Normalization of IZF with Replacement[*]

Wojciech Moczydłowski

Department of Computer Science, Cornell University, Ithaca, NY, 14853, USA,
wojtek@cs.cornell.edu

Abstract. IZF is a well investigated impredicative constructive version of Zermelo-Fraenkel set theory. Using set terms, we axiomatize IZF with Replacement, which we call IZF_R, along with its intensional counterpart IZF_R^-. We define a typed lambda calculus corresponding to proofs in IZF_R^- according to the Curry-Howard isomorphism principle. Using realizability for IZF_R^-, we show weak normalization of the calculus by employing a reduction-preserving erasure map from lambda terms to realizers. We use normalization to prove disjunction, numerical existence, set existence and term existence properties. An inner extensional model is used to show the properties for full, extensional IZF_R.

1 Introduction

There are four salient properties of constructive theories:

- Numerical Existence Property (NEP): From a proof of a statement "there exists a natural number x such that ..." a witness $n \in \mathbb{N}$ can be extracted.
- Disjunction Property (DP): If a disjunction is provable, then one of the disjuncts is provable.
- Set Existence Property (SEP): If a $\exists x.\ \phi(x)$ is provable, then there is a formula $\psi(x)$ such that $\exists! x.\ \phi(x) \land \psi(x)$ is provable, where both ϕ and ψ are term-free.
- Term Existence Property (TEP): If $\exists x.\ \phi(x)$ is provable, then $\phi(t)$ is provable for some term t.

How to prove these properties for a given theory? Methods abound. Cut-elimination, proof normalization, realizability, Kripke models.... Normalization proofs, based on Curry-Howard isomorphism, have the advantage of providing an explicit method of witness and program extraction from the proofs. They also provide information about the behaviour of the proof system.

We are interested in intuitionistic set theory IZF. It is essentially what remains of ZF set theory after excluded middle is carefully taken away. An important decision to make on the way is whether to use Replacement or Collection axiom schema. We will call the version with Collection IZF_C and the version with Replacement IZF_R. In the literature, IZF usually denotes IZF_C. Both theories with excluded middle added are equivalent to ZF.

[*] This research was partly supported by NSF grants DUE-0333526 and 0430161.

Both versions have been investigated. Results up to 1985 are presented in [Bee85] and in [Ŝ85], later research was concentrated on weaker subsystems, in particular on predicative constructive set theory CZF. [AR01] describes the set-theoretic apparatus available in CZF and provides further references.

IZF_C is equiconsistent with ZF ([Fri73]), has the same set of Π^0_2 statements ([Fri78]) and satisfies NEP and DP ([Bee79]). It does not satisfy SEP ([FS85]).

Classically, using Foundation, one can show that Collection is equivalent to Replacement. This is not the case in the constructive world, as shown in [FS85]. In the author's view, Collection in the constructive context seems to be as nonconstructive as the Axiom of Choice in the classical world. It asserts the existence of a certain set without pointing it out or, more formally, defining it. We therefore think that IZF_R makes more sense from a constructive point of view.

Myhill in [Myh73] has shown that IZF_R satisfies NEP, DP, SEP and a version of TEP. Its exact proof-theoretic power is unknown; [FS85] conjectures that ZF proves consistency of IZF_R.

We define an axiomatization of IZF_R with set-terms, along with its intensional version IZF_R^-. We define typed lambda calculus λZ corresponding to proofs in IZF_R^-. We also define realizability for IZF_R^-, in the spirit of [McC84]. We show weak normalization of λZ by employing a reduction-preserving erasure map from lambda terms to realizers. Strong normalization of λZ does not hold; moreover, we show that in non-well-founded IZF even weak normalization fails.

With normalization in hand, the properties NEP, DP, SEP and TEP follow easily. To show these properties for full, extensional IZF_R, we define an inner model T of IZF_R, consisting of what we call transitively L-stable sets. We show that a formula is true in IZF_R iff its relativization to T is true in IZF_R^-. Therefore IZF_R is interpretable in IZF_R^-. This allows us to use properties proven for IZF_R^-.

The importance of these properties in the context of computer science stems from the fact that they make it possible to extract programs from constructive proofs. For example, suppose $\mathrm{IZF}_R \vdash \forall n \in \mathbb{N} \exists m \in \mathbb{N}.\ \phi(n, m)$. From this proof a program can be extracted — take a natural number n, construct a proof $\mathrm{IZF}_R \vdash \overline{n} \in \mathbb{N}$ in T. Combine the proofs to get $\mathrm{IZF}_R \vdash \exists m \in \mathbb{N}.\ \phi(\overline{n}, m)$ and apply NEP to get a number m such that $\mathrm{IZF}_R \vdash \phi(\overline{n}, \overline{m})$. We will present in details program extraction from IZF_R proofs in the forthcoming [CM06].

There are many provers with the program extraction capability. However, they are usually based on a variant of type theory, which is a foundational basis very different from set theory. This makes the process of formalizing program specification more difficult, as an unfamiliar new language and logic have to be learned from scratch. [LP99] strongly argues *against* using type theory for the specification purposes, instead promoting standard set theory.

IZF_R provides therefore the best of both worlds. It is a set theory, with familiar language and axioms. At the same time, programs can be extracted from proofs. Our λZ calculus and the normalization theorem make the task of constructing the prover based on IZF_R not very difficult. Non-constructive reasoning could be supported as well, by simply adding the excluded middle and the Axiom of Choice.

Moreover, we believe in the importance of IZF_R in the process of formalizing mathematics. The standard foundational ground for mathematics is ZFC. However, many proofs could be formalized using only the axioms of IZF_R. A theorem proved with these restricted means would provide extra computational content. For example, the proof that the addition function exists could give rise to the actual *program* computing the sum of two natural numbers.

This paper is organized as follows. In sections 2 and 3 we define IZF_R along with its intensional version IZF_R^-. In section 4 we define a lambda calculus λZ corresponding to IZF_R^- proofs. Realizability for IZF_R^- is defined in section 5 and used to prove normalization of λZ in section 6. We prove the properties in section 7, and show how to derive them for IZF_R in section 8. Comparison with other results can be found in section 9.

2 Intuitionistic first-order logic

We start by presenting the intuitionistic first-order logic (IFOL). We use a natural deduction style of proof rules. The terms will be denoted by letters t, s, u. The logical variables will be denoted by letters a, b, c, d, e, f. The notation $\overline{a}$ denotes a finite sequence, treated as a set when convenient. The i-th element of a sequence is denoted by a_i. We consider α-equivalent formulas equal. Contexts, denoted by Γ, are sets of formulas. The free variables of a formula ϕ, denoted by $FV(\phi)$, are defined as usual. Free variables of a context Γ, denoted by $FV(\Gamma)$, are the free variables of all formulas in Γ. The notation $\phi(\overline{a})$ means that all free variables of ϕ are among $\overline{a}$. The proof rules are as follows:

$$\frac{}{\Gamma, \phi \vdash \phi} \qquad \frac{\Gamma \vdash \phi \to \psi \quad \Gamma \vdash \phi}{\Gamma \vdash \psi} \qquad \frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \to \psi} \qquad \frac{\Gamma \vdash \phi \land \psi}{\Gamma \vdash \phi} \qquad \frac{\Gamma \vdash \phi \land \psi}{\Gamma \vdash \psi}$$

$$\frac{\Gamma \vdash \phi \quad \Gamma \vdash \psi}{\Gamma \vdash \phi \land \psi} \qquad \frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \lor \psi} \quad \frac{\Gamma \vdash \psi}{\Gamma \vdash \phi \lor \psi} \quad \frac{\Gamma \vdash \phi \lor \psi \quad \Gamma, \phi \vdash \vartheta \quad \Gamma, \psi \vdash \vartheta}{\Gamma \vdash \vartheta}$$

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \forall a.\ \phi}\ a \notin FV(\Gamma) \qquad \frac{\Gamma \vdash \forall a.\ \phi}{\Gamma \vdash \phi[a := t]} \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash \phi}$$

$$\frac{\Gamma \vdash \phi[a := t]}{\Gamma \vdash \exists a.\ \phi} \qquad \frac{\Gamma \vdash \exists a.\ \phi \quad \Gamma, \phi \vdash \psi}{\Gamma \vdash \psi}\ a \notin FV(\Gamma) \cup \{\psi\}$$

Negation in IFOL is an abbreviation: $\neg\phi \equiv \phi \to \bot$. So is the symbol $\leftrightarrow$: $\phi \leftrightarrow \psi \equiv (\phi \to \psi \land \psi \to \phi)$. For any theory T, the notation $\Gamma \vdash_T \phi$ means $T + \Gamma \vdash \phi$. Note that IFOL does not contain equality. The excluded middle rule added to IFOL makes it equivalent to classical first-order logic without equality.

3 IZF$_R$

Intuitionistic set theory IZF$_R$ is a first-order theory. It is equivalent to ZF, if extended with excluded middle. It's a definitional extension of term-free versions presented in [Myh73], [Bee85] and [FS85] among others. The signature consists of one binary relational symbol $\in$ and function symbols used in the axioms below. The relational symbol $t = u$ is an abbreviation for $\forall z.\ z \in t \leftrightarrow z \in u$. Function symbols 0 and $S(t)$ are abbreviations for $\{x \in \omega \mid \bot\}$ and $\bigcup\{t, \{t, t\}\}$. Bounded quantifiers and the quantifier $\exists! a$ (there exists exactly one a) are also abbreviations defined in the standard way.

- (PAIR) $\forall a, b \forall c.\ c \in \{a, b\} \leftrightarrow c = a \lor c = b$
- (INF) $\forall c.\ c \in \omega \leftrightarrow c = 0 \lor \exists b \in \omega.\ c = S(b)$
- (SEP$_{\phi(a,\overline{f})}$) $\forall \overline{f} \forall a \forall c.\ c \in S_{\phi(a,\overline{f})}(a, \overline{f}) \leftrightarrow c \in a \land \phi(c, \overline{f})$
- (UNION) $\forall a \forall c.\ c \in \bigcup a \leftrightarrow \exists b \in a.\ c \in b$
- (POWER) $\forall a \forall c.\ c \in P(a) \leftrightarrow \forall b.\ b \in c \to b \in a$
- (REPL$_{\phi(a,b,\overline{f})}$) $\forall \overline{f} \forall a \forall c. c \in R_{\phi(a,b,\overline{f})}(a, \overline{f}) \leftrightarrow (\forall x \in a \exists! y. \phi(x, y, \overline{f}))) \land ((\exists x \in a.\ \phi(x, c, \overline{f}))$
- (IND$_{\phi(a,\overline{f})}$) $\forall \overline{f}.\ (\forall a. (\forall b \in a. \phi(b, \overline{f})) \to \phi(a, \overline{f})) \to \forall a. \phi(a, \overline{f})$
- (L$_{\phi(a,\overline{f})}$) $\forall \overline{f}, \forall a, b.\ a = b \to \phi(a, \overline{f}) \to \phi(b, \overline{f})$

Axioms SEP$_\phi$, REPL$_\phi$, IND$_\phi$ and L$_\phi$ are axiom schemas, and so are the corresponding function symbols — there is one for each formula ϕ. Formally, we define formulas and terms by mutual induction:

$$\phi ::= t \in t \mid t = t \mid \ldots \qquad\qquad t ::= a \mid \{t, t\} \mid\ S_{\phi(a,\overline{f})}(t, \overline{t}) \mid R_{\phi(a,b,\overline{f})}(t, \overline{t}) \mid \ldots$$

IZF$_R^-$ will denote IZF$_R$ without the Leibniz axiom schema L$_\phi$. IZF$_R^-$ is an intensional version of IZF$_R$ — even though extensional equality is used in the axioms, it does not behave as the "real" equality. The terms $S_\phi(a, \overline{f})$ and $R_\phi(a, \overline{f})$ could be displayed as $\{x \in a \mid \phi(x, \overline{f})\}$ and $\{y \mid \exists x \in a.\ \phi(x, y, \overline{f}) \land \forall x \in a \exists! y.\ \phi(x, y, \overline{f})\}$.

Axioms (PAIR), (INF), (SEP$_\phi$), (UNION), (POWER) and (REPL$_\phi$) all assert the existence of certain classes and have the same form: $\forall \overline{a}. \forall c.\ c \in t_A(\overline{a}) \leftrightarrow \phi_A(\overline{a}, c)$, where t_A is a function symbol and ϕ_A a corresponding formula for the axiom A. For example, for (POWER), t_{POWER} is P and ϕ_{POWER} is $\forall b.\ b \in c \to b \in a$. We reserve the notation t_A and ϕ_A to denote the term and the corresponding formula for the axiom A.

4 The λZ calculus

We present a lambda calculus λZ for IZF$_R^-$, based on the Curry-Howard isomorphism principle. The purely logical part is essentially $\lambda P1$ from [SU98].

4.1 Terms

The lambda terms in λZ will be denoted by letters M, N, O, P. Letters x, y, z will be used for lambda variables. There are two kinds of lambda abstractions, one used for proofs of implications, the other for proofs of universal quantification. Since variables in the latter abstractions correspond very closely to the variables in IFOL, we also use letters a, b, c for them. Letters t, s, u are reserved for IZF_R terms. The types in the system are IZF_R formulas.

$$M ::= x \mid M\ N \mid \lambda a.\ M \mid \lambda x : \phi.\ M \mid \mathrm{inl}(M) \mid \mathrm{inr}(M) \mid \mathrm{fst}(M) \mid \mathrm{snd}(M) \mid [t, M]$$

$$M\ t \mid \langle M, N\rangle \mid \mathrm{case}(M, x.N, x.O) \mid \mathrm{magic}(M) \mid \mathrm{let}\ [a, x : \phi] = M \ \mathrm{in}\ N$$

$$\mathrm{ind}_{\phi(a,\overline{b})}(M, \overline{t}) \mid \mathrm{ind}'_{\phi(a,\overline{b})}(M, \overline{t}, u)$$

$$\mathrm{pairProp}(t, u_1, u_2, M) \mid \mathrm{pairRep}(t, u_1, u_2, M)$$

$$\mathrm{unionProp}(t, u, M) \mid \mathrm{unionRep}(t, u, M)$$

$$\mathrm{sep}_{\phi(a,\overline{f})}\mathrm{Prop}(t, u, \overline{u}, M) \mid \mathrm{sep}_{\phi(a,\overline{f})}\mathrm{Rep}(t, u, \overline{u}, M)$$

$$\mathrm{powerProp}(t, u, M) \mid \mathrm{powerRep}(t, u, M)$$

$$\mathrm{infProp}(t, M) \mid \mathrm{infRep}(t, M)$$

$$\mathrm{repl}_{\phi(a,b,\overline{f})}\mathrm{Prop}(t, u, \overline{u}) \mid \mathrm{repl}_{\phi(a,b,\overline{f})}\mathrm{Rep}(t, u, \overline{u})$$

The ind terms correspond to the (IND) axiom, and Prop and Rep terms correspond to the respective axioms. To avoid listing all of them every time, we adopt a convention of using axRep and axProp terms to tacitly mean all Rep and Prop terms, for ax being one of pair, union, sep, power, inf and repl. With this convention in mind, we can summarize the definition of the Prop and Rep terms as:

$$\mathrm{axProp}(t, \overline{u}, M) \mid \mathrm{axRep}(t, \overline{u}, M),$$

where the number of terms in the sequence $\overline{u}$ depends on the particular axiom.

The free variables of a lambda term are defined as usual, taking into account that variables in λ, case and let terms bind respective terms. The relation of α-equivalence is defined taking this information into account. We consider α-equivalent terms equal. We denote all free variables of a term M by $FV(M)$ and the free logical variables of a term by $FV_L(M)$. Free (logical) variables of a context Γ are denoted by $FV(\Gamma)$ ($FV_L(\Gamma)$) and defined in a natural way.

4.2 Reduction rules

The deterministic reduction relation $\to$ arises from the following reduction rules and evaluation contexts:

$$(\lambda x : \phi.\ M)N \to M[x := N] \qquad (\lambda a.\ M)t \to M[a := t]$$

$$\mathrm{fst}(\langle M, N\rangle) \to M \qquad \mathrm{snd}(\langle M, N\rangle) \to N$$

$$\mathrm{case}(\mathrm{inl}(M), x.N, x.O) \to N[x := M] \qquad \mathrm{case}(\mathrm{inr}(M), x.N, x.O) \to O[x := M]$$
$$\mathrm{let}\ [a, x : \phi] = [t, M]\ \mathrm{in}\ N \to N[a := t][x := M]$$
$$\mathrm{axProp}(t, \overline{u}, \mathrm{axRep}(t, \overline{u}, M)) \to M$$
$$\mathrm{ind}_{\phi(a,\overline{b})}(M, \overline{t}) \to \lambda c.\ M\ c\ (\lambda b.\lambda x : b \in c.\ \mathrm{ind}'_{\phi(a,\overline{b})}(M, \overline{t}, b))$$
$$\mathrm{ind}'_{\phi(a,\overline{b})}(M, \overline{t}, u) \to M\ u\ (\lambda b.\lambda x : b \in u.\ \mathrm{ind}'_{\phi(a,\overline{b})}(M, \overline{t}, b))$$
$$[\circ] ::= \mathrm{fst}([\circ]) \mid \mathrm{snd}([\circ]) \mid \mathrm{case}([\circ], x.M, x.N) \mid \mathrm{axProp}(t, \overline{u}, [\circ])$$
$$\mathrm{let}\ [a, y : \phi] = [\circ]\ \mathrm{in}\ N \mid [\circ]\ M \mid \mathrm{magic}([\circ])$$

In the reduction rules for ind terms, the variable x is new. In other words, the reduction relation arises by lazily evaluating the rules above.

Definition 1. *We write $M \downarrow$ if the reduction sequence starting from M terminates. We write $M \downarrow v$ if we want to state that v is the term at which this reduction sequence terminates. We write $M \to^* M'$ if M reduces to M' in some number of steps.*

We distinguish certain λZ terms as values. The values are generated by the following abstract grammar, where M is an arbitrary term. Clearly, there are no reductions possible from values.

$$V ::= \lambda a.\ M \mid \lambda x : \phi.\ M \mid \mathrm{inr}(M) \mid \mathrm{inl}(M) \mid [t, M] \mid \langle M, N \rangle \mid \mathrm{axRep}(t, \overline{u}, M)$$

4.3 Types

The type system for λZ is constructed according to the principle of the Curry-Howard isomorphism for IZF_R^-. Types are IZF_R formulas, and terms are λZ terms. Contexts Γ are finite sets of pairs (x_1, ϕ_i). The *range* of a context Γ is the corresponding IFOL context that contains only formulas and is denoted by $rg(\Gamma)$. The proof rules follow:

$$\frac{}{\Gamma, x : \phi \vdash x : \phi} \qquad \frac{\Gamma \vdash M : \phi \to \psi \quad \Gamma \vdash N : \phi}{\Gamma \vdash M\ N : \psi} \qquad \frac{\Gamma, x : \phi \vdash M : \psi}{\Gamma \vdash \lambda x : \phi.M : \phi \to \psi}$$

$$\frac{\Gamma \vdash M : \phi \quad \Gamma \vdash N : \psi}{\Gamma \vdash \langle M, N \rangle : \phi \wedge \psi} \qquad \frac{\Gamma \vdash M : \phi \wedge \psi}{\Gamma \vdash \mathrm{fst}(M) : \phi} \qquad \frac{\Gamma \vdash M : \phi \wedge \psi}{\Gamma \vdash \mathrm{snd}(M) : \psi}$$

$$\frac{\Gamma \vdash M : \phi}{\Gamma \vdash \mathrm{inl}(M) : \phi \vee \psi} \qquad \frac{\Gamma \vdash M : \psi}{\Gamma \vdash \mathrm{inr}(M) : \phi \vee \psi} \qquad \frac{\Gamma \vdash M : \phi}{\Gamma \vdash \lambda a.\ M : \forall a.\ \phi}\ a \notin FV_L(\Gamma)$$

$$\frac{\Gamma \vdash M : \phi \vee \psi \quad \Gamma, x : \phi \vdash N : \vartheta \quad \Gamma, x : \psi \vdash O : \vartheta}{\Gamma \vdash \mathrm{case}(M, x.N, x.O) : \vartheta} \qquad \frac{\Gamma \vdash M : \forall a.\ \phi}{\Gamma \vdash M\ t : \phi[a := t]}$$

$$\frac{\Gamma \vdash M : \phi[a := t]}{\Gamma \vdash [t, M] : \exists a.\ \phi} \qquad \frac{\Gamma \vdash M : \bot}{\Gamma \vdash \mathrm{magic}(M) : \phi}$$

$$\frac{\Gamma \vdash M : \exists a.\ \phi \quad \Gamma, x : \phi \vdash N : \psi}{\Gamma \vdash \mathrm{let}\ [a, x : \phi] := M\ in\ N : \psi}\ a \notin FV_L(\Gamma, \psi)$$

$$\frac{\Gamma \vdash M : \phi_A(t, \overline{u})}{\Gamma \vdash \mathrm{axRep}(t, \overline{u}, M) : t \in t_A(\overline{u})} \qquad \frac{\Gamma \vdash M : t \in t_A(\overline{u})}{\Gamma \vdash \mathrm{axProp}(t, \overline{u}, M) : \phi_A(t, \overline{u})}$$

$$\frac{\Gamma \vdash M : \forall c.\ (\forall b.\ b \in c \to \phi(b, \overline{t})) \to \phi(c, \overline{t})}{\Gamma \vdash \mathrm{ind}'_{\phi(b,\overline{c})}(M, \overline{t}, u) : \phi(u, \overline{t})}$$

$$\frac{\Gamma \vdash M : \forall c.\ (\forall b.\ b \in c \to \phi(b, \overline{t})) \to \phi(c, \overline{t})}{\Gamma \vdash \mathrm{ind}_{\phi(b,\overline{c})}(M, \overline{t}) : \forall a.\ \phi(a, \overline{t})}$$

Lemma 1 (Curry-Howard isomorphism, part 1). *If $\Gamma \vdash O : \phi$ then $rg(\Gamma) \vdash_{IZF_R^-} \phi$. If $\Gamma \vdash_{IZF_R^-} \phi$, then there exists a term M such that $\overline{\Gamma} \vdash M : \phi$, where $\overline{\Gamma} = \{(x_\phi, \phi) \mid \phi \in \Gamma\}$.*

Proof. Straightforward. Use

$$\lambda\overline{a}\lambda c.\langle \lambda x : c \in t_A(\overline{a}).\ \mathrm{axProp}(c, \overline{a}, x), \lambda x : \phi_A(c, \overline{a}).\ \mathrm{axRep}(c, \overline{a}, x)\rangle$$

and

$$\lambda\overline{f}\lambda x : (\forall a.(\forall b.\ b \in a \to \phi(b, \overline{f})) \to \phi(a, \overline{f})).\ \mathrm{ind}(x, \overline{f})$$

to witness IZF_R^-axioms.

Lemma 2 (Canonical forms). *Suppose M is a value and $\vdash M : \vartheta$. Then:*

- *If $\vartheta = \phi \vee \psi$, then ($M = \mathrm{inl}(N)$ and $\vdash N : \phi$) or ($M = \mathrm{inr}(N)$ and $\vdash N : \psi$).*
- *If $\vartheta = \tau \wedge \sigma$, then $M = \langle N, O\rangle$.*
- *If $\vartheta = \tau \to \sigma$, then $M = \lambda x : \tau.\ N$.*
- *If $\vartheta = \forall a.\ \tau$, then $M = \lambda a.\ N$.*
- *If $\vartheta = \exists a.\ \phi$ then $M = [t, N]$ and $\vdash N : \phi[a := t]$.*
- *If $\vartheta = t \in t_A(\overline{u})$ then $M = \mathrm{axRep}(t, \overline{u}, N)$ and $\vdash N : \phi_A(t, \overline{u})$.*

Proof. Immediate from the typing rules and from the possible forms of values.

Lemma 3 (Progress). *If $\vdash M : \phi$, then either M is a value or there is a N such that $M \to N$.*

Proof. Straightforward induction on $\vdash M : \phi$.

Lemma 4 (Subject reduction). *If $\Gamma \vdash M : \phi$ and $M \to N$, then $\Gamma \vdash N : \phi$.*

Proof. By induction on the definition of $M \to N$, using appropriate substitution lemmas on the way.

Corollary 1. *If $\vdash M : \phi$ and $M \downarrow v$, then $\vdash v : \phi$ and v is a value.*

5 Realizability for $\mathbf{IZF}_{\boldsymbol{R}}^{-}$

In this section we work in ZF.

We use terms of type-free version of lambda calculus for realizers. We call this calculus $\lambda\overline{Z}$. The terms of $\lambda\overline{Z}$ are generated by the following grammar and are denoted by $\Lambda_{\overline{Z}}$. The set of $\lambda\overline{Z}$ values is denoted by $\lambda\overline{Z}_v$.

$$M ::= x \mid M\ N \mid \lambda x.\ M \mid \mathrm{inl}(M) \mid \mathrm{inr}(M) \mid \mathrm{magic}(M) \mid \mathrm{fst}(M) \mid \mathrm{snd}(M) \mid \langle M, N\rangle$$
$$\mathrm{case}(M, x.N, x.O) \mid \mathrm{axRep}(M) \mid \mathrm{axProp}(M) \mid \mathrm{ind}(M) \mid \mathrm{ind}'(M)$$

In other words, $\lambda\overline{Z}$ results from λZ by erasing of all first-order information. This can be made precise by the definition of the erasure map $\overline{M}$ from terms of λZ to $\lambda\overline{Z}$:

$$\overline{x} = x \qquad \overline{M\ N} = \overline{M}\ \overline{N} \qquad \overline{\lambda a.M} = \overline{M} \qquad \overline{\lambda x : \tau.M} = \lambda x.\ \overline{M}$$
$$\overline{[t, M]} = \overline{M} \qquad \overline{\langle M, N\rangle} = \langle\overline{M}, \overline{N}\rangle \qquad \overline{\mathrm{inl}(M)} = \mathrm{inl}(\overline{M}) \qquad \overline{\mathrm{inr}(M)} = \mathrm{inr}(\overline{M})$$
$$\overline{\mathrm{fst}(M)} = \mathrm{fst}(\overline{M}) \qquad \overline{\mathrm{snd}(M)} = \mathrm{snd}(\overline{M}) \qquad \overline{\mathrm{magic}(M)} = \mathrm{magic}(\overline{M})$$
$$\overline{\mathrm{let}[a, y] = M \text{ in } N} = (\lambda y.\ \overline{N})\ \overline{M} \qquad \overline{M\ t} = \overline{M}$$
$$\overline{\mathrm{axRep}(t, \overline{u}, M)} = \mathrm{axRep}(\overline{M}) \quad \overline{\mathrm{axProp}(t, \overline{u}, M)} = \mathrm{axProp}(\overline{M})$$
$$\overline{\mathrm{ind}'_\phi(M, \overline{t}, u)} = \mathrm{ind}'(\overline{M}) \qquad \overline{\mathrm{ind}_\phi(M, \overline{t}, u)} = \mathrm{ind}(\overline{M})$$

We call a λZ reduction *atomic* if it is of the form $(\lambda a.\ M)\ t \to M[a := t]$. The reduction rules and values in $\lambda\overline{Z}$ are induced in an obvious way from λZ, so that if $M \to M'$ is a nonatomic reduction in λZ, then $\overline{M} \to \overline{M'}$, if $M \to M'$ is an atomic reduction in λZ, then $\overline{M} = \overline{M'}$ and if M is a value in λZ, then $\overline{M}$ is a value in $\lambda\overline{Z}$. In particular, $\mathrm{ind}'(M) \to M\ (\lambda x.\ \mathrm{ind}'(M))$ and $\mathrm{ind}(M) \to M\ (\lambda x.\ \mathrm{ind}'(M))$.

Lemma 5. *If $\overline{M}$ normalizes, so does M.*

Proof. Any infinite chain of reductions starting from M must contain an infinite number of nonatomic reductions, which map to reductions in $\overline{M}$ in a natural way.

5.1 Realizability relation

Definition 2. *A set A is a λ-name iff A is a set of pairs (v, B) such that $v \in \lambda\overline{Z}_v$ and B is a λ-name.*

In other words, λ-names are sets hereditarily labelled by $\lambda\overline{Z}$ values.

Definition 3. *The class of λ-names is denoted by V^λ.*

Formally, V^λ is generated by the following transfinite inductive definition on ordinals:

$$V^\lambda_\alpha = \bigcup_{\beta<\alpha} P(\lambda\overline{Z}_v \times V^\lambda_\beta) \qquad V^\lambda = \bigcup_{\alpha \in ORD} V^\lambda_\alpha$$

The λ-*rank* of a λ-name A is the smallest α such that $A \in V^\lambda_\alpha$.

Definition 4. *For any $A \in V^\lambda$, A^+ denotes $\{(M, B) \mid M \downarrow v \wedge (v, B) \in A\}$.*

Definition 5. *A (class-sized) first-order language L arises by enriching the IZF_Rsignature with constants for all λ-names.*

From now on until the end of this section, symbols M, N, O, P range exclusively over $\lambda\overline{Z}$-terms, letters a, b, c vary over logical variables in the language, letters A, B, C vary over λ-names and letter ρ varies over finite partial functions from logic variables in L to V^λ. We call such functions *environments*.

Definition 6. *For any formula ϕ of L, any term t of L and ρ defined on all free variables of ϕ and t, we define by metalevel mutual induction a realizability relation $M \Vdash_\rho \phi$ in an environment ρ and a meaning of a term $[\![t]\!]_\rho$ in an environment ρ:*

1. $[\![a]\!]_\rho \equiv \rho(a)$
2. $[\![A]\!]_\rho \equiv A$
3. $[\![\omega]\!]_\rho \equiv \omega'$, *where ω' is defined by the means of inductive definition: ω' is the smallest set such that:*
   - $(\mathrm{infRep}(N), A) \in \omega'$ *if* $N \downarrow \mathrm{inl}(O)$, $O \Vdash A = 0$ *and* $A \in V^\lambda_\omega$.
   - *If* $(M, B) \in \omega'^+$, *then* $(\mathrm{infRep}(N), A) \in \omega'$ *if* $N \downarrow \mathrm{inr}(O)$, $O \downarrow \langle M, P\rangle$, $P \Vdash A = S(B)$ *and* $A \in V^\lambda_\omega$.

   It is easy to see that any element of ω' is in V^λ_α for some finite α and so that $\omega' \in V^\lambda_{\omega+1}$.
4. $[\![t_A(\overline{u})]\!]_\rho \equiv \{(\mathrm{axRep}(N), B) \in \lambda\overline{Z}_v \times V^\lambda_\gamma \mid N \Vdash_\rho \phi_A(B, [\![\overline{u}]\!]_\rho)\}$
5. $M \Vdash_\rho \bot \equiv \bot$
6. $M \Vdash_\rho t \in s \equiv M \downarrow v \wedge (v, [\![t]\!]_\rho) \in [\![s]\!]_\rho$
7. $M \Vdash_\rho \phi \wedge \psi \equiv M \downarrow \langle M_1, M_2\rangle \wedge M_1 \Vdash_\rho \phi \wedge M_2 \Vdash_\rho \psi$
8. $M \Vdash_\rho \phi \vee \psi \equiv (M \downarrow \mathrm{inl}(M_1) \wedge M_1 \Vdash_\rho \phi) \vee (M \downarrow \mathrm{inr}(M_1) \wedge M_1 \Vdash_\rho \psi)$
9. $M \Vdash_\rho \phi \to \psi \equiv (M \downarrow \lambda x.\ M_1) \wedge \forall N.\ (N \Vdash_\rho \phi) \to (M_1[x := N] \Vdash_\rho \psi)$
10. $M \Vdash_\rho \forall a.\ \phi \equiv \forall A \in V^\lambda.\ M \Vdash_\rho \phi[a := A]$
11. $M \Vdash_\rho \exists a.\ \phi \equiv \exists A \in V^\lambda.\ M \Vdash_\rho \phi[a := A]$

Note that $M \Vdash_\rho A \in B$ iff $(M, A) \in B^+$.

The definition of the ordinal γ in item 4 depends on $t_A(\overline{u})$. This ordinal is close to the rank of the set denoted by $t_A(\overline{u})$ and is chosen so that Lemma 8 can be proven. Let $\overline{\alpha} = \overline{rank([\![u]\!]_\rho)}$. Case $t_A(\overline{u})$ of:

- $\{u_1, u_2\}$ — $\gamma = max(\alpha_1, \alpha_2)$
- $P(u)$ — $\gamma = \alpha + 1$.
- $\bigcup u$ — $\gamma = \alpha$.
- $S_{\phi(a,\overline{f})}(u, \overline{u})$ — $\gamma = \alpha_1$.
- $R_{\phi(a,b,\overline{f})}(u, \overline{u})$. This case is more complicated. The names are chosen to match the corresponding clause in the proof of Lemma 8. Let $\psi(B, d, \overline{F}) \equiv \phi(B, d, \overline{F}) \wedge \forall e.\ \phi(B, e, \overline{[\![u]\!]_\rho}) \to e = d)$. Let $G = \{(N_1, (N_{21}, B)) \in \Lambda_{\overline{Z}} \times [\![u]\!]^+_\rho \mid \exists d \in V^\lambda.\ (N_1 \downarrow \lambda x.\ O) \wedge (O[x := N_{21}] \Vdash_\rho \psi(B, d, \overline{[\![u]\!]_\rho}))\}$. Then for all $g \in G$ there is D and $(N_1, (N_{21}, B))$ such that $g = (N_1, (N_{21}, B))$ and

$N_1 \downarrow \lambda x.\ O$ and $O[x := N_{21}] \Vdash_\rho \psi(B, D, \overline{[\![u]\!]_\rho})$. Use Collection to collect all these C's in one set H. Apply Replacement to H to get the set of λ-ranks of sets in H. Then $\beta \equiv \bigcup H$ is an ordinal and for any $C \in H$, $rank(C) < \beta$. Therefore for all $g \in G$ there is $D \in V^\lambda_\beta$ and $(N_1, (N_{21}, B))$ such that $g = (N_1, (N_{21}, B))$ and $N_1 \downarrow \lambda x.\ O$ and $O[x := N_{21}] \Vdash_\rho \psi(B, D, \overline{[\![u]\!]_\rho})$. Set $\gamma = \beta + 1$.

Lemma 6. *The definition of realizability is well-founded.*

Proof. We define a measure function m which takes a clause in the definition and returns a triple of integers:

- $m(M \Vdash_\rho \phi)$ = ("number of constants ω in ϕ", "number of function symbols in ϕ", "structural complexity of ϕ")
- $m([\![t]\!]_\rho)$ = ("number of constants ω in t", "number of function symbols in t", 0)

With lexicographical order in $\mathbb{N}^3$, it is trivial to check that the measure of the definiendum is always greater than the measure of the definiens — number of terms does not increase in the clauses for realizability and formula complexity goes down, in the clause for ω, ω disappears, and in the rest of clauses for terms, the topmost t_A disappears.

Since the definition is well-founded, (metalevel) inductive proofs on the definition of realizability are justified.

Lemma 7. *If $A \in V^\lambda_\alpha$, then there is $\beta < \alpha$ such that for all B, if $M \Vdash_\rho B \in A$, then $B \in V^\lambda_\beta$. Also, if $M \Vdash_\rho B = A$, then $B \in V^\lambda_\alpha$.*

Proof. Take $A \in V^\lambda_\alpha$. Then there is $\beta < \alpha$ such that $A \in P(\lambda\overline{Z}_v \times V^\lambda_\beta)$. Take any B. If $M \Vdash B \in A$, then $M \downarrow v$ and $(v, B) \in A$, so $B \in V^\lambda_\beta$.

For the second part, suppose $M \Vdash_\rho A = B$. This means that $M \Vdash_\rho \forall c.\ c \in A \leftrightarrow c \in B$, so $\forall C.\ M \Vdash C \in A \leftrightarrow C \in B$, so $\forall C.\ M \downarrow \langle M_1, M_2\rangle$, $M_1 \Vdash C \in A \to C \in B$ and $M_2 \Vdash C \in B \to C \in A$. Thus, for all C, $M_2 \downarrow \lambda x.\ M_3$ and for all $N \Vdash C \in B$, $M_3[x := N] \Vdash C \in A$. Take any element $(v, C) \in B$. Then $v \Vdash C \in B$, so $M_3[x := v] \Vdash C \in A$. Thus by the first part, $C \in V^\lambda_\beta$. Therefore $B \subseteq \lambda\overline{Z}_v \times V^\lambda_\beta$, so $B \in P(\lambda\overline{Z}_v \times V^\lambda_\beta) = V^\lambda_{\beta+1}$, so $B \in V^\lambda_\alpha$.

The following lemma states the crucial property of the realizability relation.

Lemma 8. $(M, A) \in [\![t_A(\overline{u})]\!]_\rho$ *iff* $M = \mathrm{axRep}(N)$ *and* $N \Vdash_\rho \phi_A(A, [\![\overline{u}]\!]_\rho)$.

Proof. We first do the proof for all terms apart from ω, then we prove the claim for ω.

The left-to-right direction is immediate. For the right-to-left direction, suppose $N \Vdash_\rho \phi_A(A, [\![\overline{u}]\!]_\rho)$ and $M = \mathrm{axRep}(N)$. To show that $(M, A) \in [\![t_A(\overline{u})]\!]_\rho$, we need to show that $A \in V^\lambda_\gamma$. The proof proceeds by case analysis on $t_A(\overline{u})$. Let $\overline{\alpha} = \overline{rank([\![u]\!]_\rho)}$. Case $t_A(\overline{u})$ of:

- $\{u_1, u_2\}$. Suppose that $N \Vdash_\rho A = [\![u_1]\!]_\rho \lor A = [\![u_2]\!]_\rho$. Then either $N \downarrow \mathrm{inl}(N_1) \land N_1 \Vdash_\rho A = [\![u_1]\!]_\rho$ or $N \downarrow \mathrm{inr}(N_1) \land N_1 \Vdash_\rho A = [\![u_2]\!]_\rho$. By Lemma 7, in the former case $A \in V^\lambda_{\alpha_1}$, in the latter $A \in V^\lambda_{\alpha_2}$, so $A \in V^\lambda_{max(\alpha_1,\alpha_2)}$.
- $P(u)$. Suppose that $N \Vdash_\rho \forall c.\ c \in A \to c \in [\![u]\!]_\rho$. Then $\forall C.\ N \Vdash_\rho C \in A \to C \in [\![u]\!]_\rho$, so $\forall C.\ N \downarrow \lambda x.\ N_1$ and $\forall O.\ (O \Vdash C \in A) \Rightarrow N_1[x := O] \Vdash_\rho C \in [\![u]\!]_\rho$. Take any $(v, B) \in A$. Then $v \Vdash_\rho B \in A$. So $N_1[x := v] \Vdash_\rho B \in [\![u]\!]_\rho$. Thus any such B is in V^λ_α, so $A \in V^\lambda_{\alpha+1}$.
- $\bigcup u$. Suppose $N \Vdash_\rho \exists c.\ c \in [\![u]\!]_\rho \land A \in c$. It is easy to see that $A \in V^\lambda_\alpha$.
- $S_{\phi(a,\overline{f})}(u, \overline{u})$. Suppose $N \Vdash_\rho A \in [\![u]\!]_\rho \land \ldots$. It follows that $A \in V^\lambda_{\alpha_1}$.
- $R_{\phi(a,\overline{f})}(u, \overline{u})$. Suppose

$$N \Vdash_\rho (\forall x \in [\![u]\!]_\rho \exists! y.\ \phi(x, y, \overline{[\![u]\!]_\rho})) \land \exists x \in [\![u]\!]_\rho.\ \phi(x, A, \overline{[\![u]\!]_\rho})$$

  Then $N \downarrow \langle N_1, N_2\rangle$ and $N_2 \Vdash_\rho \exists x \in [\![u]\!]_\rho.\ \phi(x, A, \overline{[\![u]\!]_\rho})$. Thus there is B such that $N_2 \Vdash_\rho B \in [\![u]\!]_\rho \land \phi(B, A, \overline{[\![u]\!]_\rho})$. So $N_2 \downarrow \langle N_{21}, N_{22}\rangle$, $N_{21} \Vdash_\rho B \in [\![u]\!]_\rho$ and $N_{22} \Vdash_\rho \phi(B, A, \overline{[\![u]\!]_\rho})$. We also have $N_1 \Vdash_\rho \forall x \in [\![u]\!]_\rho \exists! y.\ \phi(x, y, \overline{[\![u]\!]_\rho})$. So for all C, $N_1 \downarrow \lambda x.\ O$ and for all $P \Vdash_\rho C \in [\![u]\!]_\rho$, $O[x := P] \Vdash_\rho \exists! y.\ \phi(C, y, \overline{[\![u]\!]_\rho})$. So taking $C = B$ and $P = N_{21}$, there is D such that $N_1 \downarrow \lambda x.\ O$ and $O[x := N_{21}] \Vdash_\rho \phi(B, D, \overline{[\![u]\!]_\rho}) \land \forall e.\ \phi(B, e, \overline{[\![u]\!]_\rho}) \to e = D$. Therefore $(N_1, (N_{21}, B)) \in G$ from the definition of γ, so there is $D \in V^\lambda_\gamma$ such that $N_1 \downarrow \lambda x.O$ and $O[x := N_{21}] \Vdash_\rho \phi(B, D, \overline{[\![u]\!]_\rho}) \land \forall e.\ \phi(B, e, \overline{[\![u]\!]_\rho}) \to e = D$. So $O[x := N_{21}] \downarrow \langle O_1, O_2\rangle$ and $O_2 \Vdash_\rho \forall e.\ \phi(B, e, \overline{[\![u]\!]_\rho}) \to e = D$. Therefore, $O_2 \downarrow \lambda x.\ Q$ and $Q[x := N_{22}] \Vdash_\rho A = D$. By Lemma 7, $A \in V^\lambda_\gamma$.

Now we can tackle ω. For the left-to-right direction, obviously $M = infRep(N)$. For the claim about N we proceed by induction on the definition of ω':

- The base case. Then $N \downarrow \mathrm{inl}(O)$ and $O \Vdash_\rho A = 0$, so $N \Vdash_\rho A = 0 \lor \exists y \in \omega'.\ A = S(y)$.
- Inductive step. Then $N \downarrow \mathrm{inr}(O)$, $O \downarrow \langle M', P\rangle$, $(M', B) \in \omega'^+$, $P \Vdash_\rho A = S(B)$. Therefore there is C (namely B) such that $M' \Vdash_\rho C \in \omega'$ and $P \Vdash_\rho A = S(C)$. Thus $\langle M', P\rangle \Vdash_\rho \exists y.\ y \in \omega' \land A = S(y)$, so $N \Vdash_\rho A = 0 \lor \exists y \in \omega'.\ A = S(y)$.

For the right-to-left direction, suppose $N \Vdash_\rho A = 0 \lor \exists y.\ y \in \omega' \land A = S(y)$. Then either $N \downarrow \mathrm{inl}(O)$ or $N \downarrow \mathrm{inr}(O)$. In the former case, $O \Vdash_\rho A = 0$ and by Lemma 7 $A \in V^\lambda_\omega$. In the latter, $O \Vdash_\rho \exists y.\ y \in \omega' \land A = S(y)$. So there is B such that $O \Vdash_\rho B \in \omega' \land A = S(B)$. So $O \downarrow \langle M', P\rangle$, $(M', B) \in \omega'^+$ and $P \Vdash_\rho A = S(B)$. This is exactly the inductive step of the definition of ω', so it remains to show that $A \in V^\lambda_\omega$. Since $(M', B) \in \omega'^+$, there is a finite ordinal α such that $B \in V^\lambda_\alpha$. Now, suppose $(M, C) \in [\![\{B, \{B, B\}\}]\!]_\rho$. Then $M = pairRep(N)$ and $N \Vdash_\rho C = B \lor C = [\![\{B, B\}]\!]_\rho$. Thus either $N \downarrow \mathrm{inl}(N_1)$ and $N_1 \Vdash C = B$, or $N \downarrow \mathrm{inr}(N_1)$ and $N_1 \Vdash C = [\![\{B, B\}]\!]_\rho$. In the former case, by Lemma 7 $C \in V^\lambda_\alpha$. In the latter, suppose $(O, D) \in [\![\{B, B\}]\!]_\rho$. Then it similarly follows that $D \in V^\lambda_\alpha$, so $[\![\{B, B\}]\!]_\rho \in V^\lambda_{\alpha+1}$, so by Lemma 7, $C \in V^\lambda_{\alpha+1}$. Therefore $[\![\{B, \{B, B\}\}]\!]_\rho \in V^\lambda_{\alpha+2}$ and by Lemma 7, $A \in V^\lambda_{\alpha+2}$.

Lemma 9. *$[\![t[a := s]]\!]_\rho = [\![t]\!]_{\rho[a:=[\![s]\!]_\rho]}$ and $M \Vdash_\rho \phi[a := s]$ iff $M \Vdash_{\rho[a:=[\![s]\!]_\rho]} \phi$.*

Proof. Induction on definition of terms and formulas.

Lemma 10. *$[\![t[a := s]]\!]_\rho = [\![t[a := [\![s]\!]_\rho]]\!]_\rho$ and $M \Vdash_\rho \phi[a := s]$ iff $M \Vdash_\rho \phi[a := [\![s]\!]_\rho]$.*

Proof. Induction on definition of terms and formulas.

Lemma 11. *If $(M \Vdash_\rho \phi)$ then $M \downarrow$.*

Proof. Straightforward induction on ϕ.

Lemma 12. *If $M \to^* M'$ then $M' \Vdash_\rho \phi$ iff $M \Vdash_\rho \phi$.*

Proof. Induction on ϕ. If ϕ doesn't start with $\forall, \exists$, then the relation $M \Vdash_\rho \phi$ depends only on normalization of M and the behaviour of its value, and these properties do not change with reduction. The quantifier cases are straightforward.

Lemma 13. *If $M \Vdash_\rho \phi \to \psi$ and $N \Vdash_\rho \phi$, then $M\ N \Vdash_\rho \psi$.*

Proof. If $M \Vdash_\rho \phi \to \psi$, then $M \downarrow (\lambda x.\ O)$ and for all $P \Vdash_\rho \phi$, $O[x := P] \Vdash_\rho \psi$. Since $M\ N \to^* (\lambda x.\ O)N \to O[x := N]$, Lemma 12 gives us the claim.

6 Normalization

In this section, environments ρ map lambda variables to $\lambda\overline{Z}$ terms and logic variables to sets in V^λ. Any such environment can be used as a realizability environment by ignoring the mapping of lambda variables.

Definition 7. *For a sequent $\Gamma \vdash \phi$, $\rho \models \Gamma \vdash \phi$ means that $\rho : FV(\Gamma, \phi) \to (V^\lambda \cup \Lambda_{\overline{Z}})$, for all $a \in FV_L(\Gamma, \phi)$, $\rho(a) \in V^\lambda$ and for all $(x_i, \phi_i) \in \Gamma$, $\rho(x_i) \Vdash_\rho \phi_i$.*

Note that if $\rho \models \Gamma \vdash \phi$, then for any term t in Γ, ϕ, $[\![t]\!]_\rho$ is defined and so is the realizability relation $M \Vdash_\rho \phi$.

Definition 8. *For a sequent $\Gamma \vdash \phi$, if $\rho \models \Gamma \vdash \phi$ and $M \in \Lambda_{\overline{Z}}$, then $M[\rho]$ is $M[x_1 := \rho(x_1), \ldots, x_n := \rho(x_n)]$.*

Theorem 1. *If $\Gamma \vdash M : \vartheta$ then for all $\rho \models \Gamma \vdash \vartheta$, $\overline{M}[\rho] \Vdash_\rho \vartheta$.*

Proof. For any $\lambda\overline{Z}$ term M, M' in the proof denotes $\overline{M}[\rho]$. We proceed by metalevel induction on $\Gamma \vdash M : \vartheta$. We show some interesting cases. Case $\Gamma \vdash M : \vartheta$ of:

–
$$\frac{}{\Gamma, x : \phi \vdash x : \phi}$$

Then $M' = \rho(x)$, the claim follows.

–
$$\frac{\Gamma \vdash M : \phi \to \psi \quad \Gamma \vdash N : \phi}{\Gamma \vdash M\ N : \psi}$$

By inductive hypothesis, $M' \Vdash_\rho \phi \to \psi$ and $N' \Vdash_\rho \phi$. Lemma 13 gives the claim.

–
$$\frac{\Gamma, x : \phi \vdash M : \psi}{\Gamma \vdash \lambda x : \phi.\ M : \phi \to \psi}$$

We need to show that for any $N \Vdash_\rho \phi$, $M'[x := N] \Vdash_\rho \psi$. Take any such N. Let $\rho' = \rho[x := N]$. Then $\rho' \models \Gamma, x : \phi$, so by inductive hypothesis $\overline{M}[\rho'] \Vdash_{\rho'} \psi$. However, $\overline{M}[\rho'] = \overline{M}[\rho][x := N] = M'[x := N]$, so $M'[x := N] \Vdash_{\rho'} \psi$. But ρ' agrees with ρ on logic variables, so $M'[x := N] \Vdash_\rho \psi$.

–
$$\frac{M : \bot}{\Gamma \vdash magic(M) : \phi}$$

By inductive hypothesis, $M' \Vdash_\rho \bot$, which is not the case, so anything holds, in particular $magic(M') \Vdash_\rho \phi$.

–
$$\frac{\Gamma \vdash M : \tau \quad \Gamma \vdash N : \sigma}{\Gamma \vdash \langle M, N \rangle : \tau \wedge \sigma}$$

All we need to show that $M' \Vdash_\rho \tau$ and $N' \Vdash_\rho \sigma$, which we get from the inductive hypothesis.

–
$$\frac{\Gamma \vdash M : \tau}{\Gamma \vdash \mathrm{inl}(M) : \tau \vee \sigma}$$

As trivial as the previous one, similarly for inr.

–
$$\frac{\Gamma \vdash M : \tau \wedge \sigma}{\Gamma \vdash \mathrm{fst}(M) : \tau}$$

By inductive hypothesis, $M' \Vdash_\rho \tau \wedge \sigma$, so $M' \downarrow \langle M_1, M_2 \rangle$ and $M_1 \Vdash_\rho \tau$. Therefore $\mathrm{fst}(M) \to^* \mathrm{fst}(\langle M_1, M_2 \rangle) \to M_1$. Lemma 12 gives the claim. The case for *snd* works the same.

–
$$\frac{\Gamma \vdash M : \phi_A(t, \overline{u})}{\Gamma \vdash \mathrm{axRep}(t, \overline{u}, M) : t \in t_A(\overline{u})}$$

By inductive hypothesis, $M' \Vdash_\rho \phi_A(t, \overline{u})$. By Lemma 10 this is equivalent to $M' \Vdash_\rho \phi_A([\![t]\!]_\rho, \overline{[\![u]\!]_\rho})$. By Lemma 8 $(\mathrm{axRep}(M'), [\![t]\!]_\rho) \in [\![t_A(\overline{u})]\!]_\rho$, so $\mathrm{axRep}(M') \Vdash_\rho t \in t_A(\overline{u})$, so also $\overline{\mathrm{axRep}(t, \overline{u}, M)}[\rho] \Vdash_\rho t \in t_A(\overline{u})$.

–
$$\frac{\Gamma \vdash M : t \in t_A(\overline{u})}{\Gamma \vdash \mathrm{axProp}(t, \overline{u}, M) : \phi_A(t, \overline{u})}$$

By inductive hypothesis, $M' \Vdash_\rho t \in t_A(\overline{u})$. This means that $M' \downarrow v$ and $(v, [\![t]\!]_\rho) \in [\![t_A(\overline{u})]\!]$. By Lemma 8, $v = \mathrm{axRep}(N)$ and $N \Vdash_\rho \phi_A([\![t]\!]_\rho, \overline{[\![u]\!]_\rho})$. By Lemma 10, $N \Vdash_\rho \phi_A(t, \overline{u})$. Moreover, $\overline{\mathrm{axProp}(t, \overline{u}, M)} = \mathrm{axProp}(M') \to^* \mathrm{axProp}(\mathrm{axRep}(N)) \to N$. Lemma 12 gives us the claim.

–
$$\frac{\Gamma \vdash M : \phi}{\Gamma \vdash \lambda a.\ M : \forall a.\ \phi}$$

By inductive hypothesis, for all $\rho \models \Gamma \vdash M : \phi$, $\overline{M}[\rho] \Vdash \phi$. We need to show that for all $\rho \models \Gamma \vdash \lambda a.\ M : \forall a.\ \phi$, $\overline{\lambda a.\ M} = \overline{M}[\rho] \Vdash_\rho \forall a.\ \phi(a)$. Take any such ρ. We need to show that $\forall A.\ \overline{M}[\rho] \Vdash_\rho \phi[a := A]$. Take any A. By Lemma 9, it suffices to show that $\overline{M}[\rho] \Vdash_{\rho[a:=A]} \phi$. However, $\rho[a := A] \models \Gamma \vdash M : \phi$, so we get the claim by inductive hypothesis.

–
$$\frac{\Gamma \vdash M : \forall a.\ \phi}{\Gamma \vdash M\ t : \phi[a := t]}$$

By inductive hypothesis, $M' \Vdash_\rho \forall a.\ \phi$, so $\forall A. M' \Vdash_\rho \phi[a := A]$. in particular $M' \Vdash_\rho \phi[a := [\![t]\!]_\rho]$, so by Lemma 10 $M' = \overline{(M\ t)}[\rho] \Vdash_\rho \phi[a := t]$.

–
$$\frac{\Gamma \vdash M : \forall c.\ (\forall b.\ b \in c \to \phi(b, \overline{t})) \to \phi(c, \overline{t})}{\Gamma \vdash \mathrm{ind}'_{\phi(b,\overline{c})}(M, \overline{t}, u) : \phi(u, \overline{t})}$$

By inductive hypothesis, we have $M' \Vdash_\rho \forall c.\ (\forall b.\ b \in c \to \phi(b, \overline{t})) \to \phi(c, \overline{t})$. We need to show that $\mathrm{ind}'(M') \Vdash_\rho \phi(u, \overline{t})$. By Lemma 10, it suffices to show that $\mathrm{ind}'(M') \Vdash_\rho \phi([\![u]\!]_\rho, \overline{t})$. We will show more general statement: for all A, $\mathrm{ind}'(M') \Vdash_\rho \phi(A, \overline{t})$. We prove it by induction on λ-rank of A. Since $\mathrm{ind}'(M') \to M'\ (\lambda x.\ \mathrm{ind}'(M'))$, by Lemma 12 it suffices to show that $M'\ (\lambda x.\ \mathrm{ind}'(M')) \Vdash_\rho \phi(A, \overline{t})$. By inductive hypothesis, $M' \Vdash_\rho (\forall b.\ b \in A \to \phi(b, \overline{t})) \to \phi(A, \overline{t})$. By Lemma 13, it suffices to show that $(\lambda x.\ \mathrm{ind}'(M')) \Vdash_\rho (\forall b.\ b \in A \to \phi(b, \overline{t}))$. That is, that for all B, $(\lambda x.\ \mathrm{ind}'(M')) \Vdash_\rho B \in A \to \phi(B, \overline{t}))$. That is, that for all $O \Vdash_\rho B \in A$, $\mathrm{ind}'(M')[x := O] \Vdash \phi(B, \overline{t}))$. Take any such O. We know that $x \notin FV(M')$. Thus we need to show that $\mathrm{ind}'(M') \Vdash \phi(B, \overline{t})$. Since $O \Vdash_\rho B \in A$, the λ-rank of B is smaller than the λ-rank of A and the inner inductive hypothesis gives us the claim.

–
$$\frac{\Gamma \vdash M : \forall c.\ (\forall b.\ b \in c \to \phi(b, \overline{t})) \to \phi(c, \overline{t})}{\Gamma \vdash \mathrm{ind}_{\phi(b,\overline{c})}(M, \overline{t}) : \forall a.\ \phi(a, \overline{t})}$$

By inductive hypothesis, we have $M' \Vdash_\rho \forall c.\ (\forall b.\ b \in c \to \phi(b, \overline{t})) \to \phi(c, \overline{t})$. We need to show that $\mathrm{ind}(M') \Vdash_\rho \forall a.\ \phi(a, \overline{t})$. That is, that for all A, $\mathrm{ind}(M') \Vdash_\rho \phi(A, \overline{t})$. Since $\mathrm{ind}(M') \to M'\ (\lambda x.\ \mathrm{ind}'(M'))$, by Lemma 12 it suffices to show that $M'\ (\lambda x.\ \mathrm{ind}'(M')) \Vdash_\rho \phi(A, \overline{t})$. But this has been shown in the previous case, with the same assumptions about M'.

Corollary 2 (Normalization). *If* $\vdash M : \phi$, *then* $M \downarrow$.

Proof. By Theorem 1, for any $\rho \models (\vdash M : \phi)$, we have $\overline{M}[\rho] \Vdash_\rho \phi$. Take any such ρ, for example mapping all free logic variables of M and ϕ to $\emptyset$. By Lemma 11, $\overline{M}[\rho] \downarrow$, and since $\overline{M} = \overline{M}[\rho]$, $\overline{M} \downarrow$. Lemma 5 gives us the claim.

As the reduction system is deterministic, the distinction between strong and weak normalization does not exist. If the reduction system is extended to allow reductions anywhere inside of the term, the Corollary 2 shows only weak normalization. Strong normalization, then, surprisingly, does not hold. One reason, trivial, are ind terms. However, even without them, the system would not strongly normalize, as the following counterexample, invented by Crabbé and adapted to our framework shows:

Theorem 2 (Crabbé's counterexample). *There is a formula ϕ and term M such that $\vdash M : \phi$ and M does not strongly normalize.*

Proof. Let $t = \{x \in 0 \mid x \in x \to \bot\}$. Consider the terms:

$$N \equiv \lambda y : t \in t.\, \mathrm{snd}(\mathrm{sepProp}(t, 0, y))\; y \qquad M \equiv \lambda x : t \in 0.\, N\; (\mathrm{sepRep}(t, 0, \langle x, N\rangle))$$

Then it is easy to see that $\vdash N : t \in t \to \bot$, $\vdash M : t \in 0 \to \bot$ and that M does not strongly normalize.

Moreover, a slight (from a semantic point of view) modification to IZF_R^-, namely making it non-well-founded, results in a system which is not even weakly normalizing. A very small fragment is sufficient for this effect to arise. Let T be an intuitionistic set theory consisting of 2 axioms:

- (C) $\forall a.\ a \in c \leftrightarrow a = c$
- (D) $\forall a.\ a \in d \leftrightarrow a \in c \land a \in a \to a \in a$.

The constant c denotes a non-well-founded set. The existence of d can be derived from separation axiom: $d = \{a \in c \mid a \in a \to a \in a\}$. The lambda calculus corresponding to T is defined just as for IZF_R^-.

Theorem 3. *There is a formula ϕ and term M such that $\vdash_T M : \phi$ and M does not weakly normalize.*

Proof. It is relatively easy to find a term N such that $\vdash_T N : d \in c$. Take $\phi = d \in d \to d \in d$ and consider the terms:

$$O \equiv \lambda x : d \in d.\ \mathrm{snd}(\mathrm{dRep}(d, c, x))\; x \qquad M \equiv O\; (\mathrm{dProp}(d, c, \langle N, O\rangle)).$$

Then M does not have a normal form and $\vdash_T M : \phi$.

In both cases, it is easy to find a term $N : \tau$ which does strongly normalize. An interesting question is whether there is a theorem of IZF_R^- without a strongly normalizing proof.

7 Applications

The normalization theorem provides immediately several results.

Corollary 3 (Disjunction Property). *If $IZF_R^- \vdash \phi \lor \psi$, then $IZF_R^- \vdash \phi$ or $IZF_R^- \vdash \psi$.*

Proof. Suppose $\mathrm{IZF}_R^- \vdash \phi \vee \psi$. By Curry-Howard isomorphism, there is a λZ term M such that $\vdash M : \phi \vee \psi$. By Corollary 1, $M \downarrow v$ and $\vdash v : \phi \vee \psi$. By Canonical Forms, either $v = \mathrm{inl}(N)$ and $\vdash N : \phi$ or $v = \mathrm{inr}(N)$ and $\vdash N : \psi$. By applying the other direction of Curry-Howard isomorphism we get the claim.

Corollary 4 (Term Existence Property). *If $IZF_R^- \vdash \exists x.\ \phi(x)$, then there is a term t such that $IZF_R^- \vdash \phi(t)$.*

Proof. By Curry-Howard isomorphism, there is a λZ-term M such that $\vdash M : \exists x.\ \phi$. By normalizing M and applying Canonical Forms, we get $[t, N]$ such that $\vdash N : \phi(t)$. and thus by Curry-Howard isomorphism $\mathrm{IZF}_R^- \vdash \phi(t)$.

Corollary 5 (Set Existence Property). *If $IZF_R^- \vdash \exists x.\ \phi(x)$, then there is a formula $\psi(x)$ such that $IZF_R^- \vdash \exists! x.\ \phi(x) \wedge \psi(x)$.*

Proof. Take t from Term Existence Property and $\psi(x) \equiv x = t$. We need to show that $\mathrm{IZF}_R^- \vdash \exists x.\ \phi(x) \wedge \psi(x) \wedge \forall y.\ \phi(y) \wedge \psi(y) \to y = x$. Taking $x = t$, we get $\phi(x)$ and $\psi(x)$. Take any y. If $\psi(y)$, then $y = t$, so also $y = x$.

As any theory can be enriched to have term existence property and thus set existence property, as the proof of completeness theorem for IFOL shows, a different version of SEP is also of interest:

Corollary 6 (Set Existence Property). *If $IZF_R^- \vdash \exists x.\ \phi(x)$ and $\phi(x)$ is term-free, then there is a term-free formula $\psi(x)$ such that $IZF_R^- \vdash \exists! x.\ \phi(x) \wedge \psi(x)$.*

Proof. Take t from Term Existence Property. It is not difficult to see that there is a term-free formula $\psi(x)$, defining t (show first by $\in$-induction that ω is the smallest inductive set), so that $\mathrm{IZF}_R^- \vdash (\exists! x.\ \psi(x)) \wedge \psi(t)$. Then $\mathrm{IZF}_R^- \vdash \exists! x.\ \phi(x) \wedge \psi(x)$ can be easily derived.

7.1 Numerical Existence Property

To show numerical existence property, we first define an extraction function F which takes a proof $\vdash M : t \in \omega$ and returns a natural number n. F works as follows:

It normalizes M to natRep(N). By Canonical Forms, $\vdash N : t = 0 \vee \exists y \in \omega.\ t = S(y)$. F then normalizes N to either $\mathrm{inl}(O)$ or $\mathrm{inr}(O)$. In the former case, F returns 0. In the latter, $\vdash O : \exists y. y \in \omega \wedge t = S(y)$. Normalizing O it gets $[t_1, P]$, where $\vdash P : t_1 \in \omega \wedge t = S(t_1)$. Normalizing P it gets Q such that $\vdash Q : t_1 \in \omega$. Then F returns $F(\vdash Q : t_1 \in \omega) + 1$.

To show that F terminates for all its arguments, consider the sequence of terms $t, t_1, t_2, \ldots$ obtained throughout the life of F. We have $\mathrm{IZF}_R^- \vdash t = S(t_1)$, $\mathrm{IZF}_R^- \vdash t_1 = S(t_2)$ and so on. Thus, the length of the sequence is at most the rank of the set denoted by t, so F must terminate after at most $rank([\![t]\!])$ steps.

Corollary 7 (Numerical existence property). *If $IZF_R^- \vdash \exists x \in \omega.\ \phi(x)$, then there is a natural number n and term t such that $IZF_R^- \vdash \phi(t) \wedge t = \overline{n}$.*

Proof. As before, use Curry-Howard isomorphism to get a value $[t, M]$ such that $\vdash [t, M] : \exists x.\ x \in \omega \wedge \phi(x)$. Thus $M \vdash t \in \omega \wedge \phi(t)$, so $M \downarrow \langle M_1, M_2 \rangle$ and $\vdash M_1 : t \in \omega$. Take $n = F(\vdash M_1 : t \in \omega)$. It's easy to see that patching together in an appropriate way proofs obtained throughout the execution of F, a proof of $t = \overline{n}$ for some natural number n can be produced.

This version of (NEP) differs from the one usually found in the literature, where in the end $\phi(\overline{n})$ is derived. However, IZF_R^- does not have the Leibniz axiom for the final step. We conjecture that it is the only version which holds in non-extensional set theories.

8 The Leibniz axiom

We will show that we can extend our results to full IZF_R. We work in IZF_R^-.

Lemma 14. *Equality is an equivalence relation.*

Definition 9. *A set C is* L-stable*, if $A \in C$ and $A = B$ implies $B \in C$.*

Definition 10. *A set C is* transitively L-stable *if it is L-stable and every element of C is transitively L-stable.*

This definition is formalized in a standard way, using transitive closure, available in IZF_R^-, as shown i.e. in [AR01]. We write $TLS(A)$ to express that A is transitively L-stable and denote the class of transitively L-stable sets by T. The statement $V = T$ means that $\forall A.\ TLS(A)$. Class T in IZF_R^- plays a similar role to the class of well-founded sets in ZF without Foundation.

Lemma 15. *$IZF_R \vdash V = T$.*

Proof. By $\in$-induction.

The restriction of a formula ϕ to T, denoted by ϕ^T, is defined as usual, taking into account the following translation of terms:

$$a^T \equiv a \quad \{t, u\}^T \equiv \{t^T, u^T\} \qquad \omega^T \equiv \omega \qquad (\bigcup t)^T \equiv \bigcup t^T \qquad (P(t))^T \equiv P(t^T) \cap T$$

$$(S_{\phi(a,\overline{f})}(u, \overline{u}))^T \equiv S_{\phi^T(a,\overline{f})}(u^T, \overline{u^T}) \qquad (R_{\phi(a,b,\overline{f})}(t, \overline{u}))^T \equiv R_{b \in T \wedge \phi^T(a,b,\overline{f})}(t^T, \overline{u^T})$$

The notation $T \models \phi$ means that ϕ^T holds.

Lemma 16. *T is transitive.*

Lemma 17. *If $A = C$ and $A \in T$, then $C \in T$.*

Proof. This is not obvious, since the Leibniz axiom is not present in the logic. However, equality is defined by Δ_0-formula and the claim follows by transitivity of T.

Lemma 18. *$T \models$ "every set is L-stable".*

Lemma 19. *Equality is absolute for T.*

The following three lemmas are proved together by mutual induction on the definition of terms and formulas.

Lemma 20. *For any term $t(a, \overline{f})$, $T \models \forall a, b, \overline{f}.\ a = b \to t(a, \overline{f}) = t(b, \overline{f})$.*

Lemma 21. *For any term $t(a, \overline{f})$, $\forall a, \overline{f} \in T.\ \ t^T(a, \overline{f}) \in T$.*

Lemma 22. *$T \models L_{\phi(a, \overline{f})}$.*

Proof. The only interesting case is when ϕ is atomic. Suppose $t(A, \overline{F}) \in s(A, \overline{F})$ for some terms t, s. We need to show that if $A, B \in T$, $A = B$ and $t^T(A, \overline{F}) \in s^T(A, \overline{F})$, then $t^T(B, \overline{F}) \in s^T(B, \overline{F})$. By Lemma 20, $t^T(A, \overline{F}) = t^T(B, \overline{F})$. By Lemma 21, $s^T(A, \overline{F}) \in T$, so by Lemma 18 $t^T(B, \overline{F}) \in s^T(A, \overline{F})$. By Lemma 20, $s^T(A, \overline{F}) = s^T(B, \overline{F})$, so $t^T(B, \overline{F}) \in s^T(B, \overline{F})$.

Theorem 4. *$T \models IZF_R$.*

Proof. Straightforward. To prove (IND) use $\in$-induction.

Lemma 23. *$IZF_R \vdash \forall \overline{a}.\ t^T(\overline{a}) = t(\overline{a})$ and $IZF_R \vdash \forall \overline{a}.\ \phi^T(\overline{a}) \leftrightarrow \phi(\overline{a})$.*

Proof. By induction on the definition of terms and formulas.

Lemma 24. *$IZF_R \vdash \phi$ iff $IZF_R^- \vdash \phi^T$.*

Proof. The left-to-right direction follows by Theorem 4, the right-to-left direction by Lemma 23.

Note that this means that IZF_R^- can interpret IZF_R, so any argument formalizable in IZF_R can be also formalized in IZF_R^-, by relativizing everything to T.

Corollary 8. *IZF_R satisfies DP and NEP.*

Proof. For DP, suppose $\mathrm{IZF}_R \vdash \phi \vee \psi$. By Lemma 24, $\mathrm{IZF}_R^- \vdash \phi^T \vee \psi^T$. By DP for IZF_R^-, either $\mathrm{IZF}_R^- \vdash \phi^T$ or $\mathrm{IZF}_R^- \vdash \psi^T$. Using Lemma 24 again we get either $\mathrm{IZF}_R \vdash \phi$ or $\mathrm{IZF}_R \vdash \psi$.

For NEP, suppose $\mathrm{IZF}_R \vdash \exists x.\ x \in \omega \wedge \phi(x)$. By Lemma 24, $\mathrm{IZF}_R^- \vdash \exists x.\ x \in T \wedge x \in \omega^T.\ \phi^T(x)$, so $\mathrm{IZF}_R^- \vdash \exists x \in \omega^T.\ x \in T \wedge \phi^T(x)$. Since $\omega^T = \omega$, using NEP for IZF_R^-we get a natural number n such that $\mathrm{IZF}_R^- \vdash \exists x.\ \phi^T(x) \wedge x = \overline{n}$. By Lemma 24 and $\overline{n} = \overline{n}^T$, we get $\mathrm{IZF}_R \vdash \exists x.\ \phi(x) \wedge x = \overline{n}$. By the Leibniz axiom, $\mathrm{IZF}_R \vdash \phi(\overline{n})$.

We cannot establish TEP and SEP for IZF_R as easily, since it is not the case that $t^T = t$ for all terms t (in other words, not all operations defined by terms are absolute with respect to T). However, a simple modification to the axiomatization of IZF_R yields these results too. It suffices to guarantee that whenever a set is defined, it must be in T. To do this, we modify three axioms and add one new, axiomatizing transitive closure. Let $PTC(a, c)$ be a formula that says: $a \subseteq c$ and c is transitive. The axioms are:

(SEP'$_{\phi(a,\overline{f})}$) $\forall \overline{f} \forall a \forall c.\ c \in S_{\phi(a,\overline{f})}(a, \overline{f}) \leftrightarrow c \in a \wedge \phi^T(c, \overline{f})$
(POWER') $\forall a \forall c. c \in P(a) \leftrightarrow c \in T \wedge \forall b.\ b \in c \to b \in a$
(REPL'$_{\phi(a,b,\overline{f})}$) $\forall \overline{f} \forall a \forall c. c \in R_{\phi(a,b,\overline{f})}(a, \overline{f}) \leftrightarrow (\forall x \in a \exists! y \in T. \phi^T(x, y, \overline{f})) \wedge (\exists x \in a.\ \phi^T(x, c, \overline{f}))$
(TC) $\forall a, c.\ c \in TC(a) \leftrightarrow (c \in a \vee \exists d \in TC(a).\ c \in d) \wedge \forall d.\ PTC(a, d) \to c \in d.$

In the modified axioms, the definition of T is written using TC and relativization of formulas to T this time leaves terms intact, we set $t^T \equiv t$ for all terms t. Let us call IZF$_R$ with modified axioms IZF$_R$'. It is not difficult to see that IZF$_R$' is equivalent to IZF$_R$ and is also a definitional extension of term-free presentations of IZF$_R$ from [Myh73], [Bee85] and [FS85]. We can therefore adopt it as the official axiomatization of IZF$_R$. All the developments in sections 4-8 can be done for the new axiomatization in the similar way. In the end we get:

Corollary 9. *IZF$_R$ satisfies DP, NEP, TEP and SEP.*

Proof. DP and NEP follow in the same way as in Corollary 8. For TEP, if IZF$_R \vdash \exists x.\ \phi(x)$, then IZF$_R^- \vdash \exists x \in T.\ \phi^T(x)$, so there is a term t such that IZF$_R^- \vdash t \in T \wedge \phi^T(t)$, so since $t^T = t$, IZF$_R \vdash \phi(t)$. To prove SEP proceed as in Corollary 6.

9 Related work

In [Myh73], DP, NEP, SEP are proven for IZF$_R$ without terms. TEP is proven for comprehension terms, the full list of which is not recursive. It is easy to see that IZF$_R$ is a definitional extension of Myhill's version. Our results therefore improve on [Myh73], by providing an explicit recursive list of terms corresponding to IZF$_R$ axioms to witness TEP.

In [Bai88] strong normalization of a constructive set theory without induction and replacement axioms is shown using Girard's method. As both normalization and theory are defined in a nonstandard way, it is not clear if the results could entail any of DP, NEP, SEP and TEP for the theory.

Krivine in [LK01] defines realizability using lambda calculus for classical set theory conservative over ZF. The types for his calculus are defined. However, it seems that the types correspond more to the truth in the realizability model, not to provable statements in the theory. Moreover, there are typable terms which do not weakly normalize.

In [Miq03], a set theory without the induction and replacement axioms is interpreted in the lambda calculus with types based on $F\omega.2$. Strong normalization of the calculus is proved. As this is an intepretation, not an isomorphism, we do not think it could be used to show any of DP, NEP, SEP and TEP. This has been extended with conservativeness result in [DM06], which might yield the properties for the theory.

In [Rat05], DP and NEP along with other properties are derived for CZF using a combination of realizability and truth. The technique likely extends to IZF$_R$ and IZF$_C$, however, it does not seem to be strong enough to prove SEP and TEP for IZF$_R$.

10 Conclusion

We believe that this work can serve as a basis for a practical prover based on set theory with extraction mechanisms. We envision a prover for IZF + EM + AC = ZFC, which would have a pleasant property that constructive proofs yield extracts. We will describe precisely extraction in [CM06].

I would like to thank my advisor, Bob Constable, for giving me the idea for this research and support, Richard Shore for helpful discussions and Daria Walukiewicz-Chrząszcz for the counterexample, thanks to which I could prove Theorem 3.

References

[AR01] P. Aczel and M. Rathjen. Notes on constructive set theory. Technical reports, Elsevier, September 2001.

[Bai88] Sidney C. Bailin. A normalization theorem for set theory. *J. Symb. Log.*, 53(3):673–695, 1988.

[Bee79] M.J. Beeson. Continuity in intuitionistic set theories. In M. Boffa, D. van Dalen, and K. McAloon, editors, *Logic Colloquium '78*, pages 1–52. North-Holland Publishing Company, 1979.

[Bee85] Michael Beeson. *Foundations of Constructive Mathematics.* Springer-Verlag, 1985.

[CM06] Robert Constable and Wojciech Moczydłowski. Extracting Programs from Constructive HOL Proofs via IZF Set-Theoretic Semantics. 2006. To be submitted.

[DM06] Gilles Dowek and Alexandre Miquel. Cut elimination for Zermelo's set theory. 2006. Manuscript, available from the web pages of the authors.

[Fri73] Harvey Friedman. The consistency of classical set theory relative to a set theory with intuitionistic logic. *Journal of Symbolic Logic*, 38:315–319, 1973.

[Fri78] Harvey Friedman. Classically and intuitionistically provably recursive functions. In D. S. Scott and G. H. Muller, editors, *Higher Set Theory*, volume 699 of *Lecture Notes in Mathematics*, pages 21–28. Springer-Verlag, 1978.

[FS85] Harvey Friedman and Andre Ŝĉedrov. The lack of definable witnesses and provably recursive functions in intuitionistic set theories. *Advances in Mathematics*, 57:1–13, 1985.

[LK01] Jean Louis Krivine. Typed lambda-calculus in classical Zermelo-Fraeænkel set theory. *Archive for Mathematical Logic*, 40(3):189–205, 2001.

[LP99] Lamport and Paulson. Should your specification language be typed? *ACM-TOPLAS: ACM Transactions on Programming Languages and Systems*, 21, 1999.

[McC84] D.C. McCarty. *Realizability and Recursive Mathematics.* D.Phil. Thesis, University of Oxford, 1984.

[Miq03] Alexandre Miquel. A strongly normalising Curry-Howard correspondence for IZF set theory. In *CSL*, pages 441–454, 2003.

[Myh73] John Myhill. Some properties of intuitionistic Zermelo-Fraenkel set theory. In *Cambridge Summer School in Mathematical Logic*, volume 29, pages 206–231. Springer, 1973.

[Rat05] Michael Rathjen. The disjunction and related properties for constructive Zermelo-Fraenkel set theory. *Journal of Symbolic Logic*, 70:1233–1254, 2005.

[Ŝ85] Andre Ŝĉedrov. Intuitionistic set theory. In *Harvey Friedman's Research on the Foundations of Mathematics*, pages 257–284. Elsevier, 1985.

[SU98] M.H.B. Sørensen and P. Urzyczyn. Lectures on the Curry-Howard isomorphism. DIKU rapport 98/14, DIKU, 1998.