Metamathematical Properties of Intuitionistic Set Theories with Choice Principles

Michael Rathjen*
Department of Mathematics, Ohio State University
Columbus, OH 43210, U.S.A.
rathjen@math.ohio-state.edu

Abstract

This paper is concerned with metamathematical properties of intuitionistic set theories with choice principles. It is proved that the *disjunction property*, the *numerical existence property*, *Church's rule*, and several other metamathematical properties hold true for Constructive Zermelo-Fraenkel Set Theory and full Intuitionistic Zermelo-Fraenkel augmented by any combination of the principles of Countable Choice, Dependent Choices and the Presentation Axiom. Also Markov's principle may be added. Moreover, these properties hold effectively. For instance from a proof of a statement $\forall n \in \omega\, \exists m \in \omega\, \varphi(n, m)$ one can effectively construct an index e of a recursive function such that $\forall n \in \omega\, \varphi(n, \{e\}(n))$ is provable. Thus we have an explicit method of witness and program extraction from proofs involving choice principles.

As for the proof technique, this paper is a continuation of [32]. [32] introduced a self-validating semantics for **CZF** that combines realizability for extensional set theory and truth.

MSC:03F50, 03F35

Keywords: Constructive set theory, intuitionistic set theory, realizability, metamathematical property

1 Introduction

The objective of this paper is to investigate several metamathematical properties of Constructive Constructive Zermelo-Fraenkel Set Theory, **CZF**, and Intuitionistic Zermelo-Fraenkel Set theory, **IZF**, augmented by choice principles, and to provide an explicit method for extracting computational information from proofs of such theories.

IZF and **CZF** have the same language as **ZF**. Both theories are based on intuitionistic logic. While **IZF** is squarely built on the idea of basing Zermelo-Fraenkel set theory on intuitionistic logic, **CZF** is a standard reference theory for developing constructive predicative mathematics (cf. [1, 2, 3, 4]).

The axioms of **IZF** comprise Extensionality, Pairing, Union, Infinity, Separation, and Powerset. Instead of Replacement **IZF** has Collection

$$\forall x \in a\, \exists y\, \varphi(x, y) \rightarrow \exists z\, \forall x \in a\, \exists y \in z\, \varphi(x, y)$$

and rather than Foundation it has the Set Induction scheme

$$\forall x\, [\forall y \in x\, \psi(y) \rightarrow \psi(x)] \rightarrow \forall x\, \psi(x).$$

*This material is based upon work supported by the National Science Foundation under Award No. DMS-0301162.

The set theoretic axioms of **CZF** are Extensionality, Pairing, Union, Infinity, the Set Induction scheme, and the following:
Restricted Separation scheme $\forall a\,\exists x\,\forall y\ (y \in x \leftrightarrow y \in a \wedge \varphi(y))$, for every *restricted* formula $\varphi(y)$, where a formula $\varphi(x)$ is restricted, or Δ_0, if all the quantifiers occurring in it are restricted, i.e. of the form $\forall x{\in}b$ or $\exists x{\in}b$;
Subset Collection scheme

$$\forall a\,\forall b\,\exists c\,\forall u\,[\forall x{\in}a\,\exists y{\in}b\,\psi(x,y,u) \rightarrow \\ \exists d{\in}c\,(\forall x{\in}a\,\exists y{\in}d\,\psi(x,y,u) \wedge \forall y{\in}d\,\exists x{\in}a\,\psi(x,y,u))]$$

Strong Collection scheme

$$\forall x{\in}a\,\exists y\,\varphi(x,y) \rightarrow \exists b\ [\forall x{\in}a\,\exists y{\in}b\,\varphi(x,y) \wedge \forall y{\in}b\,\exists x{\in}a\,\varphi(x,y)]$$

for all formulae $\psi(x,y,u)$ and $\varphi(x,y)$.

There are well-known metamathematical properties such as the disjunction and the numerical existence property that are often considered to be hallmarks of intuitionistic theories. The next definition gives a list of the well-known and some of the lesser-known metamathematical properties that intuitionistic theories may or may not have.

Definition 1.1 Let T be a theory whose language, $L(T)$, encompasses the language of set theory. Moreover, for simplicity, we shall assume that $L(T)$ has a constant ω denoting the set of von Neumann natural numbers and for each n a constant $\bar{n}$ denoting the n-th element of ω.[1]

1. T has the *disjunction property*, **DP**, if whenever $T \vdash \psi \vee \theta$ holds for sentences ψ and θ of T, then $T \vdash \psi$ or $T \vdash \theta$.

2. T has the *numerical existence property*, **NEP**, if whenever $T \vdash (\exists x{\in}\omega)\phi(x)$ holds for a formula $\phi(x)$ with at most the free variable x, then $T \vdash \phi(\bar{n})$ for some n.

3. T has the *existence property*, **EP**, if whenever $T \vdash \exists x\phi(x)$ holds for a formula $\phi(x)$ having at most the free variable x, then there is a formula $\vartheta(x)$ with exactly x free, so that

$$T \vdash \exists! x\,[\vartheta(x) \wedge \phi(x)].$$

4. T has the *weak existence property*, **wEP**, if whenever

$$T \vdash \exists x\phi(x)$$

holds for a formula $\phi(x)$ having at most the free variable x, then there is a formula $\vartheta(x)$ with exactly x free, so that

$$\begin{aligned} T &\vdash \exists! x\,\vartheta(x), \\ T &\vdash \forall x\,[\vartheta(x) \rightarrow \exists u\, u \in x], \\ T &\vdash \forall x\,[\vartheta(x) \rightarrow \forall u \in x\,\phi(x)]. \end{aligned}$$

[1]The usual language of set theory does not have numerals, strictly speaking. Instead of adding numerals to the language one could take $\varphi(\bar{n})$ to mean $\exists x\,[\eta_n(x) \wedge \varphi(x)]$, where η_n is a formula defining the natural number n in a canonical way.

5. T is closed under *Church's rule*, **CR**, if whenever $T \vdash (\forall x\in \omega)(\exists y\in\omega)\phi(x,y)$ holds for some formula of T with at most the free variables shown, then, for some number e,

$$T \vdash (\forall x\in\omega)\phi(x, \{\bar{e}\}(x)),$$

   where $\{e\}(x)$ stands for the result of applying the e-th partial recursive function to x.

6. T is closed under the *Extended Church's rule*, **ECR**, if whenever

$$T \vdash (\forall x\in \omega)[\neg\psi(x) \rightarrow (\exists y\in\omega)\phi(x,y)]$$

   holds for formulae of T with at most the free variables shown, then, for some number e,

$$T \vdash (\forall x\in\omega)[\neg\psi(x) \rightarrow \{\bar{e}\}(x) \in \omega \wedge \phi(x, \{\bar{e}\}(x))].$$

   Note that $\neg\psi(x)$ could be replaced by any formula which is provably equivalent in T to its double negation. This comprises arithmetic formulae that are both $\vee$-free and $\exists$-free.

7. Let $f : \omega \rightarrow \omega$ convey that f is a function from ω to ω. T is closed under the variant of *Church's rule*, $\mathbf{CR_1}$, if whenever $T \vdash \exists f\,[f : \omega \rightarrow \omega \wedge \psi(f)]$ (with $\psi(f)$ having no variables but f), then, for some number e, $T \vdash (\forall x \in \omega)(\exists y \in \omega)(\{\bar{e}\}(x) = y) \wedge \psi(\{\bar{e}\})$.

8. T is closed under the *Unzerlegbarkeits rule*, **UZR**, if whenever $T \vdash \forall x[\psi(x) \vee \neg\psi(x)]$, then

$$T \vdash \forall x\,\psi(x) \quad \text{or} \quad T \vdash \forall x\,\neg\psi(x).$$

9. T is closed under the *Uniformity rule*, **UR**, if whenever $T \vdash \forall x\,(\exists y \in \omega)\psi(x,y)$, then

$$T \vdash (\exists y \in \omega)\,\forall x\,\psi(x,y).$$

Slightly abusing terminology, we shall also say that T enjoys any of these properties if this, strictly speaking, holds only for a definitional extension of T.

Actually, **DP** follows easily from **NEP**, and conversely, **DP** implies **NEP** for systems containing a modicum of arithmetic (see [13]).

Also note that **ECR** entails **CR**, taking $\psi(x)$ to be $x \neq x$.

A detailed historical account of metamathematical properties of intuitionistic set theories can be found in [32]. However, for the reader's convenience we will quote from the preface to [32]:

"Realizability semantics are of paramount importance in the study of intuitionistic theories. They were first proposed by Kleene [17] in 1945. It appears that the first realizability definition for set theory was given by Tharp [33] who used (indices of) Σ_1 definable partial (class) functions as realizers. This form of realizability is a straightforward extension of Kleene's 1945 realizability for numbers in that a realizer for a universally quantified statement $\forall x\phi(x)$ is an index e of a Σ_1 partial function such that $\{e\}(x)$ is a realizer for $\phi(x)$ for all sets x. In the same vein, e realizes $\exists x\phi(x)$ if e is a pair $\langle a, e'\rangle$ with e' being a realizer for $\phi(a)$. A markedly different strand of realizability originates with Kreisel's and Troelstra's [21] 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. On the intuitionistic view, the only way to arrive at the truth of a statement $\forall X \phi(X)$ is a proof. A collection of objects may be called generic if no member of it has an intensional aspect that can make any difference to a proof.

Kreisel-Troelstra realizability was applied to systems of higher order arithmetic and set theory by Friedman [12]. A realizability-notion akin to Kleene's slash [18, 19] was extended to various intuitionistic set theories by Myhill [26, 27]. [26] showed that intuitionistic **ZF** with Replacement instead of Collection (dubbed $\mathbf{IZF}_R$ henceforth) has the **DP**, **NEP**, and **EP**. [27] proved that the constructive set theory **CST** enjoys the **DP** and the **NEP**, and that the theory without the axioms of countable and dependent choice, $\mathbf{CST}^-$, also has the **EP**. It was left open in [27] whether the full existence property holds in the presence of relativized dependent choice, **RDC**. Friedman and Ščedrov [15] then established that $\mathbf{IZF}_R + \mathbf{RDC}$ satisfies the **EP** also. The Myhill-Friedman approach [26, 27] proceeds in two steps. The first, which appears to make the whole procedure non effective, consists in finding a conservative extension T' of the given theory T which contains names for all the objects asserted to exist in T. T' is obtained by inductively adding names and defining an increasing sequence of theories T_α through all the countable ordinals $\alpha < \omega_1$ and letting $T' = \bigcup_{\alpha<\omega_1} T_\alpha$.[2] The second step consists in defining a notion of realizablity for T' which is a variant of Kleene's "slash".

Several systems of set theory for the constructive mathematical practice were propounded by Friedman in [14]. The metamathematical properties of these theories and several others as well were subsequently investigated by Beeson [5, 6]. In particular, Beeson showed that **IZF** has the **DP** and **NEP**. He used a combination of Kreisel-Troelstra realizability and Kleene's [17, 18, 19, 20] q-realizability. However, while Myhill and Friedman developed realizablity directly for extensional set theories, Beeson engineered his realizability for non-extensional set theories and obtained results for the extensional set theories of [14] only via an interpretation in their non-extensional counterparts. This detour had the disadvantage that in many cases (where the theory does not have full Separation or Powerset) the **DP** and **NEP** for the corresponding extensional set theory T-ext could only be established for a restricted class of formulas; [5] Theorem 5.2 proves that **NEP** holds for T-ext when $T\text{-}ext \vdash (\exists x \in \omega)(x \in Q)$, where Q is a definable set of T. It appears unlikely that the Myhill-Friedman techniques or Beeson's detour through q-realizability for non-extensional set theories can be employed to yield the **DP** and **NEP** for **CZF**. The theories considered by Myhill and Friedman have Replacement instead of Collection and, in all probability, their approach is limited to such theories, whereas Beeson's techniques yield numerical explicit definability, not for all formulae $\varphi(u)$, but only for $\varphi(u)$ of the form $u \in Q$, where Q is a specific definable set. But there was another approach available. McCarty [23, 24] adapted Kreisel-Troelstra realizability directly to extensional set theories. [23, 24], though, were concerned with realizability for intuitionistic Zermelo-Fraenkel set theory (having Collection instead of Replacement), **IZF**, and employed transfinite iterations of the powerset operation through all the ordinals in defining a realizability (class) structure. Moreover, in addition to the powerset axiom this approach also availed itself of unfettered separation axioms. At first blush, this seemed to render the approach unworkable for **CZF** as this theory lacks the powerset axiom and has only bounded separation. Notwithstanding that, it was shown in [29] that these obstacles can be overcome. Indeed, this notion of realizability provides a self-validating semantics for **CZF**, viz. it can be formalized in **CZF** and demonstrably in **CZF** it can be verified that every theorem of **CZF** is realized." ([32], pp. 1234-1236)

The paper [32] introduced a new realizability structure $\mathtt{V}^*$, which arises by amalgamating the realizability structure with the universe of sets in a coherent, albeit rather complicated way. The main semantical notion presented and utilized in [32] combines realizability for extensional set

[2] This type of construction is due to J.R. Moschovakis [25] §8&9.

theory over $\mathtt{V}^*$ with truth in the background universe V. A combination of realizability with truth has previously been considered in the context of realizability notions for first and higher order arithmetic. It was called rnt-realizability in [34]. The main metamathematical result obtained via this tool were the following.

Theorem 1.2 *The* **DP** *and the* **NEP** *hold true for* **CZF** *and* **CZF** + **REA**. *Both theories are closed under* **CR**, **ECR**, $\mathbf{CR_1}$, **UZR**, *and* **UR**, *too.*

Proof: [32], Theorem 1.2. □

In the present paper presents another proof of Beeson's result that **IZF** has the **DP** and the **NEP** and a proof that **IZF** is closed under **CR**, **ECR**, $\mathbf{CR_1}$, **UZR**, and **UR**. There are a number of further metamathematical results that can be obtained via this technology. For example, it will be shown that Markov's principle can be added to any of the foregoing theories. But the main bulk of this paper is devoted to showing that the technology is particularly suited to the choice principles of Countable Choice, Dependent Choices and the Presentation Axiom. In consequence of that we are able to deduce that **CZF** augmented by any combination of these principles also has the properties stated in Theorem 1.2. The same holds for **IZF**.

2 Choice principles

In many a text on constructive mathematics, axioms of countable choice and dependent choices are accepted as constructive principles. This is, for instance, the case in Bishop's constructive mathematics (cf. [8]) as well as Brouwer's intuitionistic analysis (cf. [35], Chap. 4, Sect. 2). Myhill also incorporated these axioms in his constructive set theory [27].

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

Let xRy stand for $\langle x, y\rangle \in R$. A mathematically very useful axiom to have in set theory is the **Dependent Choices Axiom**, **DC**, i.e., for all sets a and (set) relations $R \subseteq a \times a$, whenever

$$(\forall x{\in}a)\,(\exists y{\in}a)\,xRy$$

and $b_0 \in a$, then there exists a function $f : \omega \to a$ such that $f(0) = b_0$ and

$$(\forall n \in \omega)\, f(n)Rf(n+1).$$

Even more useful in constructive set theory is the *Relativized Dependent Choices Axiom*, **RDC**. It asserts that for arbitrary formulae ϕ and ψ, whenever

$$\forall x[\phi(x) \;\to\; \exists y(\phi(y) \;\wedge\; \psi(x,y))]$$

and $\phi(b_0)$, then there exists a function f with domain ω such that $f(0) = b_0$ and

$$(\forall n \in \omega)[\phi(f(n)) \;\wedge\; \psi(f(n), f(n+1))].$$

Let $\mathbf{CZF}^-$ be **CZF** without Subset Collection.

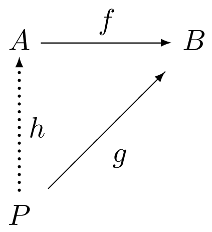
Proposition 2.1 *Provably in* $\mathbf{CZF}^-$ *the following hold:*

(i) **DC** *implies* $\mathbf{AC}_\omega$.

(ii) **RDC** *implies* **DC**.

Proof: This is a well known fact. □

The *Presentation Axiom*, **PAx**, is an example of a choice principle which is validated upon interpretation in type theory. In category theory it is also known as the *existence of enough projective sets*, **EPsets** (cf. [7]). In a category $\mathbb{C}$, an object P in $\mathbb{C}$ is *projective* (in $\mathbb{C}$) if for all objects A, B in $\mathbb{C}$, and morphisms $A \xrightarrow{f} B$, $P \xrightarrow{g} B$ with f an epimorphism, there exists a morphism $P \xrightarrow{h} A$ such that the following diagram commutes



It easily follows that in the category of sets, a set P is projective if for any P-indexed family $(X_a)_{a \in P}$ of inhabited sets X_a, there exists a function f with domain P such that, for all $a \in P$, $f(a) \in X_a$.

PAx (or **EPsets**), is the statement that every set is the surjective image of a projective set.

Alternatively, projective sets have also been called *bases*, and we shall follow that usage henceforth. In this terminology, $\mathbf{AC}_\omega$ expresses that ω is a base whereas **AC** amounts to saying that every set is a base.

Proposition 2.2 ($\mathbf{CZF}^-$) **PAx** *implies* **DC**.

Proof: See [1] or [7], Theorem 6.2. □

The implications of Propositions 2.1 and 2.2 cannot be reversed, not even on the basis of **ZF**.

Proposition 2.3 $\mathbf{ZF} + \mathbf{DC}$ *does not prove* **PAx**.

Proof: See [30] Proposition 5.2. □

3 The partial combinatory algebra Kl

In order to define a realizability interpretation we must have a notion of realizing functions on 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*. These structures are best described as the models of a theory **APP** (cf. [10, 11, 6, 35]). The language of **APP** is a first-order language with a ternary relation symbol App, a unary relation symbol N (for a copy of the natural numbers) and equality, $=$, as primitives. The language has an infinite collection of variables, denoted $x, y, z, \ldots$, and nine distinguished constants: $\mathbf{0}, \mathbf{s}_N, \mathbf{p}_N, \mathbf{k}, \mathbf{s}, \mathbf{d}, \mathbf{p}, \mathbf{p_0}, \mathbf{p_1}$ for, respectively, zero, successor on N, predecessor on N, the two basic combinators, definition by cases, pairing and the corresponding two projections. There is no arity associated with the various constants. The *terms* of **APP** are just the variables and constants. We write $t_1t_2 \simeq t_3$ for $\mathrm{App}(t_1, t_2, t_3)$.

Formulae are then generated from atomic formulae using the propositional connectives and the quantifiers.

In order to facilitate the formulation of the axioms, the language of **APP** is expanded definitionally with the symbol $\simeq$ and the auxiliary notion of an *application term* is introduced. The set of application terms is given by two clauses:

1. all terms of **APP** are application terms; and
2. if s and t are application terms, then (st) is an application term.

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

$$s \simeq t \quad := \quad \forall y(s \simeq y \leftrightarrow t \simeq y),$$

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

$$s \simeq a \quad \text{is} \quad \begin{cases} s = a, & \text{if } s \text{ is a term of } \mathbf{APP}, \\ \exists x, y[s_1 \simeq x \wedge s_2 \simeq y \wedge \mathrm{App}(x, y, a)] & \text{if } s \text{ is of the form } (s_1s_2). \end{cases}$$

Some abbreviations are $t_1t_2 \dots t_n$ for $((...(t_1t_2)...)t_n)$; $t\downarrow$ for $\exists y(t \simeq y)$ and $\phi(t)$ for $\exists y(t \simeq y \wedge \phi(y))$.

Some further conventions are useful. Systematic notation for *n-tuples* is introduced as follows: (t) is t, (s, t) is $\mathbf{p}st$, and $(t_1, \dots, t_n)$ is defined by $((t_1, \dots, t_{n-1}), t_n)$. In this paper, the **logic** of **APP** is assumed to be that of intuitionistic predicate logic with identity. **APP**'s **non-logical axioms** are the following:

Applicative Axioms

1. $\mathrm{App}(a, b, c_1) \wedge \mathrm{App}(a, b, c_2) \rightarrow c_1 = c_2$.
2. $(\mathbf{k}ab)\downarrow \wedge \mathbf{k}ab \simeq a$.
3. $(\mathbf{s}ab)\downarrow \wedge \mathbf{s}abc \simeq ac(bc)$.
4. $(\mathbf{p}a_0a_1)\downarrow \wedge (\mathbf{p_0}a)\downarrow \wedge (\mathbf{p_1}a)\downarrow \wedge \mathbf{p_i}(\mathbf{p}a_0a_1) \simeq a_i$ for $i = 0, 1$.
5. $N(c_1) \wedge N(c_2) \wedge c_1 = c_2 \rightarrow \mathbf{d}abc_1c_2\downarrow \wedge \mathbf{d}abc_1c_2 \simeq a$.
6. $N(c_1) \wedge N(c_2) \wedge c_1 \neq c_2 \rightarrow \mathbf{d}abc_1c_2\downarrow \wedge \mathbf{d}abc_1c_2 \simeq b$.
7. $\forall x\,(N(x) \rightarrow [\mathbf{s}_Nx\downarrow \wedge \mathbf{s}_Nx \neq \mathbf{0} \wedge N(\mathbf{s}_Nx)])$.
8. $N(\mathbf{0}) \wedge \forall x\,(N(x) \wedge x \neq \mathbf{0} \rightarrow [\mathbf{p}_Nx\downarrow \wedge \mathbf{s}_N(\mathbf{p}_Nx) = x])$.
9. $\forall x\,[N(x) \rightarrow \mathbf{p}_N(\mathbf{s}_Nx) = x]$
10. $\varphi(\mathbf{0}) \wedge \forall x[N(x) \wedge \varphi(x) \rightarrow \varphi(\mathbf{s}_Nx)] \rightarrow \forall x[N(x) \rightarrow \varphi(x)]$.

Let $\mathbf{1} := \mathbf{s}_N\,\mathbf{0}$. The applicative axioms entail that $\mathbf{1}$ is an application term that evaluates to an object falling under N but distinct from $\mathbf{0}$, i.e., $\mathbf{1}\downarrow$, $N(\mathbf{1})$ and $\mathbf{0} \neq \mathbf{1}$.

Employing the axioms for the combinators $\mathbf{k}$ and $\mathbf{s}$ one can deduce an abstraction lemma yielding λ-terms of one argument. This can be generalized using n–tuples and projections.

Lemma 3.1 (cf. [10]) (**Abstraction Lemma**) *For each application term t there is a new application term t^* such that the parameters of t^* are among the parameters of t minus $x_1, \ldots, x_n$ and such that*

$$\mathbf{APP} \vdash t^* \downarrow \;\wedge\; t^* x_1 \ldots x_n \simeq t.$$

$\lambda(x_1, \ldots, x_n).t$ is written for t^*.

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. [10], [11], [6], VI.2.7). Actually, one can prove a uniform version of the following in **APP**.

Corollary 3.2 **(Recursion Theorem)**

$$\forall f \exists g \forall x_1 \ldots \forall x_n \, g(x_1, \ldots, x_n) \simeq f(g, x_1, \ldots, x_n).$$

The "standard" applicative structure is **Kl** in which the universe $|\mathbf{Kl}|$ is ω and $\mathrm{App}^{\mathbf{Kl}}(x, y, z)$ is Turing machine application:

$$\mathrm{App}^{\mathbf{Kl}}(x, y, z) \quad \text{iff} \quad \{x\}(y) \simeq z.$$

The primitive constants of **APP** are interpreted over $|\mathbf{Kl}|$ in the obvious way. Thus there are nine distinguished elements $\mathbf{0}^{Kl}, \mathbf{s}_N^{Kl}, \mathbf{p}_N^{Kl}, \mathbf{k}^{Kl}, \mathbf{s}^{Kl}, \mathbf{d}^{Kl}, \mathbf{p}^{Kl}, \mathbf{p_0}^{Kl}, \mathbf{p_1}^{Kl}$ of ω pertaining to the axioms of **APP**. For details see [23], chap.3, sec.2 or [6], VI.2.7. In the following we will be solely concerned with the standard applicative structure **Kl**. We will also be assuming that the notion of an applicative structure and in particular the structure **Kl** have been formalized in **CZF**, and that **CZF** proves that **Kl** is a model of **APP**. We will usually drop the superscript "^{Kl}" when referring to any of the special constants of **Kl**.

4 The general realizability structure

If a is an ordered pair, i.e., $a = \langle x, y \rangle$ for some sets x, y, then we use $1^{st}(a)$ and $2^{nd}(a)$ to denote the first and second projection of a, respectively; that is, $1^{st}(a) = x$ and $2^{nd}(a) = y$. For a class X we denote by $\mathcal{P}(X)$ the class of all sets y such that $y \subseteq X$.

Definition 4.1 Ordinals are transitive sets whose elements are transitive also. As per usual, we use lower case Greek letters to range over ordinals.

$$\begin{aligned}
\mathtt{V}^*_\alpha &= \bigcup_{\beta\in\alpha} \{\langle a, b\rangle : \; a \in \mathtt{V}_\beta; \; b \subseteq \omega \times \mathtt{V}^*_\beta; \; (\forall x \in b)\, 1^{st}(2^{nd}(x)) \in a\} && (1)\\
\mathtt{V}_\alpha &= \bigcup_{\beta\in\alpha} \mathcal{P}(\mathtt{V}_\beta)\\
\mathtt{V}^* &= \bigcup_{\alpha} \mathtt{V}^*_\alpha\\
\mathtt{V} &= \bigcup_{\alpha} \mathtt{V}_\alpha.
\end{aligned}$$

As the power set operation is not available in **CZF** it is not clear whether the classes $\mathtt{V}$ and $\mathtt{V}^*$ can be formalized in **CZF**. However, employing the fact that **CZF** accommodates inductively defined classes this can be demonstrated in the same vein as in [29], Lemma 3.4.

The definition of $\mathtt{V}^*_\alpha$ in (1) is perhaps a bit involved. Note first that all the elements of $\mathtt{V}^*$ are ordered pairs $\langle a, b\rangle$ such that $b \subseteq \omega \times \mathtt{V}^*$. For an ordered pair $\langle a, b\rangle$ to enter $\mathtt{V}^*_\alpha$ the first conditions to be met are that $a \in \mathtt{V}_\beta$ and $b \subseteq \omega \times \mathtt{V}^*_\beta$ for some $\beta \in \alpha$. Furthermore, it is required that a contains enough elements from the transitive closure of b in that whenever $\langle e, c\rangle \in b$ then $1^{st}(c) \in a$.

Lemma 4.2 (**CZF**).

(i) $\mathtt{V}$ and $\mathtt{V}^*$ *are cumulative: for* $\beta \in \alpha$, $\mathtt{V}_\beta \subseteq \mathtt{V}_\alpha$ and $\mathtt{V}^*_\beta \subseteq \mathtt{V}^*_\alpha$.

(ii) For all sets a, $a \in \mathtt{V}$.

(iii) If a, b *are sets,* $b \subseteq \omega \times \mathtt{V}^*$ *and* $(\forall x \in b)\, 1^{st}(2^{nd}(x)) \in a$, *then* $\langle a, b\rangle \in \mathtt{V}^*$.

Proof: [32], Lemma 4.2. □

5 Defining realizability

We now proceed to define a notion of realizability over $\mathtt{V}^*$. We use lower case gothic letters $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}, \mathfrak{e}, \mathfrak{f}, \mathfrak{g}, \mathfrak{h}, \mathfrak{n}, \mathfrak{m}, \mathfrak{p}, \mathfrak{q} \ldots$ as variables to range over elements of $\mathtt{V}^*$ while variables $e, c, d, f, g, \ldots$ will be reserved for elements of ω. Each element $\mathfrak{a}$ of $\mathtt{V}^*$ is an ordered pair $\langle x, y\rangle$, where $x \in \mathtt{V}$ and $y \subseteq \omega \times \mathtt{V}^*$; and we define the components of $\mathfrak{a}$ by

$$\begin{aligned} \mathfrak{a}^\circ &:= 1^{st}(\mathfrak{a}) = x \\ \mathfrak{a}^* &:= 2^{nd}(\mathfrak{a}) = y. \end{aligned}$$

Lemma 5.1 *For every* $\mathfrak{a} \in \mathtt{V}^*$, *if* $\langle e, \mathfrak{c}\rangle \in \mathfrak{a}^*$ *then* $\mathfrak{c}^\circ \in \mathfrak{a}^\circ$.

Proof: This is immediate by the definition of $\mathtt{V}^*$. □

If φ is a sentence with parameters in $\mathtt{V}^*$, then φ° denotes the formula obtained from φ by replacing each parameter $\mathfrak{a}$ in φ with $\mathfrak{a}^\circ$.

Definition 5.2 Bounded quantifiers will be treated as quantifiers in their own right, i.e., bounded and unbounded quantifiers are treated as syntactically different kinds of quantifiers.

We define $e \Vdash_{rt} \phi$ for sentences ϕ with parameters in $\mathtt{V}^*$. (The subscript $_{rt}$ is supposed to serve as a reminder of "realizability with truth".)

We shall use the abbreviations (x, y), $(x)_0$, and $(x)_1$ for $\mathbf{p}xy$, $\mathbf{p_0}x$, and $\mathbf{p_1}x$, respectively.

$$\begin{array}{rcl}
e \Vdash_{rt} \mathfrak{a} \in \mathfrak{b} & \text{iff} & \mathfrak{a}^\circ \in \mathfrak{b}^\circ \ \wedge\ \exists \mathfrak{c}\, [\langle (e)_0, \mathfrak{c}\rangle \in \mathfrak{b}^* \ \wedge\ (e)_1 \Vdash_{rt} \mathfrak{a} = \mathfrak{c}] \\
e \Vdash_{rt} \mathfrak{a} = \mathfrak{b} & \text{iff} & \mathfrak{a}^\circ = \mathfrak{b}^\circ \ \wedge\ \forall f \forall \mathfrak{c}\, [\langle f, \mathfrak{c}\rangle \in \mathfrak{a}^* \ \rightarrow\ (e)_0 f \Vdash_{rt} \mathfrak{c} \in \mathfrak{b}] \\
 & & \wedge\ \forall f \forall \mathfrak{c}\, [\langle f, \mathfrak{c}\rangle \in \mathfrak{b}^* \ \rightarrow\ (e)_1 f \Vdash_{rt} \mathfrak{c} \in \mathfrak{a}] \\
e \Vdash_{rt} \phi \wedge \psi & \text{iff} & (e)_0 \Vdash_{rt} \phi \ \wedge\ (e)_1 \Vdash_{rt} \psi \\
e \Vdash_{rt} \phi \vee \psi & \text{iff} & [(e)_0 = 0 \wedge (e)_1 \Vdash_{rt} \phi] \ \vee\ [(e)_0 \neq 0 \ \wedge\ (e)_1 \Vdash_{rt} \psi] \\
e \Vdash_{rt} \neg\phi & \text{iff} & \neg\phi^\circ \ \wedge\ \forall f\, \neg f \Vdash_{rt} \phi \\
e \Vdash_{rt} \phi \rightarrow \psi & \text{iff} & (\phi^\circ \rightarrow \psi^\circ) \ \wedge\ \forall f\, [f \Vdash_{rt} \phi \ \rightarrow\ ef \Vdash_{rt} \psi] \\
e \Vdash_{rt} (\forall x \in \mathfrak{a})\, \phi & \text{iff} & (\forall x \in \mathfrak{a}^\circ)\phi^\circ \ \wedge
\end{array}$$

$$\begin{array}{lll} & & \forall f\,\forall\mathfrak{b}(\langle f,\mathfrak{b}\rangle\in\mathfrak{a}^* \;\rightarrow\; ef \Vdash_{rt} \phi[x/\mathfrak{b}]) \\ e \Vdash_{rt} (\exists x\in\mathfrak{a})\phi & \text{iff} & \exists\mathfrak{b}\,(\langle(e)_0,\mathfrak{b}\rangle\in\mathfrak{a}^* \;\wedge\; (e)_1 \Vdash_{rt} \phi[x/\mathfrak{b}]) \\ e \Vdash_{rt} \forall x\phi & \text{iff} & \forall\mathfrak{a}\; e \Vdash_{rt} \phi[x/\mathfrak{a}] \\ e \Vdash_{rt} \exists x\phi & \text{iff} & \exists\mathfrak{a}\; e \Vdash_{rt} \phi[x/\mathfrak{a}] \end{array}$$

Notice that $e \Vdash_{rt} u \in v$ and $e \Vdash_{rt} u = v$ can be defined for arbitrary sets u, v, viz., not just for $u, v \in \mathtt{V}^*$. The definitions of $e \Vdash_{rt} u \in v$ and $e \Vdash_{rt} u = v$ fall under the scope of definitions by transfinite recursion.

Definition 5.3 By $\in$-recursion we define for every set x a set x^{st} as follows:

$$x^{st} \;=\; \langle x, \{\langle 0, u^{st}\rangle \,:\, u \in x\}\rangle. \tag{2}$$

Lemma 5.4 *For all sets x, $x^{st} \in \mathtt{V}^*$ and $(x^{st})^\circ = x$.*

Proof: [32], Lemma 5.4. □

Lemma 5.5 *If $\psi(\mathfrak{b}^\circ)$ holds for all $\mathfrak{b} \in \mathtt{V}^*$ then $\forall x\,\psi(x)$.*

Proof: [32], Lemma 5.5. □

Lemma 5.6 *If $\mathfrak{a} \in \mathtt{V}^*$ and $(\forall\mathfrak{b} \in \mathtt{V}^*)[\mathfrak{b}^\circ \in \mathfrak{a}^\circ \rightarrow \psi(\mathfrak{b}^\circ)]$ then $(\forall x \in \mathfrak{a}^\circ)\psi(x)$.*

Proof: [32], Lemma 5.6. □

Lemma 5.7 *If $e \Vdash_{rt} \phi$ then ϕ°.*

Proof: [32], Lemma 5.7. □

Our hopes for showing **DP** and **NEP** for **CZF** and related systems rest on the following results.

Lemma 5.8 *If $e \Vdash_{rt} (\exists x \in \mathfrak{a})\phi$ then*

$$\exists\mathfrak{b}\,(\langle(e)_0,\mathfrak{b}\rangle \in \mathfrak{a}^* \;\wedge\; \phi^\circ[x/\mathfrak{b}^\circ]).$$

Proof: Obvious by 5.7. □

Lemma 5.9 *If $e \Vdash_{rt} \phi \vee \psi$ then*

$$[(e)_0 = 0 \;\wedge\; \phi^\circ] \;\;\vee\;\; [(e)_0 \neq 0 \;\wedge\; \psi^\circ].$$

Proof: Obvious by 5.7. □

Lemma 5.10 *Negated formulae are self-realizing, that is to say, if ψ is a statement with parameters in $\mathtt{V}^*$, then*

$$\neg\psi^\circ \;\rightarrow\; 0 \Vdash_{rt} \neg\psi.$$

Proof: Assume $\neg\psi^\circ$. From $f \Vdash_{rt} \psi$ we would get ψ° by Lemma 5.8. But this is absurd. Hence $\forall f\, \neg f \Vdash_{rt} \psi$, and therefore $0 \Vdash_{rt} \neg\psi$. □

Definition 5.11 Let t be an application term and ψ be a formula of set theory. Then $t \Vdash_{rt} \psi$ is short for $(\exists e \in \omega)[t \simeq e \;\wedge\; e \Vdash_{rt} \psi]$.

Theorem 5.12 *For every theorem θ of* **CZF**, *there exists a closed application term t such that*

$$\mathbf{CZF} \vdash\; (t \Vdash_{rt} \theta).$$

Moreover, the proof of this soundness theorem is effective in that the application term t can be effectively constructed from the **CZF** *proof of θ.*

Proof: [32], Theorem 6.1. □

Remark 5.13 Theorem 5.12 holds also for **CZF** augmented by other large set axioms such as *"Every set is contained in an inaccessible set"* or *"Every set is contained in a Mahlo set"*. For definitions of "inaccessible set" and "Mahlo set" see [4, 9]. For example, in the case of the so-called Regular Extension Axiom this was carried out in [32], Theorem 7.2.

6 Extending the interpretation to IZF

In this section we address several extensions of earlier results. We show that in Theorem 5.12 **CZF** can be replaced by **IZF** and also that Markov's principle may be added.

Theorem 6.1 *For every theorem θ of* **IZF**, *there exists an application term t such that*

$$\mathbf{IZF} \vdash\; (t \Vdash_{rt} \theta).$$

Moreover, the proof of this soundness theorem is effective in that the application term t can be effectively constructed from the **IZF** *proof of θ.*

Proof: In view of Theorem 5.12 we only need to show that **IZF** proves that the Power Set Axiom and the full Separation Axiom are realized with respect to $\Vdash_{rt}$.

(Full Separation): Let $\varphi(x)$ be an arbitrary formula with parameters in $\mathtt{V}^*$. We want to find $e, e' \in \omega$ such that for all $\mathfrak{a} \in \mathtt{V}^*$ there exists a $\mathfrak{b} \in \mathtt{V}^*$ such that

$$(e \Vdash_{rt} \forall x \in \mathfrak{b}\,[x \in \mathfrak{a} \,\wedge\, \varphi(x)]) \;\wedge\; (e' \Vdash_{rt} \forall x \in \mathfrak{a}[\varphi(x) \rightarrow x \in \mathfrak{b}]). \tag{3}$$

For $\mathfrak{a} \in \mathtt{V}^*$, define

$$\begin{aligned} Sep(\mathfrak{a},\varphi) &= \{\langle \mathbf{p}fg, \mathfrak{c}\rangle : f, g \in \omega \wedge \langle g, \mathfrak{c}\rangle \in \mathfrak{a}^* \wedge f \Vdash_{rt} \varphi[x/\mathfrak{c}]\}, \\ \mathfrak{b} &= \langle \{x \in \mathfrak{a}^\circ : \varphi^\circ(x)\}, Sep(\mathfrak{a},\varphi)\rangle. \end{aligned}$$

$Sep(\mathfrak{a},\varphi)$ is a set by full Separation, and hence $\mathfrak{b}$ is a set. To ensure that $\mathfrak{b} \in \mathtt{V}^*$ let $\langle h, \mathfrak{c}\rangle \in Sep(\mathfrak{a},\varphi)$. Then $\langle g, \mathfrak{c}\rangle \in \mathfrak{a}^*$ and $f \Vdash_{rt} \varphi[x/\mathfrak{c}]$ for some $f, g \in \omega$. Thus $\mathfrak{c}^\circ \in \mathfrak{a}^\circ$ and, by Lemma 5.7, $\varphi^\circ[x/\mathfrak{c}^\circ]$, yielding $\mathfrak{c}^\circ \in \{x \in \mathfrak{a}^\circ : \varphi^\circ(x)\}$. Therefore, by Lemma 4.2, we have $\mathfrak{b} \in \mathtt{V}^*$.

To verify (3), first assume $\langle h, \mathfrak{c}\rangle \in \mathfrak{b}^*$ and $\mathfrak{c}^\circ \in \mathfrak{b}^\circ$. Then $h = \mathbf{p}fg$ for some $f, g \in \omega$ and $\langle g, \mathfrak{c}\rangle \in \mathfrak{a}^*$ and $f \Vdash_{rt} \varphi[x/\mathfrak{c}]$. Since $\mathfrak{c}^\circ \in \mathfrak{b}^\circ$ holds, it follows that $\mathfrak{c}^\circ \in \mathfrak{a}^\circ$. As a result, $\mathfrak{c}^\circ \in \mathfrak{a}^\circ \wedge \langle g, \mathfrak{c}\rangle \in \mathfrak{a}^* \wedge \mathbf{i}_r \Vdash_{rt} \mathfrak{c} = \mathfrak{c}$, and consequently we have $\mathbf{p}(h)_1\mathbf{i}_r \Vdash_{rt} \mathfrak{b} \in \mathfrak{a}$ and $(h)_0 \Vdash_{rt} \varphi[x/\mathfrak{c}]$, where $\mathbf{i}_r$ is the realizer of the identity axiom $\forall x\, x = x$ (see [23], Chapter 2, sections 5 and 6). Moreover, we have $(\forall x \in \mathfrak{b}^\circ)(x \in \mathfrak{a}^\circ \wedge \varphi^\circ(x))$. Therefore with $e = \mathbf{p}(\mathbf{p}(\lambda u.(u)_1)\mathbf{i}_r)(\lambda u.(u)_0)$, we get $e \Vdash_{rt} \forall x \in \mathfrak{b}\,[x \in \mathfrak{a} \wedge \varphi(x)]$.

Now assume $\langle g, \mathfrak{c}\rangle \in \mathfrak{a}$, $\mathfrak{c}^\circ \in \mathfrak{a}^\circ$ and $f \Vdash_{rt} \varphi[x/\mathfrak{c}]$. Then $\langle \mathbf{p}fg, \mathfrak{c}\rangle \in \mathfrak{b}^*$ and also $\mathfrak{c}^\circ \in \mathfrak{b}^\circ$ as $\varphi^\circ[x/\mathfrak{c}^\circ]$ is a consequence of $f \Vdash_{rt} \varphi[x/\mathfrak{c}]$ by Lemma 5.7. Therefore $\mathbf{p}(\mathbf{p}fg)\mathbf{i}_r \Vdash_{rt} \mathfrak{c} \in \mathfrak{b}$. Finally, by the very definition of $\mathfrak{b}$ we have $(\forall x \in \mathfrak{a}^\circ)[\varphi^\circ(x) \to x \in \mathfrak{b}^\circ]$, and hence with $e' = \lambda u.\lambda v.\mathbf{p}(\mathbf{p}vu)\mathbf{i}_r$ we get $e' \Vdash_{rt} (\forall x \in \mathfrak{a})[\varphi(x) \to x \in \mathfrak{b}]$.

(Powerset): It suffices to find a realizer for the formula $\forall x\, \exists y\, \forall z\, [z \subseteq x \to z \in y]$ as it implies the Powerset Axiom with the aid of Separation. Let $\mathfrak{a} \in \mathtt{V}^*$. Put $\mathcal{A} = \{\mathfrak{d} : \exists g\, \langle g, \mathfrak{d}\rangle \in \mathfrak{a}^*\}$. For $y \subseteq \omega \times \mathcal{A}$ let

$$\mathfrak{a}_y \;:=\; \langle \{\mathfrak{c}^\circ : \exists f\, \langle f, \mathfrak{c}\rangle \in y\}, y\rangle.$$

Note that $\mathfrak{a}_y \in \mathtt{V}^*$. The role of a set large enough to comprise the powerset of $\mathfrak{a}$ in $\mathtt{V}^*$ will be played by the following set

$$\mathfrak{p} \;:=\; \langle \mathcal{P}(\mathfrak{a}^\circ), \{\langle 0, \mathfrak{a}_y\rangle : y \subseteq \omega \times \mathcal{A}\}\rangle.$$

$\mathfrak{p}$ is a set in our background theory **IZF**. For $\langle 0, \mathfrak{a}_y\rangle \in \mathfrak{p}^*$ we have $\mathfrak{a}_y^\circ \subseteq \mathfrak{a}^\circ$, and thus $\mathfrak{a}_y^\circ \in \mathcal{P}(\mathfrak{a}^\circ)$, so it follows that $\mathfrak{p} \in \mathtt{V}^*$.

Now suppose $e \Vdash_{rt} \mathfrak{b} \subseteq \mathfrak{a}$. Put

$$y_{\mathfrak{b}} \;:=\; \{\langle (d,f), \mathfrak{x}\rangle : d, f \in \omega \wedge \langle (df)_0, \mathfrak{x}\rangle \in \mathfrak{a}^* \wedge \exists \mathfrak{c}\,[\langle d, \mathfrak{c}\rangle \in \mathfrak{b}^* \wedge (df)_1 \Vdash_{rt} \mathfrak{x} = \mathfrak{c}]\}. \tag{4}$$

(Recall that (x, y) stands for $\mathbf{p}xy$.) By definition of $y_{\mathfrak{b}}$, $y_{\mathfrak{b}} \subseteq \omega \times \mathcal{A}$, and therefore $\langle 0, \mathfrak{a}_{y_{\mathfrak{b}}}\rangle \in \mathfrak{p}^*$.

If $\langle f, \mathfrak{c}\rangle \in \mathfrak{b}^*$ it follows that $ef \Vdash_{rt} \mathfrak{c} \in \mathfrak{a}$ since $e \Vdash_{rt} \mathfrak{b} \subseteq \mathfrak{a}$; and hence there exists $\mathfrak{x}$ such that $\langle (ef)_0, \mathfrak{x}\rangle \in \mathfrak{a}^*$ and $(ef)_1 \Vdash_{rt} \mathfrak{x} = \mathfrak{c}$; whence $\langle (e, f), \mathfrak{x}\rangle \in y_{\mathfrak{b}}$ and therefore $((e, f), (ef)_1) \Vdash_{rt} \mathfrak{c} \in \mathfrak{a}_{y_{\mathfrak{b}}}$. Thus we can infer that $\lambda f.((e, f), (ef)_1) \Vdash_{rt} \mathfrak{b} \subseteq \mathfrak{a}_{y_{\mathfrak{b}}}$.

Conversely, if $\langle g, \mathfrak{x}\rangle \in \mathfrak{a}^*_{y_{\mathfrak{b}}} = y_{\mathfrak{b}}$, then there exist d, f and $\mathfrak{c}$ such that $g = (d, f)$, $\langle d, \mathfrak{c}\rangle \in \mathfrak{b}^*$, and $(df)_1 \Vdash_{rt} \mathfrak{c} = \mathfrak{x}$, which entails that $((g)_0, ((g)_0(g)_1)_1) \Vdash_{rt} \mathfrak{x} \in \mathfrak{b}$. As a result, $\eta(e) \Vdash_{rt} \mathfrak{b} = \mathfrak{a}_{y_{\mathfrak{b}}}$, where $\eta(e) = (\lambda f.((e, f), (ef)_1), \lambda g.((g)_0, ((g)_0(g)_1)_1))$. Hence $(0, \eta(e)) \Vdash_{rt} \mathfrak{b} \in \mathfrak{p}$, so that

$$\lambda e.(0, \eta(e)) \Vdash_{rt} \forall y\, [y \subseteq \mathfrak{a} \to y \in \mathfrak{p}],$$

and therefore, by the genericity of quantifiers,

$$\lambda e.(0, \eta(e)) \;\Vdash_{rt}\; \forall x\, \exists y\, \forall z\, [z \subseteq x \to z \in y]. \tag{5}$$

□

Theorem 6.2 **IZF** *has the* **DP** *and* **NEP** *and* **IZF** *is closed under* **CR**, **ECR**, $\mathbf{CR_1}$, **UZR**, *and* **UR**, *too.*

Proof: This follows from Theorem 6.1 by the proof of [32], Theorem 1.2. □

Remark 6.3 [32], Theorem 1.2 and 6.2 allow for generalizations to extensions of **CZF**, **CZF** + **REA**, and **IZF** via "true" axioms that are of the form $\neg\psi$. This follows easily from the proofs of these theorems and the fact that negated statements are self-realizing (see Lemma 5.10). As a consequence we get, for example, that if $\neg\vartheta$ is a true sentence and $\mathbf{CZF} \vdash \neg\vartheta \to (\phi \vee \psi)$, then $\mathbf{CZF} \vdash \neg\vartheta \to \phi$ or $\mathbf{CZF} \vdash \neg\vartheta \to \psi$. Likewise, $\mathbf{CZF} \vdash \neg\vartheta \to (\exists x \in \omega)\theta(x)$ implies $\mathbf{CZF} \vdash (\exists x \in \omega)[\neg\vartheta \to \theta(x)]$.

Next we extended our results to theories a classically valid principle. *Markov's Principle*, **MP**, is closely associated with the work of the school of Russian constructivists. The version of **MP** most appropriate to the set-theoretic context is the schema

$$\forall n \in \omega\, [\varphi(n) \vee \neg\varphi(n)] \;\wedge\; \neg\neg\exists n \in \omega\, \varphi(n) \;\to\; \exists n \in \omega\varphi(n).$$

The variant

$$\neg\neg\exists n \in \omega\, R(n) \to \exists n \in \omega R(n),$$

with R being a primitive recursive predicate, will be denoted by $\mathbf{MP_{PR}}$. Obviously, $\mathbf{MP_{PR}}$ is implied by **MP**.

Theorem 6.4 *Let T be any of the theories* **CZF**, **CZF** + **REA**, **IZF**, *or* **IZF** + **REA**. *For every theorem θ of $T + \mathbf{MP}$, there exists an application term t such that*

$$T + \mathbf{MP} \vdash \; (t \Vdash_{rt} \theta).$$

Moreover, the proof of this soundness theorem is effective in that the application term t can be effectively constructed from the $T + \mathbf{MP}$ proof of θ.

Proof: Arguing in $T + \mathbf{MP}$, it remains to find realizing terms for **MP**. We assume that

$$(e)_0 \quad \Vdash_{rt} \quad (\forall x \in \underline{\omega})\, [\varphi(x) \;\vee\; \neg\varphi(x)] \tag{6}$$

$$(e)_1 \quad \Vdash_{rt} \quad \neg\neg(\exists x \in \underline{\omega})\, \varphi(x). \tag{7}$$

Let $e' = (e)_0$. Unravelling the definition of $\Vdash_{rt}$ for negated formulas, it is a consequence of (7) that $(\forall d \in \omega)\,\neg\,(\forall f \in \omega)\;\neg f \Vdash_{rt} (\exists x \in \underline{\omega})\varphi(x)$, and hence $\neg\,(\forall f \in \omega)\;\neg f \Vdash_{rt} (\exists x \in \underline{\omega})\varphi(x)$, which implies $\neg\neg(\exists f \in \omega) f \Vdash_{rt} (\exists x \in \underline{\omega})\varphi(x)$ (just using intuitionistic logic), and hence

$$\neg\neg(\exists f \in \omega)(f)_1 \Vdash_{rt} \varphi[x/\underline{(f)_0}]. \tag{8}$$

(6) yields that $(\forall n \in \omega) e'n \downarrow$ and

$$(\forall n \in \omega)([(e'n)_0 = 0 \;\wedge\; (e'n)_1 \Vdash_{rt} \varphi[x/\underline{n}]] \;\vee\; [(e'n)_0 \neq 0 \;\wedge\; (e'n)_1 \Vdash_{rt} \neg\varphi[x/\underline{n}]]).$$

Since $(e'n)_1 \Vdash_{rt} \neg\varphi(\underline{n})$ entails that $\neg(e'n)_1 \Vdash_{rt} \varphi(\underline{n})$ we arrive at

$$(\forall n \in \omega)[\psi(n) \vee \neg\psi(n)], \tag{9}$$

where $\psi(n)$ is the formula $(e'n)_0 = 0 \wedge (e'n)_1 \Vdash_{rt} \varphi[x/\underline{n}]$. Utilizing that **MP** holds in the background theory, from (8) and (9) we can deduce that there exists a natural number m such that $\psi(m)$ is true, i.e., $(e'm)_0 = 0$ and $(e'm)_1 \Vdash_{rt} \varphi[x/\underline{m}]$. Then, with $r := \mu n.(e'n)_0 = 0$,

$$(e'r)_1 \Vdash_{rt} \varphi[x/\underline{m}].$$

r can be computed by a partial recursive function ζ from e'. Taking into account that for any instance θ of **MP** with parameters in $\mathtt{V}^*$, θ° is an instance of **MP**, too, the upshot of the foregoing is that $\lambda e.(\zeta((e)_0), ((e)_0\zeta((e)_0))_1)$ is a realizer for **MP**. □

Theorem 6.5 *If is T any of the theories* **CZF**, **CZF**+**REA**, **IZF**, *or* **IZF**+**REA**, *then* T+**MP** *has the* **DP** *and the* **NEP**, *and* T + **MP** *is closed under* **CR**, **ECR**, $\mathbf{CR_1}$, **UZR**, *and* **UR**.

Proof: This follows from Theorem 6.4 and the proof of [32] Theorem 1.2. □

7 Realizability for choice principles

The intent of this section is to show that $\Vdash_{rt}$-realizability can be used to validate the choice principles $\mathbf{AC}_\omega$, **DC**, **RDC**, and **PAx**, providing they hold in the background theory.

7.1 Internal pairing

As choice principles assert the existence of functions, the natural first step in the investigation of choice principles over $\mathtt{V}^*$ is the isolation of the $\mathtt{V}^*$-internal versions of pairs and ordered pairs.

If φ is a formula with parameters from $\mathtt{V}^*$ we shall frequently write '$\mathtt{V}^* \models \varphi$' to convey that there is a closed application term t such such that $t \Vdash_{rt} \varphi$. It will be obvious from the context how to construct t.

If $\mathcal{SC}$ is a scheme of formulas we take $\mathtt{V}^* \models \mathcal{SC}$ to mean that there is a closed application term t such that $t \Vdash_{rt} \varphi$ holds for all instances φ of $\mathcal{SC}$.

Definition 7.1 *For* $\mathfrak{a}, \mathfrak{b} \in \mathtt{V}^*$, *set*

$$\begin{aligned} \overline{\{\mathfrak{a}, \mathfrak{b}\}} &:= \langle \{\mathfrak{a}^\circ, \mathfrak{b}^\circ\}, \{\langle 0, \mathfrak{a}\rangle, \langle 1, \mathfrak{b}\rangle\}\rangle, \\ \overline{\{\mathfrak{a}\}} &:= \overline{\{\mathfrak{a}, \mathfrak{a}\}}, \\ \overline{\langle \mathfrak{a}, \mathfrak{b}\rangle} &:= \langle \langle \mathfrak{a}^\circ, \mathfrak{b}^\circ\rangle, \{\langle 0, \overline{\{\mathfrak{a}\}}\rangle, \langle 1, \overline{\{\mathfrak{a}, \mathfrak{b}\}}\rangle\}\rangle. \end{aligned}$$

Lemma 7.2 *(i)* $\overline{\{\mathfrak{a}, \mathfrak{b}\}}^\circ = \{\mathfrak{a}^\circ, \mathfrak{b}^\circ\}$.

(ii) $\overline{\langle \mathfrak{a}, \mathfrak{b}\rangle}^\circ = \langle \mathfrak{a}^\circ, \mathfrak{b}^\circ\rangle$.

(iii) $\overline{\{\mathfrak{a}, \mathfrak{b}\}}, \overline{\langle \mathfrak{a}, \mathfrak{b}\rangle} \in \mathtt{V}^*$.

(iv) $\mathtt{V}^* \models \mathfrak{c} \in \overline{\{\mathfrak{a}, \mathfrak{b}\}} \leftrightarrow [\mathfrak{c} = \mathfrak{a} \vee \mathfrak{c} = \mathfrak{b}]$.

(v) $\mathtt{V}^* \models \mathfrak{c} \in \overline{\langle \mathfrak{a}, \mathfrak{b}\rangle} \leftrightarrow [\mathfrak{c} = \overline{\{\mathfrak{a}\}} \vee \mathfrak{c} = \overline{\{\mathfrak{a}, \mathfrak{b}\}}]$.

Proof: (i) and (ii) are obvious. To show (iii) we employ Lemma 4.2 (iii). Let $x \in \overline{\{\mathfrak{a},\mathfrak{b}\}}^*$. Then $2^{nd}(x) \in \{\mathfrak{a},\mathfrak{b}\}$ and thus $1^{st}(2^{nd}(x)) \in \overline{\{\mathfrak{a},\mathfrak{b}\}}^{\circ}$ by (i).

Now let $y \in \overline{\langle\mathfrak{a},\mathfrak{b}\rangle}^*$. Then $2^{nd}(y) \in \{\overline{\{\mathfrak{a}\}}, \overline{\{\mathfrak{a},\mathfrak{b}\}}\}$, and hence, by (i), $1^{st}(2^{nd}(y)) \in \{\{\mathfrak{a}^{\circ}\},\{\mathfrak{a}^{\circ},\mathfrak{b}^{\circ}\}\}$; thus $1^{st}(2^{nd}(y)) \in \overline{\langle\mathfrak{a},\mathfrak{b}\rangle}^{\circ}$ by (ii).

One easily checks that $(\lambda x.x, \lambda x.\mathbf{d}x(\mathbf{1},(x)_1)(x)_0\mathbf{0})$ provides a realizer for (iv).

In a similar vein one can construct a realizer for (v). □

7.2 Axioms of choice in $\mathtt{V}^*$

Theorem 7.3 *(i)* $(\mathbf{CZF}+\mathbf{AC}_\omega)$ $\quad \mathtt{V}^* \models \mathbf{AC}_\omega$.

(ii) $(\mathbf{CZF}+\mathbf{DC})$ $\quad \mathtt{V}^* \models \mathbf{DC}$.

(iii) $(\mathbf{CZF}+\mathbf{RDC})$ $\quad \mathtt{V}^* \models \mathbf{RDC}$.

(iv) $(\mathbf{CZF}+\mathbf{PAx})$ $\quad \mathtt{V}^* \models \mathbf{PAx}$.

Proof: In the following proof we will frequently use the phrase that "e' *is (effectively) computable from* $e_1,\ldots,e_k$". By this we mean that there exists a closed application term q (which we can't be bothered to exhibit) such that $qe_1\ldots e_k \simeq e'$ holds in the partial combinatory algebra **Kl**.

Ad (i): Recall from the proof of [32] Theorem 6.1 that the set ω is represented in $\mathtt{V}^*$ by $\underline{\omega}$, which is given via an injection of ω into $\mathtt{V}^*$:

$$\underline{n} \;=\; \langle n, \{\langle k,\underline{k}\rangle : \; k<n\}\rangle \tag{10}$$
$$\underline{\omega} \;=\; \langle \omega, \{\langle n,\underline{n}\rangle : \; n\in\omega\}\rangle. \tag{11}$$

Now suppose

$$e \Vdash_{rt} \forall x \in \underline{\omega}\, \exists y\, \varphi(x,y).$$

Then $\forall n\in\omega\, [en\downarrow \;\wedge\; en \Vdash_{rt} \exists y\, \varphi(\underline{n},y)]$, and hence

$$\forall n\in\omega\, \exists \mathfrak{a}\, [\, en\downarrow \;\wedge\; en \Vdash_{rt} \varphi(\underline{n},\mathfrak{a})].$$

Invoking $\mathbf{AC}_\omega$ in the background theory, there exists a function $F:\omega\to\mathtt{V}^*$ such that $\forall n \in \omega\, en \Vdash_{rt} \varphi(\underline{n},F(n))$. Next, we internalize F. Letting $F_0:\omega\to\mathtt{V}$ and $F_1:\omega\to\mathtt{V}^*$ be defined by $F_0(n) := (F(n))^{\circ}$ and $F_1(n) := \overline{\langle \underline{n}, F(n)\rangle}$, respectively, put

$$\mathfrak{f} \;=\; \langle F_0, F_1\rangle.$$

Lemma 7.2 and Lemma 4.2 (iii) entail that $\mathfrak{f}\in\mathtt{V}^*$.

First, because of the properties of internal pairing in $\mathtt{V}^*$ discerned in Lemma 7.2, it will be shown that, internally in $\mathtt{V}^*$, $\mathfrak{f}$ is a functional relation with domain $\underline{\omega}$ and that this holds with a witness obtainable independently of e. To see that $\mathfrak{f}$ is realizably functional, assume that

$$h \Vdash_{rt} \overline{\langle\mathfrak{a},\mathfrak{b}\rangle} \in \mathfrak{f} \quad\text{ and }\quad j \Vdash_{rt} \overline{\langle\mathfrak{a},\mathfrak{c}\rangle} \in \mathfrak{f}.$$

Then,

$$h_1 \Vdash_{rt} \overline{\langle\mathfrak{a},\mathfrak{b}\rangle} = \overline{\langle \underline{h_0}, F(h_0)\rangle} \quad\text{ and }\quad j_1 \Vdash_{rt} \overline{\langle\mathfrak{a},\mathfrak{c}\rangle} = \overline{\langle \underline{j_0}, F(j_0)\rangle}, \tag{12}$$

where $h_1 = (h)_1$ and $j_1 = (j)_1$. This holds strictly in virtue of the definition of $\mathfrak{f}$ and the conditions on statements of membership. (12) in conjunction with Lemma 7.2 implies that $d \Vdash_{rt} \underline{h_0} = \underline{j_0}$ for some d, and hence $(\underline{h_0})^\circ = (\underline{j_0})^\circ$ by Lemma 5.7. Thus, in view of the definition of $\underline{n}$, we have $h_0 = j_0$ and consequently $F(h_0) = F(j_0)$. As a result, $\ell(h,j) \Vdash_{rt} \mathfrak{b} = \mathfrak{c}$, with $\ell(h,j)$ an application term easily constructed from h and j.

Finally, we have to check on the realizability of $\forall x \in \underline{\omega}\, \varphi(x, \mathfrak{f}(x))$. Since $\forall n \in \omega\, en \Vdash_{rt} \varphi(\underline{n}, F(n))$ we deduce by Lemma 5.7 that $\forall n \in \omega\, \varphi^\circ(n, (\overline{F(n)})^\circ)$ and hence $\forall n \in \omega\, \varphi^\circ(n, \mathfrak{f}^\circ(n))$ as $\mathfrak{f}^\circ = F_0$. Since $\forall n \in \omega\, en \Vdash_{rt} \varphi(\underline{n}, F(n))$ and $\mathfrak{f}^* = \{\langle n, \overline{\langle \underline{n}, F(n)\rangle}\rangle : n \in \omega\}$ we can now also construct a $\mathbf{q}$ independent of e such that $\forall n \in \omega\, (\mathbf{q}e)n \Vdash_{rt} \varphi(\underline{n}, \mathfrak{f}(\underline{n}))$. So the upshot of the above is that we can cook up a realizer $\mathbf{r}$ such that

$$\mathbf{r} \Vdash_{rt} \forall x \in \underline{\omega}\, \exists y\, \varphi(x,y) \;\rightarrow\; \exists f\, [\mathbf{fun}(f) \wedge \mathbf{dom}(f) = \underline{\omega} \wedge \forall x \in \underline{\omega}\, \varphi(x, f(x))].$$

Ad (ii): Suppose

$$e \Vdash \forall x \in \mathfrak{a}\, \exists y \in \mathfrak{a}\, \varphi(x,y) \qquad \text{and} \tag{13}$$

$$d \Vdash \mathfrak{b} \in \mathfrak{a}. \tag{14}$$

Then we have $\mathfrak{b}^\circ \in \mathfrak{a}^\circ$ and there exists $\mathfrak{c}_{\mathfrak{b}}$ such that

$$\langle (d)_0, \mathfrak{c}_{\mathfrak{b}}\rangle \in \mathfrak{a}^* \wedge (d)_1 \Vdash_{rt} \mathfrak{b} = \mathfrak{c}_{\mathfrak{b}}. \tag{15}$$

Moreover, (13) entails that $\forall k\, \forall \mathfrak{c}\, (\langle k, \mathfrak{c}\rangle \in \mathfrak{a}^* \rightarrow \exists \mathfrak{d}\, [\langle (ek)_0, \mathfrak{d}\rangle \in \mathfrak{a}^* \wedge (ek)_1 \Vdash_{rt} \varphi(\mathfrak{c}, \mathfrak{d})])$, and hence

$$\forall \langle k, \mathfrak{c}\rangle \in \mathfrak{a}^*\, \exists \langle m, \mathfrak{d}\rangle \in \mathfrak{a}^*\, \varphi^{\Vdash}(\langle k, \mathfrak{c}\rangle, \langle m, \mathfrak{d}\rangle), \tag{16}$$

where $\varphi^{\Vdash}(\langle n, \mathfrak{c}\rangle, \langle m, \mathfrak{d}\rangle)$ stands for $en\downarrow \wedge m = (en)_0 \wedge (en)_1 \Vdash_{rt} \varphi(\mathfrak{c}, \mathfrak{d})$.

By **DC** in the background theory, there are functions $f : \omega \rightarrow \omega$ and $g : \omega \rightarrow \mathtt{V}^*$ such that $f(0) = (d)_0$, $g(0) = \mathfrak{c}_{\mathfrak{b}}$, $\forall n \in \omega\, \langle f(n), g(n)\rangle \in \mathfrak{a}^*$, and

$$\forall n \in \omega\, \varphi^{\Vdash}(\langle f(n), g(n)\rangle, \langle f(n+1), g(n+1)\rangle). \tag{17}$$

(17) implies that

$$\forall n \in \omega\, [f(n+1) = (e(f(n)))_0 \wedge (e(f(n)))_1 \Vdash_{rt} \varphi(g(n), g(n+1))]\,. \tag{18}$$

Now put

$$\begin{aligned} F &:= \{\langle n, (g(n))^\circ\rangle : n \in \omega\}, \\ G &:= \{\langle n, \overline{\langle \underline{n}, g(n)\rangle}\rangle : n \in \omega\}, \\ \mathfrak{g} &:= \langle F, G\rangle. \end{aligned}$$

Lemma 7.2 and Lemma 4.2 (iii) guarantee that $\mathfrak{g} \in \mathtt{V}^*$. First, because of the properties of internal pairing in $\mathtt{V}^*$ discerned in Lemma 7.2, it will be shown that, internally in $\mathtt{V}^*$, $\mathfrak{g}$ is a functional relation with domain $\underline{\omega}$ and that this holds with a witness obtainable independently of e and d. To see that $\mathfrak{g}$ is realizably functional, assume that

$$h \Vdash_{rt} \overline{\langle \mathfrak{a}, \mathfrak{b}\rangle} \in \mathfrak{g} \quad \text{and} \quad j \Vdash_{rt} \overline{\langle \mathfrak{a}, \mathfrak{c}\rangle} \in \mathfrak{g}.$$

Then,

$$h_1 \Vdash_{rt} \overline{\langle \mathfrak{a}, \mathfrak{b} \rangle} = \overline{\langle \underline{h_0}, F(h_0) \rangle} \quad \text{and} \quad j_1 \Vdash_{rt} \overline{\langle \mathfrak{a}, \mathfrak{c} \rangle} = \overline{\langle \underline{j_0}, F(j_0) \rangle}, \tag{19}$$

where $h_1 = (h)_1$ and $j_1 = (j)_1$. This holds strictly in virtue of the definition of $\mathfrak{g}$ and the conditions on statements of membership. (12) in conjunction with Lemma 7.2 implies that $d \Vdash_{rt} \underline{h_0} = \underline{j_0}$ for some d, and hence $(\underline{h_0})^\circ = (\underline{j_0})^\circ$ by Lemma 5.7. Thus, in view of the definition of $\underline{n}$, we have $h_0 = j_0$ and consequently $F(h_0) = F(j_0)$. As a result, $\ell(h, j) \Vdash_{rt} \mathfrak{b} = \mathfrak{c}$, with $\ell(h, j)$ an application term easily constructed from h and j.

Finally, we have to effectively calculate a realizer $\ell(e, d)$ from e and d such that

$$\ell(e, d) \Vdash_{rt} \mathfrak{g}(0) = \mathfrak{b} \ \wedge \ \forall x \in \underline{\omega}\, \varphi(\mathfrak{g}(x), \mathfrak{g}(x+1)). \tag{20}$$

Since $d \Vdash_{rt} \mathfrak{b} \in \mathfrak{a}$ and $g(0) = \mathfrak{c}_\mathfrak{b}$ it follows from (16) that we can construct a realizer $\tilde{d}$ from d such that $\tilde{d} \Vdash_{rt} \mathfrak{g}(0) = \mathfrak{b}$. Moreover, in view of (19) the function f is recursive. Let $\rho(n) := (e(f(n)))_0$. The S-m-n theorem shows how to compute an index of the function ρ from e. Since

$$\mathbf{p}n\mathbf{i}_r \Vdash_{rt} \overline{\langle \underline{n}, g(n) \rangle} \in \mathfrak{g}$$
$$\rho(n) \Vdash_{rt} \varphi(g(n), g(n+1))$$

this shows that we can effectively construct an index $\ell(e, d)$ from e and d such that (20) holds.

Ad (iii): **RDC** implies **DC** (see [28], Lemma 3.4) and, on the basis of **CZF** + **DC**, the scheme **RDC** follows from the scheme:

$$\forall x\, (\varphi(x) \ \rightarrow \ \exists y\, [\varphi(y) \ \wedge \ \psi(x, y)]) \ \wedge \ \varphi(\mathfrak{b}) \quad \rightarrow \tag{21}$$
$$\exists z\, (b \in z \ \wedge \ \forall x \in z\, \exists y \in z\, [\varphi(y) \ \wedge \ \psi(x, y)]).$$

Thus, in view of part (ii) of this theorem it suffices to show that, working in **CZF** + **RDC**, $\mathtt{V}^*$ validates (21). So suppose $\mathfrak{b} \in \mathtt{V}^*$ and

$$e \ \Vdash \ \forall x\, (\varphi(x) \ \rightarrow \ \exists y\, [\varphi(y) \ \wedge \ \psi(x, y)]) \qquad \text{and}$$
$$d \ \Vdash \ \varphi(\mathfrak{b}).$$

Then, for all $k \in \omega$ and $\mathfrak{a} \in \mathtt{V}^*$ we have

$$(k \Vdash \varphi(x)) \ \rightarrow \ \exists \mathfrak{c}\, [(ek)_0 \Vdash_{rt} \varphi(\mathfrak{c}) \ \wedge \ (ef)_1 \Vdash_{rt} \psi(\mathfrak{a}, \mathfrak{c})].$$

By applying **RDC** to the above, we can extract functions $\imath : \omega \to \omega$, $\jmath : \omega \to \omega$, and $\ell : \omega \to \mathtt{V}^*$ such that $\imath(0) = d$, $\ell(0) = \mathfrak{b}$, and for all $n \in \omega$:

$$\imath(n) \Vdash_{rt} \varphi(\ell(n)) \quad \text{and} \quad \jmath(n) \Vdash_{rt} \psi(\ell(n), \ell(n+1)), \tag{22}$$
$$\imath(n+1) = (e(\imath(n)))_0 \quad \text{and} \quad \jmath(n) = (e(\imath(n)))_1. \tag{23}$$

By the last line, $\imath$ and $\jmath$ are recursive functions whose indices can be effectively computed from e and d. Now set

$$\mathfrak{d} \ = \ \langle \{(\ell(n))^\circ : n \in \omega\}, \{\langle n, \ell(n) \rangle : n \in \omega\} \rangle\, .$$

Obviously, $\mathfrak{d}$ belongs to $\mathtt{V}^*$. We have

$$\mathbf{p}0\mathbf{i}_r \Vdash_{rt} \mathfrak{b} \in \mathfrak{d}. \tag{24}$$

(22) entails that

$$\forall n \in \omega \;\; \mathbf{p}(\imath(n+1))(\jmath(n)) \Vdash_{rt} \varphi(\ell(n)) \;\wedge\; \psi(\ell(n), \ell(n+1))$$

and hence

$$\forall n \in \omega \;\; \mathbf{p}(n+1)\,(\mathbf{p}(\imath(n+1))(\jmath(n))) \Vdash_{rt} \exists y \in \mathfrak{d}\; [\varphi(\ell(n)) \;\wedge\; \psi(\ell(n), y)]\,.$$

Thus choosing an index $\tilde{e}$ such that $\tilde{e}n = \mathbf{p}(n+1)\,(\mathbf{p}(\imath(n+1))(\jmath(n)))$ we arrive at

$$\tilde{e} \Vdash_{rt} \forall x \in \mathfrak{d}\, \exists y \in \mathfrak{d}\; [\varphi(x) \;\wedge\; \psi(x,y)]\,. \tag{25}$$

Note that $\tilde{e}$ can be effectively calculated from e and d. As a result, (24) and (25) entail that we can construct a realizer $\mathbf{q}$ for (21).

Ad (iv): For the proof of $\mathtt{V}^* \models \mathbf{PAx}$ fix an arbitrary $\mathfrak{a}$ in $\mathtt{V}^*$. Since $\mathbf{PAx}$ holds in the background theory we can find bases X and Y and surjections $f : X \to \mathfrak{a}^\circ$ and $g : Y \to \mathfrak{a}^*$. Define

$$\tilde{X} \;:=\; \{\langle 0, v\rangle : v \in X\}, \tag{26}$$

$$\tilde{Y} \;:=\; \{\langle g_0(u)+1, u\rangle :\; u \in Y\}, \tag{27}$$

where $g_0 : Y \to \omega$ is defined by $g_0(u) := 1^{st}(g(u))$.

As $\tilde{X}$ is in one-one correspondence with X and $\tilde{Y}$ is in one-one correspondence with Y, $\tilde{X}$ and $\tilde{Y}$ are bases, too. Moreover,

$$B \;:=\; \tilde{X} \cup \tilde{Y} \tag{28}$$

is a basis as well because $\tilde{X}$ and $\tilde{Y}$ don't have any elements in common and for an arbitrary $x \in B$ we can decide whether it belongs to $\tilde{X}$ or $\tilde{Y}$ by inspecting $1^{st}(x)$ and determining whether $1^{st}(x) = 0$ or $1^{st}(x) \neq 0$ since $1^{st}(x) \in \omega$. We thus may define a function $\mathcal{F} : B \to \mathfrak{a}^\circ$ by

$$\mathcal{F}(x) = \begin{cases} f(2^{nd}(x)) & \text{if } \; x \in \tilde{X} \\ \big(2^{nd}(g(2^{nd}(x)))\big)^\circ & \text{if } \; x \in \tilde{Y}. \end{cases} \tag{29}$$

Since for $u \in Y$ we have $\big(2^{nd}(g(2^{nd}(\langle g_0(u)+1, u\rangle))))\big)^\circ = \big(2^{nd}(g(u))\big)^\circ \in \mathfrak{a}^\circ$, $\mathcal{F}$ clearly takes its values in $\mathfrak{a}^\circ$. Moreover, $\mathcal{F}$ is surjective as f is surjective. Now set

$$\wp(u) \;:=\; \overline{\langle \underline{g_0(u)+1}, u^{st}\rangle} \qquad \text{for } u \in Y, \tag{30}$$

$$B^+ \;:=\; \{\langle\, g_0(u), \wp(u)\rangle \;:\; u \in Y\}, \tag{31}$$

$$\mathfrak{b} \;:=\; \langle B, B^+\rangle. \tag{32}$$

By Lemmata 7.2 and 5.4, and the fact that $(\underline{n})^\circ = n$ (see (10) for the definition of $\underline{n}$), we see that $(\wp(u))^\circ = \Big(\overline{\langle \underline{g_0(u)+1}, u^{st}\rangle}\Big)^\circ = \langle g_0(u)+1, u\rangle \in B$ for $u \in Y$, it follows that $\mathfrak{b} \in \mathtt{V}^*$. The latter also entails that $\wp$ is one-one and therefore $u \mapsto \langle\, g_0(u), \wp(u)\rangle$ is a one-one correspondence between Y and B^+, showing that B^+ is a base as well.

We shall verify that, internally in $\mathtt{V}^*$, $\mathfrak{b}$ is a base which can be surjected onto $\mathfrak{a}$. To define this surjection, let

$$\ell(u) \;:=\; \overline{\langle \wp(u), 2^{nd}(g(u))\rangle} \qquad \text{for } u \in Y \tag{33}$$

$$\mathcal{G} \;:=\; \{\langle g_0(u), \ell(u)\rangle \;:\; u \in Y\} \tag{34}$$

$$\mathfrak{h} \;:=\; \langle \mathcal{F}, \mathcal{G}\rangle. \tag{35}$$

To see that $\mathfrak{h} \in \mathtt{V}^*$, let $x \in \mathfrak{h}^*$. Then $x \in \mathcal{G}$, so $x = \langle g_0(u), \ell(u)\rangle$ for some $u \in Y$. Thus $1^{st}(2^{nd}(x)) = (\ell(u))^\circ = \left\langle (\wp(u))^\circ, \left(2^{nd}(g(u))\right)^\circ \right\rangle = \left\langle \langle g_0(u)+1, u\rangle, \left(2^{nd}(g(u))\right)^\circ \right\rangle \in \mathcal{F}$.

First, we aim at showing that

$$\mathtt{V}^* \models \mathfrak{h} \texttt{ is a surjection from } \mathfrak{b} \texttt{ onto } \mathfrak{a}. \tag{36}$$

To verify $\mathtt{V}^* \models \mathfrak{h} \subseteq \mathfrak{b} \times \mathfrak{a}$, suppose $e \Vdash_{rt} \overline{\langle \mathfrak{c}, \mathfrak{d}\rangle} \in \mathfrak{h}$. Then there exists $u \in Y$ such that $(e)_0 = g_0(u)$ and $(e)_1 \Vdash_{rt} \overline{\langle \mathfrak{c}, \mathfrak{d}\rangle} = \overline{\langle \wp(u), 2^{nd}(g(u))\rangle}$. Hence, because of $\mathbf{p}(g_0(u))\mathbf{i}_r \Vdash_{rt} 2^{nd}(g(u)) \in \mathfrak{a}$, one can effectively calculate an index e' from e such that $e' \Vdash_{rt} \mathfrak{c} \in \mathfrak{b} \wedge \mathfrak{d} \in \mathfrak{a}$, showing that

$$\mathtt{V}^* \models \mathfrak{h} \subseteq \mathfrak{b} \times \mathfrak{a}. \tag{37}$$

To see that $\mathfrak{h}$ is realizably total on $\mathfrak{b}$, assume that $e \Vdash_{rt} \mathfrak{c} \in \mathfrak{b}$. Then there exists $\mathfrak{d}$ such that $\langle (e)_0, \mathfrak{d}\rangle \in \mathfrak{b}^*$ and $(e)_1 \Vdash_{rt} \mathfrak{c} = \mathfrak{d}$. Moreover, by virtue of the definition of $\mathfrak{b}^*$, there exists $u \in Y$ such that $\langle (e)_0, \mathfrak{d}\rangle = \langle g_0(u), \wp(u)\rangle$, and thus, by definition of $\mathfrak{h}$, $(e)_0\mathbf{i}_r \Vdash_{rt} \overline{\langle \mathfrak{d}, 2^{nd}(g(u))\rangle} \in \mathfrak{h}$. Therefore an $\tilde{e}$ can be computed from e such that $\tilde{e} \Vdash_{rt} \mathfrak{c}$ `is in the domain of` $\mathfrak{h}$, so that with (37) we can conclude that for some e^+ effectively obtainable from e, $e^+ \Vdash_{rt} \mathfrak{b}$ `is in the domain of` $\mathfrak{h}$. As a result, $\mathtt{V}^* \models \mathfrak{b} \subseteq \mathbf{dom}(\mathfrak{h})$, so that in view of (37) we have

$$\mathtt{V}^* \models \mathbf{dom}(\mathfrak{h}) = \mathfrak{b}. \tag{38}$$

To establish realizable functionality of $\mathfrak{h}$, suppose $e \Vdash_{rt} \overline{\langle \mathfrak{c}, \mathfrak{d}\rangle} \in \mathfrak{h}$ and $d \Vdash_{rt} \overline{\langle \mathfrak{c}, \mathfrak{e}\rangle} \in \mathfrak{h}$. Then there exist $u, v \in Y$ such that $(e)_0 = g_0(u)$, $(d)_0 = g_0(v)$, $(e)_1 \Vdash_{rt} \overline{\langle \mathfrak{c}, \mathfrak{d}\rangle} = \overline{\langle \wp(u), 2^{nd}(g(u))\rangle}$, and $(d)_1 \Vdash_{rt} \overline{\langle \mathfrak{c}, \mathfrak{e}\rangle} = \overline{\langle \wp(v), 2^{nd}(g(v))\rangle}$. Hence $\Vdash_{rt} \wp(u) = \wp(v)$, i.e. $\Vdash_{rt} \overline{\langle \underline{g_0(u)+1}, u^{st}\rangle} = \overline{\langle \underline{g_0(v)+1}, v^{st}\rangle}$, and therefore $\Vdash_{rt} u^{st} = v^{st}$, yielding $u = (u^{st})^\circ = (v^{st})^\circ = v$. As a result, $q \Vdash_{rt} \mathfrak{d} = \mathfrak{e}$ for some q effectively computable from e and d. We have thus established that

$$\mathtt{V}^* \models \mathfrak{h} \text{ is a function.} \tag{39}$$

For (36) it remains to be shown that $\mathfrak{h}$ realizably maps onto $\mathfrak{a}$. So let $e \Vdash_{rt} \mathfrak{c} \in \mathfrak{a}$. Then $\langle (e)_0, \mathfrak{d}\rangle \in \mathfrak{a}^*$ and $(e)_1 \Vdash_{rt} \mathfrak{c} = \mathfrak{d}$ for some $\mathfrak{d}$. As g maps Y onto $\mathfrak{a}^*$ there exists $u \in Y$ such that $g(u) = \langle (e)_0, \mathfrak{d}\rangle = \langle g_0(u), 2^{nd}(g(u))\rangle$. Since $\langle g_0(u), \wp(u)\rangle \in \mathfrak{b}^*$ and $\left\langle g_0(u), \overline{\langle \wp(u), 2^{nd}(g(u))\rangle} \right\rangle \in \mathfrak{h}^*$ we have $\mathbf{p}(e)_0\mathbf{i}_r \Vdash_{rt} \wp(u) \in \mathfrak{b}$ and $\mathbf{p}(e)_0\mathbf{i}_r \Vdash_{rt} \overline{\langle \wp(u), \mathfrak{d}\rangle} \in \mathfrak{h}$. Therefore we can effectively compute an index $\tilde{e}$ from e such that $\tilde{e} \Vdash_{rt} \mathfrak{c}$ `is in the range of` $\mathfrak{h}$. In consequence, $\mathtt{V}^* \models \mathfrak{h}$ `maps onto` $\mathfrak{a}$. The latter in conjunction with (37), (38), and (39) yields (36).

Finally, we have to verify that

$$\mathtt{V}^* \models \mathfrak{b} \texttt{ is a base.} \tag{40}$$

So assume that

$$e \Vdash_{rt} \forall x \in \mathfrak{b}\, \exists y\, \varphi(x, y) \tag{41}$$

for some formula $\varphi(x, y)$ (parameters from $\mathtt{V}^*$ allowed). To ensure (40) we have to describe how to obtain an index e' calculably from e satisfying

$$e' \quad \Vdash_{rt} \quad \exists G\, [\mathbf{fun}(G) \wedge \mathbf{dom}(G) \supseteq \mathfrak{b} \wedge \forall x \in \mathfrak{b}\, \varphi(x, G(x))]\,. \tag{42}$$

From (41) it follows that $\forall x \in \mathfrak{b}^\circ\, \exists y\, \varphi^\circ(x, y)$, and hence, since $\mathfrak{b}^\circ = B = \tilde{X} \cup \tilde{Y}$,

$$\forall x \in \tilde{X}\, \exists y\, \varphi^\circ(x, y). \tag{43}$$

(41) also implies $\forall \langle n, \mathfrak{c}\rangle \in \mathfrak{b}^* \, \exists \mathfrak{d} \, en \Vdash_{rt} \varphi(\mathfrak{c}, \mathfrak{d})$, yielding

$$\forall u \in Y \, \exists \mathfrak{d} \; e(g_0(u)) \Vdash_{rt} \varphi(\wp(u), \mathfrak{d}). \tag{44}$$

$\tilde{X}$ and Y being bases, there exist functions K and L such that $\mathbf{dom}(K) = \tilde{X}$ and $L : Y \to \mathtt{V}^*$ satisfying

$$\forall x \in \tilde{X} \, \varphi^\circ(x, K(x)), \tag{45}$$

$$\forall u \in Y \; e(g_0(u)) \Vdash_{rt} \varphi(\wp(u), L(u)). \tag{46}$$

(46) implies that $\forall u \in Y \, \varphi^\circ\left(\langle g_0(u)+1, u\rangle, (L(u))^\circ\right)$, so that $\forall u \in \tilde{Y} \, \varphi^\circ\left(x, (L(2^{nd}(x)))^\circ\right)$. Hence, for the same reasons as in the definition of $\mathcal{F}$ (29) we can define a function M with domain $B = \tilde{X} \cup \tilde{Y}$ by

$$M(x) = \begin{cases} K(x) & \text{if } \; x \in \tilde{X} \\ \left(L(2^{nd}(x))\right)^\circ & \text{if } \; x \in \tilde{Y}. \end{cases} \tag{47}$$

As a result,

$$\forall x \in \mathfrak{b}^\circ \, \varphi^\circ(x, M(x)). \tag{48}$$

Next, to internalize M in $\mathtt{V}^*$ put

$$\mathcal{M} \;:=\; \{\langle\, g_0(u), \overline{\langle \wp(u), L(u)\rangle}\;\rangle \,:\, u \in Y\}, \tag{49}$$

$$\mathfrak{m} \;:=\; \langle M, \mathcal{M}\rangle. \tag{50}$$

For $y \in \mathfrak{m}^* = \mathcal{M}$ we have $y = \langle\, g_0(u), \overline{\langle \wp(u), L(u)\rangle}\;\rangle$ for some $u \in Y$, and thus $1^{st}(2^{nd}(y)) = \langle (\wp(u))^\circ, (L(u))^\circ\rangle = \langle\, \langle g_0(u)+1, u\rangle, (L(u))^\circ\,\rangle$, so that with $x := \langle g_0(u)+1, u\rangle$ we have $x \in \tilde{Y}$ and $(L(u))^\circ = \left(L(2^{nd}(x))\right)^\circ$, showing that $1^{st}(2^{nd}(y)) \in M$. In consequence, we see that $\mathfrak{m} \in \mathtt{V}^*$.

It remains to show that

$$e' \;\; \Vdash_{rt} \;\; \mathbf{fun}(\mathfrak{m}) \wedge \mathbf{dom}(\mathfrak{m}) \supseteq \mathfrak{b} \wedge \forall x \in \mathfrak{b} \, \varphi(x, \mathfrak{m}(x)) \tag{51}$$

for some index e' that is calculable from e.

To establish realizable functionality of $\mathfrak{m}$, suppose $a \Vdash_{rt} \overline{\langle \mathfrak{c}, \mathfrak{d}\rangle} \in \mathfrak{m}$ and $b \Vdash_{rt} \overline{\langle \mathfrak{c}, \mathfrak{e}\rangle} \in \mathfrak{m}$. Then there exist $u, v \in Y$ such that $(a)_0 = g_0(u)$, $(b)_0 = g_0(v)$, $(a)_1 \Vdash_{rt} \overline{\langle \mathfrak{c}, \mathfrak{d}\rangle} = \overline{\langle \wp(u), L(u)\rangle}$, and $(b)_1 \Vdash_{rt} \overline{\langle \mathfrak{c}, \mathfrak{e}\rangle} = \overline{\langle \wp(v), L(v)\rangle}$. Hence $\Vdash_{rt} \wp(u) = \wp(v)$, i.e. $\Vdash_{rt} \overline{\langle g_0(u)+1, u^{st}\rangle} = \overline{\langle g_0(v)+1, v^{st}\rangle}$, and therefore $\Vdash_{rt} u^{st} = v^{st}$, yielding $u = (u^{st})^\circ = (v^{st})^\circ = v$. As a result, $q \Vdash_{rt} \mathfrak{d} = \mathfrak{e}$ for some q effectively computable from a and b.

Next, we would like to verify that $\mathfrak{m}$ is realizably defined on elements of $\mathfrak{b}$. An element of $\mathfrak{b}^*$ is of the form $\langle g_0(u), \wp(u)\rangle$ for some $u \in Y$. As $\langle\, g_0(u), \overline{\langle \wp(u), L(u)\rangle}\;\rangle \in \mathfrak{m}^*$, it is obvious how to construct $\tilde{q}$ such that $\tilde{q}(g_0(u)) \Vdash_{rt} \langle g_0(u), \wp(u)\rangle \in \mathbf{dom}(\mathfrak{m})$, and hence

$$\mathtt{V}^* \models \mathfrak{b} \subseteq \mathbf{dom}(\mathfrak{m}). \tag{52}$$

Finally we have to ensure that

$$\tilde{e} \Vdash_{rt} \forall x \in \mathfrak{b} \, \varphi(x, \mathfrak{m}(x)) \tag{53}$$

for some $\tilde{e}$ computable from e. Now, each element of $\mathfrak{b}^*$ is of the form $\langle g_0(u), \wp(u)\rangle$ for some $u \in Y$. Since $\langle\, g_0(u), \overline{\langle \wp(u), L(u)\rangle}\;\rangle \in \mathfrak{m}^*$ and $e(g_0(u)) \Vdash_{rt} \varphi(\wp(u), L(u))$ holds by (46), we can cook up an index r such that $(re)(g_0(u)) \Vdash_{rt} \varphi\left(\wp(u), \mathfrak{m}(\wp(u))\right)$ and therefore, noting that $\forall x \in \mathfrak{b}^\circ \, \varphi^\circ(x, \mathfrak{m}^\circ(x))$ is true, we get $\tilde{e} \Vdash_{rt} \forall x \in \mathfrak{b} \, \varphi(x, \mathfrak{m}(x))$ for an index $\tilde{e}$ effectively computable from e. $\square$

Theorem 7.4 *If is T any of the theories* **CZF**, **CZF + REA**, **IZF**, *or* **IZF + REA**, *and $\mathcal{S}$ is any combination of the axioms and schemes* **MP**, $\mathbf{AC}_\omega$, **DC**, **RDC**, *and* **PAx**, *then $T + \mathcal{S}$ has the* **DP** *and the* **NEP**, *and $T + \mathcal{S}$ is closed under* **CR**, **ECR**, $\mathbf{CR_1}$, **UZR**, *and* **UR**.

Proof: This follows from Theorems 7.3 and 6.4 and the proof of [32] Theorem 1.2. □

Remark 7.5 Theorem 7.4 can be extended to include large set axioms such as *"Every set is contained in an inaccessible set"* or *"Every set is contained in a Mahlo set"*. For definitions of "inaccessible set" and "Mahlo set" see [4, 9]. The proofs are similar to the one for the so-called Regular Extension Axiom which was carried out in [32], Theorem 7.2.

References

[1] P. Aczel: *The type theoretic interpretation of constructive set theory.* In: MacIntyre, A. and Pacholski, L. and Paris, J, editor, *Logic Colloquium '77* (North Holland, Amsterdam 1978) 55–66.

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

[3] P. Aczel: *The type theoretic interpretation of constructive set theory: Inductive definitions.* In: R.B. et al. Marcus, editor, *Logic, Methodology and Philosophy of Science VII* (North Holland, Amsterdam 1986) 17–49.

[4] P. Aczel, M. Rathjen: *Notes on constructive set theory*, Technical Report 40, Institut Mittag-Leffler (The Royal Swedish Academy of Sciences, 2001). *http://www.ml.kva.se/preprints/archive2000-2001.php*

[5] M. Beeson: *Continuity in intuitionistic set theories*, in: M Boffa, D. van Dalen, K. McAloon (eds.): *Logic Colloquium '78* (North-Holland, Amsterdam, 1979).

[6] M. Beeson: *Foundations of Constructive Mathematics.* (Springer-Verlag, Berlin, Heidelberg, New York, Tokyo, 1985).

[7] A. Blass: *Injectivity, projectivity, and the axiom of choice.* Transactions of the AMS 255 (1979) 31–59.

[8] E. Bishop and D. Bridges: *Constructive Analysis.* (Springer-Verlag, Berlin, Heidelberg, New York, Tokyo, 1985).

[9] L. Crosilla, M. Rathjen:*Inaccessible set axioms may have little consistency strength.* Annals of Pure and Applied Logic 115 (2002) 33-70.

[10] S. Feferman: *A language and axioms for explicit mathematics*, in: J.N. Crossley (ed.): *Algebra and Logic*, Lecture Notes in Math. 450 (Springer, Berlin 1975) 87–139.

[11] S. Feferman: *Constructive theories of functions and classes* in: Boffa, M., van Dalen, D., McAloon, K. (eds.), *Logic Colloquium '78* (North-Holland, Amsterdam 1979) 159–224.

[12] H. Friedman: *Some applications of Kleene's method for intuitionistic systems.* In: A. Mathias and H. Rogers (eds.): *Cambridge Summer School in Mathematical Logic*, volume 337 of *Lectures Notes in Mathematics* (Springer, Berlin, 1973) 113–170.

[13] H. Friedman: *The disjunction property implies the numerical existence property.* Proceedings of the National Academy of Sciences of the United States of America 72 (1975) 2877-2878.

[14] H. Friedman: *Set-theoretic foundations for constructive analysis.* Annals of Mathematics 105 (1977) 868-870.

[15] H. Friedman, S. Ščedrov: *Set existence property for intuitionistic theories with dependent choice.* Annals of Pure and Applied Logic 25 (1983) 129–140.

[16] H. Friedman, S. Ščedrov: *The lack of definable witnesses and provably recursive functions in intuitionistic set theory*, Advances in Mathematics 57 (1985) 1–13.

[17] S.C. Kleene: *On the interpretation of intuitionistic number theory.* Journal of Symbolic Logic 10 (1945) 109–124.

[18] S.C. Kleene: *Disjunction and existence under implication in elementary intuitionistic formalisms.* Journal of Symbolic Logic 27 (1962) 11–18.

[19] S.C. Kleene: *An addendum.* Journal of Symbolic Logic 28 (1963) 154–156.

[20] S.C. Kleene: *Formalized recursive functionals and formalized realizability.* Memoirs of the AMS 89 (AMS, Providence, 1969).

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

[22] J. Lipton: *Realizability, set theory and term extraction.* In: *The Curry-Howard isomorphism*, Cahiers du Centre de Logique de l'Universite Catholique de Louvain, vol. 8 (1995) 257–364.

[23] D.C. McCarty: *Realizability and recursive mathematics*, PhD thesis, Oxford University (1984), 281 pages.

[24] D.C. McCarty: *Realizability and recursive set theory*, Annals of Pure and Applied Logic 32 ,(1986) 153–183.

[25] J.R. Moschovakis: *Disjunction and existence in formalized intuitionistic analysis.* In: J.N. Crossley (ed.): *Sets, models and recursion theory.* (Noth-Holland, Amsterdam, 1967) 309–331.

[26] J. Myhill: *Some properties of Intuitionistic Zermelo-Fraenkel set theory.* In: A. Mathias and H. Rogers (eds.): *Cambridge Summer School in Mathematical Logic*, volume 337 of *Lectures Notes in Mathematics* (Springer, Berlin, 1973) 206–231.

[27] J. Myhill: *Constructive set theory.* Journal of Symbolic Logic, 40:347–382, 1975.

[28] M. Rathjen: *The anti-foundation axiom in constructive set theories.* In: G. Mints, R. Muskens (eds.): *Games, Logic, and Constructive Sets.* (CSLI Publications, Stanford, 2003) 87–108.

[29] M. Rathjen: *Realizability for constructive Zermelo-Fraenkel set theory.* To appear in: J. Väänänen, V. Stoltenberg-Hansen (eds.): *Proceedings of the Logic Colloquium 2003.*

[30] M. Rathjen: *Choice principles in constructive and classical set theories.* To appear in: Z. Chatzidakis, P. Koepke, W. Pohlers (eds.): *Proceedings of the Logic Colloquium 2002.*

[31] M. Rathjen, S. Tupailo: *Characterizing the interpretation of set theory in Martin-Löf type theory.* To appear in: Annals of Pure and Applied Logic.

[32] M. Rathjen: *The disjunction and other properties for constructive Zermelo-Fraenkel set theory.* Journal of Symbolic Logic 70 (2005) 1233-1254.

[33] L. Tharp: *A quasi-intuitionistic set theory.* Journal of Symbolic Logic 36 (1971) 456–460.

[34] A.S. Troelstra: *Realizability.* In: S.R. Buss (ed.): *Handbook of proof theory* (Elsevier, Amsterdam, 1998) 407–473.

[35] A.S. Troelstra and D. van Dalen: *Constructivism in Mathematics, Volumes I, II.* (North Holland, Amsterdam, 1988).