This is the published version of an article in the *Journal of Universal Computer Science, 11 (12)*

White Rose Research Online URL for this paper:

[http://eprints.whiterose.ac.uk/id/eprint/76754](http://eprints.whiterose.ac.uk/id/eprint/76754)

**Published article:**


[http://dx.doi.org/10.3217/jucs-011-12-2008](http://dx.doi.org/10.3217/jucs-011-12-2008)
Constructive Set Theory and Brouwerian Principles

Michael Rathjen
(Department of Mathematics, The Ohio State University,
Email: rathjen@math.ohio-state.edu)

Abstract: The paper furnishes realizability models of constructive Zermelo-Fraenkel set theory, CZF, which also validate Brouwerian principles such as the axiom of continuous choice (CC), the fan theorem (FT), and monotone bar induction (BIM), and thereby determines the proof-theoretic strength of CZF augmented by these principles. The upshot is that CZF + CC + FT possesses the same strength as CZF, or more precisely, that CZF + CC + FT is conservative over CZF for \( \Pi^0_2 \) statements of arithmetic, whereas the addition of a restricted version of bar induction to CZF (called decidable bar induction, BID) leads to greater proof-theoretic strength in that CZF + BID proves the consistency of CZF.

Key Words: Constructive set theory, Brouwerian principles, partial combinatory algebra, realizability

Category:

1 Introduction

Constructive Zermelo-Fraenkel Set Theory has emerged as a standard reference theory that relates to constructive predicative mathematics as ZFC relates to classical Cantorian mathematics. The general topic of Constructive Set Theory originated in the seminal 1975 paper of John Myhill (cf. [16]), where a specific axiom system CST was introduced. Myhill developed constructive set theory with the aim of isolating the principles underlying Bishop’s conception of what sets and functions are. Moreover, he wanted “these principles to be such as to make the process of formalization completely trivial, as it is in the classical case” ([16], p. 347). Indeed, while he uses other primitives in his set theory CST besides the notion of set, it can be viewed as a subsystem of ZF. The advantage of this is that the ideas, conventions and practise of the set theoretical presentation of ordinary mathematics can be used in the set theoretical development of constructive mathematics, too. Constructive Set Theory provides a standard set theoretical framework for the development of constructive mathematics in the style of Errett Bishop and Douglas Bridges [6] and is one of several such frameworks for constructive mathematics that have been considered. Aczel subsequently modified Myhill’s CST and the resulting theory was called Zermelo-Fraenkel set theory, CZF. A hallmark of this theory is that it possesses a type-theoretic interpretation (cf. [1, 2, 3]). Specifically, CZF has a scheme called Subset Collection Axiom (which is a generalization of Myhill’s Exponentiation Axiom) whose formalization was directly inspired by the type-theoretic interpretation.

---

2 This material is based upon work supported by the National Science Foundation under Award No. DMS-0301162.
This paper studies augmentations of CZF by Brouwerian principles such as the axiom of continuous choice (CC), the fan theorem (FT), and bar induction (BI). The objective is to determine whether these principles increase the proof-theoretic strength of CZF. More precisely, the research is concerned with the question of whether any new $\Pi^0_2$ statements of arithmetic (i.e. statements of the form $\forall n \in \mathbb{N} \exists k \in \mathbb{N} P(n,k)$ with $P$ being primitive recursive) become provable upon adding CC, FT, and BI (or any combination thereof) to the axioms of CZF.

The first main result obtained here is that CZF + CC + FT is indeed conservative over CZF with respect to $\Pi^0_2$ sentences of arithmetic. The first step in the proof consists of defining a transfinite type structure over a special combinatorial algebra whose domain is the set of all arithmetical functions from $\mathbb{N}$ to $\mathbb{N}$ with application being continuous function application in the sense of Kleene’s second algebra $K_2$. The transfinite type structure serves the same purpose as a universe in Martin-Löf type theory. It gives rise to a realizability interpretation of CZF which also happens to validate the principles CC and FT. However, to be able to show that FT is realized we have to employ classical reasoning in the background theory. It turns out that the whole construction can be carried out in a classical set theory known as Kripke-Platek set theory, KP. Since CZF and KP prove the same $\Pi^0_2$ statements of arithmetic this establishes the result.

A similar result can be obtained for CZF plus the so-called Regular Extension Axiom, REA. Here it turns out that CZF + REA + CC + BI is $\Pi^0_2$ conservative over CZF + REA. This time the choice for the domain of the partial combinatory algebra is $\mathbb{N}^3 \cap L_\rho$, where $\rho = \sup_{n<\omega} \omega^\text{ck}_n$ with $\omega^\text{ck}_n$ denoting the $n$th admissible ordinal. Application is again continuous function application. The transfinite type structure also needs to be strengthened in that it has to be closed off under $W$-types as well. A background theory sufficient for these constructions is KPi, i.e. Kripke-Platek set theory plus an axiom asserting that every set is contained in an admissible set.

The question that remains to be addressed is whether CZF + BI is conservative over CZF. This is answered in the negative. It is shown that a restricted form of BI - called decidable bar induction, BI$_D$ - implies the consistency of CZF on the basis of CZF. The proof makes use of results from ordinal-theoretic proof theory.

2 Constructive Zermelo-Fraenkel Set Theory

Constructive set theory grew out of Myhill’s endeavours (cf. [16]) to discover a simple formalism that relates to Bishop’s constructive mathematics as ZFC relates to classical Cantorian mathematics. Later on Aczel modified Myhill’s set theory to a system which he called Constructive Zermelo-Fraenkel Set Theory, CZF.

**Definition: 2.1 (Axioms of CZF)** The language of CZF is the first order language of Zermelo-Fraenkel set theory, $LST$, with the non logical primitive symbol $\in$. CZF is based on intuitionistic predicate logic with equality. The set theoretic axioms of axioms of CZF are the following:

1. **Extensionality** $\forall a \forall b (\forall y (y \in a \leftrightarrow y \in b) \rightarrow a = b)$. 

2. **Pair** \( \forall a \forall b \exists x \forall y (y \in x \leftrightarrow y = a \lor y = b) \).

3. **Union** \( \forall a \exists x \forall y (y \in x \leftrightarrow \exists z \in a \, y \in z) \).

4. **Restricted Separation scheme** \( \forall a \exists x \forall y (y \in x \leftrightarrow y \in a \land \varphi(y)) \),
   for every restricted formula \( \varphi(y) \), where a formula \( \varphi(x) \) is restricted, or \( \Delta_0 \),
   if all the quantifiers occurring in it are restricted, i.e. of the form \( \forall x \in b \) or \( \exists x \in b \).

5. **Subset Collection scheme** \( \forall a \forall b \exists c \forall u \left( \forall x \in a \exists y \in b \varphi(x, y, u) \rightarrow \exists d \in c \left( \forall x \in a \exists y \in d \varphi(x, y, u) \land \forall y \in d \exists x \in a \varphi(x, y, u) \right) \right) \)
   for every formula \( \varphi(x, y, u) \).

6. **Strong Collection scheme** \( \forall a \exists x \forall y \left( y \in x \leftrightarrow y \in a \land \varphi(y) \right) \),
   for every formula \( \varphi(x, y) \).

7. **Infinity** \( \exists x \forall u \left[ u \in x \leftrightarrow \left( 0 = u \lor \exists v \in x(u = v \cup \{v\}) \right) \right] \)
   where \( y + 1 \) is \( y \cup \{y\} \), and 0 is the empty set, defined in the obvious way.

8. **Set Induction scheme** \( (IND) \forall a \left( \forall x \in a \varphi(x) \rightarrow \varphi(a) \right) \rightarrow \forall a \varphi(a) \),
   for every formula \( \varphi(a) \).

From Infinity, Set Induction, and Extensionality one can deduce that there exists exactly one set \( x \) such that
\( \forall u \left[ u \in x \leftrightarrow \left( 0 = u \lor \exists v \in x(u = v \cup \{v\}) \right) \right] \); this set will be denoted by \( \omega \).

### 2.1 Choice principles

In many a text on constructive mathematics, axioms of countable choice and dependent choices are accepted as constructive principles. This is, for instance, the case in Bishop’s constructive mathematics (cf. [6] as well as Brouwer’s intuitionistic analysis (cf. [28], Chap. 4, Sect. 2). Myhill also incorporated these axioms in his constructive set theory [16].

The weakest constructive choice principle we shall consider is the **Axiom of Countable Choice**, \( AC_\omega \), i.e. whenever \( F \) is a function with domain \( \omega \) such that \( \forall i \in \omega \exists y \in F(i) \), then there exists a function \( f \) with domain \( \omega \) such that \( \forall i \in \omega \, f(i) \in F(i) \).

Let \( xRy \) stand for \( \langle x, y \rangle \in R \). A mathematically very useful axiom to have in set theory is the **Dependent Choices Axiom**, \( DC \), i.e., for all sets \( a \) and (set) relations \( R \subseteq a \times a \), whenever
\[
\forall x \in a \exists y \in a \, xRy
\]
and \( b_0 \in a \), then there exists a function \( f : \omega \rightarrow a \) such that \( f(0) = b_0 \) and
\[
\forall n \in \omega \, f(n)Rf(n+1).
\]
Even more useful in constructive set theory is the Relativized Dependent Choices Axiom, RDC. It asserts that for arbitrary formulae $\phi$ and $\psi$, whenever
\[
\forall x [\phi(x) \rightarrow \exists y (\phi(y) \land \psi(x, y))]
\]
and $\phi(b_0)$, then there exists a function $f$ with domain $\omega$ such that $f(0) = b_0$ and
\[
(\forall n \in \omega) [\phi(f(n)) \land \psi(f(n), f(n + 1))].
\]
One easily sees that RDC implies DC and DC implies AC$_\omega$.

2.2 The strength of CZF

In what follows we shall use the notions of proof-theoretic equivalence of theories and proof-theoretic strength of a theory whose precise definitions one can find in [18]. For our purposes here we take proof-theoretic equivalence of set theories $T_1$ and $T_2$ to mean that these theories prove the same $\Pi^0_2$ statements of arithmetic and that this insight can be obtained on the basis of a weak theory such as primitive recursive arithmetic, PRA.

Theorem: Let KP be Kripke-Platek Set Theory (with the Infinity Axiom) (see [4]).

(i) CZF and CZF$^-$ are of the same proof-theoretic strength as KP and the classical theory ID$_1$ of non-iterated positive arithmetical inductive definitions. These systems prove the same $\Pi^0_2$ statements of arithmetic.

(ii) The system CZF augmented by the Power Set axiom is proof-theoretically stronger than classical Zermelo Set theory, Z (in that it proves the consistency of Z).

(iii) CZF does not prove the Power Set axiom.

Proof: Let Pow denote the Power Set axiom. (i) follows from [17] Theorem 4.14. Also (iii) follows from [17] Theorem 4.14 as one easily sees that 2-order Heyting arithmetic has a model in CZF + Pow. Since second-order Heyting arithmetic is of the same strength as classical second-order arithmetic it follows that CZF + Pow is stronger than classical second-order arithmetic (which is much stronger than KP). But more than that can be shown. Working in CZF + Pow one can iterate the power set operation $\omega + \omega$ times to arrive at the set $V_{\omega+\omega}$ which is readily seen to be a model of intuitionistic Zermelo Set Theory, Z$^i$. As Z can be interpreted in Z$^i$ by means of a double negation translation as was shown in [13] Theorem 2.3.2, we obtain (ii).

The first large set axiom proposed in the context of constructive set theory was the Regular Extension Axiom, REA, which was introduced to accommodate inductive definitions in CZF [cf. [7], [2]].

Definition: A set $c$ is said to be regular if it is transitive, inhabited (i.e. $\exists u \in c$) and for any $u \in c$ and set $R \subseteq u \times c$ if $\forall x \in u \exists y \langle x, y \rangle \in R$ then there is a set $v \in c$ such that
\[
\forall x \in u \exists y \in v \langle x, y \rangle \in R \land \forall y \in v \exists x \in u \langle x, y \rangle \in R.
\]
We write Reg$(a)$ for ‘$a$ is regular’.

REA is the principle
\[
\forall x \exists y (x \in y \land \text{Reg}(y)).
\]
Theorem: 2.4 Let KPi be Kripke-Platek Set Theory plus an axiom asserting that every set is contained in an admissible set (see [4]).

(i) CZF + REA is of the same proof-theoretic strength as KPi and the subsystem of second-order arithmetic with $\Delta^1_1$-comprehension and Bar Induction.

(ii) CZF + REA does not prove the Power Set axiom.

Proof: (i) follows from [17] Theorem 5.13. (ii) is a consequence of (i) and Theorem 2.2.

3 Russian constructivism

We give a brief review of Russian constructivism which is intended to serve the purpose of enhancing our account of Brouwerian intuitionism by contrast. The concept of algorithm or recursive function is fundamental to the Russian schools of Markov and Shanin. Contrary to Brouwer, this school takes the viewpoint that mathematical objects must be concrete, or at least have a constructive description, as a word in an alphabet, or equivalently, as an integer, for only on such objects do recursive functions operate. Furthermore, Markov adopts what he calls Church’s thesis, CT, which asserts that whenever we see a quantifier combination $\forall n \in \mathbb{N} \exists m \in \mathbb{N} A(n, m)$, we can find a recursive function $f$ which produces $m$ from $n$, i.e. $\forall n \in \mathbb{N} A(n, f(n))$. On the other hand, as far as pure logic is concerned he augments Brouwer’s intuitionistic logic by what is known as Markov’s principle, MP, which may be expressed as

$$\forall n \in \mathbb{N} \left[ A(n) \lor \neg A(n) \right] \land \neg \forall n \in \mathbb{N} \neg A(n) \rightarrow \exists n \in \mathbb{N} A(n),$$

with $A$ containing natural number parameters only. The rationale for accepting MP may be phrased as follows. Suppose $A$ is a predicate of natural numbers which can be decided for each number; and we also know by indirect arguments that there should be an $n$ such that $A(n)$. Then a computer with unbounded memory could be programmed to search through $\mathbb{N}$ for a number $n$ such that $A(n)$ and we should be convinced that it will eventually find one. As an example for an application of MP to the reals one obtains $\forall x \in \mathbb{R} (\neg x \leq 0 \rightarrow x > 0)$.

In the next section we shall recall that Church’s thesis is incompatible with Brouwer’s principles CC and FT$_D$.

CT is also incompatible with the axiom of choice AC$_{1,0}^1$ to be defined in Definition 4.1(2).

Lemma: 3.1 AC$_{1,0}^1$ refutes CT.

Proof: See [27] or [5], Theorem 19.1.

One of the pathologies of CT is that it refutes UC.

Theorem: 3.2 CT implies that there exists a continuous function $f : [0, 1] \rightarrow \mathbb{R}$ which is unbounded and hence not uniformly continuous.

Proof: [28], 6.4.4.

However, in Russian constructivism one can also prove that all functions from $\mathbb{R}$ to $\mathbb{R}$ are continuous. This requires a slight strengthening of CT.
**Definition: 3.3** Extended Church’s Thesis, ECT, asserts that
\[ \forall n \in \mathbb{N} \left[ \psi(n) \rightarrow \exists m \in \mathbb{N} \varphi(n,m) \right] \] implies
\[ \exists e \in \mathbb{N} \forall n \in \mathbb{N} \left[ \psi(n) \rightarrow \exists m, p \in \mathbb{N} [T(e,n,p) \wedge U(p,m) \wedge \varphi(n,m)] \right] \]
whenever \( \psi(n) \) is an almost negative arithmetic formula and \( \varphi(u,v) \) is any formula. A formula \( \theta \) of the language of CZF with quantifiers ranging over \( \mathbb{N} \) is said to be almost negative arithmetic if \( \lor \) does not appear in it and instances of \( \exists m \in \mathbb{N} \) appear only as prefixed to primitive recursive subformulae of \( \theta \).

**Theorem: 3.4** Under the assumptions ECT and MP, all functions \( f : \mathbb{R} \to \mathbb{R} \) are continuous.

**Proof:** [28], 6.4.12. \( \square \)

### 4 Brouwer’s world

This section expounds on principles specific to Brouwer’s intuitionism and describes their mathematical consequences.

Intuitionistic mathematics diverges from other types of constructive mathematics in its interpretation of the term ‘sequence’. This led to the following principle of continuous choice, abbreviated CC, which we divide into a continuity part and a choice part:

**Definition: 4.1** CC is the conjunction of (1) and (2):

1. Any function from \( \mathbb{N}^\mathbb{N} \) to \( \mathbb{N} \) is continuous.
2. If \( P \subseteq \mathbb{N}^\mathbb{N} \times \mathbb{N} \), and for each \( \alpha \in \mathbb{N}^\mathbb{N} \) there exists \( n \in \mathbb{N} \) such that \( (\alpha,n) \in P \), then there is a function \( f : \mathbb{N}^\mathbb{N} \to \mathbb{N} \) such that \( (\alpha,f(\alpha)) \in P \) for all \( \alpha \in \mathbb{N}^\mathbb{N} \).

The first part of CC will also be denoted by \( \text{Cont}(\mathbb{N}^\mathbb{N}, \mathbb{N}) \). The second part of CC is often denoted by \( \text{AC}_{1,0} \).

The justification for CC springs from Brouwer’s ideas about choice sequences. Let \( P \subseteq \mathbb{N}^\mathbb{N} \times \mathbb{N} \), and suppose that for each \( \alpha \in \mathbb{N}^\mathbb{N} \) there exists \( n \in \mathbb{N} \) such that \( (\alpha, n) \in P \). According to Brouwer, the construction of an element of \( \mathbb{N}^\mathbb{N} \) is forever incomplete. A generic sequence \( \alpha \) is purely extensional, in the sense that at any given moment we can know nothing about \( \alpha \) other than a finite number of its terms. It follows that for a given sequence \( \alpha \), our procedure for finding an \( n \in \mathbb{N} \) such that \( (\alpha, n) \in P \) must be able to calculate \( n \) from some finite initial sequence \( \hat{\alpha}(m) \). If \( \beta \) is another such sequence, and \( \hat{\alpha}(m) = \hat{\beta}(m) \), then our procedure must return the same \( n \) for \( \beta \) as it does for \( \alpha \). So this procedure defines a continuous function \( f : \mathbb{N}^\mathbb{N} \to \mathbb{N} \) such that \( (\alpha, f(\alpha)) \in P \) for all \( \alpha \in \mathbb{N}^\mathbb{N} \), where we assume the topology on \( \mathbb{N}^\mathbb{N} \) to be the product topology.

It is plain that \( \text{Cont}(\mathbb{N}^\mathbb{N}, \mathbb{N}) \) is incompatible with classical logic.

The other principle central to Brouwerian mathematics is the so-called Fan Theorem which is also classically valid and equivalent to König’s lemma, KL.

\[ \hat{\alpha}(0) := (\), \hat{\alpha}(k+1) = (\alpha(0), \ldots, \alpha(k)) \]

\[3\]
Definition: 4.2 Let $2^\mathbb{N}$ be the set of all binary sequences $\alpha : \mathbb{N} \to \{0, 1\}$ and let $2^*$ be the set of finite sequences of 0s and 1s. For $s, t \in 2^*$ we write $s \subseteq t$ to mean that $s$ is an initial segment of $t$. A bar of $2^*$ is subset $R$ of $2^*$ such that the following property holds:

$$\forall \alpha \in 2^\mathbb{N} \exists n \alpha(n) \in R.$$ 

The bar $R$ is decidable if it also satisfies

$$\forall s \in 2^* (s \in R \lor s \notin R).$$

$\text{FT}_D$ is the statement that every decidable bar $R$ of $2^*$ is uniform, i.e., there exists a natural number $m$ such that

$$\forall \alpha \in 2^\mathbb{N} \exists m \alpha(k) \in R.$$ 

The Fan Theorem or General Fan Theorem, $\text{FT}$, is the statement that every bar $R$ of $2^*$ is uniform.

Lemma: 4.3 $\text{FT}_D$ refutes CT.

Proof: Apply $\text{FT}_D$ to Kleene’s singular tree. For details see [28] 4.7.6. $\square$

4.1 Decidable Bar induction

Brouwer justified $\text{FT}_D$ by appealing to a principle known as decidable Bar Induction, $\text{BI}_D$.

Definition: 4.4 Let $\mathbb{N}^*$ be the set of all finite sequences of natural numbers. If $s \in \mathbb{N}^*$, $m \in \mathbb{N}$ and $s = \langle s_0, \ldots, s_k \rangle$ then $s \ast \langle m \rangle$ denotes the sequence $\langle s_0, \ldots, s_k, m \rangle$. A bar of $\mathbb{N}^*$ is defined in the same vein as a bar of $2^*$.

$\text{BI}_D$ is asserts that for every decidable bar $R$ of $\mathbb{N}^*$ and arbitrary class $Q$,

$$\forall s \in \mathbb{N}^* (s \in R \rightarrow s \in Q) \land$$

$$\forall s \in \mathbb{N}^* [\forall k \in \mathbb{N} s \ast \langle k \rangle \in Q \rightarrow s \in Q] \rightarrow$$

$$\langle \rangle \in Q.$$ 

Monotone Bar Induction, $\text{BI}_M$, asserts that for every bar $R$ of $\mathbb{N}^*$ and arbitrary class $Q$,

$$\forall s, t \in \mathbb{N}^* (s \in R \rightarrow s \ast t \in R) \land$$

$$\forall s \in \mathbb{N}^* (s \in R \rightarrow s \in Q) \land$$

$$\forall s \in \mathbb{N}^* [\forall k \in \mathbb{N} s \ast \langle k \rangle \in Q \rightarrow s \in Q] \rightarrow$$

$$\langle \rangle \in Q.$$ 

It is easy to see that $\text{BI}_M$ entails $\text{BI}_D$ (cf. [10], Theorem 3.7).

Corollary: 4.5 $\text{BI}_D$ implies $\text{FT}_D$ and $\text{BI}_M$ implies $\text{FT}$.

Proof: See [15], Ch.I,§6.10 (or exercise). $\square$
4.2 Local continuity

In connection with Brouwer’s intuitionism, one often works with the local continuity, LCP, rather than CC. LCP entails \( \text{Cont}(\mathbb{N}^\mathbb{N}, \mathbb{N}) \) but not \( \text{AC}_{1,0} \).

**Definition:** 4.6 For \( \alpha, \beta \in \mathbb{N}^\mathbb{N} \) we write \( \beta \in \bar{\alpha}(n) \) to mean \( \beta(n) = \bar{\alpha}(n) \).

The **Local Continuity Principle**, LCP, states that
\[
\forall \alpha \in \mathbb{N}^\mathbb{N} \exists n \in \mathbb{N} A(\alpha, n) \rightarrow \forall \alpha \in \mathbb{N}^\mathbb{N}, m \in \mathbb{N} \forall \beta \in \mathbb{N}^\mathbb{N} [\beta \in \bar{\alpha}(m) \rightarrow A(\beta, n)].
\]

LCP is also known as the **Weak Continuity Principle** (WC-N) (see [28], p. 371) or **Brouwer’s Principle for Numbers** (BP_0).

Some obvious deductive relationships between some of the principles are recorded in the next lemma.

**Lemma:** 4.7 (i) LCP \( \Rightarrow \text{Cont}(\mathbb{N}^\mathbb{N}, \mathbb{N}) \).

(ii) CC \( \iff \) LCP \( \land \text{AC}_{1,0} \).

**Proof:** Obvious. \( \Box \)

While CC entails the choice principle \( \text{AC}_{1,0} \), it is not compatible with choice for higher type objects. In point of fact, the incompatibility already occurs in connection with a consequence of CC.

**Lemma:** 4.8 Let \( \text{AC}_{2,0} \) be the following principle:

If \( P \) is a subset of \( (\mathbb{N}^\mathbb{N} \rightarrow \mathbb{N}) \times \mathbb{N} \) such that for every \( f : \mathbb{N}^\mathbb{N} \rightarrow \mathbb{N} \) there exists \( n \in \mathbb{N} \) such that \( (f, n) \in P \), then there exists a function \( F : (\mathbb{N}^\mathbb{N} \rightarrow \mathbb{N}) \rightarrow \mathbb{N} \) such that for all \( f : \mathbb{N}^\mathbb{N} \rightarrow \mathbb{N} \), \( (f, F(f)) \in P \).

\( \text{AC}_{2,0} \) refutes \( \text{Cont}(\mathbb{N}^\mathbb{N}, \mathbb{N}) \).

**Proof:** See [27] or [5], Theorem 19.1. \( \Box \)

LCP and \( \text{a fortiori} \) CC refute principles of omniscience. For \( \alpha \in 2^\mathbb{N} \) let \( \alpha_n := \alpha(n) \).

**Definition:** 4.9 **Limited Principle of Omniscience** (LPO):

\[
\forall \alpha \in 2^\mathbb{N} [\exists n \alpha_n = 1 \lor \forall n \alpha_n = 0].
\]

**Lesser Limited Principle of Omniscience** (LLPO):

\[
\forall \alpha \in 2^\mathbb{N} (\forall n, m [\alpha_n = \alpha_m = 1 \rightarrow n = m] \rightarrow [\forall n \alpha_{2n} = 0 \lor \forall n \alpha_{2n+1} = 0]).
\]

**Lemma:** 4.10 (i) LCP \( \Rightarrow \neg \text{LPO} \).

(ii) CC \( \Rightarrow \neg \text{LLPO} \).

**Proof:** (i) follows from [28] 4.6.4. (ii) is proved in [7], 5.2.1. \( \Box \)

LCP is also incompatible with Church’s thesis.

**Lemma:** 4.11 LCP implies \( \neg \text{CT} \).
Proof: [28], 4.6.7. Apply LCP to CT.
With the help of LCP one deduces Brouwer’s famous theorem.

Theorem: 4.12 If LCP holds, then every map \( f : \mathbb{R} \rightarrow \mathbb{R} \) is pointwise continuous.

Proof: [28] Theorem 6.3.4.
Brouwer needed the fan theorem to derive the classically valid Uniform Continuity Principle:

\[ \text{UC} \quad \text{Every pointwise continuous function from } 2^\mathbb{N} \text{ to } \mathbb{N} \text{ is uniformly continuous.} \]

Lemma: 4.13 FT implies UC.

Under LCP we can drop the condition of continuity.

Corollary: 4.14 If LCP and FT hold, then every \( f : [a,b] \rightarrow \mathbb{R} \) is uniformly continuous and has a supremum.


Theorem: 4.15 Under the hypothesis CC, the statements UC and FT_D are equivalent.

Proof. See [7] Theorem 5.3.2 and Corollary 5.3.4.

Corollary: 4.16 If CC and FT_D hold, then every mapping of a nonvoid compact metric space into a metric space is uniformly continuous.

Proof: [7], Theorem 5.3.6.

5 More Continuity Principle

Another continuity principle one finds in the literature is Strong Continuity for Numbers:

\[ \text{C-N} \quad \forall \alpha \in \mathbb{N}^\mathbb{N} \exists x \in \mathbb{N} \ A(\alpha,x) \rightarrow \exists \gamma \in K^* \forall \alpha \in \mathbb{N}^\mathbb{N} A(\alpha,\gamma(\alpha)), \quad (1) \]

where \( K^* \) is the class of neighbourhood functions, i.e. \( \gamma \in K^* \) iff \( \gamma : \mathbb{N}^* \rightarrow \mathbb{N} \) and \( \gamma(\bar{0}) = 0 \land \forall s,t \in \mathbb{N}^* [\gamma(s) \neq 0 \rightarrow \gamma(s) = \gamma(s*t)] \land \forall \alpha \in \mathbb{N}^\mathbb{N} \exists n \in \mathbb{N} \gamma(\bar{\alpha}(n)) \neq 0 \)

and

\( \gamma(\alpha) = n \text{ iff } \exists m \in \mathbb{N} [\gamma(\bar{\alpha}(m)) = n + 1] \).

Dummett in [10], p. 60 refers to C-N as ‘the Continuity Principle’ and assigns it the acronym CP_3n.

In point of fact, C-N is just a different rendering of CC.
Definition: 5.1 We introduce abbreviations for partial continuous application:
\[
\begin{align*}
\alpha(\beta) = x & := \exists y [\alpha(\beta(y)) = x + 1 \land \forall y' < y (\alpha(\beta(y')) = 0)] , \\
\alpha|\beta = \gamma & := \forall x [\lambda n.\alpha(x + n)(\beta) = \gamma(x)] \land \alpha(0) = 0.
\end{align*}
\]

A yet stronger continuity principle is functional continuous choice \(F-CC\) or \(\text{CONT}_1\) (cf. [28], 7.6.15) (also denoted by C-C in [28], 7.6.15 and by CP\(_{\exists \beta}\) in [10], p. 60):
\[
F-CC \quad \forall \alpha \in \mathbb{N}^{\mathbb{N}} \exists \beta \in \mathbb{N}^{\mathbb{N}} A(\alpha, \beta) \rightarrow \exists \gamma \in \mathbb{K}^* \forall \alpha \in \mathbb{N}^{\mathbb{N}} A(\alpha, \gamma|\alpha).
\]

\(F-CC\) is not considered to be part of Brouwer’s realm as it is actually inconsistent with some of Brouwer’s later, though controversial, proposals about the “creative subject” (see [10] 6.3).

In point of fact, \(F-CC\) is equivalent to the schema
\[
F-CC' \quad \forall \alpha \in \mathbb{N}^{\mathbb{N}} \exists \beta \in \mathbb{N}^{\mathbb{N}} A(\alpha, \beta) \rightarrow \exists \gamma \in \mathbb{N}^{\mathbb{N}} \forall \alpha \in \mathbb{N}^{\mathbb{N}} A(\alpha, \gamma|\alpha)
\]

because if \(\gamma|\alpha\) is defined for all \(\alpha\), one can define \(\gamma^* \in \mathbb{K}^*\) such that \(\gamma^*|\alpha = \gamma|\alpha\) for all \(\alpha \in \mathbb{N}^{\mathbb{N}}\) where \(\gamma^*\) is recursive in \(\gamma\): Put \(\gamma^*(\langle \rangle) = 0\) and
\[
\gamma^*(s * \langle n \rangle) = \begin{cases} 
\gamma^*(s) & \text{if } \gamma^*(s) > 0 \\
\gamma(s) & \text{if } \gamma^*(s) = 0 \text{ and } \gamma(s) > 0 \\
0 & \text{if } \gamma^*(s) = \gamma(s) = 0.
\end{cases}
\]

Lemma: 5.2 (i) C-N \(\leftrightarrow\) CC.
(ii) \(F-CC\) implies CC.

Proof: For (i) see [7], p. 119. (ii) is to be found in [28], 7.6.15. \(\square\)

In the presence of CC, one can actually dispense with the decidability of the bar in FT\(_D\) and BI\(_D\).

Lemma: 5.3 Assuming CC, FT\(_D\) implies FT and BI\(_D\) implies BI\(_M\).

Proof: This follows from C-N \(\leftrightarrow\) CC by [10], Theorem 3.8 and the proof of the general fan theorem of [10], page 64. \(\square\)

6 Elementary analysis augmented by Brouwerian principles

Realizability interpretations of Brouwerian principles have been given for elementary analysis. It should be instructive to review these results before venturing to the more complex realizability models required for set theory.

Elementary analysis, \(EL\), is a two-sorted intuitionistic formal system with variables \(x, y, z, \ldots\) intended to range over natural numbers and variables \(\alpha, \beta, \gamma, \ldots\) intended to range over one-place total functions from \(\mathbb{N}\) to \(\mathbb{N}\). The language of \(EL\) is an extension of the language of of Heyting Arithmetic. In particular, \(\pi\) is a symbol for a primitive-recursive pairing function on \(\mathbb{N} \times \mathbb{N}\) and \(S\) is the symbol for the successor function.

\(EL\) is a conservative extension of Heyting Arithmetic. The details of this theory are described in [15] Ch.I and [28], Ch.3,Sect.6. There is \(\lambda\)-abstraction
for explicit definitions of functions, and a recursion-operator Rec such that (t a numerical term, φ a function term; φ(∗) := φ(π(∗)))

\[ 
\text{Rec}(t, φ)(0) = t, \quad \text{Rec}(t, φ)(Sx) = φ(x, \text{Rec}(t, φ)(x)). 
\]

Induction is extended to all formulas in the new language. The functions of EL are assumed to be closed under “recursive in”, which is expressed by including a weak choice axiom for quantifier-free A:

\[ \text{QF-AC} \quad \forall x \exists y A(x, y) \rightarrow \exists x A(x, α(x)). \]

We may introduce the operations |, · of Definition 5.1 as primitive operators in a conservative extension EL∗ based on the logic of partial terms.

It was shown by Kleene in [15], Ch.II that EL augmented by the principles BI and C-N is consistent. For this purpose he used a realizability interpretation based on continuous function application, i.e. the second Kleene algebra K2. As this paper will follow a similar strategy for gauging the strength of CZF extended by Brouwerian principles it is instructive to review Kleene’s results.

**Definition: 6.1 (Function realizability)** In EL equality of functions α = β is not a prime formula and defined by ∀x α(x) = β(x).

The function realizability interpretation is an inductively defined translation of a formula A of EL into a formula α rf A of EL, where α is a fresh variable not occurring in A:

\[ 
\alpha \text{ rf } \bot \quad \text{iff} \quad \bot \\
\alpha \text{ rf } t = s \quad \text{iff} \quad t = s \\
\alpha \text{ rf } A \land B \quad \text{iff} \quad \pi_0 α \text{ rf } A \land \pi_1 α \text{ rf } B \\
\alpha \text{ rf } A \lor B \quad \text{iff} \quad [α(0) = 0 \rightarrow α^+ \text{ rf } A] \land [α(0) ≠ 0 \rightarrow α^+ \text{ rf } B] \\
\alpha \text{ rf } A \rightarrow B \quad \text{iff} \quad \forall β [β \text{ rf } A \rightarrow α[β] \land α[β] \text{ rf } B] \\
\alpha \text{ rf } \exists x A(x) \quad \text{iff} \quad \forall x [α[λn.x \downarrow ] \land α[λn.x \text{ rf } A(x)]] \\
\alpha \text{ rf } \forall β A(β) \quad \text{iff} \quad \forall β [α[β] \land α[β] \text{ rf } A(β)] \\
\alpha \text{ rf } \exists β A(β) \quad \text{iff} \quad π_1 α \text{ rf } A(παα) 
\]

with π₀, π₁ being the projection functions with respect to some fixed primitive recursive pairing function π : N × N → N and α⁺ being the tail of α (i.e. α = (α0) * α⁺).

**Lemma: 6.2** Let A be a closed formula of EL. If EL + C-N ⊨ A, then EL ⊨ ∃α α rf A.

**Proof:** See [26], theorem 3.3.11.

Kleene shows in [15], Ch.II, Lemma 9.10 that the arithmetical functions constitute the least class of functions C ⊆ N N closed under general recursiveness and the jump operation ’ (look there for precise definitions).

An inhabited set C ⊆ N N gives rise to a structure R C for the language of EL as follows: The domain of R C is N ∪ C, the number variables range over N; the function variables range over C, and the other primitives of EL are interpreted in the standard way.
Lemma: 6.3 (KP) For any set of functions $\mathcal{C} \subseteq \mathbb{N}^\mathbb{N}$ closed under general recursiveness and the jump operation $'$: the fan theorem $\text{FT}$ holds in the classical model $\mathcal{N}^\mathcal{C}$ of $\text{EL}$, when the representing function of the bar $R$ belongs to $\mathcal{C}$.

Proof: [15], Lemma 9.12.

Theorem: 6.4 (KP) For any set of functions $\mathcal{C} \subseteq \mathbb{N}^\mathbb{N}$ closed under general recursiveness and the jump operation $'$ (e.g. the arithmetical functions): If $\text{EL} + \mathcal{C} \cdot \text{N} + \text{FT} \vdash A$, then $\mathcal{N}^\mathcal{C} \models \exists \alpha \alpha \text{rf} A$.

Proof: [15], Ch.11 Theorem 9.13. □

Kleene’s proof of Theorem 6.4 can actually be extended to include $\text{BI}_M$.

Definition: 6.5 An inhabited set of functions $\mathcal{C} \subseteq \mathbb{N}^\mathbb{N}$ is said to be a $\beta$-model if $\mathcal{C}$ is closed under general recursiveness and the jump operation $'$ and whenever $\prec$ is a binary relation on $\mathbb{N}$ whose representing function is in $\mathcal{C}$ and $\mathcal{N}^\mathcal{C} \models \forall \alpha \exists n \neg \alpha(n+1) \prec \alpha(n)$, then $\prec$ is well-founded.

Lemma: 6.6 (KPi) If $\mathcal{C} \subseteq \mathbb{N}^\mathbb{N}$ is a $\beta$-model then monotone bar induction holds in the classical model $\mathcal{N}^\mathcal{C}$ of $\text{EL}$, when the representing function of the bar $R$ belongs to $\mathcal{C}$.

Proof: Similar to [15], Ch.11 Lemma 9.12.

Theorem: 6.7 (KPi) For any $\beta$-model $\mathcal{C} \subseteq \mathbb{N}^\mathbb{N}$ (e.g. the functions in $\mathbb{N}^\mathbb{N} \cap L_\rho$, where $\rho = \sup_{\alpha < \omega} \omega^{3^\alpha}$ with $\omega^{3^\alpha}$ being the $\alpha$th admissible ordinal; cf. [4]): If $\text{EL} + \mathcal{C} \cdot \text{N} + \text{BI}_M \vdash A$, then $\mathcal{N}^\mathcal{C} \models \exists \alpha \alpha \text{rf} A$.

Proof: Since $\text{BI}_M$ follows from $\text{BI}_D$ on the basis of $\text{EL} + \mathcal{C} \cdot \text{N}$ it suffices to find realizers for instances of $\text{BI}_D$.

So assume that

\begin{align*}
\beta \text{ rf } & \forall n [R(n) \lor \neg R(n)], \\
\gamma \text{ rf } & \forall \alpha \exists n R(\bar{\alpha}(n)), \\
\delta \text{ rf } & \forall s [R(s) \rightarrow Q(s)], \\
\eta \text{ rf } & \forall s \forall x Q(s * \langle x \rangle) \rightarrow Q(s). 
\end{align*}

Set $\beta_n := \beta(\lambda x. n)$. (2) implies that

$$\beta_n(0) \rightarrow \beta_n^+ \text{ rf } \forall n R(n) \text{ and } \beta_n(0) \neq 0 \rightarrow \beta_n^+ \text{ rf } \forall n \neg R(n)$$

while (3) yields that

$$\forall \alpha \pi_1(\gamma | \alpha) \text{ rf } R(\bar{\alpha}((\pi_0(\gamma | \alpha))(0)))$$

so that

$$\forall \alpha \exists m \beta_{\delta(m)}(0) = 0.$$  

Now define $a \prec s$ on $\mathbb{N}$ by $t \prec s := \beta_n(0) \neq 0 \land \exists u t = s * \langle u \rangle$. On account of (7) and $\mathcal{C}$ being a $\beta$-model, it follows that $\prec$ is well-founded relation.
Define a function \( \psi : \mathbb{N} \to \mathbb{C} \) by transfinite recursion on \( \prec \) as follows:

\[
\psi(s) = \begin{cases} 
\delta|\beta^+ \quad &\text{if } \beta_s(0) = 0 \\
(\eta|\lambda u.s)|\ell(\psi, s) &\text{if } \beta_s(0) \neq 0,
\end{cases}
\]

where \( \ell \) is a \( \mathbb{C} \)-valued operation to the effect that \( \ell(\alpha, s)|\lambda u.k = \alpha(s * \langle k \rangle) \). Note that formal terms denoting \( \psi \) and \( \ell \) in the model \( \mathcal{N}_\mathbb{C} \) (uniformly in the parameters \( \beta, \gamma, \delta, \eta \)) can be defined in the system \( \text{EL}^* \) (based on the logic of partial terms) using the recursion theorem and other gadgets.

By transfinite induction on \( \prec \) we shall prove that for all \( s \in \mathbb{N} \),

\[
\psi(s) \ni Q(s)
\]

Case 1: Suppose that \( \beta_s = 0 \). Using (6) we get \( \beta^+_s \ni R(s) \), and hence \( \delta|\beta^+_s \ni Q(s) \) by (4); thus \( \psi(s) \ni Q(s) \).

Case 2: Now suppose that \( \beta_s \neq 0 \). Then \( s * \langle k \rangle \prec s \) for all \( k \in \mathbb{N} \), and the inductive hypothesis yields \( \psi(s * \langle k \rangle) \ni Q(s * \langle k \rangle) \) for all \( k \); thence \( \ell(\psi, s) \ni \forall x Q(s * \langle x \rangle) \). By (5) we have \( \eta|\lambda u.s \ni \ell(\psi, s) \ni Q(s) \).

In sum, we have \( \psi(s) \ni Q(s) \), confirming (8).

In view of the above we conclude the realizability of \( \text{BI}_\mathbb{D} \) in the model \( \mathcal{N}_\mathbb{C} \).

\( \square \)

7 Combinatory Algebras

The notion of function is crucial to any concrete BHK-interpretation in that it will determine the set theoretic and mathematical principles validated by it. The most important semantics for intuitionistic theories, known as realizability interpretations, also require that we have a set of (partial) functions on hand that serve as realizers for the formulae of the theory. An abstract and therefore “cleaner” approach to this semantics considers realizability over general domains of computations allowing for recursion and self-application. These structures have been variably called partial combinatory algebras, applicative structures, or Schönfinkel algebras. They are closely related to models of the \( \lambda \)-calculus.

Let \( (M, \cdot) \) be a structure equipped with a partial operation, that is, \( \cdot \) is a binary function with domain a subset of \( M \times M \) and co-domain \( M \). We often omit the sign “.” and adopt the convention of “association to the left”. Thus \( e \cdot x \cdot y \) means \( (e \cdot x) \cdot y \). We also sometimes write \( e \cdot x \) in functional notation as \( e(x) \). Extending this notion to several variables, we write \( e(x, y) \) for \( e(xy) \) etc.

**Definition:** 7.1 A \( \text{PCA} \) is a structure \( (M, \cdot) \), where \( \cdot \) is a partial binary operation on \( M \), such that \( M \) has at least two elements and there are elements \( k \) and \( s \) in \( M \) such that \( kxy \) and \( szx \) are always defined, and

\[
\begin{align*}
(i) \quad & kxy = x \\
(ii) \quad & szx \simeq x(yz),
\end{align*}
\]
where \( \simeq \) means that the left hand side is defined iff the right hand side is defined, and if one side is defined then both sides yield the same result.

\((M, \cdot)\) is a total PCA if \(a \cdot b\) is defined for all \(a, b \in M\).

**Definition: 7.2** Partial combinatory algebras are best described as the models of a formal theory \(\text{PCA}\). The language of \(\text{PCA}\) has two distinguished constants \(k\) and \(s\). To accommodate the partial operation in a standard first order language, the language of \(\text{PCA}\) has a trinary relation symbol \(\text{Ap}\). The terms of \(\text{PCA}\) are just the variables and constants. \(\text{Ap}\) will almost never appear in what follows as we prefer to write \(t_1t_2 \simeq t_3\) for \(\text{Ap}(t_1, t_2, t_3)\). In order to facilitate the formulation of the axioms, the language of \(\text{PCA}\) is expanded definitionally with the symbol \(\simeq\) and the auxiliary notion of an application term or partial term is introduced.

The set of application terms is given by two clauses:

1. All terms of \(\text{PCA}\) are application terms; and
2. If \(s\) and \(t\) are application terms, then \((st)\) is an application term.

For \(s\) and \(t\) application terms, we have auxiliary, defined formulae of the form:

\[ s \simeq t := \forall y (s \simeq y \leftrightarrow t \simeq y), \]

if \(t\) is not a variable. Here \(s \simeq a\) (for \(a\) a free variable) is inductively defined by:

\[ s \simeq a \quad \text{is} \quad \begin{cases} s = a, & \text{if } s \text{ is a term of } \text{PCA}, \\ \exists x, y [s_1 \simeq x \land s_2 \simeq y \land \text{Ap}(x, y, a)] & \text{if } s \text{ is of the form } (s_1s_2). \end{cases} \]

Some abbreviations are \(t_1t_2\ldots t_n\) for \((\ldots((t_1t_2)...t_n))\); \(t \downarrow\) for \(\exists y(t \simeq y)\) and \(\phi(t)\) for \(\exists y(t \simeq y \land \phi(y))\).

In this paper, the logic of \(\text{PCA}\) is assumed to be that of intuitionistic predicate logic with identity. \(\text{PCA}\)'s non-logical axioms are the following:

**Axioms of PCA**

1. \(ab \simeq c_1 \land ab \simeq c_2 \rightarrow c_1 = c_2\).
2. \((kab) \downarrow \land kab \simeq a\).
3. \((sab) \downarrow \land sabc \simeq ac(bc)\).

The following shows how \(\lambda\)-terms can be constructed in \(\text{PCA}\).

**Lemma: 7.3** For each application term \(t\) and variable \(x\), one can construct a term \(\lambda x.t\), whose free variables are those of \(t\), excluding \(x\), such that \(\text{PCA} \vdash \lambda x.t \downarrow\) and \(\text{PCA} \vdash (\lambda x.t)u \simeq t[x/u]\) for all application terms \(u\), where \(t[x/u]\) results from \(t\) by replacing \(x\) in \(t\) throughout by \(u\).

**Proof:** We proceed by induction on the buildup of \(t\). (i) \(\lambda x.x\) is \(\text{skk}\); (ii) \(\lambda x.t\) is \(kt\) for \(t\) a constant of \(\text{PCA}\) or variable other than \(x\); (iii) \(\lambda x.t_1t_2\) is \(s(\lambda x.t_1)(\lambda x.t_2)\).

Having \(\lambda\)-terms on hand, one can easily prove the recursion or fixed point theorem in \(\text{PCA}\), and consequently that all recursive functions are definable in \(\text{PCA}\). The elegance of the combinators arises from the fact that, at least in theory, anything that can be done in a programming language can be done using solely \(k\) and \(s\).
Lemma: 7.4 (Recursion Theorem) There is an application term $r$ such that PCA proves:

$$rx \downarrow \land rxy \simeq x(rx)y.$$ 

Proof: Take $r$ to be $\lambda x.gg$ where $g := \lambda y.x(zz)y$. Then $rx \simeq gg \simeq (\lambda y.x(zz)y)g \simeq \lambda y.x(gg)y$, so that $rx \downarrow$ by Lemma 7.3. Moreover, $rxy \simeq x(gg)y \simeq x(rx)y$. \hfill $\square$

Corollary: 7.5 $\text{PCA} \vdash \forall f \exists g \forall x_1 \ldots \forall x_n g(x_1, \ldots, x_n) \simeq f(g, x_1, \ldots, x_n)$.

It often convenient to equip a PCA with additional structure such as pairing, natural numbers, and some form of definition by cases. In fact, these gadgets can be constructed in any PCA, as Curry showed. Nonetheless, it is desirable to consider richer structures as the natural models for PCAs we are going to study come already furnished with a “natural” copy of the natural numbers, natural pairing functions, etc., which are different from the constructions of combinatory logic.

Definition: 7.6 The language of $\text{PCA}^+$ is that of $\text{PCA}$, with a unary relation symbol $N$ (for a copy of the natural numbers) and additional constants $0, s_N, p_N, d, p, p_0, p_1$ for, respectively, zero, successor on $N$, predecessor on $N$, definition by cases on $N$, pairing, and the corresponding two projections.

The axioms of $\text{PCA}^+$ are those of $\text{PCA}$, augmented by the following:

1. $(p_0a_1) \downarrow \land (p_0a) \downarrow \land (p_1a) \downarrow \land p_i(p_0a_1) \simeq a_i$ for $i = 0, 1$.
2. $N(c_1) \land N(c_2) \land c_1 = c_2 \rightarrow dabc_1c_2 \downarrow \land dabc_1c_2 \simeq a$.
3. $N(c_1) \land N(c_2) \land c_1 \neq c_2 \rightarrow dabc_1c_2 \downarrow \land dabc_1c_2 \simeq b$.
4. $\forall x (N(x) \rightarrow [s_Nx \downarrow \land s_Nx \neq 0 \land N(s_Nx)])$.
5. $N(0) \land \forall x (N(x) \land x \neq 0 \rightarrow [p_Nx \downarrow \land s_N(p_Nx) = x])$.
6. $\forall x [N(x) \rightarrow p_0(s_Nx) = x]$.

The extension of $\text{PCA}^+$ by the schema of induction for all formulae,

$$\varphi(0) \land \forall x [N(x) \land \varphi(x) \rightarrow \varphi(s_Nx)] \rightarrow \forall x [N(x) \rightarrow \varphi(x)]$$

is is known by the acronym EON (elementary theory of operations and numbers) or APP (applicative theory). For full details about $\text{PCA}$, $\text{PCA}^+$, and EON see [11, 12, 5, 28].

Let $1 := s_N0$. The applicative axioms entail that $1$ is an application term that evaluates to an object falling under $N$ but distinct from $0$, i.e., $1 \downarrow$, $N(1)$ and $0 \neq 1$. More generally, we define the standard integers of a PCA to be the interpretations of the numerals, i.e. the terms $n$ defined by $0 = 0$ and $n + 1 = s_Nn$ for $n \in \mathbb{N}$. Note that $\text{PCA}^+ \vdash n \downarrow$.

A $\omega$-$\text{PCA}^+$ ($\omega$-$\text{APP}$) whose integers are standard, meaning that $\{x \in M \mid M \models N(x)\}$ is the set consisting of the interpretations of the numerals in $M$, will be called an $\omega$-$\text{PCA}^+$. Note that an $\omega$-$\text{PCA}^+$ is also a model of APP.

Some further conventions are useful. Systematic notation for $n$-tuples is introduced as follows: $(t)$ is $t$, $(s, t)$ is $p_{st}$, and $(t_1, \ldots, t_n)$ is defined by $((t_1, \ldots, t_{n-1}), t_n)$.

Lemma: 7.7 $\text{PCA}^+$ is conservative over PCA.

Proof: See [5], VI, 2.9. \hfill $\square$
7.1 Kleene’s Examples of Combinatory Algebras

The primordial PCA is furnished by Turing machine application on the integers. There are many other interesting PCAs that provide us with a laboratory for the study of computability theory. As the various definitions are lifted to more general domains and notions of application other than Turing machine applications some of the familiar results break down. By studying the notions in the general setting one sees with a clearer eye the truths behind the results on the integers.

7.1.1 Kleene’s first model

The “standard” applicative structure is Kleene’s first model, called $K_1$, in which the universe $|K_1|$ is $\mathbb{N}$ and $\text{Ap}^{K_1}(x, y, z)$ is Turing machine application:

$$\text{Ap}^{K_1}(x, y, z) \text{ iff } \{x\}(y) \simeq z.$$ 

The primitive constants of PCA$^\dagger$ are interpreted over $\mathbb{N}$ in the obvious way, and $\mathbb{N}$ is interpreted as $\mathbb{N}$.

Kleene’s second model

The universe of “Kleene’s second model” of $\text{APP}$, $K_2$, is $\mathbb{N}^2$. The most interesting feature of $K_2$ is that in the type structure over $K_2$, every type-2 functional is continuous.

We shall use $\alpha, \beta, \gamma, \ldots$ as variables ranging over functions from $\mathbb{N}$ to $\mathbb{N}$. In order to describe this PCA, it will be necessary to review some terminology.

Definition: 7.8 We assume that every integer codes a finite sequence of integers. For finite sequences $\sigma$ and $\tau$, $\sigma \subset \tau$ means that $\sigma$ is an initial segment of $\tau$; $\sigma \ast \tau$ is concatenation of sequences; $\langle \rangle$ is the empty sequence; $\langle n_0, \ldots, n_k \rangle$ displays the elements of a sequence; if this sequence is $\tau$ then $lh(\tau) = k + 1$ (read “length of $\tau$”); $\alpha(m) = (\alpha(0), \ldots, \alpha(m - 1))$ if $m > 0$; $\alpha(0) = \langle \rangle$. A function $\alpha$ and an integer $n$ produce a new function $\langle n \rangle \ast \alpha$ which is the function $\beta$ with $\beta(0) = n$ and $\beta(k + 1) = \alpha(k)$.

Application requires the following operations on $\mathbb{N}^N$:

$$\alpha \circ \beta = m \text{ iff } \exists n [\alpha(\beta n) = m + 1 \land \forall i < n \alpha(\beta i) = 0]$$

$$(\alpha|\beta)(n) = \alpha \circ (\langle n \rangle \ast \beta)$$

We would like to define application on $\mathbb{N}^N$ by $\alpha|\beta$, but this is in general only a partial function, therefore we set:

$$\alpha \cdot \beta = \gamma \text{ iff } \forall n (\alpha|\beta)(n) = \gamma(n). \quad (9)$$

Theorem: 7.9 $K_2$ is a model of APP.

Proof: For the natural numbers of $K_2$ take $N := \{\hat{n} | n \in \mathbb{N}\}$, where $\hat{n}$ denotes the constant function on $\mathbb{N}$ with value $n$. For pairing define the function $P : \mathbb{N}^N \to \mathbb{N}^N$ by $P(\alpha, \beta)(n) = \alpha(n/2)$ if $n$ is even and $P(\alpha, \beta)(n) = \beta(\frac{n+1}{2})$ if $n$ is odd. We then have to find a specific $\pi \in \mathbb{N}^N$ such that $(\pi|\alpha)|\beta = P(\alpha, \beta)$ for all $\alpha$ and $\beta$. Details on how to define all the constants of APP in $K_2$ can be found in [28],Ch.9,Sect.4.
Substructures of Kleene’s second model

Inspection of the definition of application in $K_2$ shows that subcollections of $\mathbb{N}^\mathbb{N}$ closed under “recursive in” give rise to substructures of $K_2$ that are models of $\text{APP}$ as well. Specifically, the set of unary recursive functions forms a substructure of $K_2$ as does the set of arithmetical functions from $\mathbb{N}$ to $\mathbb{N}$, i.e., the functions definable in the standard model of Peano Arithmetic, furnish a model of $\text{APP}$ when equipped with the application of (9).

8 Type Structures over Combinatory Algebras

We shall define an “internal” version of a transfinite type structure with dependent products and dependent sums over any applicative structure.

Definition: 8.1 Let $\mathbb{P} = (P, \cdot, \ldots)$ be an $\omega$-$\text{PCA}^+$. The types of $\mathbb{P}$ and their elements are defined inductively. The set of elements of a type $A$ is called its extension and denoted by $\hat{A}$. The type structure will be denoted by $\mathcal{T}_P$.

1. $\mathbb{N}^\mathbb{P}$ is a type with extension the set of integers of $\mathbb{P}$, i.e., $\{x \in P \mid P \models N(x)\}$.
2. For each integer $n$, $\mathbb{N}_n^\mathbb{P}$ is a type with extension $\{\vec{k} \mid k = 0, \ldots, n-1\}$ if $n > 0$ and $\mathbb{N}_0^\mathbb{P} = \emptyset$.
3. $U^\mathbb{P}$ is a type with extension $P$.
4. If $A$ and $B$ are types, then $A+_\mathbb{P} B$ is a type with extension $\{(0, x) \mid x \in \hat{A}\} \cup \{(1, x) \mid x \in \hat{B}\}$.
5. If $A$ is a type and for each $x \in \hat{A}$, $F(x)$ is a type, where $F \in P$ and $F(x)$ means $F \cdot x$, then $\prod_{x \in A} F(x)$ is a type with extension $\{f \in P \mid \forall x \in \hat{A} f \cdot x \in F(x)\}$.
6. If $A$ is a type and for each $x \in \hat{A}$, $F(x)$ is a type, where $F \in P$, then $\sum_{x \in A} F(x)$ is a type with extension $\{(x, u) \mid x \in \hat{A} \land u \in F(x)\}$.

The obvious question to ask is: Why should we distinguish between a type $A$ and its extension $\hat{A}$. Well, the reason is that we want to apply the application operation of $\mathbb{P}$ to types. For this to be possible, types have to be elements of $P$. Thus types aren’t sets. Alternatively, however, we could identify types with sets and require that they be representable in $\mathbb{P}$ in some way. This can be arranged by associating Gödel numbers in $\mathbb{P}$ with types and operations on types. This is easily achieved by employing the coding facilities of the $\text{PCA}^+ \mathbb{P}$. For instance, if the types $A$ and $B$ have Gödel numbers $\uparrow A$ and $\uparrow B$, respectively, then
$A + B$ has Gödel number $(1, \forall A \forall C \forall B \land C \land S \land T)$, and if $C$ is a type with Gödel number \( C \), $F \in P$, and for all $x \in C$, $F(x)$ is the Gödel number of a type $B_x$, then $(2, \forall C \forall F \land F \land S \land T)$ is the Gödel number of the dependent type $\prod_{x \in C} B_x$, etc. In what follows we will just identify types with their extensions (or their codes) as such ontological distinctions are always retrievable from the context.

**Remark 8.2** The ordinary product and arrow types can be defined with the aid of dependent products and sums, respectively. Let $A, B$ be types and $F \in P$ be a function such that $F(x) = B$ for all $x \in P$.

$$A \times B := \sum_{x \in A} F(x) \quad \quad A \to B := \prod_{x \in A} F(x).$$

**Definition 8.3 (The set-theoretic universe $V^\varphi$)** Starting from the internal type structure over an $\omega$-PCA $\mathbb{P}$, we are going to construct a universe of sets for intuitionistic set theory. The rough idea is that a set $X$ is given by a type $A$ together with a set-valued function $f$ defined on $A$ (or rather the extension of $A$) such that $X = \{ f(x) \mid x \in \tilde{A} \}$. Again, the objects of this universe will be coded as elements of $P$. The above set will be coded as sup($A, f$), where sup($A, f$) = $\langle 8, (A, f) \rangle$ or whatever. We sometimes write $\{ f(x) \mid x \in A \}$ for sup($A, f$).

Frequently we shall write $x \in A$ rather than $x \in \tilde{A}$.

The universe of sets over the type structure of $\mathbb{P}$, $V^\varphi$, is defined inductively by a single rule:

*if $A$ is a type over $\mathbb{P}$, $f \in P$, and $\forall x \in A \ f \cdot x \in V^\varphi$, then $\text{sup}(A, f) \in V^\varphi$.***

We shall use variables $\tilde{x}, \tilde{\eta}, \tilde{z}, \ldots$ to range over elements of $V^\varphi$. Each $\tilde{x} \in V^\varphi$ is of the form sup($A, f$). Define $\tilde{x} := A$ and $\tilde{f} := f$.

An essential characteristic of set theory is that sets having the same elements are to be identified. So if $\{ f(x) \mid x \in A \}$ and $\{ g(y) \mid y \in B \}$ are in $V^\varphi$ and for every $x \in A$ there exists $y \in B$ such that $f(x)$ and $g(y)$ represent the same set and conversely for every $y \in B$ there exists $x \in A$ such that $f(x)$ and $g(y)$ represent the same set, then $\{ f(x) \mid x \in A \}$ and $\{ g(y) \mid y \in B \}$ should be identified as sets. This idea gives rise to an equivalence relation on $V^\varphi$.

**Definition 8.4 (Kleene realizability over $V^\varphi$)** We will introduce a semantics for sentences of set theory with parameters from $V^\varphi$. Bounded set quantifiers will be treated as quantifiers in their own right, i.e., bounded and unbounded quantifiers are treated as syntactically different kinds of quantifiers. Let $\tilde{x}, \tilde{\eta} \in V^\varphi$ and $e, f \in P$. We write $\varepsilon_{i,j}$ for $\langle (e_i)_j \rangle$.

\[
\begin{align*}
e \vDash_{\tilde{x}} \tilde{x} \in \tilde{\eta} & \iff (e)_0 \in \tilde{\eta} \land (e_1)_0 \vDash_{\tilde{x}} \tilde{x} = \tilde{\eta}_0 \\
e \vDash_{\tilde{x}} \tilde{x} = \tilde{\eta} & \iff \forall i \in \tilde{x} [e_{0,0}i \in \tilde{\eta} \land (e_{0,1}i)_1 \vDash_{\tilde{x}} \tilde{\eta}_i = \tilde{\eta}(e_{0,0}i)] \land \\
& \forall i \in \tilde{\eta} [e_{1,0}i \in \tilde{x} \land (e_{1,1}i)_1 \vDash_{\tilde{x}} \tilde{\eta}_i = \tilde{\eta}(e_{1,0}i)] \\
e \vDash_{\tilde{x}} \phi \land \psi & \iff (e)_0 \vDash_{\tilde{x}} \phi \land (e)_1 \vDash_{\tilde{x}} \psi
\end{align*}
\]
The definitions of $V$ transfinite recursion, i.e. by recursion on the inductive definition of $\text{ord}$ with at most the free variables exhibited. If

Let $\text{Theorem: 8.5}$

then there exists a closed application term $t_\varphi$ of $\text{PCA}^+$ such that for all $\xi_1, \ldots, \xi_r \in V^\varphi$,

$$\mathbb{P} \models t_{\varphi \xi_1 \ldots \xi_r} \downarrow$$

and

$$t_{\varphi \xi_1 \ldots \xi_r} \models_\varphi \varphi(\xi_1, \ldots, \xi_r).$$

The term $t_\varphi$ can be effectively constructed from the $\text{CZF}$-deduction of $\varphi(\xi_1, \ldots, \xi_r)$.

**Remark: 8.6** A background theory sufficient for carrying out the definition of $V^\varphi$ and establishing Theorem 8.5 is $\text{KP}$. More precisely, if $\text{KP}$ proves that $\mathbb{P}$ is an $\omega$-$\text{PCA}^+$ and $\text{CZF + RDC} \vdash \varphi(\xi_1, \ldots, \xi_r)$, then there exists a closed application term $t_\varphi$ of $\text{PCA}^+$ such that $\text{KP}$ proves for all $\xi_1, \ldots, \xi_r \in V^\varphi$, $\mathbb{P} \models t_{\varphi \xi_1 \ldots \xi_r} \downarrow$ and $t_{\varphi \xi_1 \ldots \xi_r} \models_\varphi \varphi(\xi_1, \ldots, \xi_r)$.

To obtain a similar result for $\text{CZF}$ plus the regular extension axiom we need a stronger type structure.

**Definition: 8.7** Let $\mathbb{P} = (P, \ldots)$ be an $\omega$-$\text{PCA}^+$.

The type structure $T^\mathbb{P}_W$ is defined by adding one more inductive clause to Definition 8.1.

(7) If $A$ is a type and for each $x \in \hat{A}$, $F(x)$ is a type, where $F \in P$ and $F(x)$ means $F \cdot x$, then

$$W^\varphi_x A F(x)$$

is a type with extension $S$, where $S$ is the set inductively defined by the following clause:

If $a \in \hat{A}$, $f \in P$, and $\forall x \in F(a)$ $f \cdot x \in S$, then $p(a, f) \in S$.

The set-theoretic universe $V^\mathbb{P}_w$ is defined in the same vein as $V^\varphi$ except that it is built over the type structure $T^\mathbb{P}_W$.

Realizability over $V^\mathbb{P}_w$ is defined similarly as in Definition 8.4 with $V^\varphi_w$ replacing $V^\varphi$. 
Theorem: 8.8 Let $\mathbb{P}$ be an $\omega$-PCA$^+$. Let $\varphi(v_1,\ldots,v_r)$ be a formula of set theory with at most the free variables exhibited. If

$$\text{CZF} + \text{REA} + \text{RDC} \vdash \varphi(v_1,\ldots,v_r)$$

then there exists a closed application term $t_\varphi$ of PCA$^+$ such that for all $x_1,\ldots,x_r \in V^w$,

$$\mathbb{P} \models t_\varphi x_1 \ldots x_r \downarrow$$

and

$$t_\varphi x_1 \ldots x_r \models \varphi(x_1,\ldots,x_r).$$

The term $t_\varphi$ can be effectively constructed from the CZF + REA-deduction of $\varphi(v_1,\ldots,v_r)$.

Remark: 8.9 A background theory sufficient for carrying out the definition of $V^w$ and establishing Theorem 8.8 is KPi.

9 The set-theoretic universe over Kleene’s second model

Henceforth let $U$ be a subset of $\mathbb{N}^\mathbb{N}$ closed under ‘recursive in’ and the jump operator. Let $\mathbb{A}$ be Kleene’s second model based on $U$, i.e. the applicative structure with domain $U$ and application being continuous function application, $\cdot$. The interpretation of the natural numbers in $\mathbb{A}$ that is the interpretation $N^\mathbb{A}$ of the predicate symbol $N$ in $\mathbb{A}$ is the set of all constant functions. We use $\hat{n}$ to denote the constant function with value $n$. In particular there are the interpretations $k^\mathbb{A},s^\mathbb{A},0^\mathbb{A},p^\mathbb{A},d^\mathbb{A},p_0^\mathbb{A},p_1^\mathbb{A}$ of the constants of APP in $U$. We shall, however, mostly drop the superscript $\mathbb{A}$.

Our goal is to show that in addition to the axioms of CZF, $V^\mathbb{A}$ also realizes CC and FT. The first step is to single out the element of $V^\mathbb{A}$ that plays the role of $\omega$ and the Baire space $\omega^\omega$, respectively. We use variables $\alpha,\beta,\gamma,\ldots$ to range over $U$. Let $V := V^\mathbb{A}$. Define

$$\emptyset := \sup(N_0^\mathbb{A},\lambda\alpha.\alpha)$$
$$\emptyset' := \sup\left(\emptyset+\lambda_{n+1}N_1^\mathbb{A},\lambda\beta.d(\emptyset(p_1\beta),\emptyset,p_0\beta,0)\right)$$

and $\Delta \in U$ by

$$\Delta \cdot \eta = \begin{cases} \emptyset & \text{if } \eta(0) = 0 \\ (\Delta \cdot (\eta - 1))' & \text{if } \eta(0) \neq 0, \end{cases}$$

where $\eta - 1$ is the function $\gamma$ with $\gamma(n) = \eta(n) - 1$ if $\eta(n) > 0$ and $\gamma(n) = 0$ otherwise. The definition of $\Delta$ appeals to the recursion theorem for $\mathbb{A}$. Finally, $\omega$ is defined by

$$\omega := \sup(N^\mathbb{A},\Delta).$$

By induction on $n$ one shows that $\Delta \cdot \hat{n} \downarrow$ and $\Delta \cdot \hat{n} \in V$, thus $\omega \in V$.

The representation $\omega$ of the set of von Neumann integers has an important property.

---

4 The recursion theorem for partial continuous function application and other details of recursion theory in $\mathbb{A}$ can be found in [28] 3.7.
Definition: 9.1 We use $\models_{\lambda} A$ to convey that $\eta \models_{\lambda} A$ for some $\eta \in U$.

$x \in V$ is injectively presented if for all $\alpha, \beta \in \bar{x}$, whenever $\models_{\lambda} \tilde{\eta}(\tilde{\alpha}) = \tilde{\eta}(\tilde{\beta})$

then $\alpha = \beta$.

Lemma: 9.2 $\omega$ is injectively presented.

Proof: We must show that $\models_{\lambda} \Delta \cdot \tilde{n} = \Delta \cdot \tilde{m}$ implies $n = m$. This can be verified by a routine double induction, first on $n$ and within that on $m$. For details see [1] Lemma 5.5 or [23] Theorem 4.24. □

Corollary: 9.3 The Axiom of Countable Choice, $AC_\omega$, and the Dependent Choices Axiom, $RDC$, are validated in $V$.

Proof: This is an immediate consequence of the injective presentation of $\omega$. The details are similar to the proof of [1] Theorem 5.7 or [23] Theorem 4.26. □

Next we aim at finding an injective presentation of Baire space in $V$. We will need internal versions of unordered and ordered pairs in $V$.

Definition: 9.4 There is a closed application term OP of APP such that $A \models \downarrow$ and

$A \models OP(\alpha, \beta, \hat{0}) = \alpha \land OP(\alpha, \beta, \hat{1}) = \beta$

for all $\alpha, \beta \in U$. Now let

$\{x, y\}_V = \sup (N^A, \lambda\alpha. OP(x, y, \alpha)); \quad \langle x, y \rangle_V = \{\{x, \hat{x}\}_V, \{x, y\}_V\}_V$

for $x, y \in V$. The internal versions of $\alpha \in U$, denoted $\alpha_V$, and of Baire space, denoted $B_V$, are the following:

$\alpha_V := \sup (N^A, \lambda\gamma. (\Delta \cdot \gamma(0), \Delta \cdot \alpha(\gamma(0))))_V$

$B_V := \sup (U^A, \lambda\alpha. \alpha_V)$.

Corollary: 9.5 For all $x, y \in V$, $\{x, y\}_V, \langle x, y \rangle_V \in V$. For all $\alpha \in U$, $\alpha_V \in V$. Moreover, $B_V \in V$.

Proof: These claims are obviously true. □

Corollary: 9.6 $B_V$ is injectively presented.

Proof: Let $\Delta^*(n) := \Delta \cdot \tilde{n}$. As a first step, one must show that

$\models_{\lambda} (\Delta^*(n_1), \Delta^*(m_1))_V = (\Delta^*(n_2), \Delta^*(m_2))_V$

implies $n_1 = m_1$ and $n_2 = m_2$. This follows from the fact that $\models_{\lambda}$ “$\langle x, y \rangle_V$ is the ordered pair of $x$ and $y$” holds and that $\omega$ is injectively presented according to Corollary 9.2. □

Notice the important role of the type $U^A$ in obtaining an injective presentation of Baire space. This will enable us to verify that $CC$ holds in $V$. 

Lemma: 9.7 There is a closed application term $t$ such that $\mathcal{A} \models t \downarrow$ and
\[ \alpha_t \vdash \text{“} \mathcal{B}_t \text{” is the set of all functions from } \omega \text{ to } \omega \]
where $t$ evaluates to $\alpha_t$ in $\mathcal{A}$.

Proof: Suppose $\beta_1 \models \text{“} f \text{” is function from } \omega \text{ to } \omega$. Then from $\beta$ one can distill $\beta^*$ such that $\beta^* \models \forall n \in \omega \exists k \in \omega \langle n, k \rangle \in f$. Thus $\beta^* \cdot \hat{n} \models \exists k \in \omega \langle \Delta \cdot \hat{n}, k \rangle \in f$, so that $(\beta^* \cdot \hat{n})_n \models N^A$ and $(\beta^* \cdot \hat{n})_1 \models \langle \Delta \cdot \hat{n}, \Delta \cdot (\beta^* \cdot \hat{n}) \rangle \in f$. Now define $\beta^\#_1$ by $\beta^\#_1(\eta) = (\beta^* \cdot \hat{n})_0(0)$. Then one can effectively construct $\beta^\#_1$ from $\beta$ such that $\beta^\#_1 \models \text{“} f \text{” is function from } \omega \text{ to } \omega \text{”}$. 

Conversely, if $\gamma \models \text{“} f \text{” is function from } \omega \text{ to } \omega \text{”}$, one can construct $\gamma^\dagger$ from $\gamma$ such that $\gamma^\dagger \models \text{“} f \text{” is function from } \omega \text{ to } \omega \text{”}$. As all of the above transformations can be effected by application terms, the desired assertion follows. \qed

Theorem: 9.8 The principles $\mathbb{CC}$ and $\mathbb{AC}_2$ are valid in $\mathbb{V}$.

Proof: Suppose $\eta \models \forall f \in \mathcal{B}_\eta \exists n \in \omega \ A(f, n)$. (10)
Then, for all $\alpha \in \mathcal{U}$, $\eta \cdot \alpha \models \exists n \in \omega \ A(\alpha, n)$, so that
\[ (\eta \cdot \alpha)_0 \models N^A \land (\eta \cdot \alpha)_1 \models \forall \alpha \ A(\alpha, \Delta \cdot (\eta \cdot \alpha)_0). \] (11)
Define
\[ \eta^* := \sup \left( U^\eta, \lambda \alpha. \langle \alpha, \Delta \cdot (\eta \cdot \alpha)_0 \rangle \right). \]
Obviously we can construct a closed term $t^\#$ such that $\mathcal{A} \models t^\# \downarrow$ and with $\theta \in \mathcal{U}$ such that $\mathcal{A} \models t^\# \models \theta$ we obtain
\[ \theta \cdot \eta \models \eta^* : \mathcal{B}_\eta \rightarrow \omega \land \forall f \in \mathcal{B}_\eta \ A(f, \eta^*(f)). \] (12)
We can thus cook up another closed application term $t^\dagger$ which evaluates to a function $\Xi$ in $\mathcal{A}$ such that
\[ \Xi \cdot \eta = p(\eta^*, \theta \cdot \eta). \]
In view of (12) we arrive at
\[ \Xi \models \forall f \in \mathcal{B}_\eta \exists n \in \omega \ A(f, n) \rightarrow \exists F : \mathcal{B}_\eta \rightarrow \omega \land \forall f \in \mathcal{B}_\eta \ A(f, F(f)). \]
One can also show that the function $\eta^*$ in (12) constructed from $\eta$ is a continuous function in the realizability model $\mathbb{V}$. By the previous Lemma 9.7, $\mathcal{B}_\eta$ is also realizable the Baire space. So the upshot is that $\mathbb{CC}$ is realized.

Moreover, for the above proof the restriction of the existential quantifier to $\omega$ in (10) is immaterial. As a result, the above proof establishes realizability of $\mathbb{AC}_2$ in $\mathbb{V}$ as well, whereby $\mathbb{AC}_2$ stands for the following statement: If $F$ is a function with domain $\mathbb{N}^\omega$ such that $\forall \alpha \in \mathbb{N}^\omega \exists x \in F(\alpha)$ then there exists a function $f$ with domain $\mathbb{N}^\omega$ such that $\forall \alpha \in \mathbb{N}^\omega f(\alpha) \in F(\alpha)$.

Furthermore, a similar proof establishes the realizability of $\mathbb{F-CC}$ in $\mathbb{V}$. \qed
Theorem: 9.9 Let $\varphi(v_1,\ldots,v_r)$ be a formula of set theory with at most the free variables exhibited.

(i) If

$\text{CZF} + \text{CC} + \text{FT} + \text{AC}_2 + \text{RDC} \vdash \varphi(v_1,\ldots,v_r)$

then there exists a closed application term $t_\varphi$ of $\text{PCA}^+$ such that for all $x_1,\ldots,x_r \in V^\kappa$,

$A \models t_\varphi x_1 \ldots x_r \downarrow$

and

$t_\varphi x_1 \ldots x_r \models^x \varphi(x_1,\ldots,x_r)$.

The term $t_\varphi$ can be effectively constructed from the deduction of $\varphi(v_1,\ldots,v_r)$.

(ii) Suppose that the domain of $A$ is a $\beta$-model and that

$\text{CZF} + \text{REA} + \text{CC} + \text{BI}_M + \text{AC}_2 + \text{RDC} \vdash \varphi(v_1,\ldots,v_r)$.

Then there exists a closed application term $s_\varphi$ of $\text{PCA}^+$ such that for all $x_1,\ldots,x_r \in V^\kappa$,

$A \models s_\varphi x_1 \ldots x_r \downarrow$

and

$s_\varphi x_1 \ldots x_r \models^x \varphi(x_1,\ldots,x_r)$.

The term $s_\varphi$ can be effectively constructed from the deduction of $\varphi(v_1,\ldots,v_r)$.

Proof: (i): In view of Theorem 8.5 and Theorem 9.8, it suffices to show realizability of $\text{FT}$. This is basically the same proof as for Theorem 6.4 only in a more involved context. So we omit the details.

(ii): By Theorem 8.8 and Theorem 9.8, it remains to verify realizability of $\text{BI}_M$. This is similar to the proof of Theorem 6.7.

Theorem: 9.10 (i) $\text{CZF}$ and $\text{CZF} + \text{CC} + \text{FT} + \text{AC}_2 + \text{RDC}$ have the same proof-theoretic strength and prove the same $\Pi^0_2$ sentences of arithmetic.

(ii) $\text{CZF} + \text{REA}$ and $\text{CZF} + \text{REA} + \text{CC} + \text{BI}_M + \text{AC}_2 + \text{RDC}$ have the same proof-theoretic strength and prove the same $\Pi^0_2$ sentences of arithmetic.

(i) follows from Theorem 9.9(i), the fact that the proof of 9.9(i) can be carried out in the background theory $\text{KP}$, and that $\text{CZF}$ and $\text{KP}$ prove the same $\Pi^0_2$ sentences.

(ii) follows from Theorem 9.9(ii) together with the insight that the existence of $\mathbb{N}^\kappa \cap L_\rho$ (where $\rho = \sup_{n<\omega} \omega^{\kappa}_n$) can be shown in $\text{KPi}$ and that $\text{KPi}$ is a background theory sufficient for the construction of $V_\kappa$. Moreover, $\text{KPi}$ is of the same strength as $\text{CZF} + \text{REA}$ and the theories prove the same $\Pi^0_2$ sentences of arithmetic.
10 \( \text{BI}_D \) strengthens CZF

The last section will show that the addition of \( \text{BI}_D \) to CZF is not a conservative extension of CZF with respect to \( \Pi^0_1 \) sentences in that we shall prove that CZF + BI\(_D\) proves the 1-consistency of CZF.

To set the stage for the proof we will be needing some definitions.

**Definition: 10.1** Let CZF be the acronym for Constructive Zermelo-Fraenkel set theory (see [7, 3]). Let CZF\(^0\) be the system CZF without Subset Collection. CZF\(^0\) results from CZF by deleting Subset Collection and replacing Strong Collection with Replacement. Let CZF\(_R,E\) be obtained from CZF by replacing Strong Collection with Replacement and Subset Collection with Exponentiation, respectively. Note that Strong Collection implies Replacement and that Subset Collection implies Exponentiation. Thus, both CZF\(^0\) and CZF\(_R,E\) are subtheories of CZF.

Another important axiom for constructive set theory is the so-called regular extension axiom, REA (see [2, 19]). A weaker version of REA is the functional regular extension axiom, fREA, which is formulated in terms of functions in place of multi-valued functions.

**Definition: 10.2** If \( R \) is a binary relation, that is a set of ordered pairs, we write \( xRy \) for \( \langle x, y \rangle \in R \).

A partial ordering is a pair \( \langle A, R \rangle \) such that \( R \) partially orders \( A \) - that is, \( A \) is a set, \( R \) is a binary relation, \( R \) is transitive on \( A \): \( \forall x, y, z \in A \ [xRy \land yRz \rightarrow xRz] \), and \( R \) is irreflexive on \( A \): \( \forall x \in A \ [\neg xRx] \).

Note that we do not assume \( R \subseteq A \times A \). So if \( \langle A, R \rangle \) is a partial ordering, then for any \( B \subseteq A \), \( \langle B, R \rangle \) is a partial ordering.

\( \langle A, R \rangle \) is a total ordering if it is a partial ordering and trichotomy holds: \( \forall x, y \in A \ [xRy \lor x = y \lor yRx] \).

**Theorem: 10.3** (CZF\(^0\)) If \( \langle A, R \rangle \) is a partial ordering then there is a smallest class \( X \) such that for all \( a \in A \), whenever \( \forall u \in A \ [aRu \rightarrow u \in X] \) then \( a \in X \). This class will be denoted by WF\((A, R)\) (the well-founded part of \( \langle A, R \rangle \)).

**Proof:** [22] Theorem 2.6. \( \Box \)

**Definition: 10.4** Suppose \( \langle A, R \rangle \) is a partial ordering and \( \phi(u) \) is a set-theoretic formula. Let

\[
\text{Prog}_{\langle A, R \rangle}(\phi) \text{ iff } (\forall u \in A) \ [((\forall v \in A) (vRu \rightarrow \phi(v)) \rightarrow \phi(u))].
\]

If \( X \) is a class \( \{ u \mid \phi(u) \} \) we also write \( \text{Prog}_{\langle A, R \rangle}(X) \) instead of \( \text{Prog}_{\langle A, R \rangle}(\phi) \).

**Corollary: 10.5** Let \( \langle A, R \rangle \) be a partial ordering and \( \phi(u) \) be a set-theoretic formula.

(i) \( \forall x \in A \ [x \in \text{WF}(A, R) \leftrightarrow (\forall u \in A)(uRx \rightarrow u \in \text{WF}(A, R))] \).

(ii) \( \text{Prog}_{\langle A, R \rangle}(\phi) \rightarrow (\forall x \in \text{WF}(A, R)) \phi(x) \).

**Proof:** (i) and (ii) are immediate consequences of Theorem 10.3. \( \Box \)
Theorem: 10.6 (CZF$_{R,E}$ + BID) Let $(A, \prec)$ be a partial ordering such that $A \subseteq \mathbb{N}$, $\prec \subseteq A \times A$, and $A$ and $\prec$ are decidable, i.e., $\forall n \in \mathbb{N} \,(n \in A \lor n \notin A)$ and $\forall n, m \in \mathbb{N} \,(n < m \lor n \neq m)$. Then $\text{WF}(A, \prec)$ is a set.

Proof: Set

\[ X = \{ x \in A \mid \forall f \in \mathbb{N}^A \, f(0) \prec x \rightarrow \exists n \in \mathbb{N} \, f(n + 1) \neq f(n) \}. \]  

(13)

Note that $X$ is a set owing to Exponentiation and Bounded Separation. We claim that

\[ \text{WF}(A, \prec) \subseteq X. \]  

(14)

According to Corollary 10.5 (ii) it suffices to show $\text{Prog}_{(A,R)}(X)$. So suppose $a \in A$ and for all $u \prec a$, $u \in X$. To show $a \in X$ suppose $f \in \mathbb{N}^A$ and $f(0) \prec a$. We have to find a $k \in \mathbb{N}$ such that $f(k + 1) \neq f(k)$. Owing to the decidability of $\prec$ we either have $f(1) \prec f(0)$ or $f(1) \neq f(0)$. In the latter case choose $k = 0$. In the former case define $f^* : \mathbb{N} \rightarrow \mathbb{N}$ by $f^*(n) = f(n + 1)$. As $f^*(0) = f(1) \prec f(0)$ and $f(0) \in X$ there exists $m \in \mathbb{N}$ such that $f^*(m + 1) \neq f^*(m)$. Thus with $k = m + 1$ it holds that $f(k + 1) \neq f(k)$.

As a result of the foregoing we have $a \in X$.

Next we show

\[ X \subseteq \text{WF}(A, \prec). \]  

(15)

This part will require BID. Fix $a \in X$. For a finite sequence $\sigma$ of natural numbers we use $S_a(\sigma)$ to convey that $\sigma = \langle \rangle$ or $\sigma = \langle \sigma_0, \ldots, \sigma_r \rangle$ with $r \geq 0$, $\sigma_0 \prec a$, and $\sigma_{i+1} \prec \sigma_i$ for all $0 \leq i < r$. Define $R_a(\sigma)$ by $\neg S_a(\sigma)$. Note that $R_a$ is decidable because $\prec$ is decidable.

Let $f : \mathbb{N} \rightarrow \mathbb{N}, f(0) \neq a$ yields $R_a(f(1))$. If $f(0) \prec a$ then there exists $m \in \mathbb{N}$ such $f(m + 1) \neq f(m)$ because $a \in X$; and hence $R_a(f(m + 2))$. Therefore we can conclude that

\[ \forall f \in \mathbb{N}^A \exists k \in \mathbb{N} \, R_a(f(k)). \]  

(16)

We say that $W(\tau)$ holds if $\tau$ is of the form $\langle \tau_0, \ldots, \tau_r \rangle$ with $r \geq 0$ and $\tau_r \in \text{WF}(A, \prec)$. Further define

\[ Q_a(\sigma) \iff R_a(\sigma) \lor W(\langle a \rangle \ast \sigma). \]

Clearly,

\[ R_a(\sigma) \rightarrow Q_a(\sigma). \]  

(17)

Suppose that $\forall m \in \mathbb{N} \, Q_a(\sigma \ast \langle m \rangle)$. $R_a(\sigma)$ implies $Q_a(\sigma)$. So assume $\neg R_a(\sigma)$. Then $\langle a \rangle \ast \sigma$ is of the form $\langle \tau_0, \ldots, \tau_r \rangle$ with $r \geq 0$, $\tau_0 = a$, and $\tau_0 \succ \ldots \succ \tau_r$. For all $u \prec \tau_r$ we then also have $\neg R_a(\sigma \ast \langle u \rangle)$ by definition of $R_a$. Thus, as $Q_a(\sigma \ast \langle m \rangle)$ holds for all $m$ by supposition, we conclude that $W(\langle a \rangle \ast \sigma \ast \langle m \rangle)$ holds for all $u \prec \tau_r$. This entails that $u \in \text{WF}(A, \prec)$ for all $u \prec \tau_r$, yielding $\tau_r \in \text{WF}(A, \prec)$; and consequently, $W(\langle a \rangle \ast \sigma)$ and $Q_a(\sigma)$. As a result, we have shown that

\[ \forall m \in \mathbb{N} \, Q_a(\sigma \ast \langle m \rangle) \rightarrow Q_a(\sigma). \]  

(18)
In view of (16), (17), and (18), $\text{BI}_D$ allows us to conclude that $Q_a(\langle \rangle)$, i.e. $a \in \text{WF}(A, \prec)$. This completes the proof of (15).

From (14) and (15) we get $X = \text{WF}(A, \prec)$, showing that $\text{WF}(A, \prec)$ is a set.

**Definition 10.7** If $T$ is a theory, the $1$-consistency of $T$ is the schema
\[ \forall u \in \mathbb{N} \left[ \text{Pr}_T(\lceil F(u) \rceil) \rightarrow F(u) \right] \]
for $\Sigma^0_1$ formulae $F(u)$ with one free variable $u$.

**Corollary 10.8** $\text{CZF}_{R,E} + \text{BI}_D$ proves the $1$-consistency of $\text{CZF}$ and $\text{KP}$.

**Proof:** From Theorem 10.6 it follows that the class $\text{Acc}$ of [22] Definition 4.2 is a set. The order-type of this set is the Bachmann-Howard ordinal which is the proof-theoretic ordinal of $\text{CZF}$ and $\text{KP}$ (see [19] Theorem 2.1 (i)). As a result, the ordinal analyses of $\text{CZF}$ and $\text{KP}$ can be carried in $\text{CZF}_{R,E} + \text{BI}_D$, yielding the provability of the 1-consistency of these theories in $\text{CZF}_{R,E} + \text{BI}_D$. For more details see [22] remark 4.14.

**References**