Logic Colloquium '77
A. Macintyre, L. Pacholski, J. Paris (eds.)

THE TYPE THEORETIC INTERPRETATION OF CONSTRUCTIVE SET THEORY*

Peter Aczel
Manchester University
England

By adding to Martin-Löf's intuitionistic theory of types a 'type of sets' we give a constructive interpretation of constructive set theory. This interpretation is a constructive version of the classical conception of the cumulative hierarchy of sets.

INTRODUCTION

Intuitionistic mathematics can be structured into two levels. The first level arises directly out of Brouwer's criticism of certain methods and notions of classical mathematics. In particular the notion of 'truth' that gives rise to the law of excluded middle was rejected and instead the meaning of mathematical statements was to be based on the notion of 'proof'. While implicit in this first level of intuitionism was a theory of meaning quite different from the classical one, it was nevertheless the case that the body of mathematics that could be developed within this level remained a part of classical mathematics. Because Brouwer felt that Mathematical analysis could not be developed adequately on this basis he was led to formulate his own conception of the continuum. This conception involved the mathematical treatment of incompletely specified objects such as free choice sequences. The second level of intuitionism builds on the first level but also includes these radical ideas that turn out to be incompatible with classical mathematics. Although considerable effort has been made over the years to make these ideas more transparent they have remained rather obscure to most mathematicians and the mathematics based on them has had a very limited following.

Since Bishop's book [3] appeared, it has become clear that, in spite of Brouwer's views, constructive analysis can be developed perfectly adequately while staying within the first level of intuitionism. This fact has led to a renewed

*The ideas for this paper were germinating during a visit to Caltech, supported by NSF grant MPS 75-07562 , and came to fruition while visiting Utrecht University. The results were first announced in an abstract for the 1976 Oxford Logic Colloquium.

interest in this part of intuitionism. The desire has been to find an analogue, for Bishop's constructive mathematics, of the generally accepted formal system ZF for classical mathematics. Several approaches have been tried and there has been some controversy over their relative merits. Two such approaches are 'Constructive Set Theory' (see [7] and [13] and 'Intuitionistic Type theory' (see [11]). In this paper we take the view that these, and perhaps other approaches, are not necessarily in conflict with each other. Constructive set theory suppresses all explicit constructive notions in order to be as familiar as possible to the classical mathematician. On the other hand type theory aims to give a rigorous foundation for the primitive notions of constructive mathematics.

The appeal of Bishop's book is that it wastes little time on the analysis of constructive concepts but instead developes analysis in a language mostly familiar to the classical mathematician. In constructive set theory this is taken a stage further. As in ZF there are just the notions of set and set membership with an axiom system that is a subsystem of ZF using intuitionistic logic, and including the axiom of extensionality. In such a system the direct constructive content of Bishop's notions has been lost and there arises the crucial question: What is the constructive meaning of the notion of set used in constructive set theory? We aim to answer that question in this paper. What is needed is a rigorous framework in which the primitive notions of constructive mathematics are directly displayed, together with a natural interpretation of constructive set theory in that framework. We shall give such a framework based on the intuitionistic type theory of [11]. We could have taken instead a system of 'Explicit Mathematics' (see [5] and [2]). But systems of Explicit mathematics leave the logical notions unanalysed, whereas type theory is a logic free theory of constructions within which the logical notions can be defined. For this reason we consider type theory to be more fundamental.

The axiom system CZF (Constructive ZF) is set out in §1 and some elementary properties are given in §2. The system is closely related to the systems considered by Myhill and Friedman in their papers. In §3 we summarise the type theoretic notions of [11] and introduce the type of sets. The interpretation of CZF is set up in §4 and its correctness is proved in §5 and §6. Finally in §7 we consider a new principle of choice for constructive set theory.

Formally, the type of sets was first introduced by Leversha in [10] where it was used to give a complicated type theoretic interpretation of Myhill's original formulation of constructive set theory in [13]. Unfortunately it was not realised at that time that the type itself gave a constructive notion of set. Instead it was only used as an appropriate constructive notion of ordinal to use in indexing the stages of Leversha's construction.

1. THE AXIOM SYSTEM CZF

We formulate CZF in a first order language $\mathcal{L}$ having the logical primitives $\bot, \vee, \wedge, \rightarrow, \forall x, \exists x$, the restricted quantifiers $(\forall x \varepsilon y)$, $(\exists x \varepsilon y)$ and the binary relation symbols ε and $=$. We assume a standard axiomatisation of intuitionistic logic. The remaining axioms of CZF are divided into two groups.

Structural axioms

Defining schemes for the restricted quantifiers.

$$(\forall x \varepsilon y)\phi(x) \longleftrightarrow \forall x(x \varepsilon y \rightarrow \phi(x))$$
$$(\exists x \varepsilon y)\phi(x) \longleftrightarrow \exists x(x \varepsilon y \wedge \phi(x))$$

Equality axioms.

$$x = y \longleftrightarrow \forall z(z \varepsilon x \leftrightarrow z \varepsilon y)$$
$$x = y \wedge y \varepsilon z \longrightarrow x \varepsilon z$$

Set Induction scheme.

$$\forall y[(\forall x \varepsilon y)\phi(x) \longrightarrow \phi(y)] \longrightarrow \forall x \phi(x)$$

Set existence axioms

Pairing. $\exists z(x \varepsilon z \wedge y \varepsilon z)$

Union. $\exists z(\forall y \varepsilon x)(\forall u \varepsilon y)(u \varepsilon z)$

Restricted Separation. For restricted $\phi(x)$

$$\exists z[(\forall y \varepsilon z)(y \varepsilon x \wedge \phi(y)) \wedge (\forall y \varepsilon x)(\phi(y) \rightarrow y \varepsilon z)]$$

If $\phi(x,y)$ is a formula let $\phi'(a,b)$ denote $(\forall x \varepsilon a)(\exists y \varepsilon b)\phi(x,y) \wedge (\forall y \varepsilon b)(\exists x \varepsilon a)\phi(x,y)$.

Strong Collection

$$(\forall x \varepsilon a)\exists y \phi(x,y) \longrightarrow \exists b \phi'(a,b)$$

Subset Collection

$$\exists c \forall u[(\forall x \varepsilon a)(\exists y \varepsilon b)\phi(x,y) \longrightarrow (\exists d \varepsilon c)\phi'(a,d)]$$

where u may occur free in $\phi(x,y)$.

Infinity. $\exists z \mathrm{Nat}(z)$

where Nat(z) is the conjunction of $(\forall x \varepsilon z)(\mathrm{Zero}(x) \vee (\exists y \varepsilon z)\mathrm{Succ}(y,x))$, $(\exists x \varepsilon z)\mathrm{Zero}(x)$ and $(\forall y \varepsilon z)(\exists x \varepsilon z)\mathrm{Succ}(y,x)$. Here Zero(x) is $(\forall y \varepsilon x)\bot$ and Succ(y,x) is $(\forall z \varepsilon y)(z \varepsilon x) \wedge y \varepsilon x \wedge (\forall z \varepsilon x)(z \varepsilon y \vee z = y)$.

Remarks. Our formulation has been designed to make the correctness proof for our interpretation as smooth as possible. The axioms could have been written in a more standard way. Our formulation of the axiom of infinity expresses the existence of a set ω such that

$$n \varepsilon \omega \longleftrightarrow n = \emptyset \vee (\exists m \varepsilon \omega)(n = m \cup \{m\}).$$

The mathematical induction scheme can be proved in CZF using set induction. Recall that in the usual way strong collection implies replacement. Ordinary collection is not good enough in the presence of only restricted separation. The significance of subset collection will become clear in the next section.

2. ELEMENTARY PROPERTIES OF CZF

We give some simple results that spell out the relationship of CZF to ZF. In particular we reformulate the subset collection scheme as a single axiom and bring out its relationship to the power set axiom and Myhill's exponentiation axiom. We show that ZF results from CZF by adding classical logic.

We use standard set theoretic notation and definitions. So ordered pairs $\langle x,y\rangle$, cartesian products $A\times B$ and the notion of a function $f: A\to B$ etc... are all defined as usual. Let $R: A \prec B$ if $R\subseteq A\times B$ such that $(\forall x\in A)(\exists y\in B)\langle x,y\rangle\in R$, and let $R: A \succ\!\prec B$ if in addition $(\forall y\in B)(\exists x\in A)\langle x,y\rangle\in R$. A set C of subsets of B is <u>A - full</u> if $R: A\prec B$ implies that $R: A\succ\!\prec D$ for some $D\in C$.

Results 2.1-2.6 will be proved informally inside the system CZF^- of CZF without subset collection.

<u>2.1. PROPOSITION</u>. The subset collection scheme is equivalent to the axiom:

$$\forall A\forall B\exists C(C \text{ is an } A - \text{full set of subsets of } B)$$

<u>PROOF</u>. The above axiom is an immediate consequence of the special instance of subset collection where $\phi(x,y)$ expresses $\langle x,y\rangle\in u$. For the converse, let C be an A - full set of subsets of B and suppose that $(\forall x\in A)(\exists y\in B)\phi(x,y)$. We show that $\phi'(A,D)$ for some $D\in C$. Let $\psi(x,z)$ denote $(\exists y\in B)(\phi(x,y) \wedge \langle x,y\rangle = z)$. Then $(\forall x\in A)\exists z\psi(x,z)$ so that by strong collection there is a set R such that $(\forall x\in A)(\exists z\in R)\psi(x,z) \wedge (\forall z\in R)(\exists x\in A)\psi(x,y)$. Hence $R: A\prec B$ and $\forall x\forall y(\langle x,y\rangle\in R\to\phi(x,y))$. As C is an A - full set of subsets of B we can find $D\in C$ such that $R: A\succ\!\prec D$. It follows that $\phi'(A,D)$.

<u>2.2. PROPOSITION</u>. The power set axiom implies subset collection, which in turn implies the exponentiation axiom:

$$\forall A\forall B\exists C(C \text{ is the set of functions from } A \text{ to } B).$$

<u>PROOF</u>. If C is the powerset of B then it is trivially an A - full set of subsets of B. Hence the first implication. For the second one, let C be an A - full set of subsets of $A\times B$. If $f: A\to B$ then $f': A\to A\times B$ where $f'(x) = \langle x,f(x)\rangle$ for $x\in A$. Then $f': A\prec A\times B$ and hence there is a set $D\in C$ such that $f': A\succ\!\prec D$. As f' is a function, $D = \{f'(x)\mid x\in A\} = f$, so that $f\in C$. So, using restricted separation we can define the set of functions from A to B as $\{f\in C\mid f \text{ is a function from } A \text{ to } B\}$.

<u>Remarks</u>. The power set axiom is much stronger than subset collection, as CZF can be interpreted in weak subsystems of analysis while simple type theory can be interpreted in CZF with the power set axiom. I do not know if subset collection is a consequence of the exponentiation axiom (although it is easily seen to be, in the presence of the presentation axiom of §7.) It seems unlikely.

<u>2.3. PROPOSITION</u>. The power set axiom is equivalent to the exponentiation axiom combined with the axiom: $\{\emptyset\}$ has a power set.

<u>PROOF</u>. One direction is clear. For the other, let B be the power set of $\{\emptyset\}$. For any set A let $C = \{\{x\in A\mid\emptyset\in f(x)\}\mid f\in{}^{A}B\}$ where ${}^{A}B$ is the set of functions from A to B. This is a set by the exponentiation axiom, restricted separation and

replacement. Clearly C is a set of subsets of A. If $z \subseteq A$ let $f(x) = \{y \in \{\emptyset\} | x \in z\}$ for $x \in A$. Then $f \in {}^A B$ and hence $z = \{x \in A | \emptyset \in f(x)\} \in C$. Hence C is the power set of A.

2.4. PROPOSITION. The exponentiation axiom and restricted excluded middle, $(\phi \vee \neg \phi)$ for all restricted ϕ, together imply the powerset axiom.

PROOF. By 2.3 it suffices to show that $\{\emptyset\}$ has a power set. In fact we show that $\{\emptyset, \{\emptyset\}\}$ is its power set. So let $x \subseteq \{\emptyset\}$. By hypothesis $\emptyset \in x \vee \emptyset \notin x$. If $\emptyset \in x$ then $x = \{\emptyset\}$. If $\emptyset \notin x$ then $x = \emptyset$. In either case $x \in \{\emptyset, \{\emptyset\}\}$.

Remark. It follows that the implications of 2.2. can be replaced by equivalences in the presence of restricted excluded middle.

2.5. PROPOSITION. Restricted excluded middle is equivalent to the axiom: $\forall x(\emptyset \in x \vee \emptyset \notin x)$.

PROOF. One direction is trivial. For the other let ϕ be a restricted formula. Then we may define the set $x = \{y \in \{\emptyset\} | \phi\}$ where y is not free in ϕ. Then $\emptyset \in x \leftrightarrow \phi$, so that by the axiom $\phi \vee \neg \phi$.

2.6. PROPOSITION. The full separation scheme is equivalent to the scheme: $\exists x(\phi \leftrightarrow \emptyset \in x)$ where x is not free in ϕ.

PROOF. Given full separation and a formula ϕ let $x = \{y \in \{\emptyset\} | \phi\}$ where y is not free in ϕ. Then $\emptyset \in x \leftrightarrow \phi$. Conversely let A be a set and $\phi(y)$ a formula. By assumption there is a set x such that $\phi(y) \leftrightarrow \emptyset \in x$, for each $y \in A$. We may assume that $x \subseteq \{\emptyset\}$ in which case x is uniquely determined by $y \in A$. By strong collection there is a function f defined on A such that $(\forall y \in A)(\phi(y) \leftrightarrow \emptyset \in f(y))$. By restricted separation we can form the set $\{y \in A | \emptyset \in f(y)\}$. But this set is $\{y \in A | \phi(y)\}$ so that we have proved the full separation scheme.

2.7. PROPOSITION. The following systems have the same theorems.

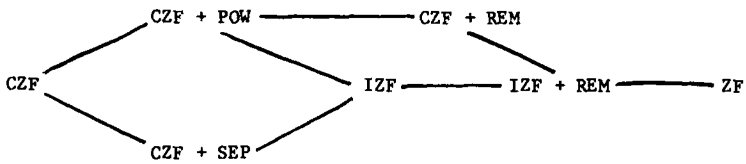
(i) CZF with classical logic.

(ii) CZF with restricted excluded middle and the full separation scheme.

(iii) ZF.

PROOF. Clearly (iii) includes both (i) and (ii). By 2.4 the powerset axiom is a theorem of both (i) and (ii). Full separation is also a theorem of (i) because for any formula ϕ we have $\phi \vee \neg \phi$. So choose $x = \{\emptyset\}$ if ϕ and $x = \emptyset$ if $\neg \phi$. In either case $\phi \leftrightarrow \emptyset \in x$ and we get full separation by 2.6. Finally we observe that classical logic holds in (ii). For if ϕ is a formula then by 2.6 there is an x such that $\phi \leftrightarrow \emptyset \in x$. By restricted excluded middle $\emptyset \in x \vee \emptyset \notin x$ so that $\phi \vee \neg \phi$.

Remark. Let POW denote the powerset axiom, SEP the full separation scheme, REM the restricted excluded middle and let IZF be $CZF^- +$ POW + SEP. We have the following diagram of systems, increasing in strength from left to right.



IZF (Intuitionistic ZF) arises naturally as the system that is modelled when the classical topological interpretation of intuitionistic logic is extended to set theory (see [8]). IZF would seem to be the impredicative version of CZF. Friedman (in [6]) has shown that ZF has a finitist reduction to IZF. (An elegant alternative proof of this appears in [8] where ZF is given a Boolean valued model in IZF) CZF + REM is a natural formalisation of the Liberal intuitionist conception. This is the viewpoint that classical logic holds when quantifying over sets, but only intuitionistic logic holds when quantifying over the universe (See [14] and also the recent [12].

3. THE TYPE THEORETIC FRAMEWORK

We shall assume that the reader is familiar with the informal notions of intuitionistic type theory as developed in [11]. For most of the purposes of this paper it is sufficient that he has read §1 of [11].

Here we shall only summarise these notions. In type theory the basic forms of statement are 'A is a type' and '$a \in A$' ('a is an object of type A'). In addition there are definitional equalities between types and between objects of each type. We shall just use '=' for definitional equality rather than the notation '$=_{def}$' used in [11]. The basic forms of type are N (the type of natural numbers), N_k (the k-element type for k = 0,1,...), A + B (binary disjoint union) $(\Pi x \in A)B(x)$ (cartesian product) and $(\Sigma x \in A)B(x)$ disjoint union). As special cases of the last two forms, when B(x) is a constant type B, we have the types $A \to B$ (function type) and $A \times B$ (binary cartesian product).

In addition to these basic forms of type we need the type V of small types. This is obtained by a reflection on the basic forms of type. Thus we have rules giving $N \in V$, $N_k \in V$ for k = 0,1,... and $A + B \in V$ if $A \in V$ and $B \in V$, and $(\Pi x \in A)B(x) \in V$, $(\Sigma x \in A)B(x) \in V$ if $A \in V$ and $B(x) \in V$ for $x \in A$. It follows that $A \to B \in V$ and $A \times B \in V$ if $A \in V$ and $B \in V$. We shall use the notation of λ-abstraction. Thus if ...x... is an expression such that ...a.. $\in B(a)$ for $a \in A$ then by the introduction rule for $(\Pi x \in A)B(x)$ we introduce a function $f = \lambda x \ldots x \ldots \in (\Pi x \in A)B(x)$ such that $f(a) = \ldots a \ldots$ for $a \in A$.

The key insight in the type theoretic approach to constructive mathematics is the identification of a mathematical proposition with the type of its proofs.

The logical constants are then identified with appropriate notions of type theory according to the following table:

Form of proposition	Form of type
$\bot$	N_0
$A \rightarrow B$	$A \rightarrow B$
$A \wedge B$	$A \times B$
$A \vee B$	$A + B$
$(x\varepsilon A)B(x)$	$(\Pi x\varepsilon A)B(x)$
$(x\varepsilon A)B(x)$	$(\Sigma x\varepsilon A)B(x)$

With these identifications, the natural deduction schemes for intuitionistic predicate calculus reduce to the introduction and elimination rules of type theory. Moreover this can be extended to Heyting arithmetic because the mathematical induction scheme reduces to the elimination rule for N, giving definition by primitive recursion.

In order to give our interpretation of CZF we need to introduce a further type; the type U of sets. As usual U will be specified by introduction and elimination rules. The introduction rule for U is a type theoretic reformulation of the classical conception of the cumulative hierarchy of sets. An indexed family of previously introduced sets determines a new set, if it is indexed by a small type. Below we give the rules for U in the style of §1 of [11].

U is a type, namely the type of <u>sets</u>. If $f(a)$ is a set for each $a\varepsilon A$, where A is a small type, then $\{f(x)|x\varepsilon A\}$ is a set.

If $B(\alpha)$ is a type for each set α, and $b(A,\lambda xf(x), \lambda xg(x)) \varepsilon B(\{f(x)|x\varepsilon A\})$ whenever A is a small type, $f(a)$ is a set and $g(a)\varepsilon B(f(a))$ for $a\varepsilon A$, then we may define a function F such that $F(\alpha)\varepsilon B(\alpha)$ for $\alpha\varepsilon U$, by the <u>set recursion</u> scheme.

$$F(\{f(x)|x\varepsilon A\}) = b(A, \lambda xf(x), \lambda xF(f(x))).$$

If $B(\alpha)$ represents a proposition for each set α then F is the proof of the universal proposition $(\forall\alpha\varepsilon U)B(\alpha)$ which we get by applying <u>set induction</u> to the proof b of

$$(\forall A \,\varepsilon\, V)(\forall f\varepsilon A \rightarrow U)\ [(\forall x\varepsilon A)B(f(x)) \rightarrow B(\{f(x)|x\varepsilon A\})]$$

4. THE INTERPRETATION

Before going further it may help the reader's intuition if we show how some familiar sets are built up using the introduction rule for U . Given sets $\alpha_1,\ldots\alpha_k$ let $\{\alpha_1,\ldots,\alpha_k\}$ be the set $\{f(x)|x\varepsilon N_k\}$ where $f(1) = \alpha_1,\ldots,f(k) = \alpha_k$. In particular, if $k = 0$ we obtain the empty set $\emptyset$. In this way we get all the hereditarily finite sets. If α is a set $\{f(x)|x\varepsilon A\}$ and β is a set $\{g(y)|y\varepsilon B\}$ then we can define $\alpha\cup\beta$ to be the set $\{h(z)|z\varepsilon A + B\}$ where $h(i(a)) = f(a)$ for $a\varepsilon A$ and $h(j(b)) = g(b)$ for $b\varepsilon B$. More generally, if α is a set $\{f(x)|x\varepsilon A\}$ where $f(a)$ is a set $\{g(a,y)|y\varepsilon B(a)\}$ for $a\varepsilon A$ then we can define $\cup\alpha$ to be $\{h(z)|z\varepsilon(\Sigma x\varepsilon A)B(x)\}$ where $h((a,b)) = g(a,b)$ for $a\varepsilon A$ and $b\varepsilon B(a)$. As an example of an infinite set we can define $\omega = \{\Delta(n) \mid n\epsilon N\}$ where $\Delta(0) = \emptyset$ and $\Delta(s(n)) = \Delta(n) \cup \{\Delta(n)\}$ for $n\epsilon N$.

As a first application of set recursion we define $\bar{\alpha}\epsilon V$ and $\tilde{\alpha}\epsilon\bar{\alpha} \to U$ for each set α by the schemes $\overline{\{f(x) \mid x\epsilon A\}} = A$ and $\widetilde{\{f(x) \mid x\epsilon A\}} = \lambda x f(x)$. Set recursion can be used to justify more elaborate forms of recursion. We shall define a small type $\|\alpha = \beta\|$, for sets α,β, that represents the proposition that α is extensionally equal to β. It is introduced by the following double recursion:

$$\|\{f(x) \mid x\epsilon A\} = \{g(y) \mid y\epsilon B\}\| =$$
$$(\Pi x\epsilon A)(\Sigma y\epsilon B)\|f(x) = g(y)\| \times (\Pi y\epsilon B)(\Sigma x\epsilon A)\|f(x) = g(y)\|.$$

To justify this definition we use ordinary set recursion to define a function F such that $F(\{f(x) \mid x\epsilon A\}) =$

$$\lambda\beta[(\Pi x\epsilon A)(\Sigma y\epsilon\bar{\beta})F(f(x))(\tilde{\beta}(y)) \times (\Pi y\epsilon\bar{\beta})(\Sigma y\epsilon\bar{\beta})(\Sigma x\epsilon A)F(f(x))(\tilde{\beta}(y))],$$

for $A\epsilon V$ and $f\epsilon A \to U$. Now let $\|\alpha = \beta\|$ be $F(\alpha)(\beta)$. The general form of double set recursion can also be justified in this way, as can triple set recursion etc..

Next we define the small type $\|\alpha\epsilon\beta\|$ that represents the proposition that α is a member of the set β, to be $(\Sigma y\epsilon\bar{\beta})\|\alpha = \tilde{\beta}(y)\|$.

Let $\mathcal{L}U$ be obtained from the language $\mathcal{L}$ by adding a constant for each set. We use the same symbol to denote the set and its name in $\mathcal{L}U$.

We assign a type $\|\phi\|$ to each sentence ϕ of $\mathcal{L}U$ as follows. We have already defined $\|\alpha = \beta\|$ and $\|\alpha\epsilon\beta\|$ for sets α,β. We let $\|\bot\| = N_0$, $\|\phi \to \psi\| = \|\phi\| \to \|\psi\|$, $\|\phi \wedge \psi\| = \|\phi\| \times \|\psi\|$, $\|\phi \vee \psi\| = \|\phi\| + \|\psi\|$, $\|(\forall x\epsilon\alpha)\phi(x)\| = (\Pi x\epsilon\bar{\alpha})\|\phi(\tilde{\alpha}(x))\|$, $\|(\exists x\epsilon\alpha)\phi(x)\| = (\Sigma x\epsilon\bar{\alpha})\|\phi(\tilde{\alpha}(x))\|$, $\|\forall x\phi(x)\| = (\Pi\alpha\epsilon U)\|\phi(\alpha)\|$ and $\|\exists x\phi(x)\| = (\Sigma\alpha\epsilon U)\|\phi(\alpha)\|$.

By a trivial induction on restricted sentences ϕ we have

4.1. LEMMA. $\|\phi\|$ is a small type for each restricted sentence ϕ of $\mathcal{L}U$.

A formula $\phi(x_1,\ldots,x_n)$ of $\mathcal{L}U$, in the displayed free variables, is valid if there is an expression $a(x_1,\ldots,x_n)$ such that $a(\alpha_1,\ldots,\alpha_n) \epsilon \|\phi(\alpha_1,\ldots,\alpha_n)\|$ for sets $\alpha_1,\ldots,\alpha_n$.

Our aim in this paper is to prove:

4.2. THEOREM. Every theorem of CZF is valid.

As a first step we have:

4.3. LEMMA. If ϕ is an intuitionistic logical consequence of $\phi_1,\ldots,\phi_n$ and $\phi_1,\ldots,\phi_n$ are valid then so is ϕ.

This is a consequence of the type theoretic representation of logic. With this lemma it only remains to show that every non-logical axiom of CZF is valid. We do this in the next two sections.

4.4. REMARK. In proving the validity of a formula $\phi(x_1,\ldots,x_n)$ it is convenient to argue as follows. Given sets $\alpha_1,\ldots,\alpha_n$ we find an object $a\epsilon\|\phi(\alpha_1,\ldots,\alpha_n)\|$. As our constructions will always be uniform in the parameters $\alpha_1,\ldots,\alpha_n$ we can write a as $a(\alpha_1,\ldots,\alpha_n)$ for some expression $a(x_1,\ldots,x_n)$ and hence $\phi(x_1,\ldots,x_n)$ is valid.

5. VALIDITY OF THE STRUCTURAL AXIOMS

We start with set induction. Let $\phi(x)$ be a formula of $\mathcal{L}U$ with at most x free. Let B be the type $\|\forall y((\forall x \epsilon y)\phi(x) \to \phi(y))\|$. Define $h(\alpha)\epsilon B \to \|\phi(\alpha)\|$ for each set α by the set recursion: $h(\{f(x)|x\epsilon A\}) = \lambda bb(\{f(x)|x\epsilon A\})(\lambda xh(f(x))(b))$ for $A\epsilon V$ and $f\epsilon A \to U$. Then $\lambda b\lambda\alpha h(\alpha)(b)\epsilon B \to \|\forall x\phi(x)\|$ showing that set induction is valid for the formula $\phi(x)$. By remark 4.4. the above is sufficient also for formulae with extra free variables.

The proof that the remaining structural axioms are valid is not difficult, but is a little tedious to carry through in detail. We outline the main steps in a sequence of lemmas.

5.1. LEMMA. The following are valid.

(i) $x = x$

(ii) $x = y \to y = x$

(iii) $x = y \wedge y = z \to x = z$.

These require single, double and triple set recursions to define $r_0(\alpha)\epsilon\|\alpha = \alpha\|$, $c_0(\alpha,\beta)\epsilon\|\alpha = \beta\| \to \|\beta = \alpha\|$ and $t_0(\alpha,\beta,\gamma)\epsilon\|\alpha = \beta\| \times \|\beta = \gamma\| \to \|\alpha = \gamma\|$ for sets α,β,γ.

5.2. LEMMA. The following are valid

(i) $u = v \iff (\forall x\epsilon u)(\exists u\epsilon v)(x = y) \wedge (\forall y\epsilon v)(\exists x\epsilon u)(x = y)$

(ii) $u \epsilon v \iff (\exists y\epsilon v)(u = y)$

These follow from the definitions of $\|.=.\|$. and $\|.\ \epsilon.\ \|$.

Define a formula $\phi(x)$ to be invariant in x if $x = y \to (\phi(x) \to \phi(y))$ is valid.

5.3. LEMMA. If $\phi(x)$ is invariant in x then the structural defining axioms for $(\forall x\epsilon y)\phi(x)$ and $(\exists x\epsilon y)\phi(x)$ are valid.

5.4. LEMMA. The formulae $(x = y)$ and $(x\epsilon y)$ are invariant in both x and y, and hence the equality axioms are valid.

5.5. LEMMA. Each formula of $\mathcal{L}U$ is invariant in every variable.

This is proved by induction on the way formulae are built up. 5.3 and 5.5 combine to give the validity of all the defining axioms for the restricted quantifiers.

6. VALIDITY OF THE SET EXISTENCE AXIOMS

As $(x = x)$ is valid there is a function $r_0(\alpha)\epsilon\|\alpha = \alpha\|$ for each set α. Let α^* be $\lambda x(x,r_0(\tilde{\alpha}(x))$ for each set α. Then $\alpha^*(a)\epsilon\|\tilde{\alpha}(a)\epsilon\alpha\|$ for each set α and $a\epsilon\bar{\alpha}$. We now consider each set existence axiom in turn.

Pairing. Given sets α,β let γ be the set $\{g(u)|u\epsilon N_2\}$ where $g\epsilon N_2 \to U$ satisfies $g(1) = \alpha$ and $g(2) = \beta$. Then $h\epsilon\|\alpha\epsilon\gamma \wedge \beta\epsilon\gamma\|$ where h is $(\gamma^*(1), \gamma^*(2))$, and hence $(\gamma,h)\epsilon\|\exists z(\alpha\epsilon z \wedge \beta\epsilon z)\|$. Keeping in mind remark 4.4. we see that the pairing axiom is valid.

Union. Given the set α let γ be the set $\{g(a)|a\epsilon A\}$ where A is $\overline{(\Sigma x\epsilon\bar{\alpha})\tilde{\alpha}(x)}$ and $g\epsilon A \to U$ satisfies $g((x,y)) = \tilde{\alpha}(x)(y)$ for $x\epsilon\bar{\alpha}$ and $y\epsilon\overline{\tilde{\alpha}(x)}$. Then $h\epsilon$

$\|(\forall x\epsilon\alpha)(\forall y\epsilon x)(y\epsilon\gamma)\|$, where h is $\lambda y\lambda x\gamma^*((x,y))$, and hence $(\gamma,h)\epsilon\|\exists z(\forall x\epsilon\alpha)(\forall y\epsilon x)(y\epsilon z)\|$.

<u>Restricted Separation</u>. Let $\phi(x)$ be a restricted formula of $\mathcal{L}U$ with at most x free. Given the set α let γ be the set $\{g(u)|u\epsilon A\}$ where A is the small (by lemma 4.1.) type $\|(\exists x\epsilon\alpha)\phi(x)\|$ and $g\epsilon A\to U$ satisfies $g((x,v)) = \tilde{\alpha}(x)$ for $x\epsilon\bar{\alpha}$ and $v\epsilon\|\phi(\tilde{\alpha}(x))\|$. Then $h_1\epsilon\|(\forall u\epsilon\gamma)(u\epsilon\alpha \wedge \phi(u))\|$ and $h_2\epsilon\|(\forall x\epsilon\alpha)(\phi(x)\to x\epsilon\gamma)\|$, where $h_1((x,v)) = (\alpha^*(x),v)$ and $h_2(x)(v) = \gamma^*((x,v))$ for $x\epsilon\bar{\alpha}$ and $v\epsilon\|\phi(\tilde{\alpha}(x))\|$. Hence $(\gamma,(h_1,h_2))\ \epsilon\ \|\exists z[(\forall y\epsilon z)(y\epsilon x \wedge \phi(y)) \wedge (\forall y\epsilon x)(\phi(y)\to y\epsilon z)]\|$.

In considering the collection schemes we shall need the following construction. Let $\phi(x,y)$ be a formula of $\mathcal{L}U$ with at most x and y free. Let α,β be sets such that $\bar{\alpha} = \bar{\beta}$ and $f(a)\epsilon\|\phi(\tilde{\alpha}(a),\tilde{\beta}(a))\|$ for $a\epsilon\bar{\alpha}$. Then $K(f)\epsilon\|\phi'(\alpha,\beta)\|$ where K(f) is $(\lambda x(x,f(x)), \lambda x(x,f(x)))$.

<u>Strong Collection</u>. Let $\phi(x,y)$ be as above. Let α be a set and let $a\epsilon\|(\forall x\epsilon\alpha)\exists y\phi(x,y)\|$. Let $b\epsilon\bar{\alpha}\to U$ be $\lambda xp(a(x))$ and let $c\epsilon(\Pi x\epsilon\alpha)\|\phi(\tilde{\alpha}(x),b(x))\|$ be $\lambda xq(a(x))$ where p and q denote projection functions. If β is the set $\{b(x)|x\epsilon\bar{\alpha}\}$ then $K(c)\epsilon\|\phi'(\alpha,\beta)\|$ and hence $d(a)\epsilon\|\exists z\phi'(\alpha,z)\|$ where d(a) is $(\beta,K(c))$ and we have made explicit the dependence of $(\beta,K(c))$ on a. So $\lambda ad(a)\epsilon\|(\forall x\epsilon\alpha)\exists y\phi(x,y)\to\exists z\phi'(\alpha,z)\|$.

<u>Subset Collection</u>. Given sets α,β, let γ be the set $\{G(z)|z\epsilon\bar{\alpha}\to\bar{\beta}\}$ where G is $\lambda z\{\tilde{\beta}(z(x))|x\epsilon\bar{\alpha}\}$. Now let $\phi_u(x,y)$ be a formula of U, containing at most u,x,y free, and let $\theta_u(\alpha,\beta)$ denote $(\forall x\epsilon\alpha)(\exists y\epsilon\beta)\phi_u(x,y)$. Finally let δ be a set and let $a\epsilon\|\theta'_\delta(\alpha,\beta)\|$. Then $K(c)\epsilon\|\phi'_\delta(\alpha,G(b))\|$ where $b\epsilon\bar{\alpha}\to\bar{\beta}$ is $\lambda xp(a(x))$ and $c\epsilon(\Pi x\epsilon\bar{\alpha})\|\phi_\delta(\tilde{\alpha}(x),\tilde{\beta}(b(x)))\|$ is $\lambda xq(a(x))$. Hence $d(\delta,a)\epsilon\|(\exists z\epsilon\gamma)\phi'_\delta(\alpha,z)\|$ where $d(\delta,a)$ is $(b,K(c))$ and we have made explicit the dependence of $(b,K(c))$ on δ and a. Then $(\gamma,\lambda a\lambda\delta d(\delta,a))\ \epsilon\ \|\exists v\forall u[\theta_u(\alpha,\beta)\to(\exists z\epsilon v)\phi'_u(\alpha,z)\|$.

<u>Infinity</u>. Let f_0 and g_0 be the canonical undefined functions in $N_0\to U$ and $N_0\to N_0$ respectively. Then $g_0\epsilon\|$ Zero $(\emptyset)\|$ where $\emptyset$ is the set $\{f_0(x)|x\epsilon N_0\}$. For each set α let $S(\alpha)$ be the set $\{h(\alpha)(y)|y\epsilon\bar{\alpha}+N_1\}$ where $h(\alpha)\epsilon(\bar{\alpha}+N_1)\to U$ satisfies $h(\alpha)(i(x)) = \tilde{\alpha}(x)$ for $x\epsilon\bar{\alpha}$ and $h(\alpha)(j(1)) = \alpha$. Then $S(\alpha)^*(j(1))\epsilon\|\alpha\epsilon S(\alpha)\|$. Also $g_1(\alpha)\epsilon\|(\forall x\epsilon\alpha)(x\epsilon S(\alpha))\|$ where $g_1(\alpha)$ is $\lambda xS(\alpha)^*(i(x))$, and $g_2(\alpha)\epsilon\|(\forall u\epsilon S(\alpha))(u\epsilon\alpha \vee u=\alpha)\|$ where $g_2(\alpha)(i(x)) = i(\alpha^*(x))$ for $x\epsilon\bar{\alpha}$ and $g_2(\alpha)(j(1)) = j(r_0(\alpha))$. It follows that $g(\alpha)\epsilon\|$Succ $(\alpha,S(\alpha))\|$ where $g(\alpha)$ is $((S(\alpha)^*(j(1)),g_1(\alpha)), g_2(\alpha))$. Let ω be the set $\{\Delta(n)|n\epsilon N\}$ where $\Delta(o) = \emptyset$ and $\Delta(s(n)) = S(\Delta(n))$ for $n\epsilon N$. Then $f\epsilon\|(\forall x\epsilon\omega)(\text{Zero}(x)\vee(\exists y\epsilon x)\text{Succ}(y,x))\|$ where $f(o) = i(g_0)$ and $f(s(n)) = j((n,g(d(n)))$ for $n\epsilon N$. Also $h\epsilon\|(\forall y\epsilon\omega)(\exists x\epsilon\omega)\text{Succ}(y,x)\|$ where h is $\lambda y(s(y), g(\Delta(y))$. In conclusion $(\omega,(f,((0,g_0),h)))\epsilon\|\exists z\text{Nat}(z)\|$.

7. THE PRESENTATION AXIOM

An important aspect of any formalisation of constructive mathematics is the correct treatment of possible principles of choice. In the case of constructive set theory Myhill has argued for the correctness of the scheme of dependent choices DC. We can support his informal argument with the following result.

7.1. THEOREM. Each instance of DC is valid.

This is proved in a straightforward but tedious way as in §6.

An analysis of the informal constructive justification for DC leads to the following notions. Let us call A a base if choice functions defined on the set A can always be found. For example the countable axiom of choice states that ω is a base. A surjection of a base onto a set we call a presentation of that set. A simple argument in CZF shows us that if a set A has a presentation then DC holds for A, i.e. if R: A $\prec$ A and $a \in A$ then there is an f: $\omega \to A$ such that $f(0) = a$ and $f(n)Rf(n+1)$ for all $n \in \omega$. This suggests consideration of the following axiom

Presentation axiom (PA). Every set has a presentation.

This axiom has also been considered by A. Blass (see [4]) in a classical context. Among other things he has shown that relative to ZF, PA is strictly stronger than DC.

The constructive intuition for this axiom is that a presentation is intended to represent a particular way the set is given to us. The sets in the type U are given to us in the form $\{f(x) | x \in A\}$ where A is a small type. As shown in [11] choice functions always exist in type theory because of the type theoretic representation of the quantifiers. So to justify PA it would suffice to have a suitable representation as a set in U of each small type A. Unfortunately such a representation does not seem to be available. Nevertheless, if CZF if modified to CZF^I by allowing for a class of individuals, and the type U is modified to a type U^I by introducing an individual $a_A \in U^I$ for each small type A and each $a \in A$ then all the theorems of CZF^I + PA can be shown to be valid in the appropriate sense. Each small type A has a representation as the set $\{a_A | a \in A\}$ in U^I. In fact a strengthened version of PA is valid which requires the base of a presentation to be a set of individuals. (In order to carry out the interpretation we need to use the notion of identity discussed in [11] but not needed here so far. In addition to what is contained in [11] we also need to assume that if A and B are small types then so is I(A,B), the type which represents the proposition that A and B are identical.) An alternative approach to justifying PA is to take the realisability model of type theory. This model induces a realisability model of CZF + PA. In fact a strengthened form of PA is realised which requires that the base of a presentation is a subset of ω.
A formalised version of the realisability interpretation of type theory may be found in [1]. We hope to discuss these topics in more detail in a future paper.

References

[1] P. ACZEL, The strength of Martin-Löf's intuitionistic type theory with one universe. Proceedings of the symposium on Mathematical Logic, in Oulu 1974 Report No.2 of Dept. Philosophy, University of Helsinki (1977) pp.1-32.

[2] M. BEESON, Principles of continuous choice and continuity of functions in

formal systems for constructive mathematics, to appear in Annals of Math. Logic.

[3] E. BISHOP, Foundations of Constructive Analysis, McGraw-Hill, (1967).

[4] A. BLASS, Injectivity, Projectivity and the axiom of choice, to appear.

[5] S. FEFERMAN, A language and axioms for explicit mathematics, in Algebra and Logic, Springer Lecture Notes No. 450 (1975) pp.87-139.

[6] H. FRIEDMAN, The consistency of set theory relative to a theory with intuitionistic logic, J.S.L. Vol.38(1973) pp.315-319.

[7] ———, Set-theoretic foundations of constructive analysis, Annals of Maths., 105(1977) pp.1-28.

[8] R. GRAYSON, A sheaf approach to models of set theory, M.Sc. thesis Oxford (1975).

[9] H. JERVELL, Constructive Universes I, preprint (1977).

[10] G. LEVERSHA, Formal systems for constructive mathematics. Ph.D. thesis, Manchester University (1976).

[11] P. MARTIN-LÖF, An intuitionistic theory of types: Predicative part, in Logic Colloquium'73, eds. H.E. Rose and J.C. Shepherdson, North Holland (1975) pp.73-118.

[12] J. MAYBERRY, The Consistency Problem for Set Theory: An essay on the Cantorian Foundations of Mathematics, Brit. J. Phil. Sci., 28(1977)pp.1-34 (part I), pp.137-170 (part II).

[13] J. MYHILL, Constructive Set Theory, J.S.L. 40(1975) pp.347-382.

[14] L. POZSGAY, Liberal intuitionism as a basis for set theory, in Proc. Symp. in Pure Maths. Vol.XIII, Proc. of AMS 1967, Axiomatic Set Theory Conference, Part I, ed. D. Scott.