Article:
Rathjen, M (2013) Constructive Zermelo-Fraenkel set theory and the limited principle of omniscience. Annals of Pure and Applied Logic, 165 (2). 563 - 572. ISSN: 0168-0072

https://doi.org/10.1016/j.apal.2013.08.001

Constructive Zermelo-Fraenkel set theory and the limited principle of omniscience

Michael Rathjen

Department of Pure Mathematics, University of Leeds, Leeds LS2 9JT, England, rathjen@maths.leeds.ac.uk.

Abstract

In recent years the question of whether adding the limited principle of omniscience, **LPO**, to constructive Zermelo-Fraenkel set theory, **CZF**, increases its strength has arisen several times. As the addition of excluded middle for atomic formulae to **CZF** results in a rather strong theory, i.e. much stronger than classical Zermelo set theory, it is not obvious that its augmentation by **LPO** would be proof-theoretically benign. The purpose of this paper is to show that **CZF**+**RDC**+**LPO** has indeed the same strength as **CZF**, where **RDC** stands for relativized dependent choice. In particular, these theories prove the same Π^0_2 theorems of arithmetic.

Key words: Constructive set theory, limited principle of omniscience, bar induction, proof-theoretic strength
2000 MSC: Primary: 03F50, 03F25, Secondary: 03D65, 03B15

1. Introduction

Constructive Set Theory was introduced by John Myhill in a seminal paper [12], where a specific axiom system **CST** was introduced. Through developing constructive set theory he wanted to isolate the principles underlying Bishop's conception of what sets and functions are, and he wanted "these principles to be such as to make the process of formalization completely trivial, as it is in the classical case" ([12], p. 347). Myhill's **CST** was subsequently modified by Aczel and the resulting theory was called *Constructive Zermelo-Fraenkel Set Theory*, **CZF** (cf. [1, 2, 3]). A hallmark of this theory is that it possesses a type-theoretic interpretation (cf. [1, 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.

Certain basic principles of classical mathematics are taboo for the constructive mathematician. Bishop called them *principles of omniscience*. The limited principle of omniscience, **LPO**, is an instance of the law of excluded middle which usually serves as a line of demarcation, separating "constructive" from "non-constructive" theories. Over the last few years the question of whether adding **LPO** to constructive Zermelo-Fraenkel set theory increases its strength has arisen several times. As the addition of excluded middle for atomic formulae to **CZF** results in a rather strong theory, i.e. much stronger than classical Zermelo set theory, it is not obvious that its augmentation by **LPO** would be proof-theoretically benign.[1] The purpose of this paper is to show that $\mathbf{CZF}+\mathbf{RDC}+\mathbf{LPO}$ has indeed the same strength as **CZF**, where **RDC** stands for relativized dependent choice. In particular, these theories prove the same Π^0_2 theorems of arithmetic. The main tool will be a realizability model for $\mathbf{CZF}+\mathbf{RDC}+\mathbf{LPO}$ that is based on recursion in a type-2 object. This realizability interpretation is shown to be formalizable in the classical theory of bar induction, **BI**, which is known to have the same strength as **CZF** (for details see Theorem 2.2).

To begin with we recall some principles of omniscience. Let $2^{\mathbb{N}}$ be Cantor space, i.e. the set of all functions from the naturals into $\{0,1\}$.

Definition 1.1. Limited Principle of Omniscience (**LPO**):

$$\forall f \in 2^{\mathbb{N}}\, [\exists n\, f(n)=1 \;\;\vee\;\; \forall n\, f(n)=0].$$

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

$$\begin{aligned}\forall f \in 2^{\mathbb{N}}\, \big(&\forall n,m[f(n)=f(m)=1 \to n=m] \\ &\to\; [\forall n\, f(2n)=0 \;\;\vee\;\; \forall n\, f(2n+1)=0]\big).\end{aligned}$$

LPO is incompatible with both Brouwerian mathematics and Russian constructivism. With **LLPO** the story is more complicated as it is by and large compatible with Russian constructivism, namely with Markov's principle and the form of Church thesis saying that every function from naturals to naturals is computable (recursive) even on the basis of full intuitionistic Zermelo-Fraenkel set theory (see [5, Lemmata 6.1, 6.5, 9.2]).

[1] One referee of this paper pointed out that Friedman considered semi-constructive systems of analysis with **LPO** in [7].

2. The theory BI

In the presentation of subsystems of second order arithmetic we follow [18]. It is perhaps worth pointing out that the underlying logic of all of these theories is classical logic. By $\mathcal{L}_2$ we denote the language of these theories. $\mathbf{ACA}_0$ denotes the theory of arithmetical comprehension.

Definition 2.1. For a 2-place relation $\prec$ and an arbitrary formula $F(a)$ of $\mathcal{L}_2$ we define

$\mathrm{Prog}(\prec, F) := \forall x[\forall y(y \prec x \to F(y)) \to F(x)]$ (*progressiveness*)
$\mathrm{TI}(\prec, F) := \mathrm{Prog}(\prec, F) \to \forall x F(x)$ (*transfinite induction*)
$\mathrm{WF}(\prec) := \forall X \mathrm{TI}(\prec, X) :=$
$\forall X(\forall x[\forall y(y \prec x \to y \in X) \to x \in X] \to \forall x[x \in X])$ (*well-foundedness*).

Let $\mathcal{F}$ be any collection of formulae of $\mathcal{L}_2$. For a 2-place relation $\prec$ we will write $\prec \in \mathcal{F}$, if $\prec$ is defined by a formula $Q(x, y)$ of $\mathcal{F}$ via $x \prec y := Q(x, y)$.

The bar induction scheme is the collection of all formulæ of the form

$$\mathrm{WF}(\prec) \to \mathrm{TI}(\prec, F),$$

where $\prec$ is an arithmetical relation (set parameters allowed) and F is an arbitrary formula of $\mathcal{L}_2$.

The theory $\mathbf{ACA}_0 +$ bar induction will be denoted by **BI**. In Simpson's book bar induction is called "unlimited transfinite induction" and in it our theory **BI** corresponds to the one referred to by the acronym Π^1_∞-$\mathbf{TI}_0$ (cf. [18, §VII.2]).

Theorem 2.2. *The following theories have the same proof-theoretic strength:*

(i) **BI**

(ii) **CZF**

(iii) The theory $\mathbf{ID}_1$ *of (non-iterated) arithmetical inductive definitions.*

Proof. Kreisel obtained in [11] a proof-theoretic reduction of **BI** to a subtheory of $\mathbf{ID}_1$ based on intuitionistic logic (notated as $\mathbf{ID}^i_1(\mathcal{O})$), using rather complicated and round-about arguments. By work of Gerber [8] and Howard [10], the ordinal of $\mathbf{ID}^i_1(\mathcal{O})$ was determined to be an ordinal that is now known as the Bachmann-Howard ordinal. As this ordinal provides a lower bound for the ordinal of **BI**, the proof-theoretic equivalence of **BI** and $\mathbf{ID}_1$ follows. A more recent ordinal analysis of **BI** can be found in [4] and [17, Theorem 10.2]. A direct syntactic translation of $\mathbf{ID}_1$ into **BI** will be given in Lemma 3.2. The proof-theoretic equivalence of $\mathbf{ID}_1$ with **CZF** (and thus with **BI**) follows from [13, Theorem 4.14]. $\square$

There is an interesting other way of characterizing **BI** which uses the notion of a countable coded ω-model.

Definition 2.3. Let T be a theory in the language of second order arithmetic, $\mathcal{L}_2$. A *countable coded ω-model of T* is a set $W \subseteq \mathbb{N}$, viewed as encoding the $\mathcal{L}_2$-model

$$\mathbb{M} = (\mathbb{N}, \mathcal{S}, +, \cdot, 0, 1, <)$$

with $\mathcal{S} = \{(W)_n \mid n \in \mathbb{N}\}$ such that $\mathbb{M} \models T$ (where $(W)_n = \{m \mid \langle n, m\rangle \in W\}$; $\langle\, ,\rangle$ some coding function).

This definition can be made in $\mathbf{RCA}_0$ (see [18], Definition VII.2.1).

We write $X \in W$ if $\exists n\; X = (W)_n$.

Theorem 2.4. **BI** *proves ω-model reflection, i.e., for every formula $F(\vec{X}\,)$ with all free second order $\vec{X} = X_1, \ldots, X_n$ variables exhibited,* **BI** *proves*

$$F(\vec{X}\,) \quad \rightarrow \quad \exists \mathbb{M}[\mathbb{M} \textit{ cc } \omega\textit{-model of } \mathbf{ACA}_0 \wedge \vec{X} \in \mathbb{M} \wedge \mathbb{M} \models F(\vec{X}\,)]$$

where "cc" stands for "countable coded".

Proof. [18, Lemma VIII.5.2]. $\square$

It easy to show that the scheme of ω-model reflection implies bar induction (see [18, Lemma VIII.5.3]) and hence the theories **BI** and $\mathbf{ACA}_0$ + *ω-model reflection* are equivalent, that is, they prove the same formulae (see [18, Theorem VIII.5.4]).

Definition 2.5. The scheme of Σ^1_1-**AC** is the collection of all formulae

$$\forall x\, \exists X\, F(x, X) \rightarrow \exists Y\, \forall x\, F(x, (Y)_x)$$

with $F(x, X)$ of complexity Σ^1_1.

Corollary 2.6. *(i)* **BI** *proves* Σ^1_1-**AC** *and* Δ^1_1*-comprehension.*

(ii) **BI** *proves that for every set X there exists a countable coded ω-model of* $\mathbf{ACA}_0 + \Sigma^1_1$-**AC** *containing X.*

Proof. (i) We argue in **BI**. Suppose $\forall x\, \exists X\, F(x, X, \vec{U}\,)$. Owing to Theorem 2.4 there exists a countable coded ω-model $\mathbb{M} = (\mathbb{N}, \mathcal{S}, +, \cdot, 0, 1, <)$ with $\vec{U} \in \mathbb{M}$ and

$$\mathbb{M} \models \forall x\, \exists X\, F(x, X, \vec{U}\,).$$

Let $\mathcal{S} = \{(W)_n \mid n \in \mathbb{N}\}$. Define $f(n) = m$ if $\mathbb{M} \models F(n, (W)_m, \vec{U}\,)$ and for all $k < m$ $\mathbb{M} \models \neg F(n, (W)_k, \vec{U}\,)$. Put

$$Y := \{\langle n, x\rangle \mid x \in (W)_{f(n)}\}.$$

We then have $\mathbb{M} \models F(n, (Y)_n, \vec{U}\,)$ for all n. Since F is Σ^1_1 it follows that $F(n, (Y)_n, \vec{U}\,)$ holds for all n. This shows Σ^1_1-**AC**.

(ii) To show that for any set X there is a countable coded ω-model of Σ^1_1-**AC** containing X firstly note that $\mathbf{ACA}_0 + \Sigma^1_1$-**AC** is finitely axiomatizable, say via a sentence G. By (i) we know that G holds in our background theory. Now apply Theorem 2.4 to find a countable coded ω-model that reflects G and contains X.

Finally notice that Δ^1_1-comprehension is a consequence of Σ^1_1-**AC**. $\square$

The next result was first formulated in [6] as Lemma 1.6.3 but with a different and much more involved proof.

Lemma 2.7. *Let $A(X)$ be an arithmetic formula and $F(x)$ be an arbitrary formula of $\mathcal{L}_2$. Let $A(F)$ be the formula that arises from $A(X)$ by replacing every subformula $t \in X$ by $F(t)$ (avoiding variable clashes, of course). Then we have*

$$\mathbf{BI} \vdash \forall X\, A(X) \rightarrow A(F)\,.$$

Proof. Arguing in **BI** suppose that $\neg A(F)$. Pick a countable coded ω-model $\mathbf{M}$ of $\mathbf{ACA_0}$ containing all parameters from A and F such that $\mathbf{M} \models \neg A(F)$. Letting $U = \{n \mid \mathbf{M} \models F(n)\}$ we have $\neg A(U)$ because A is an arithmetic formula and $\mathbf{M}$ is absolute for such formulae on account of being an ω-model. Thus we have shown

$$\mathbf{BI} \vdash \neg A(F) \rightarrow \exists X\, \neg A(X)$$

from which the desired assertion follows. $\square$

Conversely, one easily shows that the scheme $\forall X\, A(X) \to A(F)$ (where $A(X)$ is an arithmetic formula and $F(x)$ is an arbitrary formula of $\mathcal{L}_2$) implies bar induction and thus provides an equivalent formalization of the theory **BI** over $\mathbf{ACA}_0$.

3. Inductive definitions in BI

Definition 3.1. *Let $A(x, X)$ be an arithmetic formula in which the variable X occurs positively. Henceforth we shall convey this by writing $A(x, X^+)$.*

Define

$$\mathrm{I}_A(u) \quad :\Leftrightarrow \quad \forall X\, [\forall x\, (A(x, X) \to x \in X) \to u \in X]\,. \tag{1}$$

We write $\mathrm{I}_A \subseteq F$ for $\forall v\, (\mathrm{I}_A(v) \to F(v))$, and $F \subseteq \mathrm{I}_A$ for $\forall v\, (F(v) \to \mathrm{I}_A(v))$.

Lemma 3.2. *The following are provable in* **BI** *for every X-positive arithmetic formula $A(x, X^+)$ and arbitrary $\mathcal{L}_2$ formula $F(u)$.*

(i) $\forall u\, (A(u, \mathrm{I}_A) \to u \in \mathrm{I}_A)$.

(ii) $\forall x\, [A(x, F) \to F(x)] \to \mathrm{I}_A \subseteq F$

(iii) $\forall u\, (u \in \mathrm{I}_A \to A(u, \mathrm{I}_A))$.

Proof. (i): Assume $A(u, \mathrm{I}_A)$ and $\forall x\, (A(x, X) \to x \in X)$. The latter implies $\mathrm{I}_A \subseteq X$. Since $A(u, \mathrm{I}_A)$ holds, and owing to the positive occurrence of I_A in the latter formula, we have $A(u, X)$. Since X was arbitrary, we conclude that $\mathrm{I}_A(u)$.

(ii): Suppose $\mathrm{I}_A(u)$. Then $\forall X\, [\forall x\, (A(x, X) \to x \in X) \to u \in X]$, and hence, using Lemma 2.7, $\forall x\, (A(x, F) \to F(x)) \to F(u)$. Thus, assuming $\forall x\, (A(x, F) \to F(x))$, we have $F(u)$.

(iii): Let $F(v) :\Leftrightarrow A(v, \mathrm{I}_A)$. By (i) we have $F \subseteq \mathrm{I}_A$. Assuming $A(u, F)$ it therefore follows that $A(u, \mathrm{I}_A)$ since F occurs positively in the former formula, and hence $F(u)$. Thus, in view of (ii), we get $\mathrm{I}_A \subseteq F$, confirming (iii). $\square$

4. Recursion in a type-2 object

Using the apparatus of inductive definitions, we would like to formalize in **BI** recursion in the type-2 object $E : (\mathbb{N} \to \mathbb{N}) \to \mathbb{N}$ with $E(f) = n + 1$ if $f(n) = 0$ and $\forall i < n\, f(n) > 0$ and $E(f) = 0$ if $\forall n\, f(n) > 0$.

In the formalization we basically follow [9, VI.1.1]. We use some standard coding of tuples of natural numbers. The code of the empty tuple is $\langle\rangle := 1$, and for any $k > 0$ and tuple $(m_0, \ldots, m_{k-1})$ let $\langle m_0, \ldots m_{k-1}\rangle := p_0^{m_0+1} \cdot \ldots \cdot p_{k-1}^{m_{k-1}+1}$, where p_i denotes the $i+1$-th prime number.

Definition 4.1. Below Sb_0 denotes the primitive recursive function from [9, II.2.5] required for what is traditionally called the S-m-n theorem. Let $\mathrm{Comp}^{\mathrm{E}}$ be the smallest class such that for all k, n, p, r, and s, all $i < k$ and $\mathbf{m} = m_0, \ldots, m_{k-1}$ in $\mathbb{N}$,

(0) $\langle\langle 0, k, 0, n\rangle, \mathbf{m}, n\rangle \in \mathrm{Comp}^{\mathrm{E}}$;
$\langle\langle 0, k, 1, i\rangle, \mathbf{m}, m_i\rangle \in \mathrm{Comp}^{\mathrm{E}}$;
$\langle\langle 0, k, 2, i\rangle, \mathbf{m}, m_i + 1\rangle \in \mathrm{Comp}^{\mathrm{E}}$;
$\langle\langle 0, k+3, 4\rangle, p, q, r, s, \mathbf{m}, p\rangle \in \mathrm{Comp}^{\mathrm{E}}$ if $r = s$;
$\langle\langle 0, k+3, 4\rangle, p, q, r, s, \mathbf{m}, q\rangle \in \mathrm{Comp}^{\mathrm{E}}$ if $r \neq s$;
$\langle\langle 0, k+2, 5\rangle, p, q, \mathbf{m}, \mathrm{Sb}_0(p, q)\rangle \in \mathrm{Comp}^{\mathrm{E}}$;

(1) for any $k', b, c_0, \ldots, c_{k'-1}, q_0, \ldots, q_{k'-1}$ in $\mathbb{N}$, if for all $i < k'$ $\langle c_i, \mathbf{m}, q_i\rangle \in \mathrm{Comp}^{\mathrm{E}}$ and $\langle b, q_0, \ldots, q_{k'-1}, n\rangle \in \mathrm{Comp}^{\mathrm{E}}$, then

$$\langle\langle 1, k, b, c_0, \ldots, c_{k'-1}\rangle, \mathbf{m}, n\rangle \in \mathrm{Comp}^{\mathrm{E}};$$

(2) for any $b \in \mathbb{N}$, if $\langle b, \mathbf{m}, n\rangle \in \mathrm{Comp}^{\mathrm{E}}$, then

$$\langle\langle 2, k+1\rangle, b, \mathbf{m}, n\rangle \in \mathrm{Comp}^{\mathrm{E}}.$$

(3.1) for any $b \in \mathbb{N}$, if for all $p \in \mathbb{N}$ there exists $k_p \in \mathbb{N}$ with $k_p > 0$ and $\langle b, p, \mathbf{m}, k_p\rangle \in \mathrm{Comp}^{\mathrm{E}}$, then

$$\langle\langle 3, k, b\rangle, \mathbf{m}, 0\rangle \in \mathrm{Comp}^{\mathrm{E}}.$$

(3.2) for any $b, p \in \mathbb{N}$, if $\langle b, p, \mathbf{m}, 0\rangle \in \mathrm{Comp}^{\mathrm{E}}$ and for all $i < p$ there exists $k_i \in \mathbb{N}$ with $k_i > 0$ and $\langle b, i, \mathbf{m}, k_i\rangle \in \mathrm{Comp}^{\mathrm{E}}$, then

$$\langle\langle 3, k, b\rangle, \mathbf{m}, p+1\rangle \in \mathrm{Comp}^{\mathrm{E}}.$$

Clearly $\mathrm{Comp}^{\mathrm{E}}$ is defined by a positive arithmetical inductive definition that we denote by A_{E}, i.e., $\mathrm{Comp}^{\mathrm{E}} = \mathrm{I}_{\mathrm{A}_{\mathrm{E}}}$.

Lemma 4.2. *For all* $a, \mathbf{m} \in \mathbb{N}$ *there is at most one* $n \in \mathbb{N}$ *such that* $\langle a, \mathbf{m}, n \rangle \in \mathrm{Comp}^{\mathrm{E}}$.

Proof. Define a class $\mathfrak{X}$ by

$$\begin{aligned} \langle a, \mathbf{m}, n \rangle \in \mathfrak{X} \quad \text{iff} \quad & \langle a, \mathbf{m}, n \rangle \in \mathrm{Comp}^{\mathrm{E}} \text{ and for all } k \in \mathbb{N}, \\ & \text{if } \langle a, \mathbf{m}, k \rangle \in \mathrm{Comp}^{\mathrm{E}}, \text{ then } n = k. \end{aligned}$$

By Lemma 3.2 (ii) we only have to show that $\mathfrak{X}$ is closed under the clauses defining $\mathrm{Comp}^{\mathrm{E}}$. This is a straightforward affair, albeit a bit tedious. □

We shall put to use this notion of computability for a realizability interpretation of **CZF**+**LPO**. This, however, will require that the computability relation be a set rather than a class such as $\mathrm{Comp}^{\mathrm{E}}$. To achieve this we shall invoke Theorem 2.4.

Lemma 4.3. **BI** *proves that there exists a countable coded* ω*-model* $\mathfrak{M}$ *of* **ACA** *such that the following hold:*

(i) $\mathfrak{M} \models \forall x, \mathbf{y}, z\, [\langle x, \mathbf{y}, z \rangle \in \mathrm{Comp}^{\mathrm{E}} \leftrightarrow \mathrm{A}_{\mathrm{E}}(\langle x, \mathbf{y}, z \rangle, \mathrm{Comp}^{\mathrm{E}})]$.

(ii) $\mathfrak{M} \models \forall x, \mathbf{y}, z, z' [\langle x, \mathbf{y}, z \rangle \in \mathrm{Comp}^{\mathrm{E}} \wedge \langle x, \mathbf{y}, z' \rangle \in \mathrm{Comp}^{\mathrm{E}} \rightarrow z = z']$.

Proof. This follows from Lemma 3.2 and Lemma 4.2 using Theorem 2.4. □

We will fix a model $\mathfrak{M}$ as in the previous lemma for the remainder of the paper and shall write

$$\{a\}^{E}(\mathbf{m}) \simeq n \quad \Leftrightarrow \quad \mathfrak{M} \models \langle a, \mathbf{m}, n \rangle \in \mathrm{Comp}^{\mathrm{E}}.$$

Note that this notion of computability hinges on $\mathfrak{M}$. More computations might converge in $\mathfrak{M}$ than outside of $\mathfrak{M}$.

5. Emulating a type structure in BI

We would like to define a type-theoretic interpretation of **CZF**+**RDC**+**LPO** in **BI**. This will in a sense be similar to Aczel's interpretation of **CZF** in Martin-Löf type theory (cf. [1]). To this end, we initiate a simultaneous positive inductive definition of a type **U** together with two binary relations (of elementhood and non-elementhood) on it, and also of a type **V** of (codes of) well-founded trees over **U**. The need for defining both elementhood and non-elementhood among members of $\mathbf{U}$ is necessitated by the requirement of positivity of the inductive definition.

Below we use the pairing function $\jmath(n,m) = (n+m)^2+n+1$ and its inverses $()_0, ()_1$ satisfying $(\jmath(n,m))_0 = n$ and $(\jmath(n,m))_1 = m$. We will just write (n,m) for $\jmath(n,m)$.

Definition 5.1. Let $n_{\mathbb{N}} := (0,n)$, $\mathrm{nat} := (1,0)$, $\mathrm{pl}(n,m) := (2,(n,m))$, $\sigma(n,m) := (3,(n,m))$, $\pi(n,m) := (4,(n,m))$, and $\sup(n,m) := (5,(n,m))$.

We inductively define classes $\mathbf{U}, \mathrm{EL}, \mathrm{NEL}$ and $\mathbf{V}$ by the following clauses. Rather than $(n,m) \in \mathrm{EL}$ and $(n,m) \in \mathrm{NEL}$ we write $n \mathrel{\dot\in} m$ and $n \mathrel{\dot\notin} m$, respectively.

1. $n_{\mathbb{N}} \in \mathbf{U}$; if $k < n$ then $k \mathrel{\dot\in} n_{\mathbb{N}}$; if $k \geq n$ then $k \mathrel{\dot\notin} n_{\mathbb{N}}$.
2. $\mathrm{nat} \in \mathbf{U}$ and $n \mathrel{\dot\in} \mathrm{nat}$ for all n.
3. If $n, m \in \mathbf{U}$, then $\mathrm{pl}(n,m) \in \mathbf{U}$.
4. Assume $\mathrm{pl}(n,m) \in \mathbf{U}$.
   If $k \mathrel{\dot\in} n$, then $(0,k) \mathrel{\dot\in} \mathrm{pl}(n,m)$. If $k \mathrel{\dot\in} m$, then $(1,k) \mathrel{\dot\in} \mathrm{pl}(n,m)$.
   If $k \mathrel{\dot\notin} n$, then $(0,k) \mathrel{\dot\notin} \mathrm{pl}(n,m)$. If $k \mathrel{\dot\notin} m$, then $(1,k) \mathrel{\dot\notin} \mathrm{pl}(n,m)$. If k is neither of the form $(0,x)$ nor $(1,x)$ for some x, then $k \mathrel{\dot\notin} \mathrm{pl}(n,m)$.
5. If $n \in \mathbf{U}$ and $k \mathrel{\dot\notin} n \lor \exists x\,(\{e\}^E(k) \simeq x \land x \in \mathbf{U})$ holds for all k, then $\sigma(n,e) \in \mathbf{U}$.
6. Assume $\sigma(n,e) \in \mathbf{U}$.
   If $k \mathrel{\dot\in} n$ and $\exists x\,(\{e\}^E(k) \simeq x \land u \mathrel{\dot\in} x)$, then $(k,u) \mathrel{\dot\in} \sigma(n,e)$.
   If $k \mathrel{\dot\notin} n$ or $\exists x\,(\{e\}^E(k) \simeq x \land u \mathrel{\dot\notin} x)$, then $(k,u) \mathrel{\dot\notin} \sigma(n,e)$.
   If x is not of the form (u,v) for some u, v, then $x \mathrel{\dot\notin} \sigma(n,e)$.
7. If $n \in \mathbf{U}$ and $k \mathrel{\dot\notin} n \lor \exists x\,(\{e\}^E(k) \simeq x \land x \in \mathbf{U})$ holds for all k, then $\pi(n,e) \in \mathbf{U}$.
8. Assume $\pi(n,e) \in \mathbf{U}$.
   If $k \mathrel{\dot\notin} n \lor \exists x, y\,(\{e\}^E(k) \simeq x \land \{d\}^E(k) \simeq y \land y \mathrel{\dot\in} x)$ holds for all k, then $d \mathrel{\dot\in} \pi(n,e)$.
   If $\exists u\,(u \mathrel{\dot\in} n \land \forall z\,\neg\{d\}^E(u) \simeq z)$, then $d \mathrel{\dot\notin} \pi(n,e)$.
   If $\exists u\,\exists x\,(u \mathrel{\dot\in} n \land \{e\}^E(u) \simeq x \land \exists z\,(\{d\}^E(u) \simeq z \land z \mathrel{\dot\notin} x))$, then $d \mathrel{\dot\notin} \pi(n,e)$.
9. If $n \in \mathbf{U}$ and $k \mathrel{\dot\notin} n \lor \exists x\,(\{e\}^E(k) \simeq x \land x \in \mathbf{V})$ holds for all k, then $\sup(n,e) \in \mathbf{V}$.

Remark 5.2. Clearly, the predicates $\mathbf{U}$, $\dot{\in}$, $\dot{\notin}$ and $\mathbf{V}$ all appear positively in the above inductive definition. Moreover, it falls under the scope of arithmetical inductive definitions and is therefore formalizable in our background theory **BI** owing to Lemma 3.2. Note also that for this it was important to move from the Π^1_1 computability notion of Definition 4.1 to E-recursion in the ω-model $\mathfrak{M}$.

$\dot{\in}$ and $\dot{\notin}$ are complementary in the following sense.

Lemma 5.3. *For all $n \in \mathbf{U}$,*

$$\forall x\,(x \mathrel{\dot{\in}} n \leftrightarrow \neg\, x \mathrel{\dot{\notin}} n)\,.$$

Proof. This can be proved by the induction principle of Lemma 3.2(ii). ☐

Corollary 5.4. *For each $n \in \mathbf{U}$, $\{x \mid x \mathrel{\dot{\in}} n\}$ is a set.*

Proof. Note that $\dot{\in}$ and $\dot{\notin}$ are Π^1_1 as they are given by positive arithmetical inductive definitions. Since **BI** proves Δ^1_1-comprehension by Corollary 2.6, it follows from Lemma 5.3 that $\{x \mid x \mathrel{\dot{\in}} n\}$ is a set. ☐

Definition 5.5. We shall use lower case Greek letters $\alpha, \beta, \gamma, \delta, \ldots$ to range over elements of $\mathbf{V}$.

Using the induction principle from Lemma 3.2(ii), one readily shows that every $\alpha \in \mathbf{V}$ is of the form $\sup(n, e)$ with $n \in \mathbf{U}$ and $\forall x \mathrel{\dot{\in}} n\ \{e\}^E(x) \in \mathbf{V}$, where $\{e\}^E(x) \in \mathbf{V}$ is an abbreviation for $\exists y\ (\{e\}^E(x) \simeq y \wedge y \in \mathbf{V})$.

If $\alpha = \sup(n, e)$ we denote n by $\bar{\alpha}$ and e by $\tilde{\alpha}$. For $i \mathrel{\dot{\in}} \bar{\alpha}$ we shall denote by $\tilde{\alpha}i$ the unique x such that $\{\tilde{\alpha}\}^E(i) \simeq x$.

If $\wp$ is an $r+1$-ary partial E-recursive function we denote by $\lambda x.\wp(x, \vec{a}\,)$ an index of the function $x \mapsto \wp(x, \vec{a}\,)$ (say provided by the S-m-n theorem or parameter theorem).

Lemma 5.6. *There is a 2-ary partial E-recursive function $\dot{=}$ such that $\dot{=}(\alpha, \beta)$ is defined for all $\alpha, \beta \in \mathbf{V}$ and (writing in infix notation $\alpha \dot{=} \beta$ for $\dot{=}(\alpha, \beta)$) the following equation holds*

$$\begin{aligned}(\alpha \dot{=} \beta) = {} & \\ & \sigma(\pi(\bar{\alpha}, \lambda x.\sigma(\bar{\beta}, \lambda y.(\tilde{\alpha}x \dot{=} \tilde{\beta}y))), \lambda z.\pi(\bar{\beta}, \lambda y.\sigma(\bar{\alpha}, \lambda x.(\tilde{\alpha}x \dot{=} \tilde{\beta}y))))\,.\end{aligned} \tag{2}$$

Moreover, $(\alpha \dot{=} \beta) \in \mathbf{U}$ holds for all $\alpha, \beta \in \mathbf{V}$.

Proof. Such a function can be defined by the recursion theorem for E-recursion (see [9, p. 261]), using (2) as the defining recursion equation. Totality on $\mathbf{V}\times\mathbf{V}$ follows from the induction principle for $\mathbf{V}$. In the same vein (2) yields $\dot{=}(\alpha,\beta)\in\mathbf{U}$ for all $\alpha,\beta\in\mathbf{V}$ by employing the induction principle for $\mathbf{V}$. $\square$

6. Realizability

We will introduce a realizability semantics for sentences of set theory with parameters from $\mathbf{V}$. 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 $\alpha,\beta\in\mathbf{V}$ and $e,f\in\mathbb{N}$. We write $e_{i,j}$ for $((e)_i)_j$.

Definition 6.1 (Kleene realizability over $\mathbf{V}$). *Below variables e,d range over natural numbers. We define*

$$\begin{array}{rll}
e\Vdash\alpha=\beta & \textit{iff} & e\,\dot{\in}\,(\alpha\dot{=}\beta)\\
e\Vdash\alpha\in\beta & \textit{iff} & (e)_0\,\dot{\in}\,\bar{\beta}\ \wedge\ (e)_1\Vdash\alpha=\tilde{\beta}(e)_0\\
e\Vdash\phi\wedge\psi & \textit{iff} & (e)_0\Vdash\phi\ \wedge\ (e)_1\Vdash\psi\\
e\Vdash\phi\vee\psi & \textit{iff} & \big[(e)_0=\mathbf{0}\wedge(e)_1\Vdash\phi\big]\ \vee\ \big[(e)_0=\mathbf{1}\ \wedge\ (e)_1\Vdash\psi\big]\\
e\Vdash\neg\phi & \textit{iff} & \forall d\,\neg d\Vdash\phi\\
e\Vdash\phi\to\psi & \textit{iff} & \forall d\,\big[d\Vdash\phi\ \to\ \{e\}^E(d)\Vdash\psi\big]\\
e\Vdash\forall x\in\alpha\;\phi(x) & \textit{iff} & \forall i\,\dot{\in}\,\bar{\alpha}\ \{e\}^E(i)\Vdash\phi(\tilde{\alpha}i)\\
e\Vdash\exists x\in\alpha\;\phi(x) & \textit{iff} & (e)_0\,\dot{\in}\,\bar{\alpha}\ \wedge\ (e)_1\Vdash\phi(\tilde{\alpha}(e)_0)\\
e\Vdash\forall x\phi(x) & \textit{iff} & \forall\alpha\in\mathbf{V}\ \{e\}^E(\alpha)\Vdash\phi(\alpha)\\
e\Vdash\exists x\phi(x) & \textit{iff} & (e)_0\in\mathbf{V}\ \wedge\ (e)_1\Vdash\phi((e)_0).
\end{array}$$

Theorem 6.2. *Let $\varphi(v_1,\ldots,v_r)$ be a formula of set theory with at most the free variables exhibited. If*

$$\mathbf{CZF}+\mathbf{LPO}+\mathbf{RDC}\vdash\varphi(v_1,\ldots,v_r)$$

then one can explicitly construct (an index of) a partial E-recursive function f from that proof such that

$$\mathbf{BI}\vdash\forall\alpha_1,\ldots,\alpha_r\in\mathbf{V}\ f(\alpha_1,\ldots,\alpha_r)\Vdash\varphi(\alpha_1,\ldots,\alpha_r).$$

Proof. Realizability of the axioms of **CZF**+**RDC** is just a special case of realizability over an ω-PCA$^+$ as described in [14, Theorem 8.5] and is closely related to Aczel's [1] interpretation of $\mathbf{CZF}+\mathbf{RDC}$ in type theory and the realizability interpretations of $\mathbf{CZF}+\mathbf{RDC}$ presented in [13, 15, 16]. Note that to ensure realizability of Δ_0 separation it is necessary that all types in $\mathbf{U}$ correspond to sets (Corollary 5.4).

We shall thus only address the realizability of **LPO**. To avoid the niceties involved in coding functions in set theory, we shall demonstrate realizability of a more general type of statement which implies **LPO** on the basis of **CZF**:

$$(*)\quad (\forall x\in\omega)[P(x)\ \vee\ R(x)]\rightarrow[(\exists x\in\omega)P(x)\ \vee\ (\forall x\in\omega)R(x)].$$

To see that $(*)$ implies **LPO** assume that $f\in 2^{\mathbb{N}}$. Then let $P(x)$ and $R(x)$ stand for $f(x)=1$ and $f(x)=0$, respectively.

Arguing in **BI**, we want to show that $(*)$ is realizable. The first step is to single out the element of $\mathbf{V}$ that plays the role of the natural numbers in $\mathbf{V}$. By the recursion theorem for E-computability define a function $g:\mathbb{N}\rightarrow\mathbb{N}$ with index d by $\{d\}^E(0)=\sup(0_{\mathbb{N}},\lambda x.x)$ and

$$\{d\}^E(n+1)=\sup((n+1)_{\mathbb{N}},d\restriction n)$$

where $d\restriction n$ is an index of the function $g_n:\mathbb{N}\rightarrow\mathbb{N}$ with $g_n(k)=\{d\}^E(k)$ if $k\leq n$ and $g_n(k)=0$ otherwise. Finally, let

$$\omega=\sup(\mathrm{nat},d).$$

Then $\omega\in\mathbf{V}$ and ω realizably plays the role of the natural numbers in $\mathbf{V}$.

Now assume that

$$e\Vdash(\forall x\in\omega)[P(x)\ \vee\ R(x)].\tag{3}$$

Unraveling the definition of (3) we get $(\forall i\,\dot{\in}\,\bar{\omega})\{e\}^E(i)\Vdash P(\tilde{\omega}i)\ \vee\ R(\tilde{\omega}i)$, whence

$$(\forall n\in\mathbb{N})\{e\}^E(n)\Vdash P(\tilde{\omega}n)\ \vee\ R(\tilde{\omega}n).\tag{4}$$

From (4) we get that for all $n\in\mathbb{N}$,

$$\begin{aligned}&[(f(n))_0=0\ \wedge\ (f(n))_1\Vdash P(\tilde{\omega}n)]\\ \vee\ \ &[(f(n))_0=1\ \wedge\ (f(n))_1\Vdash R(\tilde{\omega}n)],\end{aligned}\tag{5}$$

where $f(n) = \{e\}^E(n)$. There is an index b such that $\{b\}^E(n, x) = (f(n))_0$ for all n, x. If there exists n such that $(f(n))_0 = 0$ then by clause (3.2) of Definition 5.1 we get $\{\langle 3, 1, b\rangle\}^E(0) = n_0 + 1$ where n_0 is the smallest number such that $(f(n_0))_0 = 0$. Otherwise, by clause (3.1) of Definition 5.1, we have $\{\langle 3, 1, b\rangle\}^E(0) = 0$. We also find an index c such that $\{c\}^E(k) = (n, (f(n))_1)$ if $k = n + 1$ for some n and $\{c\}^E(k) = \lambda x.(f(x))_1$ if $k = 0$ (where $\lambda x.(f(x))_1$ denotes an index of the mapping $x \mapsto (f(x))_1$ which can be effectively computed from an index for f via the S-m-n theorem). Let sg be the primitive recursive function with $\mathrm{sg}(n + 1) = 1$ and $\mathrm{sg}(0) = 0$. Then we have

$$(\mathrm{sg}(\{\langle 3, 1, b\rangle\}^E(0)), \{c\}^E(\{\langle 3, 1, b\rangle\}^E(0))) \quad \Vdash \quad (\exists x \in \omega)P(x) \vee (\forall x \in \omega)R(x).$$

Since there is an index b^* such that

$$\{b^*\}^E(e) \simeq (\mathrm{sg}(\{\langle 3, 1, b\rangle\}^E(0)), \{c\}^E(\{\langle 3, 1, b\rangle\}^E(0)))$$

this ensures the realizability of $(*)$. $\square$

Acknowledgement:. This material is based upon work supported by the EPSRC of the UK through grants No. EP/G029520/1 and No. EP/G058024/1.

References

[1] P. Aczel: *The type theoretic interpretation of constructive set theory: Choice principles.* In: A.S. Troelstra and D. van Dalen, editors, *The L.E.J. Brouwer Centenary Symposium* (North Holland, Amsterdam, 1982) 1–40.

[2] P. Aczel, M. Rathjen: *Notes on constructive set theory*, Technical Report 40, Institut Mittag-Leffler (The Royal Swedish Academy of Sciences, 2001). `http://www.mittag-leffler.se/preprints/0001/`, Preprint No. 40.

[3] P. Aczel, M. Rathjen: *Notes on constructive set theory*, Preprint (2010) 243 pages. http://www1.maths.leeds.ac.uk/ rathjen/book.pdf

[4] W. Buchholz and K. Schütte: *Proof Theory of Impredicative Subsystems of analysis* (Bibliopolis, Naples, 1988).

[5] R.-M. Chen, M. Rathjen: *Lifschitz Realizability for Intuitionistic Zermelo-Fraenkel Set Theory.* Archive for Mathematical Logic 51 (2012) 789–818.

[6] S. Feferman: *Formal theories for transfinite iterations of generalized inductive definitions and some subsystems of analysis.* In: J. Myhill, A. Kino, R.F. Vesley (eds.): *Proof theory and Intuitionism* (North Holland, Amsterdam, 1970) 303–325.

[7] H. Friedman: *Set-theoretic foundations of constructive analysis.* Annals of Mathematics 105 (1977) 1–28.

[8] H. Gerber: *Brouwer's bar theorem and a system of ordinal notations.* In: J. Myhill, A. Kino, R.F. Vesley (eds.): *Proof theory and Intuitionism* (North Holland, Amsterdam, 1970) 327–338.

[9] P.G. Hinman: *Recursion-theoretic hierarchies.* (Springer, Berlin,1978).

[10] W.A. Howard: *A system of abstract constructive ordinals.* Journal of Symbolic Logic 37 (1972) 355-374.

[11] G. Kreisel: *A survey of proof theory.* Journal of Symbolic Logic 33 (1968) 321–388.

[12] J. Myhill: *Constructive set theory.* Journal of Symbolic Logic 40 (1975) 347–382.

[13] M. Rathjen: *The strength of some Martin–Löf type theories.* Archive for Mathematical Logic 33 (1994) 347–385.

[14] M. Rathjen: *Constructive set theory and Brouwerian principles.* Journal of Universal Computer Science 11 (2005) 2008–2033.

[15] M. Rathjen: *The formulae-as-classes interpretation of constructive set theory.* In: H. Schwichtenberg, K. Spies (eds.): *Proof Technology and Computation* (IOS Press, Amsterdam, 2006) 279–322.

[16] M. Rathjen, S. Tupailo: *Characterizing the interpretation of set theory in Martin-Löf type theory.* Annals of Pure and Applied Logic 141 (2006) 442–471.

[17] M. Rathjen, A. Weiermann: *Proof–theoretic investigations on Kruskal's theorem.* Annals of Pure and Applied Logic 60 (1993) 49–88.

[18] S.G. Simpson: *Subsystems of Second Order Arithmetic*, second edition, (Cambridge University Press, 2009).