$ be injectively presented.

(i) Let $\beta \in V$ such that $\bar{\beta} = \bar{\alpha}$, $\delta \in V$ and $x \in \bar{\alpha}$. Then

$$\begin{aligned} <\alpha(x), \delta> \varepsilon S(\alpha, \beta) &\equiv \exists y \in \bar{\alpha}\ (<\tilde{\alpha}(x), \delta> \doteq <\tilde{\alpha}(y), \tilde{\beta}(y)>) \\ &\equiv \exists y \in \bar{\alpha}\ (\tilde{\alpha}(x) \doteq \tilde{\alpha}(y)\ \&\ \delta \doteq \tilde{\beta}(y)) \\ &\equiv \exists y \in \bar{\alpha}\ (x =_{\alpha} y\ \&\ \delta \doteq \tilde{\beta}(y)) \\ &\equiv \delta \doteq \tilde{\beta}(x). \end{aligned}$$

(ii) If $\gamma \in V$ is a function with domain α then it is certainly a relation with domain α so that by 5.1 (ii) there is $\beta \in V$ such that $\bar{\beta} = \bar{\alpha}$ and $S(\alpha, \beta) \subseteq \gamma$. As γ is a function with domain α and $S(\alpha, \beta)$ is a relation with domain α it follows that $S(\alpha, \beta) \doteq \gamma$. For the converse let $\gamma \doteq S(\alpha, \beta)$ where $\beta \in V$ such that $\bar{\beta} = \bar{\alpha}$. By 5.1 (i) γ is a relation with domain α. Also, for $x, y \in \bar{\alpha}$, if $<\tilde{\alpha}(x), \tilde{\beta}(y)> \varepsilon \gamma$ then, by (i), $\tilde{\beta}(y) \doteq \tilde{\beta}(x)$. Hence

$$\forall x \varepsilon \alpha\ \forall y_1 \varepsilon \beta\ \forall y_2 \varepsilon \beta\ (<x, y_1> \varepsilon \gamma\ \&\ <x, y_2> \varepsilon \gamma \supset y_1 \doteq y_2),$$

so that γ is a function with domain α.

(iii) Let $\beta_1, \beta_2 \in V$ such that $\bar{\beta}_1 = \bar{\beta}_2 = \bar{\alpha}$. Then

$$\begin{aligned} S(\alpha, \beta_1) \subseteq S(\alpha, \beta_2) &\equiv \forall x \in \bar{\alpha}\ (<\tilde{\alpha}(x), \tilde{\beta}_1(x)> \varepsilon S(\alpha, \beta_2)) \\ &\equiv \forall x \in \bar{\alpha}\ (\tilde{\beta}_1(x) \doteq \tilde{\beta}_2(x)). \end{aligned}$$

Similarly with β_1 and β_2 interchanged, giving the desired result.

5.4. THEOREM. Every injectively presented set is a base.

PROOF. Let $\alpha \in V$ be injectively presented and let $\gamma \in V$ be a relation with domain α. Then by 5.1 (ii) $S(\alpha, \beta) \subseteq \gamma$ for some $\beta \in V$ such that $\bar{\beta} = \bar{\alpha}$. By 5.3 (ii) $S(\alpha, \beta)$ is a function with domain α. Hence α is a base.

The next result gives some examples of injectively presented sets. A more extensive range of examples will be available in the next section.

5.5. LEMMA. The following are injectively presented.

(i) ϕ,

(ii) $\{\alpha\}$ for any $\alpha \in V$,

(iii) ω.

PROOF. (i) Recall that $\phi = (\sup z \in N_0)R_0(z)$. But, by N_0-existence in 1.17, $(\forall z \in N_0)\perp$ so that for all $z_1, z_2 \in N_0$ any proposition is true, and in particular

$$R_0(z_1) \doteq R_0(z_2) \supset z_1 =_{N_0} z_2.$$

So ϕ is injectively presented.

(ii) Recall that $\{\alpha\} = (\sup z \in N_1)R_1(z, \alpha)$. For $z_1, z_2 \in N_1$, $z_1 = z_2$ and hence $z_1 =_{N_1} z_2$ so that $R_1(z_1, \alpha) \doteq R_1(z_2, \alpha) \supset z_1 =_{N_1} z_2$. Hence $\{\alpha\}$ is injectively presented.

(iii) Recall that $\omega = (\sup z \in N)\Delta(z)$ where $\Delta(0) = \phi$ and $\Delta(s(n) = (\Delta(n))'$ for $n \in N$. We must show that for $n, m \in N$

$$\Delta(n) \doteq \Delta(m) \supset n =_N m.$$

This can be shown by a routine double N-induction, first on $n \in N$ and within that on $m \in N$. At the key steps 2.10 (iii) and 2.10 (iv) are needed.

By 5.4 and 5.5 (iii) ω is a base, and we have proved CC, the countable choice axiom. But we have the following stronger result.

5.6. THEOREM. Let B be an extensional species over V and let F be an extensional species over $V \times V$ (i.e. extensional in each argument) such that

$$\forall x \in V\ (B(x) \supset \exists y \in V\ (B(y)\ \&\ F(x, y))).$$

Then for each $\alpha \in V$ such that $B(\alpha)$ there is $\delta \in V$ such that δ is a function with domain ω, $<\phi, \alpha> \varepsilon\ \delta$ and for every $x \in \omega$ and all $\beta, \gamma \in V$

$$(<x, \beta> \varepsilon\ \delta\ \&\ <x', \gamma> \varepsilon\ \delta) \supset (B(\beta)\ \&\ F(\beta, \gamma)).$$

PROOF. Let $\alpha \in V$ such that $B(\alpha)$. Then by the type theoretical version of DC in 1.15 there is $c \in N \to V$ such that $c(0) = \alpha$ and for $n \in N$

$$(*) \qquad B(c(n))\ \&\ F(c(n), c(s(n))).$$

Let $\eta = \sup(N, c)$. Then $\eta \in V$ with $\bar{\eta} = \bar{\omega}$, so that if $\delta = S(\omega, \eta)$ then $\delta \in V$ and by 5.3 (ii), as ω is injectively presented, δ is a function with domain α. As $<\phi, \alpha> \doteq <\Delta(0), c(0)> \doteq <\tilde{\omega}(0), \tilde{\eta}(0)> \doteq \tilde{\delta}(0)$ it follows that $<\phi, \alpha> \varepsilon\ \delta$. Finally, let $x \varepsilon\ \omega$ and $\beta, \gamma \in V$ such that $<x, \beta> \varepsilon\ \delta$ and $<x', \gamma> \varepsilon\ \delta$. Then for some $n \in N$ $x \doteq \Delta(n)$, so that $x' \doteq \Delta(s(n))$ and hence, by 5.3 (i), $\beta \doteq c(n)$ and $\gamma \doteq c(s(n))$. Hence, by (*) and the assumption that B and F are extensional, we get $B(\beta)\ \&\ F(\beta, \gamma)$.

If we apply this result to the extensional predicates defined by formulae in the language of set theory we get the main result of this section.

5.7. THEOREM. The set theoretical DC is valid.

§6. THE $\Pi\Sigma$I-AXIOM OF CHOICE

The aim of this section is to show that every $\Pi\Sigma$I-generated set is a base. We do this using the following notion.

6.1. DEFINITION. $\alpha \in V$ is a <u>strong base</u> if $\alpha \doteq \beta$ for some injectively presented $\beta \in V$.

Note that this is an extensional version of the notion of an injectively presented set. It will be convenient to extend our use of the terminology associated with classes to such extensional notions, even though they may not be definable in the purely set-theoretical language. By the results in §2 the axiom schemes of CZF still apply to this wider context. As the notion of base is extensional it follows from 5.4 that every strong base is a base. Hence the result that we are aiming at will be a consequence of the result that every $\Pi\Sigma$I-generated set is a strong base, and for this it suffices to show that the class of strong bases is $\Pi\Sigma$I-closed. We shall need to formulate explicit intensional versions of the set theoretical $\Pi\Sigma$I operations.

In the following definitions we shall define $\Sigma(\alpha, \beta) \in V$ and $\Pi(\alpha, \beta) \in V$ for $\alpha, \beta \in V$ such that $\bar{\alpha} = \bar{\beta}$. We then show that when α is injectively presented then these are the disjoint union and cartesian product, respectively, of the family of sets $S(\alpha, \beta)$ indexed by the set α.

Let $\alpha, \beta \in V$ with $\bar{\alpha} = \bar{\beta}$.

6.2. DEFINITION OF $\Sigma(\alpha, \beta)$. As $\bar{\alpha} \in U$ and $\overline{\tilde{\beta}(x)} \in U$ for $x \in \bar{\alpha}$ it follows that $C \in U$, where $C = (\Sigma x \in \bar{\alpha})\ \overline{\tilde{\beta}(x)}$. For $z \in C$, $p(z) \in \bar{\alpha}$ so that $\tilde{\alpha}(p(z)) \in V$ and $\tilde{\beta}(p(z)) \in V$, $q(z) \in \overline{\tilde{\beta}(p(z))}$ so that $f(z) \in V$ where $f(z) = (\tilde{\beta}(p(z)))^{\sim}(q(z))$. Now define

$$\Sigma(\alpha, \beta) = (\sup z \in C) \langle\tilde{\alpha}(p(z)), f(z)\rangle.$$

Then $\Sigma(\alpha, \beta) \in V$.

6.3. DEFINITION OF $\Pi(\alpha, \beta)$. Note that $D \in U$, where $D = (\Pi x \in \bar{\alpha})\ \overline{\tilde{\beta}(x)}$. Let $z \in D$. For $x \in \bar{\alpha}$, $\tilde{\alpha}(x) \in V$, $\tilde{\beta}(x) \in V$ and $z(x) \in \overline{\tilde{\beta}(x)}$ so that

$(\tilde{\beta}(x))^{\sim}(z(x)) \in V$. Hence $g(z) \in V$ and $\overline{g(z)} = \bar{\alpha}$ where $g(z) = (\sup x \in \bar{\alpha})(\tilde{\beta}(x))^{\sim}(z(x))$. So $S(\alpha, g(z)) \in V$. Now define

$$\Pi(\alpha, \beta) = (\sup z \in D)\ S(\alpha, g(z)).$$

Then $\Pi(\alpha, \beta) \in V$.

6.4. THEOREM. Let $\alpha \in V$ be injectively presented and let $\beta \in V$ such that $\bar{\beta} = \bar{\alpha}$.

(i) $\Sigma(\alpha, \beta)$ is the disjoint union and $\Pi(\alpha, \beta)$ is the cartesian product of the family of sets $S(\alpha, \beta)$.

(ii) If $\tilde{\beta}(x)$ is injectively presented for all $x \in \bar{\alpha}$ then both $\Sigma(\alpha, \beta)$ and $\Pi(\alpha, \beta)$ are injectively presented.

PROOF. By 5.3 (ii) $S(\alpha, \beta)$ is a function with domain α, i.e. a family of sets indexed by the set α.

(i) Let $\eta \in V$. Then η is in the disjoint union of $S(\alpha, \beta)$

$$\begin{aligned}
&\equiv \exists x \varepsilon \alpha\, \exists \delta \in V\, (<x, \delta> \varepsilon S(\alpha, \beta)\ \&\ \exists y \varepsilon \delta\, (\eta \doteq <x, y>)) \\
&\equiv \exists x \in \bar{\alpha}\, \exists \delta \in V\, (<\tilde{\alpha}(x), \delta> \varepsilon S(\alpha, \beta)\ \&\ \exists y \varepsilon \delta\, (\eta \doteq <\tilde{\alpha}(x), y>)) \\
&\equiv \exists x \in \bar{\alpha}\, \exists \delta \in V\, (\delta \doteq \tilde{\beta}(x)\ \&\ \exists y \varepsilon \delta (\eta \doteq <\tilde{\alpha}(x), y>)) \\
&\equiv \exists x \in \bar{\alpha}\, \exists y \varepsilon \tilde{\beta}(x)\, (\eta \doteq <\tilde{\alpha}(x), y>) \\
&\equiv \exists z \in C\, (\eta \doteq <\tilde{\alpha}(p(z)), f(z)>) \\
&\equiv \eta \varepsilon \Sigma(\alpha, \beta).
\end{aligned}$$

The third of the above $\equiv$ uses 5.3 (i) and the fifth uses the Σ-existence principle of 1.17. For the cartesian product first note that by 5.3 (ii) η is a function with domain α if and only if

$$\exists \gamma \in V\, (\bar{\gamma} = \bar{\beta}\ \&\ \eta \doteq S(\alpha, \beta)).$$

Hence η is in the cartesian product of $S(\alpha, \beta)$ if and only if

$$\exists \gamma \in V\, (\bar{\gamma} = \bar{\beta}\ \&\ \eta \doteq S(\alpha, \gamma)\ \&\ F(\alpha, \beta, \gamma)),$$

where, if $\gamma \in V$ with $\bar{\gamma} = \bar{\beta}$,

$$F(\alpha, \beta, \gamma) = \forall x \varepsilon \alpha\, \exists \delta \in V\, (<x, \delta> \varepsilon S(\alpha, \beta)\ \&\ \exists y \varepsilon \delta(<x, y> \varepsilon S(\alpha, \gamma))).$$

Using 5.3 (i) twice, the AC from 1.15 and 5.3 (ii) we get that

$$\begin{aligned}
F(\alpha, \beta, \gamma) &\equiv \forall x \in \bar{\alpha}\, \exists \delta \in V\, (<\tilde{\alpha}(x), \delta> \varepsilon S(\alpha, \beta)\ \&\ \exists y \varepsilon \delta(<\tilde{\alpha}(x), y> \varepsilon S(\alpha, \gamma))) \\
&\equiv \forall x \in \bar{\alpha}\, \exists y \varepsilon \tilde{\beta}(x)\, (y \doteq \tilde{\gamma}(x)) \\
&\equiv \forall x \in \bar{\alpha}\, \exists y \in \overline{\tilde{\beta}(x)}\, ((\tilde{\beta}(x))^{\sim}(y) \doteq \tilde{\gamma}(x)) \\
&\equiv \exists z \in D\, \forall x \in \bar{\alpha}\, ((\tilde{\beta}(x))^{\sim}(z(x)) \doteq \tilde{\gamma}(x)) \\
&\equiv \exists z \in D\, (S(\alpha, g(z)) \doteq S(\alpha, \gamma)).
\end{aligned}$$

It follows that η is in the cartesian product of $S(\alpha, \beta)$ if and only if $\exists z \in D\ (\eta \doteq S(\alpha, g(z)))$, and hence if and only if $\eta \varepsilon \Pi(\alpha, \beta)$.

(ii) Let $\gamma = \Sigma(\alpha, \beta)$ and let $z_1, z_2 \in C$ such that $\tilde{\gamma}(z_1) \doteq \tilde{\gamma}(z_2)$. We must show that $z_1 =_C z_2$. Let $x_i = p(z_i)$ and $y_i = q(z_i)$ for $i = 1, 2$. As $\tilde{\gamma}(z_1) \doteq \tilde{\gamma}(z_2)$ it follows that

$$<\tilde{\alpha}(x_1),\ (\tilde{\beta}(x_1))^{\sim}(y_1)> \doteq <\tilde{\alpha}(x_2),\ (\tilde{\beta}(x_2))^{\sim}(y_2)>$$

so that

$$\tilde{\alpha}(x_1) \doteq \tilde{\alpha}(x_2)$$
$$(\tilde{\beta}(x_1))^{\sim}(y_1) \doteq (\tilde{\beta}(x_2))^{\sim}(y_2).$$

As α is injectively presented $x_1 =_{\bar{\alpha}} x_2$ and hence

$$(\tilde{\beta}(x_1))^{\sim}(y_1) \doteq (\tilde{\beta}(x_1))^{\sim}(y_2).$$

As $\tilde{\beta}(x_1)$ is injectively presented $y_1 =_B y_2$ where $B = \overline{\tilde{\beta}(x_1)}$. Hence $z_1 =_C (x_1, y_1) =_C (x_2, y_2) =_C z_2$. Thus $\Sigma(\alpha, \beta)$ is injectively presented. Now let $\gamma = \Pi(\alpha, \beta)$ and let $z_1, z_2 \in D$ such that $\tilde{\gamma}(z_1) \doteq \tilde{\gamma}(z_2)$. We must show that $z_1 =_D z_2$. Note that $\tilde{\gamma}(z_i) = S(\alpha, g(z_i)) = (\sup x \in \bar{\alpha})<\tilde{\alpha}(x),\ (g(z_i))^{\sim}(x)>$. Hence, as $\tilde{\gamma}(z_1) \subseteq \tilde{\gamma}(z_2)$,

$$(*) \qquad \forall x_1 \in \bar{\alpha}\ \exists x_2 \in \bar{\alpha}\ (<\tilde{\alpha}(x_1),\ (g(z_1))^{\sim}(x_1)> \doteq <\tilde{\alpha}(x_2),\ (g(z_2))^{\sim}(x_2)>).$$

But if $\tilde{\alpha}(x_1) \doteq \tilde{\alpha}(x_2)$ then $x_1 =_{\bar{\alpha}} x_2$, so that if also $g(z_1))^{\sim}(x_1) \doteq (g(z_2))^{\sim}(x_2)$ then $(\tilde{\beta}(x_1))^{\sim}(z_1(x_1)) \doteq (\tilde{\beta}(x_1))^{\sim}(z_2(x_1))$, and as $\tilde{\beta}(x_1)$ is injectively presented, $z_1(x_1) =_{B(x_1)} z_2(x_1)$ where $B(x_1) = \overline{\tilde{\beta}(x_1)}$. Hence it follows from (*) that

$$\forall x_1 \in \bar{\alpha}\ \exists x_2 \in \bar{\alpha}\ (x_1 =_{\bar{\alpha}} x_2\ \&\ z_1(x_1) =_{B(x_1)} z_2(x_1)),$$

so that

$$\forall x \in \bar{\alpha}\ (z_1(x) =_{B(x)} z_2(x)),$$

which yields $z_1 =_D z_2$ using the extensionality principle 1.16.

The following result, needed in §7, can be proved along the lines of the previous result.

6.5. LEMMA. For $\alpha, \beta \in V$, $\alpha + \beta \in V$ where

$$\alpha + \beta = (\sup z \in \bar{\alpha} + \bar{\beta})\ D(z,\ (x)<\phi,\ \tilde{\alpha}(x)>,\ (y)<\{\phi\},\ \tilde{\beta}(y)>),$$

and

(i) $\alpha + \beta$ is the disjoint union of α and β,

(ii) if α and β are injectively presented then so is $\alpha + \beta$.

The next result will be needed for the next theorem and also in §7.

6.6. LEMMA. For $A \in U$ and $a, b \in A$, $\hat{I}(A, a, b) \in V$ where

$$\hat{I}(A, a, b) = (\sup z \in I(A, a, b))\phi,$$

and

(i) $\hat{I}(A, a, b)$ is injectively presented,

(ii) if $\alpha \in V$ is injectively presented and $\bar{\alpha} = A$ then for all $\eta \in V$

$$\eta \in \hat{I}(A, a, b) \equiv (\eta \doteq \phi \ \& \ \tilde{\alpha}(a) \doteq \tilde{\alpha}(b)).$$

PROOF. As $I(A, a, b) \in U$ and $\phi \in V$ it follows that $\hat{I}(A, a, b) \in V$

(i) Let $\gamma = \hat{I}(A, a, b)$ and let $z_1, z_2 \in I(A, a, b)$ such that $\tilde{\gamma}(z_1) \doteq \tilde{\gamma}(z_2)$. We must show that $z_1 =_{\bar{\gamma}} z_2$. But, as $z_1, z_2 \in I(A, a, b)$, $z_1 = r = z_2$ so that $z_1 =_{\bar{\gamma}} z_2$.

(ii) As $\alpha \in V$ is injectively presented and $a, b \in A = \bar{\alpha}$

$$\tilde{\alpha}(a) \doteq \tilde{\alpha}(b) \equiv a =_A b.$$

Hence for $\eta \in V$

$$\begin{aligned} \eta \in \hat{I}(A, a, b) &\equiv \exists z \in I(A, a, b)\ (\eta \doteq \phi) \\ &\equiv (a =_A b \ \& \ \eta \doteq \phi) \\ &\equiv (\eta \doteq \phi \ \& \ \tilde{\alpha}(a) \doteq \tilde{\alpha}(b)). \end{aligned}$$

6.7. THEOREM. The class of strong bases is $\Pi\Sigma I$-closed.

PROOF. ϕ is injectively presented by 5.5 and hence is a strong base. Let $\delta \in V$ be a family of strong bases indexed by a strong base. We wish to show that the cartesian product and disjoint union of the family are also strong bases. Choose $\alpha \in V$ such that δ is a function with domain α. Without loss we may assume that α is injectively presented. For each $x \in \bar{\alpha}$ there is an injectively presented $y \in V$ such that $\langle\tilde{\alpha}(x), y\rangle \in \delta$. By the type theoretic AC of 1.15 there is $f \in \bar{\alpha} \to V$ such that, for each $x \in \bar{\alpha}$, $f(x)$ is injectively presented and $\langle\tilde{\alpha}(x), f(x)\rangle \in \delta$. Then $\beta \in V$ and $\bar{\beta} = \bar{\alpha}$ where $\beta = \sup(\bar{\alpha}, f)$, and $\tilde{\beta}(x)$ is injectively presented for $x \in \bar{\alpha}$. By 5.3 (ii) $S(\alpha, \beta)$ is a function with domain α. As $S(\alpha, \beta) \subseteq \delta$ and δ is a function with domain α we must have $S(\alpha, \beta) \doteq \delta$. By 6.4 both $\Pi(\alpha, \beta)$ and $\Sigma(\alpha, \beta)$ are injectively presented and are the cartesian product and disjoint union of $S(\alpha, \beta)$, i.e. of δ. Hence the cartesian product and disjoint union of δ are strong bases. It remains to show that if $\alpha \in V$ is a strong base and $\beta_1, \beta_2 \in V$ such that $\beta_1, \beta_2 \in \alpha$ then there is a strong base $\gamma \in V$ such that for all $\eta \in V$

$$\eta \in \gamma \equiv (\eta \doteq \phi \ \&\ \beta_1 \doteq \beta_2).$$

Without loss we may assume that α is injectively presented and that $\beta_i = \tilde{\alpha}(a_i)$ where $a_i \in \bar{\alpha}$ for $i = 1, 2$. By the lemma it suffices to let $\gamma = \hat{I}(\bar{\alpha}, a_1, a_2)$.

6.8. THEOREM. The $\Pi\Sigma$I-axiom of choice is valid.

PROOF. By the previous theorem every $\Pi\Sigma$I-generated set is a strong base and hence is a base.

§7. THE $\Pi\Sigma$I-PRESENTATION AXIOM

The main aim of this final section is to show that every set has a $\Pi\Sigma$I-presentation. This is done by coding each small type A as an injectively presented $\Pi\Sigma$I-generated set $\tau(A)$ such that $\overline{\tau(A)} = A$. It then easily follows that for each set α, the set $S(\tau(\bar{\alpha}), \alpha)$ is a function with range α and domain the $\Pi\Sigma$I-generated set $\tau(\bar{\alpha})$. The section ends with a result giving several characterisations of the notion of a base.

7.1. THEOREM. There is a function $\tau \in U \to V$ such that for $A, B \in U$, $F \in A \to U$ and $a, b \in A$

$$\begin{aligned} \tau(N_0) &= \phi \\ \tau(N) &= \omega \\ \tau(\Pi(A, F)) &= \Pi(\tau(A), (\sup x \in A)\tau(F(x))) \\ \tau(\Sigma(A, F)) &= \Sigma(\tau(A), (\sup x \in A)\tau(F(x))) \\ \tau(A + B) &= \tau(A) + \tau(B) \\ \tau(I(A, a, b)) &= \hat{I}(A, a, b). \end{aligned}$$

Moreover $\overline{\tau(A)} = A$ for all $A \in U$.

Note that the symbols Π, Σ and $+$ that occur on the right hand side of these equations refer to the operations on V introduced in §6.

PROOF. Define $\tau(A) = \sup(A, \sigma(A))$ for $A \in U$ where $\sigma \in (\Pi A \in U)(A \to V)$ is defined by transfinite recursion over U so that

$$\begin{aligned} \sigma(N_0) &= R_0 \\ \sigma(N) &= \Delta \\ \sigma(\Pi(A, F)) &= (z)(\sup x \in A)\langle\sigma(A)(z), \sigma(F(x))(z(x))\rangle \\ \sigma(\Sigma(A, F)) &= (z)\langle\sigma(A)(p(z)), \sigma(F(p(z)))(q(z))\rangle \\ \sigma(A + B) &= (z)D(z, (x)\langle\phi, \sigma(A)(x)\rangle, (y)\langle\{\phi\}, \sigma(B)(y)\rangle) \end{aligned}$$

$$\sigma(I(A, a, b)) = (z)\phi$$

for $A, B \in U$, $F \in A \to U$ and $a, b \in A$. The required equations for τ now follow using the defintions of ϕ, ω, Π, Σ, $+$, $\hat{I}$ given in §6. Note that it would be incorrect to use the equations for τ to directly define τ by transfinite recursion over U. That would only work if we had that $\Pi(\alpha, \beta) \in V$ and $\Sigma(\alpha, \beta) \in V$ for $\alpha, \beta \in V$ without the assumption that $\bar{\alpha} = \bar{\beta}$.

7.2. THEOREM. For all $A \in U$ the set $\tau(A)$ is injectively presented and $\Pi\Sigma I$-generated.

PROOF. Call $A \in U$ good if $\tau(A)$ is injectively presented and $\Pi\Sigma I$-generated. We show that every $A \in U$ is good by U-induction (see 1.14). First note that N_0 and N are good by 5.5. As induction hypothesis assume that $A, B \in U$ are good and that $F \in A \to U$ such that $F(x)$ is good for $x \in A$. That $\Pi(A, F)$ and $\Sigma(A, F)$ are good follows from 6.4. By 6.5 $A + B$ is good and by 6.6 $I(A, a, b)$ is good for $a, b \in A$.

7.3. THEOREM. For each $\alpha \in V$ the set $S(\tau(\bar{\alpha}), \alpha)$ is a $\Pi\Sigma I$-presentation of α.

PROOF. Let $\alpha \in V$ and let $\beta = \tau(\bar{\alpha})$. Then $\beta \in V$, $\bar{\beta} = \bar{\alpha}$ and β is injectively presented. So by 5.1 (i) and 5.3 (ii) $S(\beta, \alpha) \in V$ is a function with domain β and range α. As, by 7.2, β is $\Pi\Sigma I$-generated the result follows.

As a consequence of this theorem and 6.8 we have the main result.

7.4. THEOREM. The $\Pi\Sigma I$-presentation axiom is valid.

We next give a type theoretic characterisation of the notion of a $\Pi\Sigma I$-generated set.

7.5. THEOREM. A set is $\Pi\Sigma I$-generated if and only if it is extensionally equal to the set $\tau(A)$ for some $A \in U$.

PROOF. The implications from right to left follows from 7.2. For the converse implication, call a set U-generated if it is extensionally equal to $\tau(A)$ for some $A \in U$. It suffices to show that the class of U-generated sets is $\Pi\Sigma I$-closed. Clearly ω is U-generated because $\omega = \tau(N)$. Now suppose that $\delta \in V$ is a family of U-generated sets indexed by a U-generated set. Then for some $A \in U$ δ is a function with domain $\tau(A)$. So

$$\forall x \in \tau(A)\ \exists y \in U\ (\langle x, \tau(y)\rangle \in \delta),$$

and hence

$$\forall x \in A\ \exists y \in U\ (\langle(\tau(A))^{\sim}(x),\ \tau(y)\rangle \varepsilon\ \delta).$$

By the type theoretic AC from 1.15 there is $F \in A \to U$ such that

$$\forall x \in A\ (\langle(\tau(A))^{\sim}(x),\ \tau(F(x))\rangle \varepsilon\ \delta).$$

It follows that

$$S(\tau(A),\ (\sup x \in A)\tau(F(x)))$$

is a subset of δ, and hence is extensionally equal to δ, as both are functions with domain $\tau(A)$. From this it follows that the cartesian product and disjoint union of δ are the U-generated sets $\tau(\Pi(A, F))$ and $\tau(\Sigma(A, F))$ respectively. Finally let $\delta \in V$ be U-generated and let $\alpha, \beta \in V$ such that $\alpha, \beta\ \varepsilon\ \delta$. As δ is U-generated it is extensionally equal to $\tau(A)$ for some $A \in U$. So for some $a, b \in A$ $\alpha \doteq \tau(A)(a)$ and $\beta \doteq \tau(A)(b)$. Let $\gamma = \tau(I(A, a, b)) = \hat{I}(A, a, b)$. Then $\gamma \in V$, and for $\eta \in V$

$$\eta\ \varepsilon\ \gamma \equiv (\eta \doteq \phi\ \&\ \alpha \doteq \beta)$$

so that the U-generated set γ is the set $I(\alpha, \beta)$ of 4.5.

We end with the promised characterisations of the notion of a base.

7.6. THEOREM. For $\alpha \in V$ the following are equivalent

(i) α is in one-one correspondence with some $\Pi\Sigma I$-generated set.

(ii) α is in one-one correspondence with some strong base.

(iii) α is a strong base.

(iv) α is a base.

PROOF. We show that (i) $\supset$ (ii) $\supset$ (iii) $\supset$ (iv) $\supset$ (i). (i) $\supset$ (ii) follows from 6.5. For (ii) $\supset$ (iii) let α be in one-one correspondence with the strong base β. Without loss we may assume that β is injectively presented. By our assumption there is $\gamma \in V$ such that γ is a one-one function with domain β and range α. By 5.1 and 5.3 it follows that $\gamma \doteq S(\beta, \delta)$ for some $\delta \in V$ such that $\bar{\delta} = \bar{\beta}$ and $\delta \doteq \alpha$. Hence, as γ is one-one and β is injectively presented, if $y_1, y_2 \in \bar{\beta}$

$$\begin{aligned}\tilde{\delta}(y_1) \doteq \tilde{\delta}(y_2) &\supset \tilde{\beta}(y_1) \doteq \tilde{\beta}(y_2)\\ &\supset y_1 =_{\bar{\beta}} y_2,\end{aligned}$$

so that δ is injectively presented and hence α is a strong base. (iii) $\supset$ (iv) is a consequence of 5.4. By 7.4 we may use 4.6 to get (iv) $\supset$ (i).

REFERENCES

Aczel, P. [1978] The type theoretic interpretation of constructive set theory, in Logic Colloquium '77, eds. A. Macintyre, L. Pacholski and J. Paris, North Holland.

Bishop, E. [1967] Foundations of Constructive Analysis, McGraw Hill.

Bridges, D.S. [1979] Constructive Functional Analysis, Research Notes in Mathematics, Vol.28, Pitman.

Diaconescu, R. [1975] Axiom of choice and complementation. Proc. Amer. Math. Soc., Vol.51, pp.176-178.

Martin-Löf, P. [1975] An intuitionistic theory of types: Predicative part, in Logic Colloquium '73, eds. H.E. Rose and J.C. Sheperdson, North Holland, pp.73-118.

Martin-Löf, P. [1979] Constructive Mathematics and Computer Programming. To appear in the Proceedings of the 6th International Congress for Logic, Methodology and Philosophy of Science at Hannover in 1979.

Myhill, J. [1975] Constructive Set Theory, J.S.L., Vol.40, pp.347-382.