Article:

Frittaion, E. orcid.org/0000-0003-4965-9271, Nemoto, T. orcid.org/0000-0003-3898-6189 and Rathjen, M. orcid.org/0000-0003-1699-4778 (Cover date: October–November 2023) Choice and independence of premise rules in intuitionistic set theory. Annals of Pure and Applied Logic, 174 (9). 103314. ISSN 0168-0072

https://doi.org/10.1016/j.apal.2023.103314

CHOICE AND INDEPENDENCE OF PREMISE RULES IN INTUITIONISTIC SET THEORY

EMANUELE FRITTAION, TAKAKO NEMOTO, AND MICHAEL RATHJEN

Abstract. Choice and independence of premise principles play an important role in characterizing Kreisel's modified realizability and Gödel's Dialectica interpretation. In this paper we show that a great many intuitionistic set theories are closed under the corresponding rules for finite types over $\mathbb{N}$. It is also shown that the existence property (or existential definability property) holds for statements of the form $\exists y^\sigma\, \varphi(y)$, where the variable y ranges over objects of finite type σ. This applies in particular to CZF (Constructive Zermelo-Fraenkel set theory) and IZF (Intuitionistic Zermelo-Fraenkel set theory), two systems known not to have the general existence property. On the technical side, the paper uses a method that amalgamates generic realizability for set theory with truth, whereby the underlying partial combinatory algebra is required to *contain* all objects of finite type.

1. Introduction

There are (at least) three types of classically valid principles that figure prominently in constructive mathematics: $\mathsf{AC}_{\mathrm{FT}}$ (*Choice in Finite Types*), MP (*Markov's principle*) and IP (*Independence of Premise principle*). All three are required for a characterization of Gödel's Dialectica interpretation (see [41, 3.5.10], [16, Proposition 8.13]), whereas Kreisel's modified realizability for intuitionistic finite type arithmetic HA^ω is axiomatized by $\mathsf{AC}_{\mathrm{FT}}$ and IP alone. To be more precise, let

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

$$\mathsf{IP}_\neg \qquad (\neg\psi \to \exists y^\sigma\, \varphi(y)) \to \exists y^\sigma\, (\neg\psi \to \varphi(y))$$

$$\mathsf{IP}_{\mathrm{ef}} \qquad (\psi_{\mathrm{ef}} \to \exists y^\sigma\, \varphi(y)) \to \exists y^\sigma\, (\psi_{\mathrm{ef}} \to \varphi(y))$$

where σ, τ signify finite types, z^ρ varies over objects of finite type ρ, and ψ_{ef} is assumed to be $\exists$-free, i.e., it neither contains existential quantifiers nor disjunctions.[1]

Then the following holds (see e.g. [41, 3.4.8], [43, Theorem 3.7], [16, Theorem 5.12]):

Theorem 1.1. *With $\Vdash_{mr}$ signifying modified realizability, we have:*

(i) $\mathsf{HA}^\omega + \mathsf{AC}_{\mathrm{FT}} + \mathsf{IP}_{\mathrm{ef}} \vdash \varphi \leftrightarrow \exists x\,(x \Vdash_{mr} \varphi)$.

2020 *Mathematics Subject Classification.* Primary: 03F03; Secondary: 03F25, 03F50, 03F55.

Emanuele Frittaion's research was supported by the Alexander von Humboldt Foundation.

Takako Nemoto's research was supported by the Japan Society for the Promotion of Science (JSPS), Core-to-Core Program (A. Advanced Research Networks).

Michael Rathjen's research was supported by the John Templeton Foundation (A new dawn of intuitionism: mathematical and philosophical advances, ID 60842).

[1] Of course, it is also assumed that y is not a free variable of $\neg\psi$ and ψ_{ef}.

Let $T \in \{\mathsf{HA}^\omega, \mathsf{E\text{-}HA}^\omega\}$.[2] *Then:*

(ii) $T + \mathsf{AC}_{\mathrm{FT}} + \mathsf{IP}_{\mathrm{ef}} \vdash \varphi$ *iff* $T \vdash (t \Vdash_{mr} \varphi)$ *for some term* t.

An important application of modified realizability (to be correct, its truth variant, aka modified realizability with truth) is that (i) T is closed under the rule of choice in finite types, (ii) T is closed under the independence of premise rule for negated formulas $\mathsf{IPR}_\neg$ (in particular, it is closed under $\mathsf{IPR}_{\mathrm{ef}}$), and (iii) T satisfies explicit definability. Short and sweet (see e.g. [43, Theorem 3.8], [16, Corollary 5.24]):

Theorem 1.2. *Let* $T \in \{\mathsf{HA}^\omega, \mathsf{E\text{-}HA}^\omega\}$. *Then:*

(i) *If* $T \vdash \forall x^\sigma \, \exists y^\tau \, \varphi(x, y)$, *then* $T \vdash \exists f^{\sigma\tau} \, \forall x^\sigma \, \varphi(x, fx)$.
(ii) *If* $T \vdash \neg\psi \to \exists y^\sigma \, \varphi(y)$, *then* $T \vdash \exists y^\sigma \, (\neg\psi \to \varphi(y))$;
(iii) *If* $T \vdash \exists y^\sigma \, \varphi(y)$, *then* $T \vdash \varphi(t)$, *for a suitable term* t.

The current paper shows that results similar to Theorem 1.2 hold for a great many set theories T, including CZF (Constructive Zermelo-Fraenkel set theory) and IZF (Intuitionistic Zermelo-Fraenkel set theory), even if augmented by suitable choice principles and large set axioms.[3] A more precise delineation of the kind of set theories eligible for this theorem is that T should be self-validating with respect to generic realizability combined with truth (cf. Theorem 4.11).

Theorem 1.3 (see Theorems 8.2, 8.5 and 8.7)**.** *An array of set theories* T *including* CZF *and* IZF *satisfy the following:*

(i) *If* $T \vdash \forall x^\sigma \, \exists y^\tau \, \varphi(x, y)$, *then* $T \vdash \exists f^{\sigma\tau} \, \forall x^\sigma \, \varphi(x, fx)$;
(ii) *If* $T \vdash \forall x \, (\neg\psi(x) \to \exists y^\sigma \, \varphi(x, y))$, *then* $T \vdash \exists y \, \forall x \, (\neg\psi(x) \to y \in \sigma \wedge \varphi(x, y))$;
(iii) *If* $T \vdash \forall x \, (\forall z \, \vartheta(x, z) \to \exists y^\sigma \, \varphi(x, y))$ *and* $T \vdash \forall z \, (\vartheta(x, z) \vee \neg\vartheta(x, z))$, *then* $T \vdash \exists y^\sigma \, \forall x \, (\forall z \, \vartheta(x, z) \to \varphi(x, y))$;
(iv) *If* $T \vdash \exists y^\sigma \, \varphi(y)$, *then* $T \vdash \exists! y^\sigma \, (\delta(y) \wedge \varphi(y))$, *for some formula* $\delta(y)$.

To properly shelve the perhaps perplexing results, i.e., from a classical viewpoint, it is good to bear in mind that our theorem applies to set theories T closed under the following rules:

(v) the *Unzerlegbarkeits rule*, namely, if $T \vdash \forall x \, (\varphi(x) \vee \psi(x))$, then $T \vdash \forall x \, \varphi(x)$ or $T \vdash \forall x \, \psi(x)$;
(vi) the *Uniformity rule*, namely, if $T \vdash \forall x \, \exists y \in \omega \, \varphi(x, y)$, then $T \vdash \exists y \in \omega \, \forall x \, \varphi(x, y)$

(see [34, Theorem 1.2] and [36, Theorem 7.4]).[4] A by-product of Theorem 1.3 (cf. Section 8.2) is that rule (vi) still holds when y ranges over objects of a given finite type.

It is known that IZF (see [27]) and CZF (see [34]) have the numerical existence property, so Theorem 1.3 part (iv) extends this property to a larger collection of existential formulas. On the other hand, it is known by work of Friedman and Ščedrov [7] that IZF does not have the general existence property EP while Swan [40] proved that EP also fails for CZF. In

[2]For a definition of HA^ω and its extensional variant $\mathsf{E\text{-}HA}^\omega$ cf. e.g. [41] or [16].
[3]The intuitionistic rendering of large cardinal axioms.
[4]Discussions of uniformity under realizability seem to appear first in the literature in Friedman's [6] and Troelstra's [42].

the latter case the culprit is CZF's Subset Collection axiom as shown by the third author [33] since the version of CZF with Exponentiation in lieu of Subset Collection has the EP.

On the technical side, the paper uses the method of generic realizability with truth from [34]. The main novelty of the paper, however, is the introduction of a special kind of partial combinatory algebra (pca) to the realizability framework. We single out the notion of a *reflexive pca over finite types* to deal specifically with objects of finite type. An instance of this new phenomenon, and its construction in weak set theories such as CZF, is duly supplied.

Generic realizability is better understood as a generalization of Kleene's 1945 realizability rather than Kreisel's modified realizability. Even so, it differs from both. On one hand, generic realizability (with truth) combined with a reflexive pca over finite types bears close similarities to modified realizability (with truth). Roughly, a truth realizer of a $\forall x^\sigma \, \exists y^\tau$ statement yields a choice functional of type $\sigma\tau$. This gives closure under the rule of choice in all finite types. On the other hand, totality is a crucial aspect of modified realizability with truth in establishing closure under independence of premise rule for (extensional) finite type arithmetic: realizers are total functionals. As it turns out, the independence of premise rules of Theorem 1.3 do not require the use of a total combinatory algebra: the inherent nature of set theory (a set is given by its members) allows us to dispense with totality. Note in contrast that truth variants of Kleene's realizability (e.g. q-realizability [41, 44]) do not yield closure under independence of premise rule for first order arithmetic HA, and one has to resort to other methods such as Kleene's or Aczel's slash instead.

Our approach to establish independence of premise rules however is not without shortcomings, as can be seen from Theorem 1.3 part (ii), and we do not know whether the following more genuine version holds true.

Problem 1.4. Is the following an admissible rule of CZF or any other familiar constructive/intuitionistic set theory T?

- If $T \vdash \neg\psi \to \exists y^\sigma \, \varphi(y)$, then $T \vdash \exists y^\sigma \, (\neg\psi \to \varphi(y))$, where y is not free in ψ.

Notice that as a special case of Theorem 1.3 part (ii) one only obtains the following weaker rule:

- if $T \vdash \neg\psi \to \exists y^\sigma \, \varphi(y)$, then $T \vdash \exists y \, (\neg\psi \to y \in \sigma \wedge \varphi(y))$,

where the y in the conclusion is guaranteed to be of type σ only in case the premise $\neg\psi$ is verified.

More in general, closure under independence of premise rule with no type restrictions remains an open problem:

Problem 1.5. Is the following an admissible rule of CZF or any other familiar constructive/intuitionistic set theory T?

- If $T \vdash \neg\psi \to \exists y \, \varphi(y)$, then $T \vdash \exists y \, (\neg\psi \to \varphi(y))$, where y is not free in ψ.

The present paper shows that this holds true when $\exists y$ is bounded by some finite type.

1.1. **Generic realizability for set theory.** Realizability semantics are ubiquitous in the study of intuitionistic theories. In the case of set theory, they differ in important aspects from Kleene's [13] realizability in their treatment of the quantifiers. Its origin is Kreisel's and Troelstra's [17] definition of realizability for second order Heyting arithmetic. This was applied to systems of higher order arithmetic and (intensional) set theory by Friedman [6] and Beeson [1]. McCarty [23] and [24] adapted Kreisel-Troelstra realizability directly to extensional intuitionistic set theories such as IZF. This type of realizability can also be formalized in CZF (see [35]) to yield a self-validating semantics for CZF.

Realizability combined with truth appears in connection with function realizability in Kleene [15] and was also studied by others (see [43] for the history). Troelstra considers realizability with truth in the arithmetic context and in connection with modified realizability in [43, 1.6, 2.1, 3.4]. In generic realizability for extensional set theory, however, the background universe V and the realizability universe $V(A)$ erected over a partial combinatory algebra A are rather different "worlds", and it is prima facie not clear how to view a statement as talking about a state of affairs in V and $V(A)$ at the same time. The paper [34] introduced a new realizability structure $V_{tr}(A)$ that arises by amalgamating the realizability structure $V(A)$ with the universe of sets in a coherent, albeit rather complicated way. This approach to realizability with truth based on $V_{tr}(A)$ will also be used in the present paper.[5] A very rough heuristics for using this method of realizability with truth is that it often works with principles that are validated in a realizability model based on a particular partial combinatory algebra and that switching to the corresponding version with the additional truth component one can derive the pertaining rule.[6]

1.2. **Comparison with other approaches to showing the independence of premise rule.** Closure under IPR has been shown for HAS (second order Heyting arithmetic) by Troelstra [42, 2.10] and for HAH (Heyting arithmetic in higher types, aka intuitionistic type theory) by Lambek and Scott [19].[7] Its admissibility is often established as a by-product of the existence property EP (also called the existential definability property) that such systems enjoy. As to the methods used in the metamathematics of HAS and HAH, one can roughly group them as follows:

(1) Proof-theoretic methods: study of the proof structure either in natural deduction systems or sequent calculi (e.g. Prawitz [29, 30], Scarpellini [37, 38], Troelstra [42], Hayashi [10, 11, 12]).
(2) Functional interpretation (e.g. Girard [8, 9]).
(3) Extensions of Kleene's slash method [14] (e.g. Moschovakis [26], Myhill [27, 28], Friedman [6], Lambek-Scott [18]).
(4) Topos-theoretic methods, conceptualizing term models as topoi ("free topos") and using techniques such as Freyd covers and topos glueing (e.g. Freyd [5], Moerdijk [25], Lambek-Scott [19, 20, 21], Ščedrov-Scott [46]).

[5] For more information, the introduction of [34] contains a historical account of realizability for set theories and the roots of generic realizability in particular.

[6] E.g. for Church's rule and Troelstra's Uniformity rule this was done in [34] using Kleene's first algebra.

[7] For a definition of HAS and HAH cf. [44, pp. 164 and 170]. HAS is a subsystem of CZF + (Full Separation). The two theories are known to be equiconsistent as shown by Lubarsky [22]. HAH is a fragment of intuitionistic Kripke-Platek set theory plus Powerset, IKP + (Powerset), but strictly weaker in terms of proof-theoretic strength. The latter theory is much weaker than intuitionistic Power Kripke-Platek set theory (see [32]), $\mathsf{IKP}(\mathcal{P})$, which proof-theoretically equates to a version of the Calculus of Constructions with one universe by [31, Theorem 15.1]. And $\mathsf{IKP}(\mathcal{P})$ is just a small fragment of IZF.

Taking intuitionistic Zermelo-Fraenkel set theory, IZF, to be the "typical" set theory of this paper, one can perhaps immediately say that such strong theories are currently not amenable to the methods of (1) and (2). The topos-theoretic methods of (4) have turned out to be equivalent in a strong sense to Friedman's modification of Kleene's slash in [6]: "*Thus Freyd's use of retracts and Friedman's impredicative assignment of indices turn out to be one and the same process*" [46, 443]. In view of the foregoing, we will only consider the Friedman slash method and point out the obstacles one faces when attempting to obtain the results of this paper via this method. For any of the slash methods to apply to a theory T one needs a language that has sufficiently many terms to serve as names for the objects that are describable in T. In the case of arithmetic this is easy as one has the numerals. In the context of higher order systems or set theories one is usually compelled to move to a theory T^* with a richer language that is conservative over T. Typically let T be a set theory with explicit set existence axioms, i.e. with axioms that define the contents of the set being asserted to exists, namely if it is of the form

$$\forall x_0 \dots \forall x_{n-1} \, [\psi(x_0, \dots, x_{n-1}) \to \exists y \, \forall u \, [u \in y \leftrightarrow \varphi(u, x_0, \dots, x_{n-1})]. \tag{1}$$

One then simultaneously inductively defines a new theory T^* and a collection of closed terms $\mathcal{T}^*$ such that T^* comprises the axioms of T and for each axiom of the form (1), whenever there is $t_0, \dots, t_{n-1} \in \mathcal{T}^*$ with $T^* \vdash \psi(t_0, \dots, t_{n-1})$, one adds a new constant $c_{\varphi,\psi}(t_0, \dots, t_{n-1})$ to $\mathcal{T}^*$ and an axiom

$$\forall u \, [u \in c_{\varphi,\psi}(t_0, \dots, t_{n-1}) \leftrightarrow \varphi(u, t_0, \dots, t_{n-1})].$$

It turns out that T^* is conservative over T. In a further step one defines the system $T^\diamond$ that is obtained by splitting up each term of T^* into many terms. Thus the terms of $T^\diamond$ are of the form $c_{\varphi,\psi}(t_0, \dots, t_{n-1})^X$, where X is any set of closed terms of T^* satisfying certain conditions. Echoing Myhill's words [28, p. 369], roughly $c_{\varphi,\psi}(t_0, \dots, t_{n-1})^X$ denotes the set $\{u \mid \varphi(u, t_0, \dots, t_{n-1})\}$ and X is the "reason" that we know $\varphi(u, t_0, \dots, t_{n-1})$. For our purposes it is not necessary to spell out the details. It suffices to know that the clauses for the quantifiers in the definition of the Friedman slash refer to the terms of $T^\diamond$. This slash interpretation works for many theories with explicit set existence axioms such as intuitionistic Zermelo-Fraenkel set theory when based on Replacement rather than Collection. As a typical application one obtains the set existence property. However, the Friedman slash is not known to work for theories whose set existence axioms are not explicit such as the Collection, Strong Collection, Subset Collection, the Regular Extension Axiom and the Presentation Axiom. Indeed, as shown by Friedman and Ščedrov [7], IZF does not have the EP and Swan [40] proved that CZF also lacks the EP, rendering it unlikely that the Friedman slash can be applied to these theories to establish closure under independence of premise rules whereas the method of realizability with truth works perfectly well.

2. Intuitionistic set theory

The language of constructive Zermelo-Fraenkel set theory CZF is same first order language as that of classical Zermelo-Fraenkel set theory ZF whose only non-logical symbol is the binary predicate $\in$. We use x, y, z, u, v, w, possibly with superscripts, for variables

in the language of CZF. The logic of CZF is intuitionistic first order logic with equality. The axioms of CZF are as follows (universal closures):
Extensionality: $\forall z\,(z \in x \leftrightarrow z \in y) \to x = y$.
Pairing: $\exists z\,(x \in z \wedge y \in z)$.
Union: $\exists y\,\forall z\,(\exists w \in x\,(z \in w) \to z \in y)$.
Infinity: $\exists w\,\forall x\,[x \in w \leftrightarrow \forall y\,(y \notin x) \vee \exists y \in w\,\forall z\,(z \in x \leftrightarrow z \in y \vee z = y)]$.
Set Induction: $\forall x\,[\forall y \in x\,\varphi(y) \to \varphi(x)] \to \forall x\,\varphi(x)$, for any formula φ,
Bounded Separation: $\exists y\,\forall z\,[z \in y \leftrightarrow z \in x \wedge \varphi(z)]$, for any *bounded* formula φ. A formula is *bounded* or *restricted* if it is constructed from prime formulae using $\to$, $\neg$, $\wedge$, $\vee$, $\forall x \in y$ and $\exists x \in y$ only.
Strong Collection:

$$\forall y \in x\,\exists z\,\varphi(y,z) \to \exists w\,[\forall y \in x\,\exists z \in w\,\varphi(y,z) \wedge \forall z \in w\,\exists y \in x\,\varphi(y,z)],$$

for any formula φ.
Subset Collection:

$$\forall x\,\forall y\,\exists z\,\forall u\,[\forall v \in x\,\exists w \in y\,\varphi(v,w,u) \to \\ \exists y' \in z\,[\forall v \in x\,\exists w \in y'\,\varphi(v,w,u) \wedge \forall w \in y'\,\exists v \in x\,\varphi(v,w,u)]],$$

for any formula φ.

In what follows, we shall assume that the language CZF has constants $\emptyset$ denoting the *empty set*, ω denoting the set of von Neumann natural numbers. One can take the axioms $\forall x\,(x \notin \emptyset)$ for $\emptyset$ and $\forall x\,[x \in \omega \leftrightarrow (x = \emptyset \vee \exists y \in \omega\,\forall z\,(z \in x \leftrightarrow z \in y \vee z = y))]$ for ω. We write $x+1$ for $x \cup \{x\}$ and use n, m, and l for elements of ω.

We consider also several extensions of CZF with other principles.
Full Separation: $\exists y\,\forall z\,[z \in y \leftrightarrow z \in x \wedge \varphi(z)]$, for any formula φ.
Powerset: $\exists y\,\forall z\,(z \subseteq x \to z \in y)$.

The system CZF+(**Full Separation**)+(**Powerset**) is called IZF (cf. [27] or [1, VIII.1]).
Markov principle (MP)**:** If $\forall n \in \omega\,(\varphi(n) \vee \neg\varphi(n))$ and $\neg\neg\exists n \in \omega\,\varphi(n)$, then $\exists n \in \omega\,\varphi(n)$.
Axiom of Countable Choice (AC_ω)**:** If $\forall n \in \omega\,\exists x\,\varphi(n,x)$, then $\exists f\,(f$ is a function $\wedge$ $\mathrm{dom}(f) = \omega \wedge \forall n \in \omega\,\varphi(n, f(n)))$.
Dependent Choices Axiom (DC)**:** If $\forall x \in z\,\exists y \in z\,\varphi(x,y)$, then $\forall x \in z\,\exists f\,(f$ is a function $\wedge$ $\mathrm{dom}(f) = \omega \wedge f(0) = x \wedge \forall n \in \omega\,\varphi(f(n), f(n+1)))$.
Relativised Dependent Choices Axiom (RDC)**:** If $\forall x\,(\psi(x) \to \exists y\,(\psi(y) \wedge \varphi(x,y))$, then for every x such that $\psi(x)$ there is a function f such that $\mathrm{dom}(f) = \omega \wedge f(0) = x \wedge \forall n \in \omega\,\varphi(f(n), f(n+1))$.

Definition 2.1. A set x is *inhabited* if $\exists y\,(y \in x)$. An inhabited set x is *regular* if x is transitive, and for every $y \in x$ and a set $z \subseteq y \times x$ if $\forall u \in y\,\exists v\,(\langle u,v\rangle \in z)$, then there is a set $w \in x$ such that

$$\forall u \in y\,\exists v \in w\,(\langle u,v\rangle \in z) \wedge \forall v \in w\,\forall u \in y\,(\langle u,v\rangle \in z).$$

Regular Extension Axiom (REA)**:** Every set is a subset of a regular set.

Definition 2.2. A set x is *projective* if for any x-indexed family $(y_u)_{u \in x}$ of inhabited sets y_u, there exists a function f with domain x such that $f(u) \in y_u$ for all $u \in x$.

Presentation Axiom (PAx)**:** Every set is the surjective image of a projective set.

2.1. **Finite types.**

Definition 2.3. Finite types σ and their extensions F_σ are defined by the following clauses:

- $o \in \Phi$ and $F_o = \omega$;
- if $\sigma, \tau \in \Phi$, then $(\sigma)\tau \in \Phi$ and $F_{(\sigma)\tau} = F_\sigma \to F_\tau = \{\text{total functions from } F_\sigma \text{ to } F_\tau\}$.

If there is no risk of confusion, we write $\sigma\tau$ or $\sigma \to \tau$ to denote the type $(\sigma)\tau$. The sets Φ of all finite types, $\mathbf{F} = \{F_\sigma : \sigma \in \Phi\}$ and $\mathbb{F} = \bigcup \mathbf{F}$ all exist in CZF.

Definition 2.4. There is a formula $\vartheta(\sigma, z)$ (also written $\vartheta_\sigma(z)$) such that:

- $\vartheta(o, z) \leftrightarrow z$ is ω;
- $\vartheta(\sigma\tau, z) \leftrightarrow \forall z_\sigma \, \forall z_\tau \, (\vartheta(\sigma, z_\sigma) \wedge \vartheta(\tau, z_\tau) \to \forall f \, (f \in z \leftrightarrow \mathrm{Fun}(f, z_\sigma, z_\tau)))$.

Here, $\mathrm{Fun}(f, x, y)$ is an abbreviation for "f is a function from x to y."

Notation 2.5 (Official)**.** $\forall x^\sigma \ldots$ stands for $\forall z_\sigma \, (\vartheta_\sigma(z_\sigma) \to \forall x \in z_\sigma \ldots)$. Similarly for $\exists x^\sigma$.

3. Partial combinatory algebras I

In order to define a realizability interpretation we must have a notion of realizing functions to hand. A particularly general and elegant approach to realizability builds on structures which have been variably called partial combinatory algebras, applicative structures, or Schönfinkel algebras. For more information on these structures see [3, 4, 1, 45].

Definition 3.1. $(A, \cdot)$ is said to be a *partial algebra* if A is a set and $\cdot$ is a binary function on some subset of $A \times A$. Since $\cdot$ is only partial on A, it is convenient to talk about application terms of $(A, \cdot)$, where these terms might not denote an object in A. Given an infinite collection $x, y, z, \ldots$ of variables, the inductive definition of application terms is as follows: every variable x and every $a \in A$ is an application term; if s, t are application terms then $(s \cdot t)$ is an application term. A closed application term is one without variables and it denotes an element a of A iff it is a itself or else it is of the form $(s \cdot t)$ and there are $b, c \in A$ such that s denotes b, t denotes c, (b, c) is in the domain of $\cdot$ and $a = b \cdot c$. If a closed application term t denotes, then we convey this by writing $t\downarrow$.

For application terms $s_1, \ldots, s_r$ we shall just write $s_1 \ldots s_r$ to refer to the application term inductively defined by letting $s_1 \ldots s_{n+1}$ be $((s_1 \ldots s_n) \cdot s_{n+1})$; so the convention is to drop $\cdot$ and assume the bracketing to be arranged to the left. We also use $s = t$ to convey that the closed application terms s and t denote the same object in A; in particular $s = t$ entails that $s\downarrow$ and $t\downarrow$. We also introduce the very helpful abbreviation $t \simeq s$ for $(t\downarrow \vee s\downarrow) \to s = t$.

A *partial combinatory algebra* (pca) is a partial algebra $(A, \cdot)$ 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

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

holds for all $a, b, c \in A$.

The combinators **k** and **s** are due to Schönfinkel [39] while the axiomatic treatment, although formulated just in the total case, is due to Curry [2]. Employing the axioms for the combinators **k** and **s** one can deduce an abstraction lemma yielding λ-terms (cf. [3]).

Lemma 3.2 (abstraction lemma)**.** *For each application term $t(x_1, \ldots, x_{n+1})$, there is a closed application term a, denoted $\lambda x_1 \cdots x_n.t$, such that for all $a_1, \ldots, a_n, b \in A$*

- $aa_1 \cdots a_n \downarrow$;
- $aa_1 \cdots a_n b \simeq t(a_1, \ldots, a_n b)$.

The most important consequence of the Abstraction Lemma is the Recursion Theorem. It can be derived in the same way as for the λ–calculus (cf. [3], [4], [1, VI.2.7]).

Corollary 3.3 (recursion theorem)**.** *For every $n > 0$ there exists a closed application term f such that for all $a, b_1, \ldots, b_n \in A$ we have:*

- $fa \downarrow$;
- $fab_1 \cdots b_n \simeq a(fa)b_1 \cdots b_n$.

In every pca, one has pairing and unpairing[8] combinators $\mathbf{p}$, $\mathbf{p_0}$, and $\mathbf{p_1}$ such that:

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

The notion of a pca is slightly impoverished compared to that of a model of Beeson's theory PCA^+ [1, VI.2] or Feferman's theory for applicative structures APP ([3, 4], [44, 9.3]). Although, as Curry showed, every pca can be expanded to a model of $\mathbf{PCA}^+$, which at the same time is also an applicative structure (see [1, VI.2.9]), we spell out the sort of structure we are interested in, that is, a model of PCA^+. Details will become more pertinent when we engineer specific ones that include all finite types (Definition 5.1).

Definition 3.4. We say that A is a *pca over* ω if there are extra combinators **succ**, **pred** (successor and predecessor combinators), **d** (definition by cases combinator), and a map $n \mapsto \bar{n}$ from ω to A such that for all $n, m \in \omega$ and $a, b \in A$

$$\mathbf{succ}\, \bar{n} \simeq \overline{n+1}, \qquad \mathbf{pred}\, \overline{n+1} \simeq \bar{n}, \qquad \mathbf{d}\bar{n}\bar{m}ab \simeq \begin{cases} a & n = m; \\ b & n \neq m. \end{cases}$$

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

4. Realizability with truth

4.1. **The general realizability structure.** [34] introduces a realizability structure with truth over Kleene's first algebra. In this paper, we define it over an arbitrary set-sized pca A (both A and the graph $\{(x, y, z) \in A^3 : xy \simeq z\}$ are sets).

Notation 4.1. For an ordered pair $x = \langle x_0, x_1 \rangle$, let

$$x^\circ = x_0$$
$$x^* = x_1.$$

[8] 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.

Definition 4.2. Ordinals are transitive sets whose elements are transitive also. As per usual, we use lower case Greek letters α and β to range over ordinals. Let A be a pca. Besides V_α and V, we define $\mathrm{V}_{tr}(A)_\alpha$ and $\mathrm{V}_{tr}(A)$ as follows:

$$\mathrm{V}_{tr}(A)_\alpha = \bigcup_{\beta\in\alpha} \{\langle x, \hat{x}\rangle \mid x \in \mathrm{V}_\beta \wedge \hat{x} \subseteq A \times \mathrm{V}_{tr}(A)_\beta \wedge \forall \langle a, u\rangle \in \hat{x}\, (u^\circ \in x)\} \tag{2}$$

$$\mathrm{V}_\alpha = \bigcup_{\beta\in\alpha} \mathcal{P}(\mathrm{V}_\beta)$$

$$\mathrm{V}_{tr}(A) = \bigcup_{\alpha} \mathrm{V}_{tr}(A)_\alpha$$

$$\mathrm{V} = \bigcup_{\alpha} \mathrm{V}_\alpha.$$

As the power set operation is not available in CZF, it is not clear whether the classes V and $\mathrm{V}_{tr}(A)$ can be formalized in CZF. However, employing the fact that CZF accommodates inductively defined classes, the classes V_α and $\mathrm{V}_{tr}(A)_\alpha$ can be defined in the same vein as in [35, Lemma 3.4].

Lemma 4.3 (CZF)**.** *The following holds:*

(i) V and $\mathrm{V}_{tr}(A)$ *are cumulative: for* $\beta \in \alpha$, $\mathrm{V}_\beta \subseteq \mathrm{V}_\alpha$ and $\mathrm{V}_{tr}(A)_\beta \subseteq \mathrm{V}_{tr}(A)_\alpha$.
(ii) *For all sets* x, $x \in \mathrm{V}$.
(iii) *If* $x, \hat{x}$ *are sets,* $\hat{x} \subseteq A \times \mathrm{V}_{tr}(A)$ *and* $\forall \langle a, u\rangle \in \hat{x}\, (u^\circ \in x)$*, then* $\langle x, \hat{x}\rangle \in \mathrm{V}_{tr}(A)$.

Proof. This is proved in the same way as [34, Lemma 4.2]. □

The definition of $\mathrm{V}_{tr}(A)_\alpha$ in (2) is perhaps a bit involved. Note first that all the elements of $\mathrm{V}_{tr}(A)$ are ordered pairs $\langle x, \hat{x}\rangle$ such that $\hat{x} \subseteq A \times \mathrm{V}_{tr}(A)$. For an ordered pair $\langle x, \hat{x}\rangle$ to enter $\mathrm{V}_{tr}(A)_\alpha$ the first conditions to be met are that $x \in \mathrm{V}_\beta$ and $\hat{x} \subseteq A \times \mathrm{V}_{tr}(A)_\beta$ for some $\beta \in \alpha$. Furthermore, it is required that enough elements of x live in the transitive closure of $\hat{x}$ in that whenever $\langle a, u\rangle \in \hat{x}$ then $u^\circ \in x$.

For all intents and purposes, the following equivalent definition of $\mathrm{V}_{tr}(A)$ is perfectly justifiable in CZF.

Definition 4.4 (universe)**.** Given a pca A, we inductively define the class $\mathrm{V}_{tr}(A)$ by the following clause:

- if $\hat{x} \subseteq A \times \mathrm{V}_{tr}(A)$ and for every $\langle a, u\rangle \in \hat{x}$ we have $u^\circ \in x$, then $\langle x, \hat{x}\rangle \in \mathrm{V}_{tr}(A)$.

Definition 4.5 (canonical name)**.** Let

$$\check{x} = \langle x, \{\langle \mathbf{0}, \check{u}\rangle : u \in x\}\rangle.$$

Then $\check{x} \in \mathrm{V}_{tr}(A)$ and $\check{x}^\circ = x$.

4.2. **Defining realizability.** We now proceed to define a notion of realizability with truth over $\mathrm{V}_{tr}(A)$, where A is any pca over ω.

Definition 4.6. Given a formula φ with parameters in $\mathrm{V}_{tr}(A)$, let φ° be the formula obtained by replacing each parameter x in φ with x°.

Notation 4.7. 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 $\exists a\, (t \simeq a \wedge \varphi(a))$.

The following truth variant of generic realizability is due to Rathjen (see [34]). Bounded quantifiers are treated as quantifiers in their own right, i.e., bounded and unbounded quantifiers are treated as syntactically different kinds of quantifiers. The subscript in $\Vdash_{tr}$ is supposed to serve as a reminder of "realizability with truth."

Definition 4.8 (realizability with truth)**.** We define the relation $a \Vdash_{tr} \varphi$, where $a \in A$ and φ is a formula with parameters in $\mathrm{V}_{tr}(A)$. The atomic cases are defined by transfinite recursion.

$$
\begin{array}{lcl}
a \Vdash_{tr} x \in y & \Leftrightarrow & x^\circ \in y^\circ \wedge \exists z\, (\langle a_0, z\rangle \in y^* \wedge a_1 \Vdash_{tr} x = z) \\
a \Vdash_{tr} x = y & \Leftrightarrow & x^\circ = y^\circ \wedge \forall \langle b, z\rangle \in x^*\, ((ab)_0 \Vdash_{tr} z \in y) \\
 & & \qquad \wedge \forall \langle b, z\rangle \in y^*\, ((ab)_1 \Vdash_{tr} z \in x) \\
a \Vdash_{tr} \varphi \wedge \psi & \Leftrightarrow & a_0 \Vdash_{tr} \varphi \wedge a_1 \Vdash_{tr} \psi \\
a \Vdash_{tr} \varphi \vee \psi & \Leftrightarrow & a_0 \simeq \mathbf{0} \wedge a_1 \Vdash_{tr} \varphi \text{ or } a_0 \simeq \mathbf{1} \wedge a_1 \Vdash_{tr} \psi \\
a \Vdash_{tr} \neg\varphi & \Leftrightarrow & \neg\varphi^\circ \wedge \forall b\, \neg(b \Vdash_{tr} \varphi) \\
a \Vdash_{tr} \varphi \to \psi & \Leftrightarrow & \varphi^\circ \to \psi^\circ \wedge \forall b \Vdash_{tr} \varphi\, (ab \Vdash_{tr} \psi) \\
a \Vdash_{tr} \forall x \in y\, \varphi & \Leftrightarrow & \forall x \in y^\circ\, \varphi^\circ \wedge \forall \langle b, x\rangle \in y^*\, (ab \Vdash_{tr} \varphi) \\
a \Vdash_{tr} \exists x \in y\, \varphi & \Leftrightarrow & \exists x\, (\langle a_0, x\rangle \in y^* \wedge a_1 \Vdash_{tr} \varphi) \\
a \Vdash_{tr} \forall x\, \varphi & \Leftrightarrow & \forall x \in \mathrm{V}_{tr}(A)\, (a \Vdash_{tr} \varphi) \\
a \Vdash_{tr} \exists x\, \varphi & \Leftrightarrow & \exists x \in \mathrm{V}_{tr}(A)\, (a \Vdash_{tr} \varphi)
\end{array}
$$

Lemma 4.9. CZF *proves*

$$(a \Vdash_{tr} \varphi) \to \varphi^\circ.$$

Proof. By induction on the build up of φ. The case of an unbounded universal quantifier follows from the fact that every set has a name in $\mathrm{V}_{tr}(A)$. □

Lemma 4.10. *Negated formulas are self-realizing, that is to say,* CZF *proves*

$$\neg\varphi^\circ \to (\mathbf{0} \Vdash_{tr} \neg\varphi) \leftrightarrow \forall a\, (a \Vdash_{tr} \neg\varphi).$$

Proof. Assume $\neg\varphi^\circ$. From $a \Vdash_{tr} \varphi$, we would get φ° by Lemma 4.9. But this is absurd. Hence $\forall a\, \neg(a \Vdash_{tr} \varphi)$, and therefore $\mathbf{0} \Vdash_{tr} \neg\varphi$. The second part is similar. □

Theorem 4.11 (Soundness)**.** *Let T be any combination of* CZF *with the axioms and schemes (Full Separation), (Powerset),* REA, MP, AC_ω, DC, RDC, *and* PAx*. Then, for every theorem θ of T, there exists an application term $\mathbf{t}$ such that $T \vdash (t \Vdash_{tr} \theta)$. In particular,* CZF, $\mathsf{CZF}+\mathsf{REA}$, IZF, $\mathsf{IZF}+\mathsf{REA}$ *satisfy this property. Moreover, the proof is effective in that the application term $\mathbf{t}$ can be constructed from the T-proof of θ.*

Proof. This is proved in the same way as [34, Theorem 6.1, Theorem 7.2] and [36, Theorem 7.4]. □

Notation 4.12. We write $\Vdash_{tr} \varphi$ for $\exists a \in A\, (a \Vdash_{tr} \varphi)$.

4.3. **Pairing.**

Definition 4.13 (internal pairing)**.** For $x, y \in \mathrm{V}_{tr}(A)$, let

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

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

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

Note that all these sets are in $\mathrm{V}_{tr}(A)$.

Notation 4.14. To avoid confusion, let $\mathrm{op}(z, x, y)$ be a formula expressing that z is the ordered pair of x and y, that is, $z = \langle x, y\rangle = \{\{x\}, \{x, y\}\}$.

As expected, all the desired properties of pairing are realized. Below we list some.

Lemma 4.15. *There are closed application terms* $\mathbf{v}$, $\mathbf{w}$, $\mathbf{z}$ *such that for all* $x, y, z, u, v \in \mathrm{V}_{tr}(A)$

$$\mathbf{v} \Vdash_{tr} \mathrm{op}(\langle x, y\rangle_A, x, y),$$

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

$$\mathbf{z} \Vdash_{tr} \mathrm{op}(z, x, y) \to z = \langle x, y\rangle_A.$$

5. Partial combinatory algebras II

To deal with the rules of choice and independence of premise in all finite types, we will use our truth variant of generic realizability with pca's *containing* all objects of finite type.

Definition 5.1 (pca over $\mathbb{F}$)**.** We say that A is a *pca over* $\mathbb{F}$ if there are extra combinators **succ**, **pred** (successor and predecessor combinators), **d** (definition by cases combinator), and a one-to-one map $x \mapsto \bar{x}$ from $\mathbb{F}$ to A such that

- $\bar{f}\bar{x} \simeq \overline{f(x)}$ for $f \in F_{\sigma\tau}$ and $x \in F_\sigma$;
- for all $n, m \in \omega$ and $a, b \in A$

$$\mathbf{succ}\,\bar{n} \simeq \overline{n+1}, \qquad \mathbf{pred}\,\overline{n+1} \simeq \bar{n}, \qquad \mathbf{d}\bar{n}\bar{m}ab \simeq \begin{cases} a & n = m; \\ b & n \neq m. \end{cases}$$

The idea is to have *nice* names of the form

$$\dot{F}_\sigma = \langle F_\sigma, \{\langle \bar{x}, \dot{x}\rangle \mid x \in F_\sigma\}\rangle$$

for every type σ. Indeed, we require a little bit more.

Definition 5.2 (reflexive pca over $\mathbb{F}$)**.** A pca A over $\mathbb{F}$ is *reflexive* on $\mathbb{F}$ if for all σ and τ there is a combinator $\mathbf{i}_{\sigma\tau}$ such that

$$\mathbf{i}_{\sigma\tau}a \simeq \bar{f},$$

whenever $f \in F_{\sigma\tau}$ and $a\bar{x} = \overline{f(x)}$ for every $x \in F_\sigma$.

Unless otherwise stated, from now on we posit a reflexive pca A over $\mathbb{F}$ within CZF. In Section 9 we will give an example and show how to carry out such construction in CZF.

6. Injective names for finite type objects

Definition 6.1 (canonical names for objects of finite type and extensions)**.** Let A be a pca over $\mathbb{F}$. Let

$$\dot{\omega} = \langle \omega, \{\langle \bar{n}, \dot{n} \rangle \mid n \in \omega\} \rangle,$$

where

$$\dot{n} = \langle n, \{\langle \bar{m}, \dot{m} \rangle \mid m < n\} \rangle.$$

For higher types, let

$$\dot{F}_{\sigma\tau} = \langle F_{\sigma\tau}, \{\langle \bar{f}, \dot{f} \rangle \mid f \in F_{\sigma\tau}\} \rangle,$$

where

$$\dot{f} = \langle f, \{\langle \bar{x}, \langle \dot{x}, \dot{y} \rangle_A \rangle \mid x \in F_\sigma \wedge f(x) = y\} \rangle.$$

Lemma 6.2. *Let A be a pca over $\mathbb{F}$. For every σ,*

- $(\dot{x})^\circ = x$ *for every* $x \in F_\sigma$*,*
- $(\dot{F}_\sigma)^\circ = F_\sigma$*.*

Definition 6.3 (injective)**.** A name $x \in \mathrm{V}_{tr}(A)$ is *injective* if

(i) $x^\circ = \{u^\circ \mid \exists a \in A\,(\langle a, u \rangle \in x^*)\}$;
(ii) if $\langle a, u \rangle, \langle b, v \rangle \in x^*$, then $a = b$ iff $u^\circ = v^\circ$.

In other words, $\{\langle a, u^\circ \rangle \mid \langle a, u \rangle \in x^*\}$ is one-to-one function from $\{a \in A \mid \exists u\,(\langle a, u \rangle \in x^*)\}$ onto x°. We say that x° is *injectively presented*.

Lemma 6.4. *Let $x \in \mathrm{V}_{tr}(A)$ be injective. Then*

$$a \Vdash_{tr} \forall u \in x\, \varphi(u) \qquad \Leftrightarrow \qquad \forall \langle b, u \rangle \in x^*\, ab \Vdash_{tr} \varphi(u).$$

Proof. Indeed, condition (i) is sufficient. □

Lemma 6.5. *Let A be a pca over $\mathbb{F}$. For every σ,*

- $\dot{x}$ *is injective for every* $x \in F_\sigma$*;*
- $\dot{F}_\sigma$ *is injective;*
- $\Vdash_{tr} \dot{x} = \dot{y}$ *implies* $x = y$ *for all* $x, y \in F_\sigma$ *(absoluteness).*

7. Realizing finite types

We want to show that CZF proves $\Vdash_{tr} \vartheta_\sigma(\dot{F}_\sigma)$ for every σ, provided that A is a reflexive pca over $\mathbb{F}$. Recall that $\vartheta_\sigma(z)$ is the formula asserting that z is the set of all objects of type σ (Definition 2.4).

Theorem 7.1 (natural numbers)**.** *There exists a closed application term* $\mathbf{e}$ *such that* CZF *proves*

$$\mathbf{e} \Vdash_{tr} \vartheta_o(\dot{\omega}).$$

Proof. See [34, Theorem 6.1 (Infinity)]. Note that any pca would do the job. □

For arrow types, we use reflexivity.

Theorem 7.2 (arrow types)**.** *For all finite types σ and τ there exists a closed application term* $\mathbf{e}$ *such that* CZF *proves*

$$\mathbf{e} \Vdash_{tr} \forall f\,(f \in \dot{F}_{\sigma\tau} \leftrightarrow \mathrm{Fun}(f, \dot{F}_\sigma, \dot{F}_\tau)).$$

Proof. Fix types σ and τ. It suffices to look for closed application terms $\mathbf{a}$ and $\mathbf{b}$ such that

$$\mathbf{a} \Vdash_{tr} \forall f \in \dot{F}_{\sigma\tau}\ \mathrm{Fun}(f, \dot{F}_\sigma, \dot{F}_\tau),$$

and for every $g \in \mathrm{V}_{tr}(A)$,

$$\mathbf{b} \Vdash_{tr} \mathrm{Fun}(g, \dot{F}_\sigma, \dot{F}_\tau) \to g \in \dot{F}_{\sigma\tau}.$$

To ease notation, we identify x with $\bar{x}$. Since $(\dot{F}_\sigma)^\circ = F_\sigma$ for every type σ, we just need to verify the second half of the pertaining clauses, namely,

- for every $f \in F_{\sigma\tau}$, $\mathbf{a}f \Vdash_{tr} \mathrm{Fun}(\dot{f}, \dot{F}_\sigma, \dot{F}_\tau)$;
- if $a \Vdash_{tr} \mathrm{Fun}(g, \dot{F}_\sigma, \dot{F}_\tau)$, then $\mathbf{b}a \Vdash_{tr} g \in \dot{F}_{\sigma\tau}$.

For $\mathbf{a}$, we need to find $\mathbf{r}, \mathbf{t}, \mathbf{f}$ such that for every $f \in F_{\sigma\tau}$,

$$\mathbf{r}f \Vdash_{tr} \forall z \in \dot{f}\ \exists x \in \dot{F}_\sigma\ \exists y \in \dot{F}_\tau\ \mathrm{op}(z, x, y), \tag{1}$$

$$\mathbf{t}f \Vdash_{tr} \forall x \in \dot{F}_\sigma\ \exists y \in \dot{F}_\tau\ \exists z \in \dot{f}\ \mathrm{op}(z, x, y), \tag{2}$$

$$\mathbf{f}f \Vdash_{tr} \forall z_0 \in \dot{f}\ \forall z_1 \in \dot{f}\ \forall x\ \forall y_0\ \forall y_1\ (\mathrm{op}(z_0, x, y_0) \wedge \mathrm{op}(z_1, x, y_1) \to y_0 = y_1). \tag{3}$$

For (1), let

$$\mathbf{r} = \lambda ax.\mathbf{p}x(\mathbf{p}(ax)\mathbf{v}),$$

where $\mathbf{v} \Vdash_{tr} \mathrm{op}(\langle x, y\rangle_A, x, y)$ for all $x, y \in \mathrm{V}_{tr}(A)$. Let us verify that $\mathbf{r}$ does the job. Let $f \in F_{\sigma\tau}$. We want to show that

$$\mathbf{r}f = \lambda x.\mathbf{p}x(\mathbf{p}(fx)\mathbf{v}) \Vdash_{tr} \forall z \in \dot{f}\ \exists x \in \dot{F}_\sigma\ \exists y \in \dot{F}_\tau\ \mathrm{op}(z, x, y).$$

As $\dot{f}$ is injective, by Lemma 6.4 it suffices to show that for $x \in F_\sigma$ and $y = f(x) \in F_\tau$ we have that

$$\mathbf{p}x(\mathbf{p}(fx)\mathbf{v}) \Vdash_{tr} \exists x_0 \in \dot{F}_\sigma\ \exists y_0 \in \dot{F}_\tau\ \mathrm{op}(\langle \dot{x}, \dot{y}\rangle_A, x_0, y_0).$$

By definition, $\langle x, \dot{x}\rangle \in (\dot{F}_\sigma)^*$. Let us check that

$$\mathbf{p}(fx)\mathbf{v} \Vdash_{tr} \exists y_0 \in \dot{F}_\tau\ \mathrm{op}(\langle \dot{x}, \dot{y}\rangle_A, \dot{x}, y_0).$$

Note that $fx \simeq y$ and $\langle y, \dot{y}\rangle \in (\dot{F}_\tau)^*$. Finally,

$$\mathbf{v} \Vdash_{tr} \mathrm{op}(\langle \dot{x}, \dot{y}\rangle_A, \dot{x}, \dot{y}).$$

For (2), use

$$\mathbf{t} = \lambda ax.\mathbf{p}(ax)(\mathbf{p}x\mathbf{v}),$$

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

For (3), use the fact that $\dot{x}^\circ = x$ for every $x \in F_\sigma$ and the properties of pairing and equality.

We now construct $\mathbf{b}$. Here is where the $\sigma\tau$ combinator $\mathbf{i}_{\sigma\tau}$ comes into play. Suppose that

$$a \Vdash_{tr} \mathrm{Fun}(g, \dot{F}_\sigma, \dot{F}_\tau).$$

We aim for

$$\mathbf{b}a \Vdash_{tr} g \in \dot{F}_{\sigma\tau}.$$

We have

$$a_0 \Vdash_{tr} \forall z \in g\ \exists x \in \dot{F}_\sigma\ \exists y \in \dot{F}_\tau\ \mathrm{op}(z, x, y), \tag{4}$$

$$a_{10} \Vdash_{tr} \forall x \in \dot{F}_\sigma\, \exists y \in \dot{F}_\tau\, \exists z \in g\; \mathrm{op}(z, x, y), \tag{5}$$

$$a_{11} \Vdash_{tr} \forall z_0 \in g\, \forall z_1 \in g\, \forall x\, \forall y_0\, \forall y_1\, (\mathrm{op}(z_0, x, y_0) \wedge \mathrm{op}(z_1, x, y_1) \to y_0 = y_1). \tag{6}$$

Since $g^\circ \in (\dot{F}_{\sigma\tau})^\circ = F_{\sigma\tau}$, we only need to find $\mathbf{b}$ such that

$$(\mathbf{b}a)_0 \simeq f \in F_{\sigma\tau} \text{ and } (\mathbf{b}a)_1 \Vdash_{tr} g = \dot{f}.$$

It follows from (5) that for every $x \in F_\sigma$ there exists (a unique) $y \in F_\tau$ such that $(a_{10}x)_0 \simeq y$ and

$$(a_{10}x)_1 \Vdash_{tr} \exists z \in g\; \mathrm{op}(z, \dot{x}, \dot{y}).$$

We now apply the $\sigma\tau$ combinator $\mathbf{i}_{\sigma\tau}$. We then have $\mathbf{i}_{\sigma\tau}\lambda x.(a_{10}x)_0 \simeq f$, for the (unique) $f \in F_{\sigma\tau}$ such that

$$(a_{10}x)_0 \simeq f(x), \text{ for all } x \in F_\sigma.$$

We set

$$\mathbf{b} = \lambda a.\mathbf{p}(\mathbf{i}_{\sigma\tau}\lambda x.(a_{10}x)_0)(\mathbf{h}a),$$

and we are left to find $\mathbf{h}$ such that

$$\mathbf{h}a \Vdash_{tr} g = \dot{f}.$$

By using (5), it is not difficult to show that $g^\circ(x) = f(x)$ for every $x \in F_\sigma$, and hence $g^\circ = f = (\dot{f})^\circ$. It remains to prove the second half of the pertaining clause.

($\subseteq$) Let $\langle b, z\rangle \in g^*$. We aim for $(\mathbf{h}ab)_0 \Vdash_{tr} z \in \dot{f}$. By (4), there are $x \in F_\sigma$ and $y_0 \in F_\tau$ such that

$$(a_0 b)_0 \simeq x \text{ and } (a_0 b)_{10} \simeq y_0 \text{ and } (a_0 b)_{11} \Vdash_{tr} \mathrm{op}(z, \dot{x}, \dot{y}_0).$$

On the other hand, by (5), there is a $\langle b_1, z_1\rangle \in g^*$ with $(a_{10}x)_{10} \simeq b_1$ such that

$$(a_{10}x)_{11} \Vdash_{tr} \mathrm{op}(z_1, \dot{x}, \dot{y}),$$

where $y = f(x)$. By (6),

$$a_{11}bb_1(\mathbf{p}(a_0 b)_{11}(a_{10}x)_{11}) \Vdash_{tr} \dot{y}_0 = \dot{y}.$$

By absoluteness (Lemma 6.5) it follows from $\Vdash_{tr} \dot{y}_0 = \dot{y}$ that $y_0 = y$. Then $\mathbf{h}$ such that

$$(\mathbf{h}ab)_0 \simeq \mathbf{p}(a_0 b)_0(\mathbf{q}(a_0 b)_{11}),$$

where $\mathbf{q}$ is some fixed term such that

$$\mathbf{q} \Vdash_{tr} \mathrm{op}(z, x, y) \to z = \langle x, y\rangle_A,$$

is as desired.

($\supseteq$) Let $\langle x, \langle \dot{x}, \dot{y}\rangle_A\rangle \in (\dot{f})^*$. By definition, $f(x) = y$. We aim for $(\mathbf{h}ax)_1 \Vdash_{tr} \langle \dot{x}, \dot{y}\rangle_A \in g$. Just let

$$(\mathbf{h}ax)_1 = \mathbf{p}(a_{10}x)_{10}(\mathbf{r}(a_{10}x)_{11}),$$

where $\mathbf{r}$ is some fixed term such that

$$\mathbf{r} \Vdash_{tr} \mathrm{op}(z, x, y) \to \langle x, y\rangle_A = z.$$

$\square$

Theorem 7.3. *For every finite type σ there exists a closed application term* $\mathbf{f}$ *such that* CZF *proves*

$$\mathbf{f} \Vdash_{tr} \vartheta_\sigma(\dot{F}_\sigma).$$

8. Admissible rules

8.1. Choice.

Lemma 8.1 (choice for injective names)**.** CZF *proves*

$$(\Vdash_{tr} \forall u \in x\, \exists v \in y\, \varphi(x,y)) \to \exists f \colon x^\circ \to y^\circ\, \forall u \in x^\circ\, \varphi^\circ(u, f(u)),$$

for all injective names $x, y \in \mathrm{V}_{tr}(A)$.

Proof. Suppose

$$e \Vdash_{tr} \forall u \in x\, \exists v \in y\, \varphi(u,v).$$

Unraveling the definition, we have that if $\langle a,u\rangle \in x^*$ then $ea \Vdash_{tr} \exists v \in y\, \varphi(u,y)$, and hence there is $\langle b,v\rangle \in y^*$, where $(ea)_0 \simeq b$, such that $(ea)_1 \Vdash_{tr} \varphi(u,v)$. In particular, $\varphi^\circ(u^\circ, v^\circ)$. Let

$$f = \{\langle u^\circ, v^\circ\rangle \colon \langle a,u\rangle \in x^* \wedge \langle b,v\rangle \in y^* \wedge (ea)_0 \simeq b\}.$$

Then f is as desired. In fact, $\mathrm{dom}(f) = x^\circ$ follows from Definition 6.3 (i). The fact that f is indeed a function follows from Definition 6.3 (ii) applied to both x and y. □

Theorem 8.2 (choice rule)**.** CZF *is closed under*

$$\frac{\forall x^\sigma\, \exists y^\tau\, \varphi(x,y)}{\exists f^{\sigma\tau}\, \forall x^\sigma\, \varphi(x, f(x))}$$

Same for IZF *and any other theory from Theorem 4.11.*

Proof. Use a reflexive pca over $\mathbb{F}$. By soundness, let $\mathbf{e} \Vdash_{tr} \forall x^\sigma\, \exists y^\tau\, \varphi(x,y)$. By Theorem 7.3 and soundness, we can compute a such that

$$a \Vdash_{tr} \forall x \in \dot{F}_\sigma\, \exists y \in \dot{F}_\tau\, \varphi(x,y).$$

By injectivity and Lemma 8.1, we conclude

$$\exists f \colon F_\sigma \to F_\tau\, \forall x \in F_\sigma\, \varphi(x, f(x)),$$

that is, $\exists f^{\sigma\tau}\, \forall x^\sigma\, \varphi(x, f(x))$. □

8.2. Uniformity rules.

Theorem 8.3. CZF *is closed under*

$$\frac{\forall \boldsymbol{x}\, (\varphi(\boldsymbol{x}) \vee \psi(\boldsymbol{x}))}{\forall \boldsymbol{x}\, \varphi(\boldsymbol{x}) \quad \textit{or} \quad \forall \boldsymbol{x}\, \psi(\boldsymbol{x})} \qquad \text{(UZR)}$$

Same for IZF *and any other theory from Theorem 4.11.*

Proof. Use generic realizability with truth and Kleene's first algebra. See [34, Theorem 1.2]. □

Theorem 8.4. CZF *is closed under*

$$\frac{\forall \boldsymbol{x}\, \exists y^\sigma\, \varphi(\boldsymbol{x}, y)}{\exists y^\sigma\, \forall \boldsymbol{x}\, \varphi(\boldsymbol{x}, y)} \qquad (\mathsf{UR}_\sigma)$$

Same for IZF *and any other theory from Theorem 4.11.*

Proof. Use a reflexive pca over $\mathbb{F}$. WLOG, let $\boldsymbol{x}$ consist of a single variable. Suppose CZF proves $\forall x\, \exists y^\sigma\, \varphi(x, y)$. By soundness, let $\mathbf{e}$ be such that CZF proves $\mathbf{e} \Vdash_{tr} \forall x\, \exists y^\sigma\, \varphi(x, y)$. According to our official convention, $\exists y^\sigma\, \varphi(x, y)$ stands for

$$\forall z\, (\vartheta_\sigma(z) \to \exists y \in z\, \varphi(x, y)).$$

Reasoning in CZF, we have that $\mathbf{e} \Vdash_{tr} \exists y^\sigma\, \varphi(\check{x}, y^\sigma)$ for every x. We know that there is a closed application term $\mathbf{f}$ such that $\mathbf{f} \Vdash_{tr} \vartheta_\sigma(\dot{F}_\sigma)$. In particular, for every x there exists $y \in F_\sigma$ such that $(\mathbf{ef})_0 \simeq \bar{y}$ and $(\mathbf{ef})_1 \Vdash_{tr} \varphi(\check{x}, \dot{y})$. Note that y does not depend on x. So let $y \in F_\sigma$ such that $(\mathbf{ef})_0 \simeq \bar{y}$. We thus have that for every x, $(\mathbf{ef})_1 \Vdash_{tr} \varphi(\check{x}, \dot{y})$, and hence $\varphi(x, y)$, as desired. □

8.3. **Independence of premise.**

Theorem 8.5 (independence of premise rules)**.** *Let $\psi(\boldsymbol{x})$, $\varphi(\boldsymbol{x}, y)$, $\theta(\boldsymbol{x}, \boldsymbol{z})$ be formulas with displayed free variables. Then* CZF *is closed under the following rules:*

$$\frac{\forall \boldsymbol{x}\, (\neg\psi(\boldsymbol{x}) \to \exists y^\sigma\, \varphi(\boldsymbol{x}, y))}{\exists y\, \forall \boldsymbol{x}\, (\neg\psi(\boldsymbol{x}) \to y \in F_\sigma \wedge \varphi(\boldsymbol{x}, y))} \qquad (1)$$

$$\frac{\forall \boldsymbol{x}\, (\neg\psi(\boldsymbol{x}) \to \exists y^\sigma\, \varphi(\boldsymbol{x}, y)) \qquad \exists \boldsymbol{x}\, \neg\psi(\boldsymbol{x})}{\exists y^\sigma\, \forall \boldsymbol{x}\, (\neg\psi(\boldsymbol{x}) \to \varphi(\boldsymbol{x}, y))} \qquad (2)$$

$$\frac{\forall \boldsymbol{x}\, (\forall \boldsymbol{z}\, \theta(\boldsymbol{x}, \boldsymbol{z}) \to \exists y^\sigma\, \varphi(\boldsymbol{x}, y)) \qquad \forall \boldsymbol{x}\, \forall \boldsymbol{z}\, (\theta(\boldsymbol{x}, \boldsymbol{z}) \vee \neg\theta(\boldsymbol{x}, \boldsymbol{z}))}{\exists y^\sigma\, \forall \boldsymbol{x}\, (\forall \boldsymbol{z}\, \theta(\boldsymbol{x}, \boldsymbol{z}) \to \varphi(\boldsymbol{x}, y))} \qquad (3)$$

$$\frac{\forall \boldsymbol{x}\, (\forall \boldsymbol{z}^{\boldsymbol{\rho}}\, \theta(\boldsymbol{x}, \boldsymbol{z}) \to \exists y^\sigma\, \varphi(\boldsymbol{x}, y)) \qquad \forall \boldsymbol{x}\, \forall \boldsymbol{z}^{\boldsymbol{\rho}}\, (\theta(\boldsymbol{x}, \boldsymbol{z}) \vee \neg\theta(\boldsymbol{x}, \boldsymbol{z}))}{\exists y\, \forall \boldsymbol{x}\, (\forall \boldsymbol{z}^{\boldsymbol{\rho}}\, \theta(\boldsymbol{x}, \boldsymbol{z}) \to y \in F_\sigma \wedge \varphi(\boldsymbol{x}, y))} \qquad (4)$$

Same for IZF *and any other theory from Theorem 4.11.*

Proof. For ease of notation, let $\boldsymbol{x}$ and $\boldsymbol{z}$ consist of a single variable x and z respectively.

Again, $\exists y^\sigma\, \varphi(x, y)$ stands for $\forall z\, (\vartheta_\sigma(z) \to \exists y \in z\, \varphi(x, y))$. On the other hand, let $y \in F_\sigma \wedge \varphi(x, y)$ be short for

$$\forall z\, (\vartheta_\sigma(z) \to y \in z \wedge \varphi(x, y)).$$

(1) Use a reflexive pca over $\mathbb{F}$. Now suppose CZF proves $\forall x\, (\neg\psi(x) \to \exists y^\sigma\, \varphi(x, y))$. By soundness, let $\mathbf{e}$ be a closed application term such that CZF proves $\mathbf{e} \Vdash_{tr} \forall x\, (\neg\psi(x) \to \exists y^\sigma\, \varphi(x, y))$. From now one we argue in CZF. It follows from the definition of generic realizability that $\mathbf{e} \Vdash_{tr} \neg\psi(\check{x}) \to \exists y^\sigma\, \varphi(\check{x}, y)$, for every x.

For the sake of argument, suppose that $\mathbf{0} \Vdash_{tr} \neg\psi(\check{x})$. Then $\mathbf{e0} \Vdash_{tr} \exists y^\sigma\, \varphi(\check{x}, y)$. We know that there is a closed application term $\mathbf{f}$ such that $\mathbf{f} \Vdash_{tr} \vartheta_\sigma(\dot{F}_\sigma)$. Then

$$\mathbf{e0f} \Vdash_{tr} \exists y \in \dot{F}_\sigma\, \varphi(\check{x}, y).$$

Therefore $(\mathbf{e0f})_0 \simeq \bar{y}$ for some (unique) $y \in F_\sigma$ and $(\mathbf{e0f})_1 \Vdash_{tr} \varphi(\check{x}, \dot{y})$. From this we conclude $\varphi(x, y)$, since $\check{x}^\circ = x$ and $\dot{y}^\circ = y$.

It is now clear how to find y. Simply, let

$$y = \{u \in \bigcup F_\sigma \mid \exists v \in F_\sigma\, (u \in v \wedge (\mathbf{e0f})_0 \simeq \bar{v})\}.$$

We claim that $\forall x\, (\neg\psi(x) \rightarrow y \in F_\sigma \wedge \varphi(x, y))$. For this it is sufficient to note that $\neg\psi(x)$ implies $\mathbf{0} \Vdash_{tr} \neg\psi(\check{x})$. Note that, as $\dot{F}_\sigma$ is injective, the y satisfying $\varphi(x, y)$ is uniquely determined.

(2) Exercise for the reader. Use a reflexive pca over $\mathbb{F}$.

(3) Exercise for the reader. Apply UZR and UR_σ.

(4) follows from (1).

□

Remark 8.6. The main use of reflexivity above consists in making sure that $\Vdash_{tr} \vartheta_\sigma(\dot{F}_\sigma)$. In general, the argument goes through if for every type σ there is a *functional* $z \in \mathrm{V}_{tr}(A)$ such that $\Vdash_{tr} \vartheta_\sigma(z)$, where by functional we mean that $\langle a, y_1\rangle, \langle a, y_2\rangle \in z^*$ implies $y_1^\circ = y_2^\circ$. In this case, one can let

$$y = \{u \in \bigcup F_\sigma \mid \exists a \in A\, \exists v\, ((\mathbf{e0}f)_0 \simeq a \wedge u \in v^\circ \wedge \langle a, v\rangle \in z^*)\},$$

where $f \Vdash_{tr} \vartheta_\sigma(z)$.

8.4. **Explicit definability.**

Theorem 8.7. CZF *is closed under*

$$\frac{\forall \boldsymbol{x}\, \exists y^\sigma\, \varphi(\boldsymbol{x}, y)}{\exists! y^\sigma\, (\delta(y) \wedge \forall \boldsymbol{x}\, \varphi(\boldsymbol{x}, y))} \quad \textit{for some formula } \delta(y)$$

Same for IZF *and any other theory from Theorem 4.11.*

Proof. Use a definable reflexive pca over $\mathbb{F}$. Note that in such case $\dot{F}_\sigma$ is also definable for every given type σ. An example of a pca over $\mathbb{F}$ definable in CZF is given in the upcoming and final section. □

9. A direct construction in CZF of a reflexive pca over finite types

We first describe the general idea in a classical setting. Recall that $\mathbb{F} = \bigcup \mathbf{F}$ with $\mathbf{F} = \{F_\sigma \mid \sigma \in \Phi\}$. Let function application be given by $fx \simeq y$ iff f is a function, $x \in \mathrm{dom}(f)$ and $f(x) = y$. Since $\mathbb{F}$ is closed under function application, this gives us a partial algebra on $\mathbb{F}$. The idea would be to define a partial application map on the powerset $\mathcal{P}(\mathbb{F})$ and take $x \mapsto \{x\}$ to be the embedding. Unfortunately, the usual constructions on $\mathcal{P}(\mathbb{F})$ do not yield a pca.[9] To solve this, we introduce the notion of arity and work with

[9] We remind the reader of a construction due to van Oosten. Given any pca A, one can define a partial binary operation on $\mathcal{P}(A)$ by letting $XY \simeq Z$ iff $Z = \{ab \mid a \in X \wedge b \in Y\}$ and application is total on $X \times Y$, that is, ab is defined for all $a \in X$ and $b \in Y$. This need not be a pca with combinators $\{\mathbf{k}\}$ and $\{\mathbf{s}\}$. Note that in general $\{\mathbf{s}\}XYZ$ is smaller than $XZ(YZ)$. However, the totality requirement makes it an ordered pca in the sense of van Oosten [45, 1.8]. A similar contruction on $\mathbb{F}$ gives rise to an ordered pca on $\mathcal{P}(\mathbb{F})$, but this fails to be a pca for the same reasons.

nonempty subsets of $\mathbb{F}\times P$, where P is the set of arities. We use arities, that is types of the form $p_0\cdots p_n\to q$, to iterate function application in a prescribed manner. For example, we can assign arity $\sigma\tau\to\rho$ to a function f of type $\sigma\to\tau\to\rho$ and thus see $(f,\sigma\tau\to\rho)$ as a function from $F_\sigma\times F_\tau$ to F_ρ by currying. We then define a partial application map on nonempty subsets of $\mathbb{F}\times P$, so that the resulting partial algebra is a pca that embeds $\mathbb{F}$ via the canonical embedding $x^\sigma\mapsto\{(x,\sigma)\}$. We require the sets to be nonempty so that the combinator $\mathbf{k}$ does its job. However, in order to obtain a reflexive pca, in particular a 'definition by cases' combinator, we also have to enlarge the type structure $\mathbf{F}$ by allowing (enough) dependent products. Formally, this is how we proceed.

Let $\mathbf{G}$ be inductively defined by:

- $\omega\in\mathbf{G}$
- if $F,G\in\mathbf{G}$, then $F\to G\in\mathbf{G}$;
- if $F_n\in\mathbf{G}$ for every $n\in\omega$, then $\prod_{n\in\omega}F_n\in\mathbf{G}$,

where in general

$$\prod_{x\in F}G_x=\{f\colon F\to\bigcup_{x\in F}G_x\mid\forall x\in F\,(f(x)\in G_x)\}.$$

Set $\mathbb{G}=\bigcup\mathbf{G}$. Note that $\mathbb{F}\subseteq\mathbb{G}$. On elements of $\mathbb{G}$ we will always consider function application. We define the set of arities P by the following inductive clauses:

- $o\in P$;
- if $p_0,\dots,p_n,q\in P$ then $p_0\cdots p_n\to q\in P$;
- if $p_n\in P$ for every $n\in\omega$, then $\prod_{n\in\omega}p_n\in P$.

Note that $\Phi\subseteq P$. If $\sigma,\tau\in\Phi$, we denote by $\sigma^n\to\tau\in P$ the arity

$$\overbrace{\sigma\cdots\sigma}^{n+1}\to\tau.$$

Let $\mathbb{G}(P)=\mathbb{G}\times P$. We use $\mathtt{x},\mathtt{y},\mathtt{z},\dots$ to denote elements of $\mathbb{G}(P)$. We define a partial function from $\mathbb{G}(P)\times\mathbb{G}(P)^{<\omega}$ to $\mathbb{G}(P)$ by letting $\mathtt{x}(\vec{\mathtt{y}})\simeq\mathtt{z}$ iff $\mathtt{x}=(x,p)$, $\mathtt{z}=(z,q)$ and either one of the following applies:

(i) $p=p_0\cdots p_n\to q$, $\vec{\mathtt{y}}=\langle(y_i,p_i)\mid i\le n\rangle$, and $xy_0\cdots y_n\simeq z$;
(ii) $n=0$, $p=\prod_{n\in\omega}p_n$, $\vec{\mathtt{y}}=\langle(m,o)\rangle$ for some $m\in\omega$, $p_m=q$ and $xm\simeq z$.

The reader should keep in mind that $xy_0\cdots y_n$ and xm are defined by (iterated) function application. We usually write $\mathtt{x}(\mathtt{y}_0,\dots,\mathtt{y}_n)$ for $\mathtt{x}(\langle\mathtt{y}_0,\dots,\mathtt{y}_n\rangle)$.

Let $\mathbb{G}(P)^*=\mathcal{P}(\mathbb{G}(P))\setminus\{\emptyset\}$. A partial application map on $\mathbb{G}(P)^*$ is then defined by letting $ab\simeq c$ iff

$$c=\{\mathtt{z}\in\mathbb{G}(P)\mid\exists\mathtt{x}\in a\,\exists\mathtt{y}_0,\dots,\mathtt{y}_n\in b\,(\mathtt{x}(\mathtt{y}_0,\dots,\mathtt{y}_n)\simeq\mathtt{z})\}.$$

We now equip $\mathbb{G}(P)^*$ with combinators.

(1) Let us define $\mathbf{k}\in\mathbb{G}(P)^*$. First, for all $F,G\in\mathbf{G}$, let $k_{FG}\colon F\to G\to F$ be the unique function such that $kx^Fy^G=x$. Note that all k's are in $\mathbb{G}$ since $\mathbf{G}$ is closed under exponentiation. Let

$$\mathbf{k}=\{(k_{FG},p\to q\to p)\mid F,G\in\mathbf{G}\wedge p,q\in P\}.$$

(2) We define $\mathbf{s} \in \mathbb{G}(P)^*$ as follows. For any choice of $n, m, n_0, \ldots, n_m \in \omega$ we consider all functions s's in $\mathbb{G}$ such that

$$sxy_0 \cdots y_m z_0 \cdots z_n z_{00} \cdots z_{0n_0} \cdots\cdots z_{n0} \cdots z_{mn_m} =$$
$$= xz_0 \cdots z_n(y_0 z_{00} \cdots z_{0n_0}) \cdots (y_m z_{m0} \cdots z_{mn_m}).$$

We suppress the type information for notational convenience. Note that all s's are in $\mathbb{G}$ since $\mathbf{G}$ is closed under exponentiation. Any such function can be assigned an arity of the form

$$p \to r_0 \cdots r_m \to q_0 \cdots q_n q_{00} \cdots q_{0n_0} \cdots\cdots q_{m0} \cdots q_{mn_m} \to q,$$

where $p = q_0 \cdots q_n \to p_0 \cdots p_m \to q$ and $r_i = q_{i0} \cdots q_{in_i} \to p_i$ for every $i \le m$.

Let

$$\mathbf{s} = S \cup C,$$

where S consists of all pairs (s, r), where s is as above and the arity r agrees with the type of s in the sense just described, and

$$C = \{(\lambda x^F y^G.0^o, p \to q \to o) \mid F, G \in \mathbf{G} \wedge p, q \in P\}.$$

We add C only to ensure that $\mathbf{s}ab\downarrow$ for all a and b.

(3) Numerical combinators are easily definable. Let $\mathbf{succ} = \{(\lambda n.n+1, o \to o)\}$ and $\mathbf{pred} = \{(\lambda n.n-1, o \to o)\}$.

(4) As for $\mathbf{d} \in \mathbb{G}(P)^*$, for all $F, G \in \mathbf{G}$, let $d_{FG} \colon \prod_{n\in\omega}\prod_{m\in\omega} F_{nm}$, where

$$F_{nm} = \begin{cases} F \to G \to F & \text{if } n = m; \\ F \to G \to G & \text{otherwise,} \end{cases}$$

such that

$$d_{FG}nm \simeq \begin{cases} k_{FG} & \text{if } n = m; \\ \bar{k}_{FG} & \text{otherwise.} \end{cases}$$

Here, $\bar{k}_{FG} \colon F \to G \to G$ is defined by $\bar{k}x^F y^G = y$. It is easy to check that for every $F, G \in \mathbf{G}$,

$$\prod_{n\in\omega}\prod_{m\in\omega} F_{nm} \in \mathbf{G},$$

and therefore $d_{FG} \in \mathbb{G}$. Similarly, for all $p, q \in P$, let $(p, q) \in P$ be defined as $\prod_{n\in\omega}\prod_{m\in\omega} p_{nm}$, where

$$p_{nm} = \begin{cases} p \to q \to p & \text{if } n = m; \\ p \to q \to q & \text{otherwise.} \end{cases}$$

Let

$$\mathbf{d} = \{(d_{FG}, (p, q)) \mid F, G \in \mathbf{G} \wedge p, q \in P\}.$$

(5) Combinator $\mathbf{i}_{\sigma\tau} \in \mathbb{G}(P)^*$ for $\sigma, \tau \in \Phi$. Let

$$\mathbf{i}_{\sigma\tau} = \{(i^n_{\sigma\tau}, (\sigma^n \to \tau) \to \sigma \to \tau) \mid n \in \omega\},$$

where $i^n_{\sigma\tau}\colon (\overbrace{F_\sigma \to \cdots \to F_\sigma}^{n+1} \to F_\tau) \to F_\sigma \to F_\tau$ is defined by $i^n_{\sigma\tau} f x = f \overbrace{x \cdots x}^{n+1}$.

One could show in IZF that $\mathbb{G}(P)^*$ is a reflexive pca over $\mathbb{F}$. On the other hand, $\mathbb{G}(P)^*$ is not even a set in CZF. Note that in CZF we could inductively define $\mathbb{G}$ as a class. For our purposes however, a class will not do. It turns out that we just need very few dependent products, as can be easily gleaned from the construction above. Also, we have to settle on the right notion of nonemptiness. But this is easily arranged: we just take inhabited sets (x is inhabited if $\exists u\,(u \in x)$). The construction in CZF proceeds as follows.

First, we can form the set $\mathbf{G} = \bigcup_{s\in\omega} \mathbf{G}_s$, where

- $\mathbf{G}_0 = \{\omega\}$;
- $\mathbf{G}_{s+1} = \mathbf{G}_s \cup \{F \to G \mid F, G \in \mathbf{G}_s\} \cup \{\prod_{n\in\omega} F_s \mid \forall n \in \omega\,(F_n \in \mathbf{G}_s)\}$.

Now, $\omega \in \mathbf{G}$ and $\mathbf{G}$ is closed under exponentiation. Let $\mathbb{G} = \bigcup \mathbf{G}$. It follows that $F_\sigma \in \mathbf{G}$ for every finite type σ, and so $\mathbb{F} \subseteq \mathbb{G}$. In a similar manner, we obtain in CZF a sufficiently large set P of arities. Let $P = \bigcup_{s\in\omega} P_s$, where

- $P_0 = \{o\}$;
- $P_{s+1} = P_s \cup \{p_0 \cdots p_n \to q \mid p_0, \ldots, p_n, q \in P_s\} \cup \{\prod_{n\in\omega} p_n \mid \forall n \in \omega\,(p_n \in P_s)\}$.

We can then form the set $\mathbb{G}(P) = \mathbb{G} \times P$. Finally, unless we work in IZF, where we have access to the full power set, we need to get by with sufficiently (set-)many subsets of $\mathbb{G}(P)$. This is how we can proceed. Consider

$$X = \{\mathbf{k}, \mathbf{s}, \mathbf{d}\} \cup \{\{(x, \sigma)\} \mid \sigma \in \Phi, x \in F_\sigma\} \cup \{\mathbf{i}_{\sigma\tau} \mid \sigma, \tau \in \Phi\}.$$

We can construct the total algebra $\bar{X} \subseteq \mathbb{G}(P)^*$ generated by X under application in $\mathbb{G}(P)^*$. To see this, we define by recursion

$$X_0 = X$$
$$X_{s+1} = X_s \cup \{ab \mid a, b \in X_s\}$$

and set $\bar{X} = \bigcup_{s\in\omega} X_s$. We then let

$$A = \{a \in \bar{X} \mid a \text{ is inhabited}\}.$$

Note that A consists of inhabited subsets of $\mathbb{G}(P)$. Also, for all $a, b \in A$, we have $ab\downarrow$ iff ab is inhabited iff $ab \in A$.

Theorem 9.1 (CZF)**.** *A is a reflexive pca over $\mathbb{F}$ with embedding $x^\sigma \mapsto \bar{x} = \{(x, \sigma)\}$.*

Proof. First, the function $x \mapsto \bar{x}$ from $\mathbb{F}$ to A is given by

$$\{\langle x, (x, \sigma)\rangle \mid x \in F_\sigma \wedge \sigma \in \Phi\}.$$

By induction on the type, one can verify that if $F_\sigma \cap F_\tau$ is inhabited, then $\sigma = \tau$. Therefore the set above is indeed a function. That this map provides an embedding of partial algebras from $\mathbb{F}$ into A is immediate. In fact, if $f \in F_{\sigma\tau}$ and $x \in F_\sigma$, then $(f, \sigma\tau)(x, \sigma) \simeq (f(x), \tau)$.

Let us check the combinators.

(1) Combinator $\mathbf{k}$. Let $a, b \in A$. We have

$$\mathbf{k}ab = \bigcup_{F,G\in\mathbf{G}} \{(k_{FG} x^F y^G, p) \mid (x, p) \in a \wedge \exists q\,((y, q) \in b)\} = a.$$

Use the fact that a and b are inhabited.

(2) Combinator $\mathbf{s}$. Notice that $\mathbf{s}ab\downarrow$ since $(0,o)\in\mathbf{s}ab$. Now, $\mathbf{s}abc$ is designed to contain exactly all elements of $ab(cb)$. The verification that $\mathbf{s}abc\simeq ac(bc)$ is a simple exercise.

(3) The verification that **succ** and **pred** behave as desired is immediate.

(4) Combinator $\mathbf{d}$. It is not difficult to see that

$$\mathbf{d}\bar{n}\bar{m}=\begin{cases}\mathbf{k} & \text{if } n=m;\\ \bar{\mathbf{k}} & \text{otherwise;}\end{cases}$$

where $\bar{\mathbf{k}}=\{(\bar{k}_{FG},p\to q\to q)\mid F,G\in\mathbf{G}\wedge p,q\in P\}$, and $\bar{k}_{FG}=\lambda x^F y^G.y$. Therefore $\mathbf{d}\bar{n}\bar{m}ab\simeq a$ if $n=m$ and b otherwise.

(5) Combinator $\mathbf{i}_{\sigma\tau}$. Let $F=F_\sigma$ and $G=F_\tau$. Suppose that $a\in A$ and that for every $x\in F$ there exists $y\in G$ such that $a\bar{x}\simeq\bar{y}$. We want to show that $\mathbf{i}_{\sigma\tau}a\simeq\bar{f}$, where $f\colon F\to G$ is such that

$$a\bar{x}\simeq\overline{f(x)}\ \text{ for every } x\in F. \tag{$*$}$$

Recall that $\mathbf{i}_{\sigma\tau}=\{(i^n_{\sigma\tau},(\sigma^n\to\tau)\to\sigma\to\tau)\mid n\in\omega\}$. Let us denote by $\mathtt{i}^n_{\sigma\tau}$ the n-th element of $\mathbf{i}_{\sigma\tau}$. Let us also write $F\to^n G$ for

$$\overbrace{F\to\cdots\to F}^{n+1}\to G.$$

Note the difference between the set $F\to^n G$ and the arity $\sigma^n\to\tau$. Recall that

$$i^n_{\sigma\tau}\colon(F\to^n G)\to F\to G.$$

By definition, $\mathbf{i}_{\sigma\tau}a=\{\mathtt{i}^n_{\sigma\tau}(\mathtt{g})\mid n\in\omega\wedge\mathtt{g}\in a\}$.

Let us point out that $\mathbf{G}$ is sparse in the sense that if $F,G\in\mathbf{G}$ have some overlap, meaning that $F\cap G$ is inhabited, then $F=G$. This is proved by induction on $F\in\mathbf{G}$ (i.e., by induction on the stage $n\in\omega$ such that $F\in\mathbf{G}_n$). This feature is crucial here and will be used without further notice.

We start off by proving that $\bar{f}\subseteq\mathbf{i}_{\sigma\tau}a$, that is, $(f,\sigma\tau)\in\mathbf{i}_{\sigma\tau}a$. Pick any $u\in F$. We can do this since every $F\in\mathbf{F}$ is inhabited. By $(*)$, there must be a $\mathtt{g}=(g,p)\in a$ such that

$$\mathtt{g}(\overbrace{(u,\sigma),\cdots,(u,\sigma)}^{n+1})\simeq(f(u),\tau).$$

It is not too difficult to check that $g\colon F^n\to G$ and $\mathtt{g}(\langle(x,\sigma)\mid i\leq n\rangle)\downarrow$ for every $x\in F$. Notice that $p=\sigma^n\to\tau$ or $p=\prod_{m\in\omega}p_m$, in which case $n=0$, $\sigma=o$ and $p_m=\tau$ for every $m\in\omega$. Since $\mathtt{g}(\langle(x,\sigma)\mid i\leq n\rangle)\in a\bar{x}$, it thus follows by $(*)$ that $\mathtt{g}(\langle(x,\sigma)\mid i\leq n\rangle)\simeq(f(x),\tau)$ for every $x\in F$. But then $\mathtt{i}^n_{\sigma\tau}(\mathtt{g})\simeq(f,\sigma\tau)$. This shows one direction.

The other direction $\mathbf{i}_{\sigma\tau}a\subseteq\bar{f}$ is similar. Let $\mathtt{g}=(g,p)\in a$ and suppose that $\mathtt{i}^n_{\sigma\tau}(\mathtt{g})\downarrow$, so that $\mathtt{i}^n_{\sigma\tau}(\mathtt{g})\in\mathbf{i}_{\sigma\tau}a$. Any element of $\mathbf{i}_{\sigma\tau}a$ is obtained this way. By definition, it must be $p=\sigma^n\to\tau$ and $i^n_{\sigma\tau}g\downarrow$. In particular, $g\colon F\to^n G$. It thus follows that for every $x\in F$ there exists $y_x\in G$ such that $\mathtt{g}(\langle(x,\sigma)\mid i\leq n\rangle)\simeq(y_x,\tau)$. On the other hand, for every $x\in F$, $(y_x,\tau)\in a\bar{x}=\overline{f(x)}$, and so $y_x=f(x)$. Therefore $\mathtt{i}^n_{\sigma\tau}(\mathtt{g})\simeq(f,\sigma\tau)$, as desired. $\Box$

References

[1] 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. 4, 6, 7, 8

[2] Haskell Brooks Curry. Grundlagen der kombinatorischen Logik. *American Journal of Mathematics*, 51:363–384, 1930. 8

[3] Solomon Feferman. A language and axioms for explicit mathematics. In *Algebra and logic (Fourteenth Summer Res. Inst., Austral. Math. Soc., Monash Univ., Clayton, 1974)*, pages 87–139. Lecture Notes in Math., Vol. 450. 1975. 7, 8

[4] Solomon Feferman. Constructive theories of functions and classes. In *Logic Colloquium '78*, Stud. Logic Found. Math., pages 159–224. North-Holland, Amsterdam, 1979. 7, 8

[5] Peter Freyd. On proving that 1 is an indecomposable projective in various free categories (manuscript). 1978. 4

[6] Harvey Friedman. Some applications of Kleene's methods for intuitionistic systems. In *Cambridge summer school in mathematical logic*, pages 113–170. Springer, 1973. 2, 4, 5

[7] Harvey Friedman and Andrej Ščedrov. The lack of definable witnesses and provably recursive functions in intuitionistic set theory. *Advances in Mathematics*, 57:1–13, 1985. 2, 5

[8] Jean-Yves Girard. Une extension de l'interprétation de Gödel à l'analyse, et son application à l'élimination des coupures dans l'analyse et la théorie des types. In *Proceedings of the Second Scandinavian Logic Symposium (Univ. Oslo, Oslo, 1970)*, pages 63–92. Studies in Logic and the Foundations of Mathematics, Vol. 63, 1971. 4

[9] Jean-Yves Girard. Quelques résultats sur les interprétations fonctionnelles. In *Cambridge Summer School in Mathematical Logic (Cambridge, England, 1971)*, pages 232–252. Lecture Notes in Math., Vol. 337. 1973. 4

[10] Susumu Hayashi. Some derived rules of intuitionistic second order arithmetic. *Proc. Japan Acad.*, 53(3):110–112, 1977. 4

[11] Susumu Hayashi. Existence property by means of a normalization method. *Comment. Math. Univ. St. Paul.*, 27(2):97–100, 1978/79. 4

[12] Susumu Hayashi. Derived rules related to a constructive theory of metric spaces in intuitionistic higher order arithmetic without countable choice. *Ann. Math. Logic*, 19(1-2):33–65, 1980. 4

[13] Stephen C. Kleene. On the interpretation of intuitionistic number theory. *J. Symbolic Logic*, 10:109–124, 1945. 4

[14] Stephen C. Kleene. Disjunction and existence under implication in elementary intuitionistic formalisms. *J. Symbolic Logic*, 27:11–18, 1962. 4

[15] Stephen C. Kleene. *Formalized recursive functionals and formalized realizability.* Memoirs of the American Mathematical Society, No. 89. American Mathematical Society, Providence, R.I., 1969. 4

[16] Ulrich Kohlenbach. *Applied proof theory: proof interpretations and their use in mathematics.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2008. 1, 2

[17] Georg Kreisel and Anne S. Troelstra. Formal systems for some branches of intuitionistic analysis. *Annals of Mathematical Logic*, 1:229–387, 1970. 4

[18] Joachim Lambek and Philip J. Scott. Intuitionist type theory and the free topos. *J. Pure Appl. Algebra*, 19:215–257, 1980. 4

[19] Joachim Lambek and Philip J. Scott. Independence of premisses and the free topos. In *Constructive mathematics (Las Cruces, N.M., 1980)*, volume 873 of *Lecture Notes in Math.*, pages 191–207. Springer, Berlin-New York, 1981. 4

[20] Joachim Lambek and Philip J. Scott. New proofs of some intuitionistic principles. *Z. Math. Logik Grundlag. Math.*, 29(6):493–504, 1983. 4

[21] Joachim Lambek and Philip J. Scott. *Introduction to higher order categorical logic*, volume 7 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, 1986. 4

[22] R.S. Lubarsky. CZF and second order arithmetic. *Ann. Pure Appl. Logic*, 141(1–2):29–34, 2006. 4

[23] David Charles McCarty. *Realizability and recursive mathematics*. Thesis (Ph.D.)–The University of Edinburgh, 1985. 4

[24] David Charles McCarty. Realizability and recursive set theory. *Ann. Pure Appl. Logic*, 32(2):153–183, 1986. 4

[25] Ieke Moerdijk. Glueing topoi and higher-order disjunction and existence. In *The L.E.J. Brouwer Centenary Symposium (Noordwijkerhout, 1981)*, volume 110 of *Studies in Logic and the Foundations of Mathematics*, pages 359–375. North-Holland, Amsterdam-New York, 1982. 4

[26] Joan R. Moschovakis. Disjunction and existence in formalized intuitionistic analysis. In *Sets, Models and Recursion Theory (Proc. Summer School Math. Logic and Tenth Logic Colloq., Leicester, 1965)*, pages 309–331. North-Holland, Amsterdam, 1967. 4

[27] John Myhill. Some properties of intuitionistic Zermelo-Frankel set theory. In *Cambridge Summer School in Mathematical Logic (1971)*, pages 206–231. Lecture Notes in Math., Vol. 337. 1973. 2, 4, 6

[28] John Myhill. Constructive set theory. *J. Symbolic Logic*, 40(3):347–382, 1975. 4, 5

[29] Dag Prawitz. Some results for intuitionistic logic with second order quantification rules. In *Intuitionism and Proof Theory (Proc. Conf., Buffalo, N.Y., 1968)*, pages 259–269. North-Holland, Amsterdam, 1970. 4

[30] Dag Prawitz. Ideas and results in proof theory. In *Proceedings of the Second Scandinavian Logic Symposium (Univ. Oslo, Oslo, 1970)*, pages 235–307. Studies in Logic and the Foundations of Mathematics, Vol. 63, 1971. 4

[31] M. Rathjen. Constructive Zermelo-Fraenkel Set Theory, Power Set, and the Calculus of Constructions. In P. Dybjer, S. Lindström, E. Palmgren, and G. Sundholm, editors, *Epistemology versus Ontology: Essays on the Philosophy and Foundations of Mathematics in Honour of Per Martin-Löf*, volume 27 of *Logic, Epistemology, and the Unity of Science*, pages 313–349. Cambridge University Press, 2012. 4

[32] M. Rathjen. Relativized ordinal analysis: The case of power Kripke-Platek set theory. *Annals of Pure and Applied Logic*, 165:316–339, 2014. 4

[33] M. Rathjen. Ordinal analysis and the set existence property for intuitionistic set theories. *Royal Society, Philosophical Transactions A*, 381: 20220019:20 pages, 2023. 3

[34] Michael Rathjen. The disjunction and related properties for constructive Zermelo-Fraenkel set theory. *J. Symbolic Logic*, 70(4):1232–1254, 2005. 2, 3, 4, 8, 9, 10, 12, 15

[35] 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. 4, 9

[36] Michael Rathjen. Metamathematical properties of intuitionistic set theories with choice principles. In *New computational paradigms*, pages 287–312. Springer, New York, 2008. 2, 10

[37] Bruno Scarpellini. On cut elimination in intuitionistic systems of analysis. In *Intuitionism and Proof Theory (Proc. Conf., Buffalo, N.Y., 1968)*, pages 271–285. North-Holland, Amsterdam, 1970. 4

[38] Bruno Scarpellini. *Proof theory and intuitionistic systems*. Lecture Notes in Mathematics, Vol. 212. Springer-Verlag, Berlin-New York., 1971. 4

[39] Moses Schönfinkel. Über die Bausteine der mathematischen Logik. *Mathematische Annalen*, 92:305–316, 1924. 8

[40] Andrew W. Swan. CZF does not have the existence property. *Ann. Pure Appl. Logic*, 165(5):1115–1147, 2014. 2, 5

[41] Anne S. Troelstra. *Metamathematical investigation of intuitionistic arithmetic and analysis*. Lecture Notes in Mathematics, Vol. 344. Springer-Verlag, Berlin, 1973. 1, 2, 3

[42] Anne S. Troelstra. Notes on intuitionistic second order arithmetic. In *Cambridge Summer School in Mathematical Logic (Cambridge, 1971)*, pages 171–205. Lecture Notes in Math., Vol. 337. 1973. 2, 4

[43] Anne S. Troelstra. Realizability. In *Handbook of proof theory*, volume 137 of *Stud. Logic Found. Math.*, pages 407–473. North-Holland, Amsterdam, 1998. 1, 2, 4

[44] Anne S. Troelstra and Dirk van Dalen. *Constructivism in Mathematics, volumes I and II*, volume 123 of *Studies in Logic and the Foundations of Mathematics*. Elsevier B. V., Amsterdam, 1988. 3, 4, 8

[45] Jaap van Oosten. *Realizability: an introduction to its categorical side*, volume 152 of *Studies in Logic and Foundations of Mathematics*. Elsevier, 2008. 7, 17

[46] Andrej Ščedrov and Philip J. Scott. A note on the Friedman slash and Freyd covers. In *The L. E. J. Brouwer Centenary Symposium (Noordwijkerhout, 1981)*, volume 110 of *Stud. Logic Found. Math.*, pages 443–452. North-Holland, Amsterdam, 1982. 4, 5

Department of Mathematics, Technische Universität Darmstadt, Germany
Email address: frittaion@mathematik.tu-darmstadt.de

Department of Architectural Design, Faculty of Environmental Study, Hiroshima Institute of Technology, 2-1-1 Miyake, Saeki-ku, Hiroshima 731-5193, Japan
Email address: t.nemoto.35@it-hiroshima.ac.jp, nemototakako@gmail.com

Department of Pure Mathematics, University of Leeds, UK
Email address: M.Rathjen@leeds.ac.uk