Article:

Frittaion, E and Rathjen, M (2020) Extensional realizability for intuitionistic set theory. Journal of Logic and Computation. exaa087. ISSN 0955-792X

https://doi.org/10.1093/logcom/exaa087

EXTENSIONAL REALIZABILITY FOR INTUITIONISTIC SET THEORY

EMANUELE FRITTAION AND MICHAEL RATHJEN

ABSTRACT. In generic realizability for set theories, realizers treat unbounded quantifiers generically. To this form of realizability we add another layer of extensionality by requiring that realizers ought to act extensionally on realizers, giving rise to a realizability universe $\mathrm{V}_{\mathrm{ex}}(A)$ in which the axiom of choice in all finite types, $\mathsf{AC}_{\mathsf{FT}}$, is realized, where A stands for an arbitrary partial combinatory algebra. This construction furnishes "inner models" of many set theories that additionally validate $\mathsf{AC}_{\mathsf{FT}}$, in particular it provides self-validating semantics for CZF (Constructive Zermelo-Fraenkel set theory) and IZF (Intuitionistic Zermelo-Fraenkel set theory). One can also add large set axioms and many other principles.

CONTENTS

2010 *Mathematics Subject Classification.* Primary: 03F03; Secondary: 03F25, 03F50.

Key words and phrases. Intuitionistic, constructive, set theory, realizability, extensionality.

The authors' research was supported by a grant from John Templeton Foundation "A new dawn of Intuitionism: Mathematical and Philosophical advances"(grant ID 60842).

1. Introduction

In this paper we define an extensional version of generic[1] realizability over any given partial combinatory algebra and prove that it provides a self-validating semantics for CZF (Constructive Zermelo-Fraenkel set theory) as well as IZF (Intuitionistic Zermelo-Fraenkel set theory), i.e., every theorem of CZF (IZF) is realized by just assuming the axioms of CZF (IZF) in the background theory. Moreover, it is shown that the axiom of choice in all finite types, $\mathsf{AC}_{\mathsf{FT}}$, also holds under this interpretation.[2] This uniform tool of realizability can be combined with forcing to show that $\mathsf{IZF} + \mathsf{AC}_{\mathsf{FT}}$ is conservative over IZF with respect to arithmetic formulae (and similar results with large set axioms). For special cases, namely, finite type dependent choice, $\mathsf{DC}_{\mathsf{FT}}$, and finite type countable choice, $\mathsf{CAC}_{\mathsf{FT}}$,[3] this has been shown in [12, Theorem 5.1] and [5, XV.2], but not for $\mathsf{AC}_{\mathsf{FT}}$. The same technology works for CZF. However, for several subtheories of CZF (with exponentiation in lieu of subset collection) such conservativity results have already been obtained by Gordeev [16] by very different methods, using total combinatory algebras and an abstract form of realizability combined with genuine proof-theoretic machinery.

Generic realizability is markedly different from Kleene's number and function realizability as well as modified realizability. It originates with Kreisel's and Troelstra's [18] definition of realizability for second order Heyting arithmetic and the theory of species. Here, the clauses for the realizability relation $\Vdash$ relating to second order quantifiers are: $e \Vdash \forall X\, \phi(X) \Leftrightarrow \forall X\, e \Vdash \phi(X)$, $e \Vdash \exists X\, \phi(X) \Leftrightarrow \exists X\, e \Vdash \phi(X)$. This type of realizability does not seem to give any constructive interpretation to set quantifiers; realizing numbers "pass through" quantifiers. However, one could also say that thereby the collection of sets of natural numbers is generically conceived. Kreisel-Troelstra realizability was applied to systems of higher order arithmetic and set theory by Friedman [14] and to further set theories by Beeson [4]. An immediate descendant of the interpretations of Friedman and Beeson was used by McCarty [19, 20], who, unlike the realizabilities of Beeson, devised realizability directly for extensional IZF: *"we found it a nuisance to interpret the extensional theory into the intensional before realizing."* ([19, p. 82]). A further generalization, inspired by a remark of Feferman in [9], that McCarty introduced was that he used realizers from applicative structures, i.e. arbitrary models of Feferman's theory APP, rather than just natural numbers.

[1]The descriptive attribute "generic" for this kind of realizability is due to David McCarty [19, p. 31].

[2]As a byproduct, we reobtain the already known result (e.g. [24, 4.31, 4.33]) that augmenting CZF by $\mathsf{AC}_{\mathsf{FT}}$ does not increase the stock of provably recursive functions. Likewise, we reobtain the result (a consequence of [13]) that augmenting IZF by $\mathsf{AC}_{\mathsf{FT}}$ does not increase the stock of provably recursive functions.

[3]$\mathsf{DC}_{\mathsf{FT}}$ is the scheme $\forall x^\sigma\, \exists y^\sigma\, \varphi(x, y) \to \forall x^\sigma\, \exists f^{0\sigma}\, [f(0) = x \wedge \forall n\, \varphi(f(n), f(n+1))]$, while $\mathsf{CAC}_{\mathsf{FT}}$ stands for the scheme $\forall n\, \exists y^\tau\, \varphi(n, y) \to \exists f^{0\tau}\, \forall n\, \varphi(n, f(n))$.

Generic realizability [19] is based on the construction of a realizability universe $\mathrm{V}(A)$ on top of an applicative structure or partial combinatory algebra A. Whereas in [19, 20] the approach is geared towards IZF, making use of transfinite iterations of the powerset operation, it was shown in [25] that CZF suffices for a formalization of $\mathrm{V}(A)$ and the generic realizability based upon it. This tool has been successfully applied to the proof-theoretic analysis of CZF ever since [22, 23, 26, 28].

With regard to $\mathsf{AC}_{\mathsf{FT}}$, it is perhaps worth mentioning that, by using generic realizability [19], one can show that $\mathsf{AC}_{0,\tau}$ for $\tau \in \{0,1\}$ holds in the realizability universe $\mathrm{V}(A)$ for any partial combinatory algebra A (cf. also [8]). For instance, one can take Kleene's first algebra. With some effort, one can also see that $\mathsf{AC}_{1,\tau}$ for $\tau \in \{0,1\}$ holds in $\mathrm{V}(A)$ by taking, e.g., Kleene's second algebra. It is conceivable that one can construct a specific partial combinatory algebra A so as to validate $\mathsf{AC}_{\mathsf{FT}}$ in $\mathrm{V}(A)$. In this paper we show that, by building extensionality into the realizability universe and by adapting the definition of realizability, it is possible to satisfy choice in all finite types at once, regardless of the partial combinatory algebra A one starts with.

Extensional variants of realizability in the context of (finite type) arithmetic have been investigated by Troelstra (see [32]) and van Oosten [34, 35], as well as [15, 33], and for both arithmetic and set theory by Gordeev in [16]. For earlier references on extensional realizability, in particular [17], where the notion for first order arithmetic first appeared, and [21], see Troelstra [32, p. 441].

2. Partial combinatory algebras

Combinatory algebras are the brainchild of Moses Schönfinkel [27] who presented his ideas in Göttingen in 1920. The quest for an optimization of his framework, singling out a minimal set of axioms, engendered much work and writings from 1929 onwards, notably by H.B. Curry [6, 7], under the heading of *combinatory logic*. Curiously, a very natural generalization of Schönfinkel's structures, where the application operation is not required to be always defined, was axiomatically characterized only in 1975 by Solomon Feferman in the shape of the most basic axioms of his theory T_0 of explicit mathematics [9][4] and in [10, p. 70]. Feferman called these structures *applicative structures*.

Notation 2.1. In order to introduce the notion of a partial combinatory algebra, we shall start with that of a partial operational structure $(M, \cdot)$, where $\cdot$ is just a partial binary operation on M. We use $a \cdot b \simeq c$ to convey that $a \cdot b$ is defined and equal to c.

[4] In the literature, this subtheory of T_0 has been christened EON (for *elementary theory of operations and numbers*; see [5, p. 102]) and APP (on account of comprising the *applicative axioms* of T_0; see [29, Ch. 9, Section 5]). However, to be precise let us point out that T_0 as formulated in [11] differs from the original formulation in [9]: [11] has a primitive classification constant $\mathbb{N}$ for the natural numbers as well as constants for successor and predecessor on $\mathbb{N}$, and more crucially, equality is not assumed to be decidable and the definition-by-cases operation is restricted to $\mathbb{N}$.

$a \cdot b \downarrow$ stands for $\exists c\,(a \cdot b \simeq c)$. In what follows, instead of $a \cdot b$ we will just write ab. We also employ the association to the left convention, meaning that e.g. $abc \simeq d$ stands for the following: there exists e such that $ab \simeq e$ and $ec \simeq d$.

Definition 2.2. A *partial combinatory algebra* (pca) is a partial operational structure $(A, \cdot)$ such that A has at least two elements and there are elements $\mathbf{k}$ and $\mathbf{s}$ in A such that $\mathbf{k}a$, $\mathbf{s}a$ and $\mathbf{s}ab$ are always defined, and

- $\mathbf{k}ab \simeq a$;
- $\mathbf{s}abc \simeq ac(bc)$.

The combinators k and s are due to Schönfinkel [27] while the axiomatic treatment, although formulated just in the total case, is due to Curry [7]. The word "combinatory" appears because of a property known as *combinatory completeness* described next. For more information on partial combinatory algebras see [9, 11, 5, 35].

Definition 2.3. Given a pca A, one can form application terms over A by decreeing that:

(i) variables $x_1, x_2, \dots$ and the constants $\mathbf{k}$ and $\mathbf{s}$ are applications terms over A;
(ii) elements of A are application terms over A;
(iii) given application terms s and t over A, (ts) is also an application term over A.

Application terms over A will also be called A-terms. Terms generated solely by clauses (i)–(iii), will be called *application terms*.

An A-term q without free variables has an obvious interpretation q^A in A by interpreting elements of A by themselves and letting $(ts)^A$ be $t^A \cdot s^A$ with $\cdot$ being the partial operation of A. Of course, q may fail to denote an element of A. We write $A \models q \downarrow$ (or just $q \downarrow$) if it does, i.e., if q^A yields an element of A.

The combinatory completeness of a pca A is encapsulated in λ-abstraction (see [9, p. 95], [11, p. 63], and [5, p. 101] for more details).

Lemma 2.4 (λ-abstraction)**.** *For every term t with variables among the distinct variables $x, x_1, \dots, x_n$, one can find in an effective way a new term s, denoted $\lambda x.t$, such that*

- *the variables of s are the variables of t except for x,*
- *$s[a_1/x_1, \dots, a_n/x_n] \downarrow$ for all $a_1, \dots, a_n \in A$,*
- *$(s[a_1/x_1, \dots, a_n/x_n])a \simeq t[a/x, a_1/x_1, \dots, a_n/x_n]$ for all $a, a_1, \dots, a_n \in A$.*

The term $\lambda x.t$ is built solely with the aid of $\mathbf{k}, \mathbf{s}$ and symbols occurring in t.

An immediate consequence of the foregoing abstraction lemma is the recursion theorem for pca's (see [9, p. 96], [11, p. 63], [5, p. 103]).

Lemma 2.5 (Recursion theorem). *There exists a closed application term* $\mathbf{f}$ *such that for every pca* A *and* $a, b \in A$ *we have* $A \models \mathbf{f}\downarrow$ *and*

- $A \models \mathbf{f}a\downarrow$;
- $A \models \mathbf{f}ab \simeq a(\mathbf{f}a)b$.

Proof. The heuristic approach consists in finding a fixed point of the form cc. Let us search for $\mathbf{f}$ satisfying $\mathbf{f}a \simeq cc$, and hence find a solution of the equation

$$ccb \simeq a(cc)b.$$

By using λ-abstraction, we can easily arrange to have, for every d,

$$cdb \simeq a(dd)b.$$

Indeed, let $\mathbf{f} := \lambda a.cc$, where $c := \lambda db.a(dd)b$. Then f is as desired. □

In every pca, one has pairing and unpairing[5] combinators $\mathbf{p}$, $\mathbf{p_0}$, and $\mathbf{p_1}$ such that:

- $\mathbf{p}ab\downarrow$;
- $\mathbf{p_i}(\mathbf{p}a_0a_1) \simeq a_i$.

Generic realizability is based on partial combinatory algebras with some additional structure (see however Remark 2.7).

Definition 2.6. We say that A is a pca over ω if there are extra combinators **succ**, **pred** (successor and predecessor combinators), $\mathbf{d}$ (definition by cases combinator), and a map $n \mapsto \bar{n}$ from ω to A such that for all $n \in \omega$

$$\mathbf{succ}\,\bar{n} \simeq \overline{n+1}, \qquad \mathbf{pred}\,\overline{n+1} \simeq \bar{n},$$

$$\mathbf{d}\bar{n}\bar{m}ab \simeq \begin{cases} a & n = m; \\ b & n \neq m. \end{cases}$$

One then defines $\mathbf{0} := \bar{0}$ and $\mathbf{1} := \bar{1}$.

The notion of a pca over ω coincides with the notion of ω-pca$^+$ in, e.g., [22].

Note that one can do without $\mathbf{k}$ by letting $\mathbf{k} := \mathbf{d00}$. The existence of $\mathbf{d}$ implies that the map $n \mapsto \bar{n}$ is one-to-one. In fact, suppose $\bar{n} = \bar{m}$ but $n \neq m$. Then $\mathbf{d}\bar{n}\bar{n} \simeq \mathbf{d}\bar{n}\bar{m}$. It then follows that $a \simeq \mathbf{d}\bar{n}\bar{n}ab \simeq \mathbf{d}\bar{n}\bar{m}ab \simeq b$ for all a, b. On the other hand, by our definition, every pca contains at least two elements.

Remark 2.7. The notion of a pca over ω is slightly impoverished one compared to that of a model of Beeson's theory $\mathbf{PCA}^+$ [5, VI.2] or Feferman's applicative structures [11]. However, for our purposes all the differences between these structures are immaterial

[5]Let $\mathbf{p} = \lambda xyz.zxy$, $\mathbf{p_0} := \lambda x.x\mathbf{k}$, and $\mathbf{p_1} := \lambda x.x\bar{\mathbf{k}}$, where $\bar{\mathbf{k}} := \lambda xy.y$. Projections $\mathbf{p_0}$ and $\mathbf{p_1}$ need not be total. For realizability purposes, however, it is not necessary to have total projections.

as every pca can be expanded to a model of $\mathbf{PCA}^+$, which at the same time is also an applicative structure (see [5, VI.2.9]).

By using, say, Curry numerals, one obtains a combinator $\mathbf{d}$ for this representation of natural numbers. So, every pca can be turned into a pca over ω by using Curry numerals. On the other hand, the notion of pca over ω allows for other possible representations of natural numbers. Note that the existence of a combinator $\mathbf{d}$ for a given representation of natural numbers (together with a predecessor combinator), entails the existence of a primitive recursion operator $\mathbf{r}$ for such representation, that is, an element $\mathbf{r}$ such that:

$$\mathbf{r}ab\bar{0} \simeq a;$$
$$\mathbf{r}ab\overline{n+1} \simeq b(\mathbf{r}ab\bar{n})\bar{n}.$$

3. The theory CZF

The logic of CZF (Constructive Zermelo-Fraenkel set theory) is intuitionistic first order logic with equality. The only nonlogical symbol is $\in$ as in classical Zermelo-Fraenkel set theory ZF.

Axioms

1. **Extensionality**: $\forall x\,\forall y\,(\forall z\,(z \in x \leftrightarrow z \in y) \to x = y)$,
2. **Pairing**: $\forall x\,\forall y\,\exists z\,(x \in z \wedge y \in z)$,
3. **Union**: $\forall x\,\exists y\,\forall u\,\forall z\,(u \in z \wedge z \in x \to u \in y)$,
4. **Infinity**: $\exists x\,\forall y\,(y \in x \leftrightarrow y = 0 \vee \exists z \in x\,(y = z \cup \{z\}))$,
5. **Set Induction**: $\forall x\,(\forall y \in x\,\varphi(y) \to \varphi(x)) \to \forall x\,\varphi(x)$, for all formulae φ,
6. **Bounded Separation**: $\forall x\,\exists y\,\forall z\,(z \in y \leftrightarrow z \in x \wedge \varphi(z))$, for φ bounded, where a formula is bounded if all quantifiers appear in the form $\forall x \in y$ and $\exists x \in y$,
7. **Strong Collection**: $\forall u \in x\,\exists v\,\varphi(u,v) \to \exists y\,(\forall u \in x\,\exists v \in y\,\varphi(u,v) \wedge \forall v \in y\,\exists u \in x\,\varphi(u,v))$, for all formulae φ,
8. **Subset Collection**: $\forall x\,\forall y\,\exists z\,\forall p\,(\forall u \in x\,\exists v \in y\,\varphi(u,v,p) \to \exists q \in z\,(\forall u \in x\,\exists v \in q\,\varphi(u,v,p) \wedge \forall v \in q\,\exists u \in x\,\varphi(u,v,p)))$, for all formulae φ.

Notation 3.1. Let $x = 0$ be $\forall y \in x\,\neg(y = y)$ and $x = y \cup \{y\}$ be $\forall z \in x\,(z \in y \vee z = y) \wedge \forall z \in y\,(z \in x) \wedge y \in x$.

4. Finite types and axiom of choice

Finite types σ and their associated extensions F_σ are defined by the following clauses:

- $o \in \mathsf{FT}$ and $F_o = \omega$;
- if $\sigma, \tau \in \mathsf{FT}$, then $(\sigma)\tau \in \mathsf{FT}$ and

$$F_{(\sigma)\tau} = F_\sigma \to F_\tau = \{\text{total functions from } F_\sigma \text{ to } F_\tau\}.$$

For brevity we write $\sigma\tau$ for $(\sigma)\tau$, if the type σ is written as a single symbol. We say that $x \in F_\sigma$ has type σ.

The set FT of all finite types, the set $\{F_\sigma \colon \sigma \in \mathsf{FT}\}$, and the set $\mathbb{F} = \bigcup_{\sigma \in \mathsf{FT}} F_\sigma$ all exist in CZF.

Definition 4.1 (Axiom of choice in all finite types)**.** The schema $\mathsf{AC}_{\mathsf{FT}}$ consists of formulae

$$\forall x^\sigma \, \exists y^\tau \, \varphi(x, y) \to \exists f^{\sigma\tau} \, \forall x^\sigma \, \varphi(x, f(x)), \tag{$\mathsf{AC}_{\sigma,\tau}$}$$

where σ and τ are (standard) finite types.

Notation 4.2. We write $\forall x^\sigma \, \varphi(x)$ and $\exists x^\sigma \, \varphi(x)$ as a shorthand for $\forall x \, (x \in F_\sigma \to \varphi(x))$ and $\exists x \, (x \in F_\sigma \wedge \varphi(x))$ respectively.

5. Defining extensional realizability in CZF

In CZF, given a pca A over ω, we inductively define a class $\mathrm{V}_{\mathrm{ex}}(A)$ such that

$$\forall x \, (x \in \mathrm{V}_{\mathrm{ex}}(A) \leftrightarrow x \subseteq A \times A \times \mathrm{V}_{\mathrm{ex}}(A)).$$

General information on how to handle inductive definitions in CZF can be found in [1, 2, 3] and specifics on the inductive definition of $\mathrm{V}_{\mathrm{ex}}(A)$ in [25, 3.4].

The intuition for $\langle a, b, x\rangle \in y$ is that a and b are *equal realizers* of the fact that $x^A \in y^A$, where $y^A = \{x^A \colon \langle a, b, x\rangle \in y$ for some $a, b \in A\}$.

Notation 5.1. We use $(a)_i$ or simply a_i for $\mathbf{p_i}a$. Whenever we write an application term t, we assume that it is defined. In other words, a formula $\varphi(t)$ stands for $\exists a \, (t \simeq a \wedge \varphi(a))$.

Definition 5.2 (Extensional realizability)**.** We define the relation $a = b \Vdash \varphi$, where $a, b \in A$ and φ is a realizability formula with parameters in $\mathrm{V}_{\mathrm{ex}}(A)$. The atomic cases fall under the scope of definitions by transfinite recursion.

$$
\begin{aligned}
a = b \Vdash x \in y \quad &\Leftrightarrow \quad \exists z\,(\langle (a)_0, (b)_0, z\rangle \in y \wedge (a)_1 = (b)_1 \Vdash x = z)\\
a = b \Vdash x = y \quad &\Leftrightarrow \quad \forall \langle c, d, z\rangle \in x\,((ac)_0 = (bd)_0 \Vdash z \in y) \text{ and}\\
&\qquad\ \ \forall \langle c, d, z\rangle \in y\,((ac)_1 = (bd)_1 \Vdash z \in x)\\
a = b \Vdash \varphi \wedge \psi \quad &\Leftrightarrow \quad (a)_0 = (b)_0 \Vdash \varphi \wedge (a)_1 = (b)_1 \Vdash \psi\\
a = b \Vdash \varphi \vee \psi \quad &\Leftrightarrow \quad (a)_0 \simeq (b)_0 \simeq \mathbf{0} \wedge (a)_1 = (b)_1 \Vdash \varphi \text{ or}\\
&\qquad\ \ (a)_0 \simeq (b)_0 \simeq \mathbf{1} \wedge (a)_1 = (b)_1 \Vdash \psi\\
a = b \Vdash \neg\varphi \quad &\Leftrightarrow \quad \forall c, d \in A\, \neg(c = d \Vdash \varphi)\\
a = b \Vdash \varphi \to \psi \quad &\Leftrightarrow \quad \forall c, d\,(c = d \Vdash \varphi \to ac = bd \Vdash \psi)\\
a = b \Vdash \forall x \in y\, \varphi \quad &\Leftrightarrow \quad \forall \langle c, d, x\rangle \in y\,(ac = bd \Vdash \varphi)\\
a = b \Vdash \exists x \in y\, \varphi \quad &\Leftrightarrow \quad \exists x\,(\langle (a)_0, (b)_0, x\rangle \in y \wedge (a)_1 = (b)_1 \Vdash \varphi)\\
a = b \Vdash \forall x\, \varphi \quad &\Leftrightarrow \quad \forall x \in \mathrm{V_{ex}}(A)\,(a = b \Vdash \varphi)\\
a = b \Vdash \exists x\, \varphi \quad &\Leftrightarrow \quad \exists x \in \mathrm{V_{ex}}(A)\,(a = b \Vdash \varphi)
\end{aligned}
$$

Notation 5.3. We write $a \Vdash \varphi$ for $a = a \Vdash \varphi$.

The above definition builds on the variant [25] of generic realizability [19], where bounded quantifiers are treated as quantifiers in their own right. Note that in the language of CZF, bounded quantifiers can be seen as syntactic sugar by letting $\forall x \in y\, \varphi := \forall x\,(x \in y \to \varphi)$ and $\exists x \in y\, \varphi := \exists x\,(x \in y \wedge \varphi)$. Nothing gets lost in translation, thanks to the following.

Lemma 5.4. *There are closed application terms* $\mathbf{u}$ *and* $\mathbf{v}$ *such that* CZF *proves*

$$\mathbf{u} \Vdash \forall x \in y\, \varphi \leftrightarrow \forall x\,(x \in y \to \varphi),$$

$$\mathbf{v} \Vdash \exists x \in y\, \varphi \leftrightarrow \exists x\,(x \in y \wedge \varphi).$$

The advantage of having special clauses for bounded quantifiers is that it simplifies a great deal the construction of realizers.

Remark 5.5. In the context of (finite type) arithmetic, extensional notions of realizability typically give rise to a partial equivalence relation. Namely, for every formula φ, the relation $\{(a, b) \in A^2 \colon a = b \Vdash \varphi\}$ is symmetric and transitive. This is usually seen by induction on φ, the atomic case being trivial. The situation, though, is somewhat different in set theory. Say that $a = b \Vdash x \in y$ and $b = c \Vdash x \in y$. All we know is that for some $u, v \in \mathrm{V_{ex}}(A)$ we have that $\langle (a)_0, (b)_0, u\rangle, \langle (b)_0, (c)_0, v\rangle \in y$, $(a)_1 = (b)_1 \Vdash x = u$, and $(b)_1 = (c)_1 \Vdash x = v$. Since u and v need not be the same set, even if elements of $\mathrm{V_{ex}}(A)$ behave as expected, that is, $\{(a, b) \colon \langle a, b, y\rangle \in x\}$ is symmetric and transitive for any given $x, y \in \mathrm{V_{ex}}(A)$,[6] we cannot conclude that $a = c \Vdash x \in y$. So, transitivity can fail.

As it turns out, for our purposes, this is not an issue at all. Note however that the canonical names for objects of finite type do indeed behave as desired and so does the relation $a = b \Vdash \varphi$ for formulas of finite type arithmetic. This is in fact key in validating the axiom of choice in all finite types (Section 8). Except for this deviation, the clauses for connectives and quantifiers follow the general blueprint of extensional realizability. We just feel justified in keeping the notation $a = b \Vdash \varphi$.

6. Soundness for intuitionistic first order logic with equality

¿From now on, let A be a pca over ω within CZF. Realizability of the equality axioms relies on the following fact about pca's.

Lemma 6.1 (Double recursion theorem)**.** *There are combinators* $\mathbf{g}$ *and* $\mathbf{h}$ *such that, for all* $a, b, c \in A$*:*

- $\mathbf{g}ab\downarrow$ *and* $\mathbf{h}ab\downarrow$*;*
- $\mathbf{g}abc \simeq a(\mathbf{h}ab)c$*;*
- $\mathbf{h}abc \simeq b(\mathbf{g}ab)c$*.*

Proof. Let $t(a,b) := \lambda xc.a(\lambda c.bxc)c$. Set $\mathbf{g} := \lambda ab.\mathbf{f}t(a,b)$, where $\mathbf{f}$ is the fixed point operator from the recursion theorem. Set $\mathbf{h} := \lambda abc.b(\mathbf{f}t(a,b))c$. Verify that $\mathbf{g}$ and $\mathbf{h}$ are as desired. ☐

Lemma 6.2. *There are closed application terms* $\mathbf{i_r}$, $\mathbf{i_s}$, $\mathbf{i_t}$, $\mathbf{i_0}$ *and* $\mathbf{i_1}$ *such that* CZF *proves, for all* $x, y, z \in \mathrm{V_{ex}}(A)$*,*

(1) $\mathbf{i_r} \Vdash x = x$;
(2) $\mathbf{i_s} \Vdash x = y \to y = x$;
(3) $\mathbf{i_t} \Vdash x = y \wedge y = z \to x = z$;
(4) $\mathbf{i_0} \Vdash x = y \wedge y \in z \to x \in z$;
(5) $\mathbf{i_1} \Vdash x = y \wedge z \in x \to z \in y$.

Notation 6.3. Write, say, a_{ij} for $\mathbf{p_j}(\mathbf{p_i}a)$.

Proof. (1) By the recursion theorem in A, we can find $\mathbf{i_r}$ such that

$$\mathbf{i_r}a \simeq \mathbf{p}(\mathbf{p}a\mathbf{i_r})(\mathbf{p}a\mathbf{i_r}).$$

[6] One could inductively define $\mathrm{V_{ex}}(A)$ so as to make $\{(a,b) \in A^2 \colon \langle a, b, y\rangle \in x\}$ symmetric and transitive. Just let $x \in \mathrm{V_{ex}}(A)$ if and only if

- x consists of triples $\langle a, b, y\rangle$ with $y \in \mathrm{V_{ex}}(A)$;
- whenever $\langle a, b, y\rangle \in x$, $\langle b, a, y\rangle \in x$;
- whenever $\langle a, b, y\rangle \in x$ and $\langle b, c, y\rangle \in x$, also $\langle a, c, y\rangle \in x$.

By **Set Induction** we show that $\mathbf{i_r} \Vdash x = x$ for every $x \in \mathrm{V_{ex}}(A)$. Let $\langle a, b, y\rangle \in x$. We want $(\mathbf{i_r}a)_0 = (\mathbf{i_r}b)_0 \Vdash y \in x$. Now $(\mathbf{i_r}a)_{00} \simeq a$ and similarly for b. On the other hand, $(\mathbf{i_r}a)_{01} \simeq (\mathbf{i_r}b)_{01} \simeq \mathbf{i_r}$. By induction, $\mathbf{i_r} \Vdash y = y$, and so we are done. Similarly for $(\mathbf{i_r}a)_1 = (\mathbf{i_r}b)_1 \Vdash y \in x$.

(2) We just need to interchange. Let

$$\mathbf{i_s} := \lambda ac.\mathbf{p}(ac)_1(ac)_0.$$

Suppose $a = b \Vdash x = y$. We want $\mathbf{i_s}a = \mathbf{i_s}b \Vdash y = x$. Let $\langle c, d, z\rangle \in y$. By definition, $(ac)_1 = (bd)_1 \Vdash z \in x$. Now $(ac)_1 \simeq (\mathbf{i_s}ac)_0$, and similarly $(bd)_1 \simeq (\mathbf{i_s}bd)_0$. Then we are done. Similarly for the other direction.

(3,4) Combinators $\mathbf{i_t}$ and $\mathbf{i_0}$ are defined by a double recursion in A. By induction on triples $\langle x, y, z\rangle$, one then shows that $\mathbf{i_t} \Vdash x = y \wedge y = z \to x = z$ and $\mathbf{i_0} \Vdash x = y \wedge y \in z \to x \in z$. Eventually, $\mathbf{i_t}$ and $\mathbf{i_r}$ are solutions of equations of the form

$$\mathbf{i_t}a \simeq \mathbf{t}\mathbf{i_0}a,$$
$$\mathbf{i_0}a \simeq \mathbf{r}\mathbf{i_t}a,$$

where $\mathbf{t}$ and $\mathbf{r}$ are given closed application terms. These are given by the fixed point operators from the double recursion theorem.

(5) Set

$$\mathbf{i_1} := \lambda a.\mathbf{p}(a_0a_{10})_{00}(\mathbf{i_t}(\mathbf{p}a_{11}(a_0a_{10})_{01})).$$

□

Theorem 6.4. *For every formula $\varphi(x_1, \ldots, x_n)$ provable in intuitionistic first order logic with equality, there exists a closed application term $\mathbf{e}$ such that* CZF *proves $\mathbf{e} \Vdash \forall x_1 \cdots \forall x_n\, \varphi(x_1, \ldots, x_n)$.*

Proof. The proof is similar to [19, 5.3] and [25, 4.3]. □

7. Soundness for CZF

We start with a lemma concerning bounded separation.

Lemma 7.1 (CZF)**.** *Let $\varphi(u)$ be a bounded formula with parameters from $\mathrm{V_{ex}}(A)$ and $x \subseteq \mathrm{V_{ex}}(A)$. Then*

$$\{\langle a, b, u\rangle \colon a, b \in A \wedge u \in x \wedge a = b \Vdash \varphi(u)\}$$

is a set.

Proof. As in [25, Lemma 4.5, Lemma 4.6, Corollary 4.7]. □

Theorem 7.2. *For every theorem φ of* CZF*, there is a closed application term $\mathbf{e}$ such that* CZF *proves $\mathbf{e} \Vdash \varphi$.*

Proof. In view of Theorem 6.4, it is sufficient to show that every axiom of CZF has a realizer. The proof is similar to that of [25, Theorem 5.1]. The rationale is simple: use the same realizers, duplicate the names. Remember that $\mathbf{e} \Vdash \varphi$ means $\mathbf{e} = \mathbf{e} \Vdash \varphi$.

Extensionality. Let $x, y \in \mathrm{V_{ex}}(A)$. Suppose $a = b \Vdash z \in x \leftrightarrow z \in y$ for all $z \in \mathrm{V_{ex}}(A)$. We look for $\mathbf{e}$ such that $\mathbf{e}a = \mathbf{e}b \Vdash x = y$. Set

$$\mathbf{e} := \lambda ac.\mathbf{p}(a_0(\mathbf{p}c\mathbf{i_r}))(a_1(\mathbf{p}c\mathbf{i_r})).$$

Suppose $\langle c, d, z\rangle \in x$. Then $\mathbf{p}c\mathbf{i_r} = \mathbf{p}d\mathbf{i_r} \Vdash z \in x$, since $\mathbf{i_r} \Vdash z = z$. Then $a_0(\mathbf{p}c\mathbf{i_r}) = b_0(\mathbf{p}d\mathbf{i_r}) \Vdash z \in y$. Therefore, $(\mathbf{e}ac)_0 = (\mathbf{e}bd)_0 \Vdash z \in y$, as desired. The other direction is similar.

Pairing. Find $\mathbf{e}$ such that for all $x, y \in \mathrm{V_{ex}}(A)$,

$$\mathbf{e} \Vdash x \in z \wedge y \in z,$$

for some $z \in \mathrm{V_{ex}}(A)$. Let $x, y \in \mathrm{V_{ex}}(A)$ be given. Define $z = \{\langle \mathbf{0}, \mathbf{0}, x\rangle, \langle \mathbf{0}, \mathbf{0}, y\rangle\}$. Let

$$\mathbf{e} = \mathbf{p}(\mathbf{p0i_r})(\mathbf{p0i_r}).$$

Union. Find $\mathbf{e}$ such that for all $x \in \mathrm{V_{ex}}(A)$,

$$\mathbf{e} \Vdash \forall u \in x\, \forall v \in u\, (v \in y),$$

for some $y \in \mathrm{V_{ex}}(A)$. Given $x \in \mathrm{V_{ex}}(A)$, let $y = \{\langle c, d, v\rangle \colon \exists \langle a, b, u\rangle \in x\, (\langle c, d, v\rangle \in u)\}$. Set $\mathbf{e} := \lambda ac.\mathbf{p}c\mathbf{i_r}$.

Infinity. Let $\dot{\omega} = \{\langle \bar{n}, \bar{n}, \dot{n}\rangle \colon n \in \omega\}$, where $\dot{n} = \{\langle \bar{m}, \bar{m}, \dot{m}\rangle \colon m < n\}$. Let us find $\mathbf{e}$ such that for all $y \in \mathrm{V_{ex}}(A)$,

$$\mathbf{e} \Vdash y \in \dot{\omega} \leftrightarrow y = 0 \vee \exists z \in \dot{\omega}\, (y = z \cup \{z\}).$$

Recall that $y = 0$ stands for $\forall x \in y\, \neg(x = x)$ and $y = z \cup \{z\}$ stands for $\forall x \in y\, (x \in z \vee x = z) \wedge (\forall x \in z\, (x \in y) \wedge z \in y)$.

Let $\vartheta(y) := y = 0 \vee \exists z \in \dot{\omega}\, (y = z \cup \{z\})$. We want $\mathbf{e}$ such that for every $y \in \mathrm{V_{ex}}(A)$

$$\mathbf{e}_0 \Vdash y \in \dot{\omega} \to \vartheta(y), \tag{1}$$

$$\mathbf{e}_1 \Vdash \vartheta(y) \to y \in \dot{\omega}. \tag{2}$$

Let us first consider (1). Suppose $a = b \Vdash y \in \dot{\omega}$. We want $\mathbf{e}_0 a = \mathbf{e}_0 b \Vdash \vartheta(y)$.

By definition, there is $n \in \omega$ such that $a_0 \simeq b_0 \simeq \bar{n}$ and $a_1 = b_1 \Vdash y = \dot{n}$.

Case $n = 0$. Then $\mathbf{0} \Vdash y = 0$, and so $\mathbf{p00} \Vdash \vartheta(y)$.

Case $n > 0$. We have $\mathbf{pred}\, a_0 \simeq \mathbf{pred}\, b_0 \simeq \bar{m}$ with $n = m+1$. We aim for a term $t(x)$ such that $t(a) = t(b) \Vdash \exists z \in \dot{\omega}\, (y = z \cup \{z\})$ by requiring

$$t(a)_0 \simeq t(b)_0 \simeq \bar{m},$$

$$t(a)_1 = t(b)_1 \Vdash y = \dot{m} \cup \{\dot{m}\}. \tag{3}$$

If we succeed, then

$$\mathbf{p1}t(a) = \mathbf{p1}t(b) \Vdash \vartheta(y).$$

Now, (3) amounts to

$$t(a)_{10} = t(b)_{10} \Vdash \forall x \in y\, (x \in \dot{m} \vee x = \dot{m}) \tag{4}$$

$$t(a)_{110} = t(b)_{110} \Vdash \forall x \in \dot{m}\, (x \in y) \tag{5}$$

$$t(a)_{111} = t(b)_{111} \Vdash \dot{m} \in y \tag{6}$$

Part (4). Let $\langle c, d, x\rangle \in y$. Then $(a_1 c)_0 = (b_1 d)_0 \Vdash x \in \dot{n}$, that is,

$$\langle (a_1 c)_{00}, (b_1 d)_{00}, \dot{k}\rangle \in \dot{n},$$

$$(a_1 c)_{01} = (b_1 d)_{01} \Vdash x = \dot{k},$$

where $(a_1 c)_{00} \simeq (b_1 d)_{00} \simeq \bar{k}$. Here we have two more cases. If $k = m$, then

$$\mathbf{p1}(a_1 c)_{01} = \mathbf{p1}(b_1 d)_{01} \Vdash x \in \dot{m} \vee x = \dot{m}.$$

If $k < m$, then $\langle \bar{k}, \bar{k}, \dot{k}\rangle \in \dot{m}$ and $\mathbf{p}\bar{k}(a_1 c)_{01} = \mathbf{p}\bar{k}(b_1 d)_{01} \Vdash x \in \dot{m}$, so that

$$\mathbf{p0}(\mathbf{p}\bar{k}(a_1 c)_{01}) = \mathbf{p0}(\mathbf{p}\bar{k}(b_1 d)_{01}) \Vdash x \in \dot{m} \vee x = \dot{m}.$$

Then $t(a)$ such that

$$t(a)_{10} \simeq \lambda c.\mathbf{d}(a_1 c)_{00}(\mathbf{pred}\, a_0)(\mathbf{p1}(a_1 c)_{01})(\mathbf{p0}(a_1 c)_0)$$

is as desired.

Parts (5) and (6). Let $t(a)$ satisfy

$$t(a)_{110} \simeq \lambda x.(a_1 x)_1,$$

$$t(a)_{111} \simeq (a_1(\mathbf{pred}\, a_0))_1.$$

We want $\mathbf{e}$ such that

$$\mathbf{e}_0 \simeq \lambda a.\mathbf{d0}a_0(\mathbf{p00})(\mathbf{p1}t(a)).$$

Then $\mathbf{e}_0$ does the job.

As for (2), suppose $a = b \Vdash \vartheta(y)$. We want $\mathbf{e}_1 a = \mathbf{e}_1 b \Vdash y \in \dot{\omega}$. By unravelling the definitions, we obtain two cases.

(i) $a_0 \simeq b_0 \simeq \mathbf{0}$ and $a_1 = b_1 \Vdash y = 0$. It follows that $y = \dot{0}$ and so $\mathbf{i_r} \Vdash y = \dot{0}$. Therefore $\mathbf{p}a_0\mathbf{i_r} = \mathbf{p}b_0\mathbf{i_r} \Vdash y \in \dot{\omega}$, as $\langle \mathbf{0}, \mathbf{0}, \dot{0}\rangle \in \dot{\omega}$.

(ii) $a_0 \simeq b_0 \simeq \mathbf{1}$ and $a_1 = b_1 \Vdash \exists z \in \dot{\omega}\,(y = z \cup \{z\})$ Then there exists $m \in \omega$ such that $a_{10} \simeq b_{10} \simeq \bar{m}$ and

$$a_{11} = b_{11} \Vdash y = \dot{m} \cup \{\dot{m}\}. \tag{7}$$

We aim for a term $s(x)$ such that $s(a) = s(b) \Vdash y = \dot{n}$, where $n = m + 1$. If we succeed, then

$$\mathbf{p}(\mathbf{succ}\, a_{10})s(a) = \mathbf{p}(\mathbf{succ}\, b_{10})s(b) \Vdash y \in \dot{\omega}.$$

Note in fact that $\mathbf{succ}\, a_{10} \simeq \mathbf{succ}\, b_{10} \simeq \bar{n}$.

For the left to right inclusion, suppose $\langle c, d, x\rangle \in y$. Our goal is $(s(a)c)_0 = (s(b)d)_0 \Vdash x \in \dot{n}$. It follows from (7) that

$$a_{110} = b_{110} \Vdash \forall x \in y\,(x \in \dot{m} \vee x = \dot{m}),$$

and therefore

$$a_{110}c = b_{110}d \Vdash x \in \dot{m} \vee x = \dot{m}. \tag{8}$$

¿From (8) we get two more cases. First case: $(a_{110}c)_0 \simeq (b_{110}d)_0 \simeq \mathbf{0}$ and $(a_{110}c)_1 = (b_{110}d)_1 \Vdash x \in \dot{m}$. Then one can verify that

$$(a_{110}c)_1 = (b_{110}d)_1 \Vdash x \in \dot{n}.$$

Second case: $(a_{110}c)_0 \simeq (b_{110}d)_0 \simeq \mathbf{1}$ and $(a_{110}c)_1 = (b_{110}d)_1 \Vdash x = \dot{m}$. Then

$$\mathbf{p}\bar{m}(a_{110}c)_1 = \mathbf{p}\bar{m}(b_{110}d)_1 \Vdash x \in \dot{n}.$$

Let $s(x)$ be such that

$$(s(a)c)_0 \simeq \mathbf{d0}(a_{110}c)_0(a_{110}c)_1(\mathbf{p}a_{10}(a_{110}c)_1).$$

For the right to left inclusion, suppose $k < n$. Our goal is $(s(a)\bar{k})_1 = (s(b)\bar{k})_1 \Vdash \dot{k} \in y$. It follows from (7) that

$$a_{1110} = b_{1110} \Vdash \forall x \in \dot{m}\,(x \in y), \tag{9}$$

$$a_{1111} = b_{1111} \Vdash \dot{m} \in y. \tag{10}$$

If $k < m$, then $\langle \bar{k}, \bar{k}, \dot{k}\rangle \in \dot{m}$, and hence $a_{1110}\bar{k} = b_{1110}\bar{k} \Vdash \dot{k} \in y$ by (9). On the other hand, if $k = m$ then (10) gives us the realizers. Therefore let $s(x)$ be such that

$$(s(a)\bar{k})_1 \simeq \mathbf{d}\bar{k}a_{10}a_{1111}(a_{1110}\bar{k}).$$

We thus want $\mathbf{e}$ such that

$$\mathbf{e}_1 \simeq \lambda a.\mathbf{d0}a_0(\mathbf{p}a_0\mathbf{i_r})(\mathbf{p}(\mathbf{succ}\, a_{10})s(a)).$$

Then $\mathbf{e}_1$ does the job.

Set Induction. By the recursion theorem, let $\mathbf{e}$ be such that $\mathbf{e}a \simeq a(\lambda c.\mathbf{e}a)$. Prove that

$$\mathbf{e} \Vdash \forall x\,(\forall y \in x\,\varphi(y) \to \varphi(x)) \to \forall x\,\varphi(x).$$

Let $a = b \Vdash \forall x\,(\forall y \in x\,\varphi(y) \to \varphi(x))$. By definition, $a = b \Vdash \forall y \in x\,\varphi(y) \to \varphi(x)$ for every $x \in \mathrm{V}_{\mathrm{ex}}(A)$. By **Set Induction** we show that $\mathbf{e}a = \mathbf{e}b \Vdash \varphi(x)$ for every $x \in \mathrm{V}_{\mathrm{ex}}(A)$. Assume by induction that $\mathbf{e}a = \mathbf{e}b \Vdash \varphi(y)$ for every $\langle c, d, y\rangle \in x$. This means that $\lambda c.\mathbf{e}a = \lambda d.\mathbf{e}b \Vdash \forall y \in x\,\varphi(y)$. Then $a(\lambda c.\mathbf{e}a) = b(\lambda d.\mathbf{e}b) \Vdash \varphi(x)$. The conclusion $\mathbf{e}a = \mathbf{e}b \Vdash \varphi(x)$ follows.

Bounded Separation. Find $\mathbf{e}$ such that for all $x \in \mathrm{V}_{\mathrm{ex}}(A)$,

$$\mathbf{e} \Vdash \forall u \in y\,(u \in x \wedge \varphi(u)) \wedge \forall u \in x\,(\varphi(u) \to u \in y),$$

for some $y \in \mathrm{V}_{\mathrm{ex}}(A)$. Given $x \in \mathrm{V}_{\mathrm{ex}}(A)$, let

$$y = \{\langle \mathbf{p}ac, \mathbf{p}bd, u\rangle \colon \langle a, b, u\rangle \in x \wedge c = d \Vdash \varphi(u)\}.$$

It follows from Lemma 7.1 that y is a set. Moreover, y belongs to $\mathrm{V}_{\mathrm{ex}}(A)$. We want $\mathbf{e}$ such that

$$\mathbf{e}_0 \Vdash \forall u \in y\,(u \in x \wedge \varphi(u)),$$
$$\mathbf{e}_1 \Vdash \forall u \in x\,(\varphi(u) \to u \in y).$$

By letting $\mathbf{e} = \mathbf{p}e_0e_1$, where

$$e_0 := \lambda f.\mathbf{p}(\mathbf{p}f_0\mathbf{i_r})f_1,$$
$$e_1 := \lambda ac.\mathbf{p}(\mathbf{p}ac)\mathbf{i_r},$$

one verifies that $\mathbf{e}$ is as desired.

Strong Collection. Set $\mathbf{e} := \lambda a.\mathbf{p}(\lambda c.\mathbf{p}c(ac))(\lambda c.\mathbf{p}c(ac))$. Let $a = b \Vdash \forall u \in x\,\exists v\,\varphi(u, v)$. By **Strong Collection**, we can find a set y such that

- $\forall \langle c, d, u\rangle \in x\,\exists v \in \mathrm{V}_{\mathrm{ex}}(A)\,(\langle c, d, v\rangle \in y \wedge ac = bd \Vdash \varphi(u, v))$, and
- $\forall z \in y\,\exists \langle c, d, u\rangle \in x\,\exists v \in \mathrm{V}_{\mathrm{ex}}(A)\,(z = \langle c, d, v\rangle \wedge ac = bd \Vdash \varphi(u, v))$.

In particular, $y \in \mathrm{V}_{\mathrm{ex}}(A)$. Show that

$$\mathbf{e}a = \mathbf{e}b \Vdash \forall u \in x\,\exists v \in y\,\varphi(u, v) \wedge \forall v \in y \exists u \in x\,\varphi(u, v).$$

Subset Collection. We look for $\mathbf{e}$ such that for all $x, y \in \mathrm{V}_{\mathrm{ex}}(A)$ there is a $z \in \mathrm{V}_{\mathrm{ex}}(A)$ such that for all $p \in \mathrm{V}_{\mathrm{ex}}(A)$

$$\mathbf{e} \Vdash \forall u \in x\,\exists v \in y\,\varphi(u, v, p) \to \exists q \in z\,\psi(x, q, p),$$

where

$$\psi(x,q,p) := \forall u \in x\, \exists v \in q\, \varphi(u,v,p) \wedge \forall v \in q\, \exists u \in x\, \varphi(u,v,p).$$

Form the set $y' = \{\langle f,g,v\rangle : f,g \in A \wedge \exists i,j \in A\, \langle i,j,v\rangle \in y\}$. By **Subset Collection** we can find a set z' such that for all a,b,p, if

$$\forall \langle c,d,u\rangle \in x\, \exists \langle \mathbf{p}ac, \mathbf{p}bd, v\rangle \in y'\, (ac)_1 = (bd)_1 \Vdash \varphi(u,v,p), \tag{11}$$

then there is a $q \in z'$ such that

$$\forall \langle c,d,u\rangle \in x\, \exists w \in q\, \vartheta \wedge \forall w \in q\, \exists \langle c,d,u\rangle \in x\, \vartheta, \tag{12}$$

where $\vartheta = \vartheta(c,d,u,w;a,b,p)$ is

$$\exists v\, (w = \langle \mathbf{p}ac, \mathbf{p}bd, v\rangle \wedge (ac)_1 = (bd)_1 \Vdash \varphi(u,v,p)).$$

Note that the $q \in z'$ asserted to exist is a subset of y' and so $q \in \mathrm{V_{ex}}(A)$. On the other hand, there might be $q \in z'$ that are not in $\mathrm{V_{ex}}(A)$, and hence z' need not be a subset of $\mathrm{V_{ex}}(A)$. Let $z'' = \{q \cap y' : q \in z'\}$. Now, $z'' \subseteq \mathrm{V_{ex}}(A)$. Finally, set

$$z = \{\langle \mathbf{0}, \mathbf{0}, q\rangle : q \in z''\}.$$

Then $z \in \mathrm{V_{ex}}(A)$. It remains to find $\mathbf{e}$. Let $p \in \mathrm{V_{ex}}(A)$ and suppose

$$a = b \Vdash \forall u \in x\, \exists v \in y\, \varphi(u,v,p). \tag{13}$$

We would like to have

$$\mathbf{e}a = \mathbf{e}b \Vdash \exists q \in z\, \psi(x,q,p).$$

By definition of z, we let $(\mathbf{e}a)_0 \simeq \mathbf{0}$ and we look for a $q \in z''$ such that $(\mathbf{e}a)_1 = (\mathbf{e}b)_1 \Vdash \psi(x,q,p)$, that is,

$$(\mathbf{e}a)_{10} = (\mathbf{e}b)_{10} \Vdash \forall u \in x\, \exists v \in q\, \varphi(u,v,p),$$
$$(\mathbf{e}a)_{11} = (\mathbf{e}b)_{11} \Vdash \forall v \in q\, \exists u \in x\, \varphi(u,v,p).$$

By (13) one can see that the parameters a,b,p satisfy (11). Let $q \in z'$ be as in (12). We have already noticed that $q \in z''$. Let $\mathbf{e}$ be such that

$$(\mathbf{e}a)_{10} \simeq \lambda c.\mathbf{p}(\mathbf{p}ac)(ac)_1,$$
$$(\mathbf{e}a)_{11} \simeq \lambda f.\mathbf{p}f_1(f_0f_1)_1.$$

One can verify that $\mathbf{e}$ is as desired. □

8. Realizing the axiom of choice in all finite types

We will make use of certain canonical names for pairs in $\mathrm{V_{ex}}(A)$.

Definition 8.1 (Internal pairing)**.** For $x, y \in \mathrm{V_{ex}}(A)$, let

$$\{x\}_A = \{\langle \mathbf{0}, \mathbf{0}, x\rangle\},$$

$$\{x, y\}_A = \{\langle \mathbf{0}, \mathbf{0}, x\rangle, \langle \mathbf{1}, \mathbf{1}, y\rangle\},$$

$$\langle x, y\rangle_A = \{\langle \mathbf{0}, \mathbf{0}, \{x\}_A\rangle, \langle \mathbf{1}, \mathbf{1}, \{x, y\}_A\rangle\}.$$

Note that all these sets are in $\mathrm{V_{ex}}(A)$.

Below we shall use $\mathrm{UP}(x, y, z)$ and $\mathrm{OP}(x, y, z)$ as abbreviations for the set-theoretic formulae expressing, respectively, that z is the unordered pair of x and y (in standard notation, $z = \{x, y\}$) and z is the ordered pair of x and y (in standard notation, $z = \langle x, y\rangle$). E.g., $\mathrm{UP}(x, y, z)$ stands for $x \in z \wedge y \in z \wedge \forall u \in z\,(u = x \vee u = y)$. Similarly, one can pick a suitable rendering of $\mathrm{OP}(x, y, z)$ according to the definition of ordered pair $\langle x, y\rangle := \{\{x\}, \{x, y\}\}$.

Lemma 8.2. *There are closed application terms* $\mathbf{u_0}$*,* $\mathbf{u_1}$*,* $\mathbf{v}$*,* $\mathbf{w}$*,* $\mathbf{z}$ *such that for all* $x, y \in \mathrm{V_{ex}}(A)$

$$\mathbf{u_0} \Vdash \mathrm{UP}(x, x, \{x\}_A),$$

$$\mathbf{u_1} \Vdash \mathrm{UP}(x, y, \{x, y\}_A),$$

$$\mathbf{v} \Vdash \mathrm{OP}(x, y, \langle x, y\rangle_A),$$

$$\mathbf{w} \Vdash \langle x, y\rangle_A = \langle u, v\rangle_A \to x = u \wedge y = v,$$

$$\mathbf{z} \Vdash \mathrm{OP}(x, y, z) \to z = \langle x, y\rangle_A.$$

Proof. This is similar to [19, 3.2, 3.4]. □

We now build a copy of the hereditarily effective operations relative to a pca A.

Definition 8.3 (HEO_A)**.** Let A be a pca over ω with map $n \mapsto \bar{n}$ from ω to A. For any finite type σ, we define $a =_\sigma b$ with $a, b \in A$ by letting:

- $a =_0 b$ iff there is $n \in \omega$ such that $a = b = \bar{n}$;
- $a =_{\sigma\tau} b$ iff for every $c =_\sigma d$ we have $ac =_\tau bd$.

Let $A_\sigma = \{a \in A \colon a =_\sigma a\}$.

Lemma 8.4. *For any type* σ*, and for all* $a, b, c \in A$*:*

- *if* $a =_\sigma b$ *and* $b =_\sigma c$*, then* $a =_\sigma a$*,* $b =_\sigma a$*, and* $a =_\sigma c$*.*

It thus follows that $A_\sigma = \bigcup_{b \in A}\{a \in A \colon a =_\sigma b\} = \bigcup_{a \in A}\{b \in A \colon a =_\sigma b\}$ *and* $=_\sigma$ *is an equivalence relation on* A_σ*.*

Proof. By induction on the type. □

Definition 8.5 (Internalization of objects of finite type)**.** For $a \in A_\sigma$, we define $a^\sigma \in \mathrm{V_{ex}}(A)$ as follows:

- if $a = \bar{n}$, let $a^o = \{\langle \bar{m}, \bar{m}, \bar{m}^o \rangle : m < n\}$;
- if $a \in A_{\sigma\tau}$, let $a^{\sigma\tau} = \{\langle c, d, \langle c^\sigma, e^\tau \rangle_A \rangle : c =_\sigma d \text{ and } ac \simeq e\}$.

Finally, for any finite type σ, let

$$\dot{F}_\sigma = \{\langle a, b, a^\sigma \rangle : a =_\sigma b\}$$

be our name for F_σ.

Note that $\dot{F}_o = \dot{\omega}$, where $\dot{\omega}$ is the name for ω used to realize the Infinity axiom in the proof of Theorem 7.2.

Notation 8.6. Write $\Vdash \varphi$ for $\exists a, b \in A\, (a = b \Vdash \varphi)$.

Lemma 8.7 (Absoluteness and uniqueness up to extensional equality)**.** *For all $a, b \in A_\sigma$,*

- $\Vdash a^\sigma = b^\sigma$ *implies* $a =_\sigma b$*,*
- $a =_\sigma b$ *implies* $a^\sigma = b^\sigma$*.*

Proof. By induction on the type.

Type o. Let $a = \bar{n}$ and $b = \bar{m}$ with $n, m \in \omega$. Suppose $\Vdash a^o = b^o$. By a double arithmetical induction one shows $n = m$. The second part is obvious as $a =_o b$ implies $a = b$.

Type $\sigma\tau$. Let $a, b \in A_{\sigma\tau}$. Suppose $\Vdash a^{\sigma\tau} = b^{\sigma\tau}$. The aim is to show that $a =_{\sigma\tau} b$. Let $c \in A_\sigma$ and $ac \simeq e$. Then $\Vdash \langle c^\sigma, e^\tau \rangle_A \in a^{\sigma\tau}$ and hence $\Vdash \langle c^\sigma, e^\tau \rangle_A \in b^{\sigma\tau}$. ¿From the latter we infer that there exist $c_0 \in A_\sigma$ and $e_0 \in A_\tau$ such that $bc_0 \simeq e_0$ and $\Vdash \langle c^\sigma, e^\tau \rangle_A = \langle {c_0}^\sigma, {e_0}^\tau \rangle_A$. By the properties of internal pairing, we obtain $\Vdash c^\sigma = {c_0}^\sigma \;\wedge\; e^\tau = {e_0}^\tau$ giving $c =_\sigma c_0$ and $e =_\tau e_0$ by the induction hypothesis. Whence $ac =_\tau bc_0 =_\tau bc$ as $b \in A_{\sigma\tau}$. As a result one has $ac =_\tau bd$ whenever $c =_\sigma d$, yielding $a =_{\sigma\tau} b$.

For the second part, suppose $a =_{\sigma\tau} b$. An element of $a^{\sigma\tau}$ is of the form $\langle c, d, \langle c^\sigma, e^\tau \rangle_A \rangle$ where $c =_\sigma d$ and $ac \simeq e$. Let $e_0 \simeq bc$. As $ac =_\tau bc$ the induction hypothesis yields $e^\tau = {e_0}^\tau$, and hence $\langle c, d, \langle c^\sigma, e^\tau \rangle_A \rangle = \langle c, d, \langle c^\sigma, {e_0}^\tau \rangle_A \rangle \in b^{\sigma\tau}$, showing $a^{\sigma\tau} \subseteq b^{\sigma\tau}$. Owing to the symmetry of the argument, we can conclude that $a^{\sigma\tau} = b^{\sigma\tau}$. □

Theorem 8.8 (Choice)**.** *There exists a closed application term* $\mathbf{e}$ *such that* CZF *proves*

$$\mathbf{e} \Vdash \forall x \in \dot{F}_\sigma\, \exists y \in \dot{F}_\tau\, \varphi(x, y) \to \exists f \colon \dot{F}_\sigma \to \dot{F}_\tau\, \forall x \in \dot{F}_\sigma\, \varphi(x, f(x)),$$

for all finite types σ and τ and for every formula φ.

Proof. Suppose $a = b \Vdash \forall x \in \dot{F}_\sigma\, \exists y \in \dot{F}_\tau\, \varphi(x, y)$. By definition, this means that for every $\langle c, d, c^\sigma \rangle \in \dot{F}_\sigma$ we have

$$\langle (ac)_0, (bd)_0, e^\tau \rangle \in \dot{F}_\tau, \tag{1}$$

$$(ac)_1 = (bd)_1 \Vdash \varphi(c^\sigma, e^\tau), \tag{2}$$

where $e \simeq (ac)_0$. Let

$$f = \{\langle c, d, \langle c^\sigma, e^\tau\rangle_A\rangle \colon c =_\sigma d \wedge e \simeq (ac)_0\}.$$

Note that $c =_\sigma d$ implies $(ac)_0\downarrow$ by (1).

Below we shall use $z = \langle x, y\rangle$ as a somewhat sloppy abbreviation for $\mathrm{OP}(x, y, z)$. We look for an $\mathbf{e}$ such that

$$(\mathbf{e}a)_0 = (\mathbf{e}b)_0 \Vdash \forall z \in f\, \exists x \in \dot{F}_\sigma\, \exists y \in \dot{F}_\tau\, (z = \langle x, y\rangle), \tag{3}$$

$$(\mathbf{e}a)_{10} = (\mathbf{e}b)_{10} \Vdash \forall x \in \dot{F}_\sigma\, \exists y \in \dot{F}_\tau\, \exists z \in f\, (z = \langle x, y\rangle \wedge \varphi(x, y)), \tag{4}$$

$$(\mathbf{e}a)_{11} = (\mathbf{e}b)_{11} \Vdash \forall z_0 \in f\, \forall z_1 \in f\, \forall x, y_0, y_1\, (z_0 = \langle x, y_0\rangle \wedge z_1 = \langle x, y_1\rangle \to y_0 = y_1). \tag{5}$$

First, note that $\lambda c.(ac)_0 =_{\sigma\tau} \lambda d.(bd)_0$. This follows from (1). In fact, $c =_\sigma d$ implies $(ac)_0 =_\tau (bd)_0$, for all $c, d \in A$. Moreover, since this is an equivalence relation, we have $\lambda c.(ac)_0 \in A_{\sigma\tau}$.

For (3), let $\mathbf{e}$ be such that

$$((\mathbf{e}a)_0 c)_0 \simeq c, \qquad ((\mathbf{e}a)_0 c)_{10} \simeq (ac)_0, \qquad ((\mathbf{e}a)_0 c)_{11} \simeq \mathbf{v},$$

where $\mathbf{v} \Vdash \langle x, y\rangle_A = \langle x, y\rangle$ for all $x, y \in \mathrm{V_{ex}}(A)$ as in Lemma 8.2. Let us show that any such $\mathbf{e}$ satisfies (3). Let $\langle c, d, \langle c^\sigma, e^\tau\rangle_A\rangle \in f$, where $e \simeq (ac)_0$. We would like

$$(\mathbf{e}a)_0 c = (\mathbf{e}b)_0 d \Vdash \exists x \in \dot{F}_\sigma\, \exists y \in \dot{F}_\tau\, (\langle c^\sigma, e^\tau\rangle_A = \langle x, y\rangle).$$

Now, $\langle c, d, c^\sigma\rangle \in \dot{F}_\sigma$, $c \simeq ((\mathbf{e}a)_0 c)_0$, and $d \simeq ((\mathbf{e}b)_0 d)_0$. Therefore, we just need to verify

$$((\mathbf{e}a)_0 c)_1 = ((\mathbf{e}b)_0 d)_1 \Vdash \exists y \in \dot{F}_\tau\, \langle c^\sigma, e^\tau\rangle_A = \langle c^\sigma, y\rangle.$$

Similarly, $\langle (ac)_0, (bd)_0, e^\sigma\rangle \in \dot{F}_\tau$ since, as noted before, $(ac)_0 =_\tau (bd)_0$. On the other hand, $(ac)_0 \simeq ((\mathbf{e}a)_0 c)_{10}$ and $(bd)_0 \simeq ((\mathbf{e}b)_0 d)_{10}$. So we just need to show that

$$((\mathbf{e}a)_0 c)_{11} = ((\mathbf{e}b)_0 d)_{11} \Vdash \langle c^\sigma, e^\tau\rangle_A = \langle c^\sigma, e^\tau\rangle.$$

Now, $((\mathbf{e}a)_0 c)_{11} \simeq ((\mathbf{e}b)_0 d)_{11} \simeq \mathbf{v}$, and $\mathbf{v} \Vdash \langle c^\sigma, e^\tau\rangle_A = \langle c^\sigma, e^\tau\rangle$. So we are done.

As for (4), Let $\mathbf{e}$ be such that

$$((\mathbf{e}a)_{10} c)_0 \simeq (ac)_0, \qquad ((\mathbf{e}a)_{10} c)_{10} \simeq (ac)_0, \qquad ((\mathbf{e}a)_{10} c)_{110} \simeq \mathbf{v}, \qquad ((\mathbf{e}a)_{10} c)_{111} \simeq (ac)_1,$$

where $\mathbf{v}$ is as in part (3). That $\mathbf{e}$ satisfies (4) is proved in similar fashion by using (1) and (2).

For (5), suppose $\langle c_i, d_i, z_i\rangle \in f$ with $z_i = \langle {c_i}^\sigma, {e_i}^\tau\rangle_A$ and $e_i \simeq (ac_i)_0$, where $i = 0, 1$. We are looking for an $\mathbf{e}$ such that

$$(\mathbf{e}a)_{11} c_0 c_1 = (\mathbf{e}b)_{11} d_0 d_1 \Vdash z_0 = \langle x, y_0\rangle \wedge z_1 = \langle x, y_1\rangle \to y_0 = y_1,$$

for all $x, y_0, y_1 \in \mathrm{V_{ex}}(A)$. Suppose

$$g = h \Vdash z_0 = \langle x, y_0 \rangle \wedge z_1 = \langle x, y_1 \rangle. \tag{6}$$

We want $(\mathbf{e}a)_{11} c_0 c_1 g = (\mathbf{e}b)_{11} d_0 d_1 h \Vdash y_0 = y_1$. Unravelling (6), we get

$$g_i = h_i \Vdash \langle {c_i}^{\sigma}, {e_i}^{\tau} \rangle_A = \langle x, y_i \rangle.$$

By Lemma 8.2,

$$\mathbf{w} g_i = \mathbf{w} h_i \Vdash {c_i}^{\sigma} = x \wedge {e_i}^{\tau} = y_i,$$

for some closed application term $\mathbf{w}$. By the realizabilty of equality, it follows that

$$\Vdash {c_0}^{\sigma} = {c_1}^{\sigma}. \tag{7}$$

Also,

$$\mathbf{p}(\mathbf{w} g_0)_1 (\mathbf{w} g_1)_1 = \mathbf{p}(\mathbf{w} h_0)_1 (\mathbf{w} h_1)_1 \Vdash {e_0}^{\tau} = y_0 \wedge {e_1}^{\tau} = y_1.$$

By absoluteness, (7) implies $c_0 =_{\sigma} c_1$. As $\lambda c.(ac)_0 \in A_{\sigma\tau}$, we have $(ac_0)_0 =_{\tau} (ac_1)_0$, that is, $e_0 =_{\tau} e_1$. By uniqueness, ${e_0}^{\tau} = {e_1}^{\tau}$. By realizability of equality, there is a closed application term $\mathbf{i}$ such that

$$\mathbf{i} \Vdash z = y_0 \wedge z = y_1 \to y_0 = y_1.$$

Therefore $\mathbf{e}$ can be chosen such that

$$(\mathbf{e}a)_{11} c_0 c_1 g \simeq \mathbf{i}(\mathbf{p}(\mathbf{w} g_0)_1 (\mathbf{w} g_1)_1)$$

is as required.

By λ-abstraction, one can find $\mathbf{e}$ satisfying (3), (4), and (5). □

Theorem 8.9 (Arrow types)**.** *There exists a closed application term* $\mathbf{e}$ *such that* CZF *proves*

$$\mathbf{e} \Vdash \dot{F}_{\sigma\tau} = \dot{F}_{\sigma} \to \dot{F}_{\tau},$$

for all finite types σ *and* τ*.*

Proof. We look for $\mathbf{e}$ such that

$$\mathbf{e}_0 \Vdash \forall f \in \dot{F}_{\sigma\tau} \, (f \colon \dot{F}_{\sigma} \to \dot{F}_{\tau}),$$

and for every $f \in \mathrm{V_{ex}}(A)$,

$$\mathbf{e}_1 \Vdash (f \colon \dot{F}_{\sigma} \to \dot{F}_{\tau}) \to f \in \dot{F}_{\sigma\tau}.$$

For $\mathbf{e}_0$, we need that for all $a =_{\sigma\tau} b$,

$$(\mathbf{e}_0 a)_0 = (\mathbf{e}_0 b)_0 \Vdash \forall z \in a^{\sigma\tau} \, \exists x \in \dot{F}_{\sigma} \, \exists y \in \dot{F}_{\tau} \, (z = \langle x, y \rangle), \tag{1}$$

$$(\mathbf{e}_0 a)_{10} = (\mathbf{e}_0 b)_{10} \Vdash \forall x \in \dot{F}_{\sigma} \, \exists y \in \dot{F}_{\tau} \, \exists z \in a^{\sigma\tau} \, (z = \langle x, y \rangle), \tag{2}$$

$$(\mathbf{e}_0 a)_{11} = (\mathbf{e}_0 b)_{11} \Vdash \forall z_0 \in a^{\sigma\tau}\, \forall z_1 \in a^{\sigma\tau}\, \forall x, y_0, y_1\, (z_0 = \langle x, y_0\rangle \wedge z_1 = \langle x, y_1\rangle \to y_0 = y_1). \tag{3}$$

For (1), let $\mathbf{e}_0$ be such that

$$(\mathbf{e}_0 a)_0 \simeq \lambda c.\mathbf{p}c(\mathbf{p}(ac)\mathbf{v}),$$

where $\mathbf{v} \Vdash \langle x, y\rangle_A = \langle x, y\rangle$ for all $x, y \in \mathrm{V}_{\mathrm{ex}}(A)$ as in Lemma 8.2.

Let us verify that $\mathbf{e}_0$ does the job. Let $a =_{\sigma\tau} b$. We want to show

$$\lambda c.\mathbf{p}c(\mathbf{p}(ac)\mathbf{v}) = \lambda d.\mathbf{p}d(\mathbf{p}(bd)\mathbf{v}) \Vdash \forall z \in a^{\sigma\tau}\, \exists x \in \dot{F}_\sigma\, \exists y \in \dot{F}_\tau\, (z = \langle x, y\rangle).$$

Let $\langle c, d, \langle c^\sigma, c^\tau\rangle_A\rangle \in a^{\sigma\tau}$, where $c =_\sigma d$ and $ac \simeq e$. We want

$$\mathbf{p}c(\mathbf{p}(ac)\mathbf{v}) = \mathbf{p}d(\mathbf{p}(bd)\mathbf{v}) \Vdash \exists x \in \dot{F}_\sigma\, \exists y \in \dot{F}_\tau\, (\langle c^\sigma, c^\tau\rangle_A = \langle x, y\rangle).$$

By definition, $\langle c, d, c^\sigma\rangle \in \dot{F}_\sigma$. Let us check that

$$\mathbf{p}(ac)\mathbf{v} = \mathbf{p}(bd)\mathbf{v} \Vdash \exists y \in \dot{F}_\tau\, (\langle c^\sigma, c^\tau\rangle_A = \langle c^\sigma, y\rangle).$$

We have $ac =_\tau bd$ and hence $\langle ac, bd, c^\tau\rangle \in \dot{F}_\tau$. Finally,

$$\mathbf{v} \Vdash \langle c^\sigma, c^\tau\rangle_A = \langle c^\sigma, c^\tau\rangle.$$

For (2), let $\mathbf{e}_0$ be such that

$$(\mathbf{e}_0 a)_{10} \simeq \lambda x.\mathbf{p}(ax)(\mathbf{p}x\mathbf{v}),$$

where $\mathbf{v}$ is as above.

For (3), let $\mathbf{e}_0$ be such that

$$(\mathbf{e}_0 a)_{11} c_0 c_1 g \simeq \mathbf{i}(\mathbf{p}(\mathbf{w}g_0)_1(\mathbf{w}g_1)_1),$$

where $\mathbf{w}$ and $\mathbf{i}$ are as in the proof of Theorem 8.8.

As for $\mathbf{e}_1$, suppose that $f \in \mathrm{V}_{\mathrm{ex}}(A)$ and

$$a = b \Vdash f\colon \dot{F}_\sigma \to \dot{F}_\tau.$$

Then

$$a_0 = b_0 \Vdash \forall z \in f\, \exists x \in \dot{F}_\sigma\, \exists y \in \dot{F}_\tau\, (z = \langle x, y\rangle), \tag{4}$$

$$a_{10} = b_{10} \Vdash \forall x \in \dot{F}_\sigma\, \exists y \in \dot{F}_\tau\, \exists z \in f\, (z = \langle x, y\rangle), \tag{5}$$

$$a_{11} = b_{11} \Vdash \forall z_0 \in f\, \forall z_1 \in f\, \forall x, y_0, y_1\, (z_0 = \langle x, y_0\rangle \wedge z_1 = \langle x, y_1\rangle \to y_0 = y_1). \tag{6}$$

We aim for

$$\mathbf{e}_1 a = \mathbf{e}_1 b \Vdash f \in \dot{F}_{\sigma\tau}.$$

As in the proof of Theorem 8.8, it follows from (5) that $\lambda c.(a_{10}c)_0 =_{\sigma\tau} \lambda d.(b_{10}d)_0$. Therefore

$$\langle \lambda c.(a_{10}c)_0, \lambda d.(b_{10}d)_0, g^{\sigma\tau}\rangle \in \dot{F}_{\sigma\tau},$$

where $g := \lambda c.(a_{10}c)_0$. We thus want $\mathbf{e}_1$ such that

$$(\mathbf{e}_1 a)_0 \simeq \lambda c.(a_{10}c)_0,$$

$$(\mathbf{e}_1 a)_1 = (\mathbf{e}_1 b)_1 \Vdash f = g^{\sigma\tau}.$$

By definition and Lemma 8.7,

$$g^{\sigma\tau} = \{\langle c, d, \langle c^\sigma, c^\tau\rangle_A\rangle \colon c =_\sigma d \wedge (a_{10}c)_0 =_\tau e\}.$$

($\subseteq$) Let $\langle \tilde{c}, \tilde{d}, z\rangle \in f$. We aim for $((\mathbf{e}_1 a)_1\tilde{c})_0 = ((\mathbf{e}_1 b)_1\tilde{d})_0 \Vdash z \in g^{\sigma\tau}$. By (4), $(a_0\tilde{c})_0 =_\sigma (b_0\tilde{d})_0$ and

$$(a_0\tilde{c})_{11} = (b_0\tilde{d})_{11} \Vdash z = \langle c^\sigma, c^\tau\rangle,$$

where $c \simeq (a_0\tilde{c})_0$ and $e \simeq (a_0\tilde{c})_{10}$. By Lemma 8.2, let $\mathbf{z}$ be a closed application term such that for all $x, y, z \in \mathrm{V}_{\mathrm{ex}}(A)$,

$$\mathbf{z} \Vdash z = \langle x, y\rangle \to z = \langle x, y\rangle_A.$$

Then

$$\mathbf{z}(a_0\tilde{c})_{11} = \mathbf{z}(b_0\tilde{d})_{11} \Vdash z = \langle c^\sigma, c^\tau\rangle_A.$$

By using (5), (6) and absoluteness, one obtains $(a_{10}c)_0 =_\tau e$. Let $\mathbf{e}_1$ satisfy

$$((\mathbf{e}_1 a)_1\tilde{c})_{00} \simeq (a_0\tilde{c})_0,$$

$$((\mathbf{e}_1 a)_1\tilde{c})_{01} \simeq \mathbf{z}(a_0\tilde{c})_{11}.$$

Then $\mathbf{e}_1$ is as desired.

($\supseteq$) Let $\langle c, d, \langle c^\sigma, c^\tau\rangle_A\rangle \in g^{\sigma\tau}$, with $e \simeq (a_{10}c)_0$. We aim for $((\mathbf{e}_1 a)_1 c)_1 = ((\mathbf{e}_1 b)_1 d)_1 \Vdash \langle c^\sigma, c^\tau\rangle_A \in f$.

By unravelling (5), we obtain that for some $z \in \mathrm{V}_{\mathrm{ex}}(A)$,

$$\langle (a_{10}c)_{10}, (b_{10}d)_{10}, z\rangle \in f,$$

$$(a_{10}c)_{11} = (b_{10}d)_{11} \Vdash z = \langle c^\sigma, c^\tau\rangle.$$

Let $\mathbf{e}_1$ be such that

$$((\mathbf{e}_1 a)_1 c)_1 \simeq \mathbf{p}(a_{10}c)_{10}(\mathbf{i_s}(\mathbf{z}(a_{10}c)_{11})),$$

where $\mathbf{z}$ is as above.

By λ-abstraction, one can find $\mathbf{e}$ satisfying the above equations. □

Theorem 8.10. *For all finite types σ and τ there exists a closed application term* $\mathbf{c}$ *such that* CZF *proves*

$$\mathbf{c} \Vdash \forall x^{\sigma}\, \exists y^{\tau}\, \varphi(x, y) \to \exists f^{\sigma\tau}\, \forall x^{\sigma}\, \varphi(x, f(x)).$$

Proof. A proof is obtained by combining Theorem 8.8 and Theorem 8.9. Let

$$\vartheta_0(z) := \text{`}z \text{ is the set of natural numbers'},$$

$$\vartheta_{\sigma\tau}(z) := \exists x\, \exists y\, (\vartheta_\sigma(x) \wedge \vartheta_\tau(y) \wedge z = x \to y).$$

We are claiming that for all finite types σ and τ there exists a closed application term $\mathbf{c}_{\sigma\tau}$ such that CZF proves

$$\mathbf{c}_{\sigma\tau} \Vdash \forall z_\sigma\, \forall z_\tau\, (\vartheta_\sigma(z_\sigma) \wedge \vartheta_\tau(z_\tau) \to \psi(z_\sigma, z_\tau)),$$

where $\psi(z_\sigma, z_\tau)$ is

$$\forall x \in z_\sigma\, \exists y \in z_\tau\, \varphi(x, y) \to \exists f \colon z_\sigma \to z_\tau\, \forall x \in z_\sigma\, \varphi(x, f(x)).$$

Let $\mathbf{e}_0$ be such that $\mathbf{e}_0 \Vdash \vartheta_0(\dot{\omega})$. By using $\mathbf{e}_0$ and Theorem 8.9, for every finite type σ, we can find $\mathbf{e}_\sigma$ such that $\mathbf{e}_\sigma \Vdash \vartheta_\sigma(\dot{F}_\sigma)$. As $\mathsf{CZF} \vdash \vartheta_\sigma(z_0) \wedge \vartheta_\sigma(z_1) \to z_0 = z_1$, by soundness (Theorem 7.2) there is a $\mathbf{u}_\sigma$ such that

$$\mathbf{u}_\sigma \Vdash \vartheta_\sigma(z_0) \wedge \vartheta_\sigma(z_1) \to z_0 = z_1$$

for all $z_0, z_1 \in \mathrm{V}_{\mathrm{ex}}(A)$. By soundness as well, there are $\mathbf{i}_{\sigma\tau}$ and $\mathbf{j}_{\sigma\tau}$ such that

$$\mathbf{i}_{\sigma\tau} \Vdash \psi(\dot{F}_\sigma, \dot{F}_\tau) \wedge z_\sigma = \dot{F}_\sigma \to \psi(z_\sigma, \dot{F}_\tau),$$
$$\mathbf{j}_{\sigma\tau} \Vdash \psi(z_\sigma, \dot{F}_\tau) \wedge z_\tau = \dot{F}_\tau \to \psi(z_\sigma, z_\tau),$$

for all $z_\sigma, z_\tau \in \mathrm{V}_{\mathrm{ex}}(A)$. Finally, with the aid of $\mathbf{e}_\sigma$, $\mathbf{e}_\tau$, $\mathbf{u}_\sigma$, $\mathbf{u}_\tau$, $\mathbf{i}_{\sigma\tau}$, $\mathbf{j}_{\sigma\tau}$, and of the closed application term $\mathbf{e}$ from Theorem 8.8, one can construct $\mathbf{c}_{\sigma\tau}$ as desired. □

Corollary 8.11. *For every theorem φ of* $\mathsf{CZF} + \mathsf{AC}_{\mathsf{FT}}$*, there is a closed application term* $\mathbf{e}$ *such that* CZF *proves* $\mathbf{e} \Vdash \varphi$. *In particular,* $\mathsf{CZF} + \mathsf{AC}_{\mathsf{FT}}$ *is consistent relative to* CZF.

Proof. By Theorem 7.2 and Theorem 8.10. □

Corollary 8.12. $\mathsf{CZF} + \mathsf{AC}_{\mathsf{FT}}$ *is conservative over* CZF *with respect to Π^0_2 sentences.*

Proof. Let $\varphi(x, y)$ be a bounded formula with displayed free variables and suppose that

$$\forall x \in \omega\, \exists y \in \omega\, \varphi(x, y)^{7}$$

[7]Of course we mean that, e.g., $\forall z\, (\vartheta_0(z) \to \forall x \in z\, \exists y \in z\, \varphi(x, y)))$ is provable, where $\vartheta_0(z)$ is a formula defining ω.

is provable in CZF plus $\mathsf{AC_{FT}}$. By the corollary above, we can find a closed application term $\mathbf{e}$ such that

$$\mathsf{CZF} \vdash \mathbf{e} \Vdash \forall x \in \dot{\omega}\, \exists y \in \dot{\omega}\, \varphi(x, y).$$

In particular,

$$\mathsf{CZF} \vdash \forall n \in \omega\, \exists m \in \omega\, (e\bar{n})_1 \Vdash \varphi(\dot{n}, \dot{m}).$$

It is a routine matter (cf. also [19, Ch. 4, Theorem 2.6]) to show that realizability equals truth for bounded arithmetic formulas, namely,

$$\mathsf{CZF} \vdash \forall n_1, \ldots, n_k \in \omega\, (\psi(n_1, \ldots, n_k) \leftrightarrow \exists a, b \in A\, (a = b \Vdash \psi(\dot{n}_1, \ldots, \dot{n}_k))),$$

for $\psi(x_1, \ldots, x_k)$ bounded with all the free variables shown. We can then conclude

$$\mathsf{CZF} \vdash \forall x \in \omega\, \exists y \in \omega\, \varphi(x, y).$$

□

9. Soundness for IZF

The theory IZF (Intuitionistic Zermelo-Fraenkel set theory) shares the logic and language of CZF. Its axioms are

1. **Extensionality**,
2. **Pairing**,
3. **Union**,
4. **Infinity**,
5. **Set Induction**,
6. **Separation**: $\forall x\, \exists y\, \forall z\, (z \in y \leftrightarrow z \in x \wedge \varphi(z))$, for all formulae φ,
7. **Collection**: $\forall u \in x\, \exists v\, \varphi(u, v) \to \exists y\, \forall u \in x\, \exists v \in y\, \varphi(u, v)$, for all formulae φ,
8. **Powerset**: $\forall x\, \exists y\, \forall z\, (\forall u \in z\, (u \in x) \to z \in y)$.

Thus IZF is a strengthening of CZF with Bounded Separation replaced by full Separation and Subset Collection replaced by Powerset. Note that Powerset implies Subset Collection and Strong Collection follows from Separation and Collection.

Note that in IZF, due to the presence of Powerset, the construction of $\mathrm{V_{ex}}(A)$ can proceed by transfinite recursion along the ordinals (cf. [19]).

Theorem 9.1. *For every theorem φ of $\mathsf{IZF} + \mathsf{AC_{FT}}$, there is a closed application term $\mathbf{e}$ such that IZF proves $\mathbf{e} \Vdash \varphi$. In particular, $\mathsf{IZF} + \mathsf{AC_{FT}}$ is consistent relative to IZF.*

Proof. The soundness for theorems of intuitionistic first order logic with equality follows immediately from Theorem 6.4. As for nonlogical axioms, in view of Corollary 8.11, it is sufficient to deal with **Separation** and **Powerset**.

The argument for **Separation** is similar to the corresponding argument for Bounded Separation in the proof of Theorem 7.2, employing full Separation in the background theory.

It thus remains to address **Powerset**. Write $z \subseteq x$ for $\forall u \in z\, (u \in x)$. We look for $\mathbf{e}$ such that for all $x \in \mathrm{V_{ex}}(A)$ there is a $y \in \mathrm{V_{ex}}(A)$ such that

$$\mathbf{e} \Vdash z \subseteq x \to z \in y,$$

for all $z \in \mathrm{V_{ex}}(A)$.

On account of **Powerset**, in IZF we can define sets $\mathrm{V_{ex}}(A)_\alpha$, with α ordinal (i.e., a transitive set of transitive sets), such that $\mathrm{V_{ex}}(A) = \bigcup_\alpha \mathrm{V_{ex}}(A)_\alpha$ and $\mathrm{V_{ex}}(A)_\alpha = \bigcup_{\beta\in\alpha} \mathcal{P}(A \times A \times \mathrm{V_{ex}}(A)_\beta)$. Note that in CZF the $\mathrm{V_{ex}}(A)_\alpha$'s are just classes.

Given $x \in \mathrm{V_{ex}}(A)_\alpha$, let

$$y = \{\langle a, b, z\rangle \in A \times A \times \mathrm{V_{ex}}(A)_\alpha \mid a = b \Vdash z \subseteq x\}.$$

The set y exists by Separation. Set

$$\mathbf{e} := \lambda a.\mathbf{p}a\mathbf{i_r}.$$

It is easy to check that y and $\mathbf{e}$ are as desired, once established that if $z \in \mathrm{V_{ex}}(A)$ and $a = b \Vdash z \subseteq x$ then $z \in \mathrm{V_{ex}}(A)_\alpha$. This is proved by **Set Induction** by showing that for all $u, v \in \mathrm{V_{ex}}(A)$:

- if $a = b \Vdash u \in v$ and $v \in \mathrm{V_{ex}}(A)_\alpha$, then $u \in \mathrm{V_{ex}}(A)_\beta$ for some $\beta \in \alpha$;
- if $a = b \Vdash u = v$ and $v \in \mathrm{V_{ex}}(A)_\alpha$, then $u \in \mathrm{V_{ex}}(A)_\alpha$.

□

As before, we obtain the following.

Corollary 9.2. $\mathsf{IZF} + \mathsf{AC_{FT}}$ *is conservative over* IZF *with respect to* Π^0_2 *sentences.*

10. Conclusions

We defined an extensional notion of realizability that validates CZF along with all finite type axiom of choice $\mathsf{AC_{FT}}$ provably in CZF. We have shown that one can replace CZF with IZF. Presumably, this holds true for many other intuitionistic set theories as well.

There is a sizable number of well-known *extra principles* P that can be added to the mix, in the sense that $T + P$ proves $\mathbf{e} \Vdash P$, for some closed application term $\mathbf{e}$, where T is either CZF or IZF. This applies to arbitrary pca's in the case of large set axioms such as REA (Regular Extension axiom) by adapting [25, Theorem 6.2]. In the case of choice principles, this also applies to arbitrary pca's for Countable Choice, DC (Dependent Choice), RDC (Relativized Dependent Choice), and PAx (Presentation

Axiom) by adapting the techniques of [8]. Specializing to the case of the first Kleene algebra, one obtains extensional realizability of MP (Markov Principle) and forms of IP (Independence of Premise) adapting results from [19, Section 11], [20] , [25, Section 7].

We claim that realizability combined with truth and the appropriate partial combinatory algebra modeled on [23, 26] yields the closure under the choice rule for finite types, i.e.,

$$\text{If } T \vdash \forall x^\sigma \, \exists y^\tau \, \varphi(x, y), \text{ then } T \vdash \exists f^{\sigma\tau} \, \forall x^\sigma \, \varphi(x, f(x))$$

for large swathes of intuitionistic set theories.

Church's thesis,

$$\forall f \colon \omega \to \omega \, \exists e \in \omega \, \forall x \in \omega \, (f(x) \simeq \{e\}(x)), \tag{CT}$$

and the finite type axiom of choice are incompatible in extensional finite type arithmetic [31] (cf. [5, Ch. 5, Theorem 6.1]).[8] A fortiori, they are incompatible on the basis of CZF, and thus of IZF. However, negative versions of Church's thesis can still obtain in a universe in which AC_{FT} holds. The assertion that no function from ω to ω is incomputable, is known as weak Church's thesis [30]:

$$\forall f \colon \omega \to \omega \, \neg\neg\exists e \in \omega \, \forall x \in \omega \, (f(x) \simeq \{e\}(x)), \tag{WCT}$$

where $\{e\}(x)$ is Turing machine application. Using Kleene's first algebra, one can easily verify that WCT is extensionally realizable in CZF. Therefore, CZF augmented with both $\mathsf{AC}_{\mathsf{FT}}$ and WCT is consistent relative to CZF, and similarly for IZF.

Continuity principles are a hallmark of Brouwer's intuitionism. They are compatible with finite type arithmetic (see [5, 30, 31, 34]) and also with set theory (see [5, 19, 23, 22]). They are known, though, to invite conflict with $\mathsf{AC}_{\mathsf{FT}}$ (see [29, Theorem 9.6.11]). However, as in the case of CT, negative versions of them are likely to be compatible with $\mathsf{AC}_{\mathsf{FT}}$ on the basis of CZF and IZF. Similar to the case of CT, one would expect that the assertion that no function from $\mathbb{R}$ to $\mathbb{R}$ is discontinuous can go together with $\mathsf{AC}_{\mathsf{FT}}$. One obvious tool that suggests itself here is extensional generic realizability based on Kleene's second algebra. We shall not venture into this here and add the verification of this claim to the task list.

We conclude with the following remark. It is currently unknown whether one can provide a realizability model for choice principles based on larger type structures. Say that I is a base if for every I-indexed family $(X_i)_{i \in I}$ of inhabited sets X_i there exists a function $f \colon I \to \bigcup_{i \in I} X_i$ such that $f(i) \in X_i$ for every $i \in I$. Let $\mathcal{C}$-AC say that every set I in the class $\mathcal{C}$ is a base. The question is whether one can realize $\mathcal{C}$-AC, where $\mathcal{C}$ is

[8] The elementary recursion-theoretic reason that prevents Church's thesis from being extensionally realizable is the usual one: there is no type 2 extensional index in Kleene's first algebra, that is, there is no $e \in \omega$ such that, for all $a, b \in \omega$, if $\{a\}(n) = \{b\}(n)$ for every $n \in \omega$, i.e., $a =_1 b$, then $\{e\}(a) = \{e\}(b)$.

the smallest $\Pi\Sigma$-closed class, or even the smallest $\Pi\Sigma W$-closed class, without assuming choice in the background theory.

References

[1] Peter Aczel. The type theoretic interpretation of constructive set theory: inductive definitions. In R.B. Marcus et al., editor, *Logic, Methodology and Philosophy of Science VII*, pages 17–49. Elsevier, 1986. 7

[2] Peter Aczel and Michael Rathjen. *Notes on constructive set theory*. Technical Report 40, Institut Mittag-Leffler, 2001. 7

[3] Peter Aczel and Michael Rathjen. Notes on constructive set theory. Available at http://www1.maths.leeds.ac.uk/~rathjen/book.pdf, 2010. 7

[4] Michael J. Beeson. Continuity in intuitionistic set theories. In *Studies in Logic and the Foundations of Mathematics*, volume 97, pages 1–52. Elsevier, 1979. 2

[5] Michael J. Beeson. *Foundations of constructive mathematics*, volume 6 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1985. 2, 3, 4, 5, 6, 25

[6] Haskell Brooks Curry. An analysis of logical substitution. *American Journal of Mathematics*, 51:509–536, 789–834, 1929. 3

[7] Haskell Brooks Curry. Grundlagen der kombinatorischen Logik. *American Journal of Mathematics*, 51:363–384, 1930. 3, 4

[8] Eman Dihoum and Michael Rathjen. Preservation of choice principles under realizability. *Logic Journal of the IGPL*, 27(5):746–765, 02 2019. 3, 25

[9] Solomon Feferman. A language and axioms for explicit mathematics. In *Algebra and logic*, pages 87–139. Springer, 1975. 2, 3, 4

[10] Solomon Feferman. Recursion theory and set theory: a marriage of convenience. In *Generalized Recursion Theory II*, Stud. Logic Found. Math., pages 55–98. North-Holland, Amsterdam, 1978. 3

[11] Solomon Feferman. Constructive theories of functions and classes. In *Logic Colloquium '78*, Stud. Logic Found. Math., pages 159–224. North-Holland, Amsterdam, 1979. 3, 4, 5

[12] H. Friedman and A. Ščedrov. Large sets in intuitionistic set theory. *Annals of Pure and Applied Logic*, 27:1–24, 1984. 2

[13] Harvey Friedman. The consistency of classical set theory relative to a set theory with intuitionistic logic. *Journal of Symbolic Logic*, 38:315–319, 1973. 2

[14] Harvey Friedman. Some applications of Kleene's methods for intuitionistic systems. In *Cambridge summer school in mathematical logic*, pages 113–170. Springer, 1973. 2

[15] Emanuele Frittaion. On Goodman realizability. *Notre Dame J. Formal Logic*, 60(3):523–550, 08 2019. 3

[16] Lew Gordeev. Proof-theoretical analysis of weak systems of functions and classes. *Annals of Pure and Applied Logic*, 38:1–121, 1988. 2, 3

[17] R.J. Grayson. Note on extensional realizability, 1981. *Handwritten notes from Münster University.* 3

[18] G. Kreisel and A.S. Troelstra. Formal systems for some branches of intuitionistic analysis. *Annals of Mathematical Logic*, 1:229–387, 1970. 2

[19] David Charles McCarty. *Realizability and recursive mathematics.* Thesis (Ph.D.)–The University of Edinburgh, 1985. 2, 3, 8, 10, 16, 23, 25

[20] David Charles McCarty. Realizability and recursive set theory. *Ann. Pure Appl. Logic*, 32(2):153–183, 1986. 2, 3, 25

[21] Andrew M. Pitts. *The theory of triposes*. Thesis (Ph.D.)–University of Cambridge, 1981. 3

[22] Michael Rathjen. Constructive set theory and Brouwerian principles. *J.UCS*, 11(12):2008–2033, 2005. 3, 5, 25

[23] Michael Rathjen. The disjunction and related properties for constructive Zermelo-Fraenkel set theory. *J. Symbolic Logic*, 70(4):1232–1254, 2005. 3, 25

[24] Michael Rathjen. The formulae-as-classes interpretation of constructive set theory. In *Proof Technology and Computation*, pages 279–322. IOS Press, Amsterdam, 2006. 2

[25] Michael Rathjen. Realizability for constructive Zermelo-Fraenkel set theory. In *Logic Colloquium '03*, volume 24 of *Lect. Notes Log.*, pages 282–314. Assoc. Symbol. Logic, La Jolla, CA, 2006. 3, 7, 8, 10, 11, 24, 25

[26] Michael Rathjen. Metamathematical properties of intuitionistic set theories with choice principles. In *New computational paradigms*, pages 287–312. Springer, New York, 2008. 3, 25

[27] Moses Schönfinkel. Über die Bausteine der mathematischen Logik. *Mathematische Annalen*, 92:305–316, 1924. 3, 4

[28] Andrew W. Swan. CZF does not have the existence property. *Ann. Pure Appl. Logic*, 165(5):1115–1147, 2014. 3

[29] Anne Troelstra and Dirk van Dalen. *Constructivism in Mathematics, volume II*, volume 123 of *Studies in Logic and the Foundations of Mathematics*. Elsevier B. V., Amsterdam, 1988. 3, 25

[30] A.S. Troelstra. *Metamathematical investigation of intuitionistic arithmetic and analysis*. Lecture Notes in Mathematics, Vol. 344. Springer-Verlag, Berlin, 1973. 25

[31] A.S. Troelstra. A note on non-extensional operations in connection with continuity and recursiveness. *Indagationes Mathematicae (Proceedings)*, 80(5):455 – 462, 1977. 25

[32] A.S. Troelstra. Realizability. In *Handbook of proof theory*, volume 137 of *Stud. Logic Found. Math.*, pages 407–473. North-Holland, Amsterdam, 1998. 3

[33] Benno van den Berg and Lotte van Slooten. Arithmetical conservation results. *Indag. Math. (N.S.)*, 29(1):260–275, 2018. 3

[34] Jaap van Oosten. Extensional realizability. *Annals of Pure and Applied Logic*, 84(3):317 – 349, 1997. 3, 25

[35] Jaap van Oosten. *Realizability: an introduction to its categorical side*, volume 152 of *Studies in Logic and the Foundations of Mathematics*. Elsevier B. V., Amsterdam, 2008. 3, 4

School of Mathematics, University of Leeds, UK

School of Mathematics, University of Leeds, UK