

NORMALIZATION OF IZF WITH REPLACEMENT

WOJCIECH MOCZYDŁOWSKI

Department of Computer Science, Cornell University, Ithaca, NY 14853, USA
e-mail address: 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 λZ corresponding to proofs in IZF_R^- according to the Curry-Howard isomorphism principle. Using realizability for IZF_R^- , we show weak normalization of λZ . We use normalization to prove the disjunction, numerical existence and term existence properties. An inner extensional model is used to show these properties, along with the set existence property, for full, extensional IZF_R .

1. INTRODUCTION

Four salient properties of constructive set theories are:

- 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 $\phi \vee \psi$ is provable, then either ϕ or ψ is provable.
- Term Existence Property (TEP): If $\exists x. \phi(x)$ is provable, then $\phi(t)$ is provable for some term t .
- Set Existence Property (SEP): If $\exists x. \phi(x)$ is provable, then there is a formula $\psi(x)$ such that $\exists! x. \phi(x) \wedge \psi(x)$ is provable, where both ϕ and ψ are term-free.

How to prove these properties for a given theory? There is a variety of methods applicable to constructive theories. Cut-elimination, proof normalization, realizability, Kripke models. . . . Normalization proofs, based on the Curry-Howard isomorphism principle, have the advantage of providing an explicit method of witness and program extraction from 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 extended with excluded middle are equivalent to ZF [Fri73].

1998 ACM Subject Classification: F.4.1.

Key words and phrases: Intuitionistic set theory, Curry-Howard isomorphism, normalization, realizability.
Partly supported by NSF grants DUE-0333526 and 0430161.

They are not equivalent [FS85]. While the proof-theoretic power of IZF_C is equivalent to that of ZF , the exact power of IZF_R is unknown. Arguably IZF_C is less constructive, as Collection, similarly to Choice, asserts the existence of a set without defining it.

Both versions have been investigated thoroughly. Results up to 1985 are presented in [Bee85, Š85]. Later research was concentrated on weaker subsystems [AR01, Lub02]. A predicative constructive set theory CZF has attracted particular interest. [AR01] describes the set-theoretic apparatus available in CZF and provides further references.

We axiomatize IZF_R , along with its intensional version IZF_R^- , using set terms. We define a typed lambda calculus λZ corresponding to proofs in IZF_R^- . We also define realizability for IZF_R^- , in the spirit of [McC84], and use it to show that λZ weakly normalizes. 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 and TEP easily follow. 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 the properties proven for IZF_R^- . In IZF_R , SEP easily follows from TEP .

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 $\text{IZF}_R \vdash \forall n \in \mathbb{N} \exists m \in \mathbb{N}. \phi(n, m)$. From this proof a program can be extracted — take a natural number n , construct a proof $\text{IZF}_R \vdash \bar{n} \in \mathbb{N}$. Combine the proofs to get $\text{IZF}_R \vdash \exists m \in \mathbb{N}. \phi(\bar{n}, m)$ and apply NEP to get a number m such that $\text{IZF}_R \vdash \phi(\bar{n}, \bar{m})$. A detailed account of program extraction from IZF_R proofs can be found in [CM06].

There are many provers with the program extraction capability. However, they are usually based on variants 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.

This paper is mostly self-contained. We assume some familiarity with set theory, proof theory and programming languages terminology, found for example in [Kun80, SU06, Pie02]. The paper is organized as follows. We start by presenting in details intuitionistic first-order logic in section 2. In section 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. We use it to prove normalization of λZ in section 6, where we also show that non-well-founded IZF does not normalize. We prove the properties in section 7, and show how to derive them for full, extensional IZF_R in section 8. Comparison with other results can be found in section 9.

2. INTUITIONISTIC FIRST-ORDER LOGIC

Due to the syntactic character of our results, we present the intuitionistic first-order logic (IFOL) in details. We use a natural deduction style of proof rules. The terms will

be denoted by letters t, s, u . The variables will be denoted by letters a, b, c, d, e, f . The notation \vec{a} stands for 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. The capture-avoiding substitution is defined as usual; the result of substituting s for a in a term t is denoted by $t[a := s]$. We write $t[a_1, \dots, a_n := s_1, \dots, s_n]$ to denote the result of substituting simultaneously s_1, \dots, s_n for a_1, \dots, a_n . Contexts, denoted by Γ , are sets of formulas. The set of free variables of a formula ϕ , denoted by $FV(\phi)$, are defined as usual. The free variables of a context Γ , denoted by $FV(\Gamma)$, are the free variables of all formulas in Γ . The notation $\phi(\vec{a})$ means that all free variables of ϕ are among \vec{a} . The proof rules are as follows:

$$\begin{array}{c}
\frac{}{\Gamma, \phi \vdash \phi} \quad \frac{\Gamma \vdash \perp}{\Gamma \vdash \phi} \quad \frac{\Gamma \vdash \phi \rightarrow \psi \quad \Gamma \vdash \phi}{\Gamma \vdash \psi} \quad \frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \rightarrow \psi} \\
\frac{\Gamma \vdash \phi \quad \Gamma \vdash \psi}{\Gamma \vdash \phi \wedge \psi} \quad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi} \quad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \psi} \\
\frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \vee \psi} \quad \frac{\Gamma \vdash \psi}{\Gamma \vdash \phi \vee \psi} \quad \frac{\Gamma \vdash \phi \vee \psi \quad \Gamma, \phi \vdash \vartheta \quad \Gamma, \psi \vdash \vartheta}{\Gamma \vdash \vartheta} \\
\frac{\Gamma \vdash \phi}{\Gamma \vdash \forall a. \phi} \quad a \notin FV(\Gamma) \quad \frac{\Gamma \vdash \forall a. \phi}{\Gamma \vdash \phi[a := t]} \\
\frac{\Gamma \vdash \phi[a := t]}{\Gamma \vdash \exists a. \phi} \quad \frac{\Gamma \vdash \exists a. \phi \quad \Gamma, \phi \vdash \psi}{\Gamma \vdash \psi} \quad a \notin FV(\Gamma) \cup \{\psi\}
\end{array}$$

Negation in IFOL is an abbreviation: $\neg\phi \equiv \phi \rightarrow \perp$. So is the symbol \leftrightarrow : $\phi \leftrightarrow \psi \equiv (\phi \rightarrow \psi \wedge \psi \rightarrow \phi)$. Note that IFOL does not contain equality. The excluded middle rule added to IFOL makes it equivalent to the classical first-order logic without equality. We adopt the “dot”-convention — a formula $\forall a. \phi$ should be parsed as $\forall a. (\phi)$. In other words¹, the dot represents a left parenthesis whose scope extends as far to the right as possible.

Lemma 2.1. For any formula ϕ , $\phi[a := t][b := u[a := t]] = \phi[b := u][a := t]$, for $b \notin FV(t)$.

Proof. Straightforward structural induction on ϕ . □

3. IZF_R

Intuitionistic set theory IZF_R is a first-order theory, equivalent to ZF when extended with excluded middle. It is a definitional extension of term-free versions presented in [Myh73, Bee85, FS85]. The signature consists of one binary relational symbol \in and function symbols used in the axioms below. The set of all IZF_R terms will be denoted by Tms . The notation $t = u$ is an abbreviation for $\forall z. z \in t \leftrightarrow z \in u$. Function symbols 0 and $S(t)$ are abbreviations for \emptyset 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. The axioms are as follows:

- (EMPTY) $\forall c. c \in \emptyset \leftrightarrow \perp$
- (PAIR) $\forall a, b \forall c. c \in \{a, b\} \leftrightarrow c = a \vee c = b$
- (INF) $\forall c. c \in \omega \leftrightarrow c = 0 \vee \exists b \in \omega. c = S(b)$
- (SEP _{$\phi(a, \vec{f})$}) $\forall \vec{f}, a \forall c. c \in S_{\phi(a, \vec{f})}(a, \vec{f}) \leftrightarrow c \in a \wedge \phi(c, \vec{f})$
- (UNION) $\forall a \forall c. c \in \bigcup a \leftrightarrow \exists b \in a. c \in b$
- (POWER) $\forall a \forall c. c \in P(a) \leftrightarrow \forall b. b \in c \rightarrow b \in a$

¹Borrowed from [SU06].

- $(\text{REPL}_{\phi(a,b,\vec{f})}) \forall \vec{f}, a \forall c. c \in R_{\phi(a,b,\vec{f})}(a, \vec{f}) \leftrightarrow (\forall x \in a \exists! y. \phi(x, y, \vec{f})) \wedge (\exists x \in a. \phi(x, c, \vec{f}))$
- $(\text{IND}_{\phi(a,\vec{f})}) \forall \vec{f}. (\forall a. (\forall b \in a. \phi(b, \vec{f})) \rightarrow \phi(a, \vec{f})) \rightarrow \forall a. \phi(a, \vec{f})$
- $(\text{L}_{\phi(a,\vec{f})}) \forall \vec{f}, a, b. a = b \rightarrow \phi(a, \vec{f}) \rightarrow \phi(b, \vec{f})$

Axioms SEP_ϕ , REPL_ϕ , IND_ϕ and L_ϕ are axiom schemas, and so are the corresponding function symbols — there is one function symbol for each formula ϕ . Formally, we define formulas and terms by mutual induction:

$$\phi ::= t \in t \mid \phi \wedge \phi \mid \dots \quad t ::= a \mid \{t, t\} \mid S_{\phi(a,\vec{f})}(t, \vec{t}) \mid R_{\phi(a,b,\vec{f})}(t, \vec{t}) \mid \dots$$

Our presentation is not minimal; for example, the empty set axiom can be derived as usual using Separation and Infinity. However, we aim for a *natural* axiomatization of IZF_R , not necessarily the most optimal one.

The Leibniz axiom schema L_ϕ is usually not present among the axioms of set theories, as it is assumed that logic contains equality and the axiom is a proof rule. We include L_ϕ among the axioms of IZF_R , because there is no obvious way to add it to intuitionistic logic in the Curry-Howard isomorphism context, as its computational content is unclear. Our axiom of Replacement is equivalent to the usual formulations, see [Moc06b] for details.

IZF_R^- will denote IZF_R without the Leibniz axiom schema L_ϕ . 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 $S_\phi(a, \vec{f})$ and $R_\phi(a, \vec{f})$ can be displayed as $\{x \in a \mid \phi(x, \vec{f})\}$ and $\{z \mid (\forall x \in a \exists! y. \phi(x, y, \vec{f})) \wedge \exists x \in a. \phi(x, z, \vec{f})\}$.

The axioms (EMPTY), (PAIR), (INF), (SEP_ϕ), (UNION), (POWER) and (REPL_ϕ) all assert the existence of certain classes and have the same form: $\forall \vec{a}. \forall c. c \in t_A(\vec{a}) \leftrightarrow \phi_A(c, \vec{a})$, 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 $\forall b. b \in c \rightarrow b \in a$. We reserve the notation t_A and ϕ_A to denote the term and the corresponding formula for the axiom A.

Lemma 3.1. Every term $T \equiv t_A(\overrightarrow{t(\vec{a})})$ of IZF_R is definable. In other words, there is a term-free formula $\phi(x, \vec{a})$ such that $\text{IZF}_R \vdash \forall \vec{a}. \phi(T, \vec{a}) \wedge \exists! x. \phi(x, \vec{a})$.

Proof. Straightforward induction on the size of T . We first show the claim for ω , then for the rest of the terms. For ω , the defining formula² is:

$$\phi(x) \equiv c \in x \leftrightarrow c = 0 \vee \exists y \in x. c = S(y)$$

Indeed, $\phi(\omega)$ holds. Suppose $\phi(z)$ for some z , we need to show that $z = \omega$. To do this, we prove by \in -induction $\forall c. c \in z \leftrightarrow c \in \omega$. Take any c and suppose $c \in z$. Then $c = 0$ or there is $y \in z$ such that $c = S(y)$. In the former case $c \in \omega$, in the latter $y \in c$, so by the induction hypothesis $y \in \omega$ and hence $c \in \omega$. The other direction is symmetric.

Consider now arbitrary $T \equiv t_A(\overrightarrow{t(\vec{a})})$. Let \vec{u} denote $\overrightarrow{t(\vec{a})}$, so $T \equiv t_A(\vec{u})$. By the induction hypothesis there are formulas $\overrightarrow{\phi(x, \vec{a})}$ defining \vec{u} . Consider the formula:

$$\phi(x, \vec{a}) \equiv \exists \vec{x}. \bigwedge \overrightarrow{\phi(x, \vec{a})} \wedge \forall c. c \in x \leftrightarrow \phi_A(c, \vec{x})$$

We will now show that $\phi(x, \vec{a})$ defines T . Take any \vec{a} and take $\vec{x} = \vec{u}$. We have $\bigwedge \overrightarrow{\phi(u, \vec{a})}$ and by the axiom (A) corresponding to t_A , we get $\forall c. c \in t_A(\vec{u}) \leftrightarrow \phi_A(c, \vec{u})$. Furthermore,

²Strictly speaking, it is not term-free, but eliminating terms used in ϕ is straightforward.

suppose $\overrightarrow{\phi(z, \vec{a})}$ for some z . Then there are \vec{b} such that $\bigwedge \overrightarrow{\phi(b, \vec{a})}$ and $\forall c. c \in z \leftrightarrow \phi_A(c, \vec{b})$. Since $\overrightarrow{\phi(x, \vec{a})}$ define \vec{u} , $\vec{b} = \vec{u}$ and thus also $\forall c. c \in z \leftrightarrow \phi_A(c, \vec{u})$. To show that $z = T$, it suffices to show that $\forall a. a \in T \leftrightarrow a \in z$, which follows easily.

It remains to consider the situation when ϕ_A contains some terms, which can happen if A is the Separation or Replacement axiom. However, by the induction hypothesis all these terms are definable as well, so there is also a term-free formula ϕ' equivalent to ϕ . \square

Corollary 3.2. For any closed term t there is a term-free formula $\phi(x)$ such that $\text{IZF}_R^- \vdash (\exists!x. \phi(x)) \wedge \phi(t)$.

4. THE λZ CALCULUS

We now present a lambda calculus λZ for IZF_R^- , based on the Curry-Howard isomorphism principle. The first-order part of λZ is essentially $\lambda P1$ from [SU06]. The lambda terms in the calculus correspond to proofs in IZF_R^- . The correspondence is captured formally by Lemma 4.10.

The lambda terms in λZ will be denoted by letters M, N, O, P . There are two kinds of lambda abstractions, one used for proofs of implications, the other for proofs of universal quantifications. We use separate sets of variables for these abstractions and call them proof and first-order variables, respectively. We use letters x, y, z for proof variables and a, b, c for first-order variables. Letters t, s, u are reserved for IZF_R^- terms. The types in the system are IZF_R^- formulas. The lambda terms are generated by an abstract grammar. The first group of terms is standard and used for IFOL proofs:

$$M ::= x \mid M N \mid \lambda a. M \mid \lambda x : \phi. M \mid \text{inl}(M) \mid \text{inr}(M) \mid \text{fst}(M) \mid \text{snd}(M) \mid [t, M] \mid M t \\ \langle M, N \rangle \mid \text{case}(M, x : \phi. N, x : \psi. O) \mid \text{magic}(M) \mid \text{let } [a, x : \phi] := M \text{ in } N$$

The rest of the terms correspond to the axioms of IZF_R^- :

$$\text{emptyProp}(t, M) \mid \text{emptyRep}(t, M) \\ \text{pairProp}(t, u_1, u_2, M) \mid \text{pairRep}(t, u_1, u_2, M) \\ \text{unionProp}(t, u, M) \mid \text{unionRep}(t, u, M) \\ \text{sep}_{\phi(a, \vec{f})}\text{Prop}(t, u, \vec{u}, M) \mid \text{sep}_{\phi(a, \vec{f})}\text{Rep}(t, u, \vec{u}, M) \\ \text{powerProp}(t, u, M) \mid \text{powerRep}(t, u, M) \\ \text{infProp}(t, M) \mid \text{infRep}(t, M) \\ \text{repl}_{\phi(a, b, \vec{f})}\text{Prop}(t, u, \vec{u}, M) \mid \text{repl}_{\phi(a, b, \vec{f})}\text{Rep}(t, u, \vec{u}, M) \\ \text{ind}_{\phi(a, \vec{b})}(\vec{t}, M)$$

The ind term corresponds to the \in -induction axiom schema ($\text{IND}_{\phi(a, \vec{f})}$), and Prop and Rep terms correspond to the respective axioms. The exact nature of the correspondence will become clear in the next section. Briefly and informally, the Rep terms are *representatives* of the fact that a t is a member of a term $t(\vec{u})$ and the Prop terms provide the defining *property* of $t \in t(\vec{u})$. 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 empty , pair , union , sep , power , inf and repl . With this convention in mind, we can summarize the definition of the Prop and Rep terms as:

$$\text{axProp}(t, \vec{u}, M) \mid \text{axRep}(t, \vec{u}, M),$$

where the number of terms in the sequence \vec{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 the set of all free variables of a term M by $FV(M)$ and the set of the free first-order variables of a term by $FV_F(M)$. The free (first-order) variables of a context Γ are denoted by $FV(\Gamma)$ ($FV_F(\Gamma)$) and defined in a natural way. The notation $M[x := N]$ stands for a term M with N substituted for x . The set of all λZ lambda terms will be denoted by Λ .

4.1. Reduction rules. The deterministic reduction relation \rightarrow arises by lazily evaluating the following base reduction rules:

$$\begin{array}{l}
(\lambda x : \phi. M) N \rightarrow M[x := N] \quad (\lambda a. M) t \rightarrow M[a := t] \\
\text{fst}(\langle M, N \rangle) \rightarrow M \quad \text{snd}(\langle M, N \rangle) \rightarrow N \\
\text{case}(\text{inl}(M), x : \phi. N, x : \psi. O) \rightarrow N[x := M] \quad \text{case}(\text{inr}(M), x : \phi. N, x : \psi. O) \rightarrow O[x := M] \\
\text{let } [a, x : \phi] := [t, M] \text{ in } N \rightarrow N[a := t][x := M] \\
\text{axProp}(t, \vec{u}, \text{axRep}(t, \vec{u}, M)) \rightarrow M \\
\text{ind}_{\phi(a, \vec{b})}(\vec{t}, M) \rightarrow \lambda c. M \ c \ (\lambda b. \lambda x : b \in c. \text{ind}_{\phi(a, \vec{b})}(\vec{t}, M) \ b) \quad c, b, x \text{ new}
\end{array}$$

The laziness is specified formally by the following evaluation contexts:

$$\begin{array}{l}
[\circ] ::= \text{fst}([\circ]) \mid \text{snd}([\circ]) \mid \text{case}([\circ], x : \phi. M, x : \psi. N) \mid \text{axProp}(t, \vec{u}, [\circ]) \\
\text{let } [a, y : \phi] := [\circ] \text{ in } N \mid [\circ] \ M \mid \text{magic}([\circ])
\end{array}$$

In other words, the (small-step) reduction relation arises from the base reduction rules and the following inductive definition:

$$\begin{array}{c}
\frac{M \rightarrow M'}{\text{fst}(M) \rightarrow \text{fst}(M')} \quad \frac{M \rightarrow M'}{\text{snd}(M) \rightarrow \text{snd}(M')} \\
\frac{M \rightarrow M'}{\text{case}(M, x : \phi. N, x : \psi. O) \rightarrow \text{case}(M', x : \phi. N, x : \psi. O)} \\
\frac{M \rightarrow M'}{\text{axProp}(t, \vec{u}, M) \rightarrow \text{axProp}(t, \vec{u}, M')} \quad \frac{M \rightarrow M'}{\text{let } [a, y : \phi] := M \text{ in } N \rightarrow \text{let } [a, y : \phi] := M' \text{ in } N} \\
\frac{M \rightarrow M'}{M \ N \rightarrow M' \ N} \quad \frac{M \rightarrow M'}{\text{magic}(M) \rightarrow \text{magic}(M')}
\end{array}$$

Definition 4.1. 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 $M \rightarrow^* M'$ 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.

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

4.2. Types. The type system for λZ is constructed according to the principle of Curry-Howard isomorphism for IZF_R^- . Types are IZF_R formulas. Contexts, denoted by Γ , are finite sets of pairs (x_i, ϕ_i) , written as $x_1 : \phi_1, \dots, x_n : \phi_n$. The *domain* of a context Γ is the set $\{x \mid (x, \phi) \in \Gamma\}$ and it is denoted by $\text{dom}(\Gamma)$. The *range* of a context Γ is the corresponding first-order logic context that contains only formulas and is denoted by $\text{rg}(\Gamma)$. The first group of rules corresponds to the rules of IFOL:

$$\begin{array}{c}
\frac{}{\Gamma, x : \phi \vdash x : \phi} \quad \frac{\Gamma, x : \phi \vdash M : \psi}{\Gamma \vdash \lambda x : \phi. M : \phi \rightarrow \psi} \quad x \notin \text{dom}(\Gamma) \quad \frac{\Gamma \vdash M : \phi \rightarrow \psi \quad \Gamma \vdash N : \phi}{\Gamma \vdash M N : \psi} \\
\frac{\Gamma \vdash M : \phi \quad \Gamma \vdash N : \psi}{\Gamma \vdash \langle M, N \rangle : \phi \wedge \psi} \quad \frac{\Gamma \vdash M : \phi \wedge \psi}{\Gamma \vdash \text{fst}(M) : \phi} \quad \frac{\Gamma \vdash M : \phi \wedge \psi}{\Gamma \vdash \text{snd}(M) : \psi} \\
\frac{\Gamma \vdash M : \phi}{\Gamma \vdash \text{inl}(M) : \phi \vee \psi} \quad \frac{\Gamma \vdash M : \psi}{\Gamma \vdash \text{inr}(M) : \phi \vee \psi} \\
\frac{\Gamma \vdash M : \phi \vee \psi \quad \Gamma, x : \phi \vdash N : \vartheta \quad \Gamma, x : \psi \vdash O : \vartheta}{\Gamma \vdash \text{case}(M, x : \phi. N, x : \psi. O) : \vartheta} \\
\frac{\Gamma \vdash M : \phi}{\Gamma \vdash \lambda a. M : \forall a. \phi} \quad a \notin \text{FV}_F(\Gamma) \quad \frac{\Gamma \vdash M : \forall a. \phi}{\Gamma \vdash M t : \phi[a := t]} \\
\frac{\Gamma \vdash M : \phi[a := t]}{\Gamma \vdash [t, M] : \exists a. \phi} \quad \frac{\Gamma \vdash M : \exists a. \phi \quad \Gamma, x : \phi \vdash N : \psi}{\Gamma \vdash \text{let } [a, x : \phi] := M \text{ in } N : \psi} \quad a \notin \text{FV}_F(\Gamma, \psi) \\
\frac{\Gamma \vdash M : \perp}{\Gamma \vdash \text{magic}(M) : \phi}
\end{array}$$

The rest of the rules correspond to IZF_R^- axioms:

$$\begin{array}{c}
\frac{\Gamma \vdash M : \phi_A(t, \vec{u})}{\Gamma \vdash \text{axRep}(t, \vec{u}, M) : t \in t_A(\vec{u})} \quad \frac{\Gamma \vdash M : t \in t_A(\vec{u})}{\Gamma \vdash \text{axProp}(t, \vec{u}, M) : \phi_A(t, \vec{u})} \\
\frac{\Gamma \vdash M : \forall c. (\forall b. b \in c \rightarrow \phi(b, \vec{t})) \rightarrow \phi(c, \vec{t})}{\Gamma \vdash \text{ind}_{\phi(a, \vec{f})}(\vec{t}, M) : \forall a. \phi(a, \vec{t})}
\end{array}$$

4.3. Properties of λZ . We now prove a standard sequence of lemmas for λZ .

Lemma 4.2 (Canonical Forms). Suppose M is a value and $\vdash M : \vartheta$. Then:

- $\vartheta = t \in t_A(\vec{u})$ iff $M = \text{axRep}(t, \vec{u}, N)$ and $\vdash N : \phi_A(t, \vec{u})$.
- $\vartheta = \phi \vee \psi$ iff $(M = \text{inl}(N)$ and $\vdash N : \phi$) or $(M = \text{inr}(N)$ and $\vdash N : \psi)$.
- $\vartheta = \phi \wedge \psi$ iff $M = \langle N, O \rangle$, $\vdash N : \phi$ and $\vdash O : \psi$.
- $\vartheta = \phi \rightarrow \psi$ iff $M = \lambda x : \phi. N$ and $x : \phi \vdash N : \psi$.
- $\vartheta = \forall a. \phi$ iff $M = \lambda a. N$ and $\vdash N : \phi$.
- $\vartheta = \exists a. \phi$ iff $M = [t, N]$ and $\vdash N : \phi[a := t]$.
- $\vartheta = \perp$ never happens.

Proof. Immediate from the typing rules and the definition of values. \square

Lemma 4.3 (Weakening). If $\Gamma \vdash M : \phi$ and $\text{FV}(\psi) \cup \{x\}$ are fresh with respect to the proof tree $\Gamma \vdash M : \phi$, then $\Gamma, x : \psi \vdash M : \phi$.

Proof. Straightforward induction on $\Gamma \vdash M : \phi$. The freshness assumption is used in the treatment of the proof rules having side-conditions, such as introduction of the universal quantifier. \square

There are two substitution lemmas, one for the propositional part, the other for the first-order part of the calculus. Since the rules and terms of λZ corresponding to IZF_R axioms do not interact with substitutions in a significant way, the proofs are routine.

Lemma 4.4. If $\Gamma, x : \phi \vdash M : \psi$ and $\Gamma \vdash N : \phi$, then $\Gamma \vdash M[x := N] : \psi$.

Proof. By induction on $\Gamma, x : \phi \vdash M : \psi$. We show two interesting cases.

- $\psi = \psi_1 \rightarrow \psi_2$, $M = \lambda y : \psi_1. O$. Using α -conversion we can choose y to be new, so that $y \notin FV(\Gamma, x) \cup FV(N)$. The proof tree must end with:

$$\frac{\Gamma, x : \phi, y : \psi_1 \vdash O : \psi_2}{\Gamma, x : \phi \vdash \lambda y : \psi_1. O : \psi_1 \rightarrow \psi_2}$$

By the induction hypothesis, $\Gamma, y : \psi_1 \vdash O[x := N] : \psi_2$, so $\Gamma \vdash \lambda y : \psi_1. O[x := N] : \psi_1 \rightarrow \psi_2$. By the choice of y , $\Gamma \vdash (\lambda y : \psi_1. O)[x := N] : \psi_1 \rightarrow \psi_2$.

- $\psi = \psi_2$, $M = \text{let } [a, y : \psi_1] := M_1 \text{ in } M_2$. The proof tree ends with:

$$\frac{\Gamma, x : \phi \vdash M_1 : \exists a. \psi_1 \quad \Gamma, x : \phi, y : \psi_1 \vdash M_2 : \psi_2}{\Gamma, x : \phi \vdash \text{let } [a, y : \psi_1] := M_1 \text{ in } M_2 : \psi_2}$$

Choose a and y to be fresh. By the induction hypothesis, $\Gamma \vdash M_1[x := N] : \exists a. \psi_1$ and $\Gamma, y : \psi_1 \vdash M_2[x := N] : \psi_2$. Thus $\Gamma \vdash \text{let } [a, y : \psi_1] := M_1[x := N] \text{ in } M_2[x := N] : \psi_2$. By a and y fresh, $\Gamma \vdash (\text{let } [a, y : \psi_1] := M_1 \text{ in } M_2)[x := N] : \psi_2$ which is what we want. \square

Lemma 4.5. If $\Gamma \vdash M : \phi$, then $\Gamma[a := t] \vdash M[a := t] : \phi[a := t]$.

Proof. By induction on $\Gamma \vdash M : \phi$. Most of the rules do not interact with first-order substitution, so we show the proof just for the four of them which do.

- $\phi = \forall b. \phi_1$, $M = \lambda b. M_1$. The proof tree ends with:

$$\frac{\Gamma \vdash M_1 : \phi_1}{\Gamma \vdash \lambda b. M_1 : \forall b. \phi_1} \quad b \notin FV_F(\Gamma)$$

Without loss of generality we can assume that $b \notin FV(t) \cup \{a\}$. By the induction hypothesis, $\Gamma[a := t] \vdash M_1[a := t] : \phi_1[a := t]$. Therefore $\Gamma[a := t] \vdash \lambda b. M_1[a := t] : \forall b. \phi_1[a := t]$ and by the choice of b , $\Gamma[a := t] \vdash (\lambda b. M_1)[a := t] : (\forall b. \phi_1)[a := t]$.

- $\phi = \phi_1[b := u]$, $M = M_1 u$ for some term u . The proof tree ends with:

$$\frac{\Gamma \vdash M_1 : \forall b. \phi_1}{\Gamma \vdash M_1 u : \phi_1[b := u]}$$

Choosing b to be fresh, by the induction hypothesis we get $\Gamma[a := t] \vdash M_1[a := t] : \forall b. (\phi_1[a := t])$, so $\Gamma[a := t] \vdash M_1[a := t] u[a := t] : \phi_1[a := t][b := u[a := t]]$. By Lemma 2.1 and $b \notin FV(t)$, we get $\Gamma[a := t] \vdash (M_1 u)[a := t] : \phi_1[b := u][a := t]$.

•

$$\frac{\Gamma \vdash M : \phi[b := u]}{\Gamma \vdash [u, M] : \exists b. \phi}$$

Choosing b to be fresh, by the induction hypothesis we get $\Gamma[a := t] \vdash M[a := t] : \phi[b := u][a := t]$. By Lemma 2.1 and $b \notin FV(t)$, we get $\Gamma[a := t] \vdash M[a := t] : \phi[a := t][b := u[a := t]]$. Therefore $\Gamma[a := t] \vdash [u[a := t], M[a := t]] : \exists b. \phi[a := t]$, so also $\Gamma[a := t] \vdash ([u, M])[a := t] : (\exists b. \phi)[a := t]$.

•

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

We choose b so that $b \notin FV(t)$. By the induction hypothesis $\Gamma[a := t] \vdash M[a := t] : \exists b. \phi[a := t]$ and $\Gamma[a := t], x : \phi[a := t] \vdash N[a := t] : \psi[a := t]$. By our choice of b and $b \notin FV_F(\Gamma, \psi)$, we also have $b \notin FV_F(\Gamma[a := t], \psi[a := t])$. Thus also $\Gamma[a := t] \vdash \text{let } [b, x : \phi[a := t]] := M[a := t] \text{ in } N[a := t] : \psi[a := t]$. \square

With the lemmas at hand, Progress and Preservation easily follow:

Lemma 4.6 (Subject Reduction, Preservation). If $\Gamma \vdash M : \phi$ and $M \rightarrow N$, then $\Gamma \vdash N : \phi$.

Proof. By induction on the definition of $M \rightarrow N$. We show several cases. Case $M \rightarrow N$ of:

- $(\lambda x : \phi_1. M_1) M_2 \rightarrow M_1[x := M_2]$. The term M has the form $M = (\lambda x : \phi_1. M_1) M_2$ and the proof tree $\Gamma \vdash M : \phi$ ends with:

$$\frac{\frac{\Gamma, x : \phi_1 \vdash M_1 : \phi}{\Gamma \vdash \lambda x : \phi_1. M_1 : \phi_1 \rightarrow \phi} \quad \Gamma \vdash M_2 : \phi_1}{\Gamma \vdash (\lambda x : \phi_1. M_1) M_2 : \phi}$$

By Lemma 4.4, $\Gamma \vdash M_1[x := M_2] : \phi_1$.

- let $[a, x : \phi_1] := [t, M_1]$ in $M_2 \rightarrow M_2[a := t][x := M_1]$. The term M has the form $M = \text{let } [a, x : \phi_1] := [t, M_1] \text{ in } M_2$ and the proof tree $\Gamma \vdash M : \phi$ ends with:

$$\frac{\frac{\Gamma \vdash M_1 : \phi_1[a := t]}{\Gamma \vdash [t, M_1] : \exists a. \phi_1} \quad \Gamma, x : \phi_1 \vdash M_2 : \phi}{\Gamma \vdash \text{let } [a, x : \phi_1] := [t, M_1] \text{ in } M_2 : \phi}$$

Choose a to be fresh. Thus $M_1[a := t] = M_1$ and $\Gamma[a := t] = \Gamma$. By the side-condition of the last typing rule, $a \notin FV(\phi)$, so $\phi[a := t] = \phi$. By Lemma 4.5 we get $\Gamma[a := t], x : \phi_1[a := t] \vdash M_2[a := t] : \phi[a := t]$, so also $\Gamma, x : \phi_1[a := t] \vdash M_2[a := t] : \phi$. By Lemma 4.4, we get $\Gamma \vdash M_2[a := t][x := M_1] : \phi$.

- $\text{axProp}(t, \vec{u}, \text{axRep}(t, \vec{u}, M_1)) \rightarrow M_1$. In this case the term M is has the form $M = \text{axProp}(t, \vec{u}, \text{axRep}(t, \vec{u}, M_1))$ and the proof tree ends with:

$$\frac{\frac{\Gamma \vdash M_1 : \phi_A(t, \vec{u})}{\Gamma \vdash \text{axRep}(t, \vec{u}, M_1) : t \in t_A(\vec{u})}}{\Gamma \vdash \text{axProp}(t, \vec{u}, \text{axRep}(t, \vec{u}, M_1)) : \phi_A(t, \vec{u})}$$

The claim follows immediately.

- $\text{ind}_{\psi(a, \vec{f})}(\vec{t}, M_1) \rightarrow \lambda c. M_1 c (\lambda b. \lambda x : b \in c. \text{ind}_{\psi(a, \vec{f})}(\vec{t}, M_1) b)$. The term M has the form $M = \text{ind}_{\psi(a, \vec{f})}(\vec{t}, M_1)$ and the proof tree ends with:

$$\frac{\Gamma \vdash M_1 : \forall c. (\forall b. b \in c \rightarrow \psi(b, \vec{t})) \rightarrow \psi(c, \vec{t})}{\Gamma \vdash \text{ind}_{\psi(a, \vec{f})}(\vec{t}, M_1) : \forall a. \psi(a, \vec{t})}$$

We choose b, c, x to be fresh. By applying α -conversion we can also obtain a proof tree of $\Gamma \vdash M_1 : \forall e. (\forall d. d \in e \rightarrow \psi(d, \vec{t})) \rightarrow \psi(e, \vec{t})$, where $\{d, e\} \cap \{b, c\} = \emptyset$. Then by Weakening we get $\Gamma, x : b \in c \vdash M_1 : \forall e. (\forall d. d \in e \rightarrow \psi(d, \vec{t})) \rightarrow \psi(e, \vec{t})$, so also

$\Gamma, x : b \in c \vdash \text{ind}_{\psi(a, \vec{f})}(\vec{t}, M_1) : \forall a. \psi(a, \vec{t})$. Let the proof tree T be defined as:

$$\frac{\frac{\frac{\Gamma, x : b \in c \vdash \text{ind}_{\psi(a, \vec{f})}(\vec{t}, M_1) : \forall a. \psi(a, \vec{t})}{\Gamma, x : b \in c \vdash \text{ind}_{\psi(a, \vec{f})}(\vec{t}, M_1) b : \psi(b, \vec{t})}}{\Gamma \vdash \lambda x : b \in c. \text{ind}_{\psi(a, \vec{f})}(\vec{t}, M_1) b : b \in c \rightarrow \psi(b, \vec{t})}}{\Gamma \vdash \lambda b. \lambda x : b \in c. \text{ind}_{\psi(a, \vec{f})}(\vec{t}, M_1) b : \forall b. b \in c \rightarrow \psi(b, \vec{t})}}$$

Then the following proof tree shows the claim:

$$\frac{\frac{\frac{\Gamma \vdash M_1 : \forall c. (\forall b. b \in c \rightarrow \psi(b, \vec{t})) \rightarrow \psi(c, \vec{t})}{\Gamma \vdash M_1 c : (\forall b. b \in c \rightarrow \psi(b, \vec{t})) \rightarrow \psi(c, \vec{t})} \quad T}{\Gamma \vdash M_1 c (\lambda b. \lambda x : b \in c. \text{ind}_{\psi(a, \vec{f})}(\vec{t}, M_1) b) : \psi(c, \vec{t})}}{\Gamma \vdash \lambda c. M_1 c (\lambda b. \lambda x : b \in c. \text{ind}_{\psi(a, \vec{f})}(\vec{t}, M_1) b) : \forall c. \psi(c, \vec{t})}}$$

□

Lemma 4.7 (Progress). If $\vdash M : \phi$, then either M is a value or there is N such that $M \rightarrow N$.

Proof. Straightforward induction on the length of M . We show the cases for the terms corresponding to IZF_R axioms.

- If $M = \text{axRep}(t, \vec{u}, N)$, then M is a value.
- If $M = \text{axProp}(t, \vec{u}, O)$, then we have the following proof tree:

$$\frac{\vdash O : t \in t_A(\vec{u})}{\vdash \text{axProp}(t, \vec{u}, O) : \phi_A(t, \vec{u})}$$

By the induction hypothesis, either O is a value or there is O_1 such that $O \rightarrow O_1$. In the former case, by Canonical Forms, $O = \text{axRep}(t, \vec{u}, P)$ and $M \rightarrow P$. In the latter, by the evaluation rules $\text{axProp}(t, \vec{u}, O) \rightarrow \text{axProp}(t, \vec{u}, O_1)$.

- The ind terms always reduce. □

Corollary 4.8. If $\vdash M : \phi$ and $M \downarrow v$, then $\vdash v : \phi$ and v is a value.

Corollary 4.9. If $\vdash M : \perp$, then M does not normalize.

Proof. If M normalized, then by Corollary 4.8 we would have a value of type \perp , which by Canonical Forms is impossible. □

Finally, we state the formal correspondence between λZ and IZF_R^- :

Lemma 4.10 (Curry-Howard Isomorphism). If $\Gamma \vdash O : \phi$ then $\text{IZF}_R^- + \text{rg}(\Gamma) \vdash \phi$, where $\text{rg}(\Gamma) = \{\phi \mid (x, \phi) \in \Gamma\}$. If $\text{IZF}_R^- + \Gamma \vdash \phi$, then there exists a term M such that $\bar{\Gamma} \vdash M : \phi$, where $\bar{\Gamma} = \{(x_\phi, \phi) \mid \phi \in \Gamma\}$.

Proof. Both parts follow by easy induction on the proof. The first part is straightforward, to get the claim simply erase the lambda terms from the proof tree. For the second part, we show terms and trees corresponding to IZF_R^- axioms:

- Let ϕ be one of the IZF_R^- axioms apart from \in -Induction. Then $\phi = \forall \vec{a}. \forall c. c \in t_A(\vec{a}) \leftrightarrow \phi_A(c, \vec{a})$ for the axiom (A). Recall that $\phi_1 \leftrightarrow \phi_2$ is an abbreviation for $(\phi_1 \rightarrow \phi_2) \wedge (\phi_2 \rightarrow$

ϕ_1). Let $M = \lambda x : c \in t_A(\vec{a})$. $\text{axProp}(c, \vec{a}, x)$ and let $N = \lambda x : \phi_A(c, \vec{a})$. $\text{axRep}(c, \vec{a}, x)$. Let S be the following proof tree:

$$\frac{\frac{\Gamma, x : c \in t_A(\vec{a}) \vdash x : c \in t_A(\vec{a})}{\Gamma, x : c \in t_A(\vec{a}) \vdash \text{axProp}(c, \vec{a}, x) : \phi_A(c, \vec{a})}}{\Gamma \vdash M : c \in t_A(\vec{a}) \rightarrow \phi_A(c, \vec{a})}$$

And let T be the following proof tree:

$$\frac{\frac{\Gamma, x : \phi_A(c, \vec{a}) \vdash x : \phi_A(c, \vec{a})}{\Gamma, x : \phi_A(c, \vec{a}) \vdash \text{axRep}(c, \vec{a}, x) : c \in t_A(\vec{a})}}{\Gamma \vdash N : \phi_A(c, \vec{a}) \rightarrow c \in t_A(\vec{a})}$$

Then the following proof tree shows the claim:

$$\frac{\frac{S \quad T}{\Gamma \vdash \langle M, N \rangle : c \in t_A(\vec{a}) \leftrightarrow \phi_A(c, \vec{a})}}{\Gamma \vdash \lambda \vec{a} \lambda c. \langle M, N \rangle : \forall \vec{a}. \forall c. c \in t_A(\vec{a}) \leftrightarrow \phi_A(c, \vec{a})}$$

- Let ϕ be the \in -induction axiom. Let $M = \lambda \vec{f} \lambda x : (\forall a. (\forall b. b \in a \rightarrow \psi(b, \vec{f})) \rightarrow \psi(a, \vec{f}))$. $\text{ind}_{\psi(a, \vec{f})}(\vec{f}, x)$. The following proof tree shows the claim:

$$\frac{\frac{\Gamma, x : \forall a. (\forall b. b \in a \rightarrow \psi(b, \vec{f})) \rightarrow \psi(a, \vec{f}) \vdash x : \forall a. (\forall b. b \in a \rightarrow \psi(b, \vec{f})) \rightarrow \psi(a, \vec{f})}{\Gamma, x : \forall a. (\forall b. b \in a \rightarrow \phi(b, \vec{f})) \rightarrow \psi(a, \vec{f}) \vdash \text{ind}_{\psi(a, \vec{f})}(\vec{f}, x) : \forall a. \psi(a, \vec{f})}}{\Gamma \vdash M : \forall \vec{f}. (\forall a. (\forall b. b \in a \rightarrow \psi(b, \vec{f})) \rightarrow \psi(a, \vec{f})) \rightarrow \forall a. \psi(a, \vec{f})}$$

□

Note that all proofs in this section are constructive and quite weak from the proof-theoretic point of view — Heyting Arithmetic should be sufficient to formalize the arguments. However, by the Curry-Howard isomorphism and Corollary 4.9, normalization of λZ entails consistency of IZF_R^- , which easily interprets Heyting Arithmetic. Therefore a normalization proof must utilize much stronger means, which we introduce in the following section.

5. REALIZABILITY FOR IZF_R^-

In this section we work in ZF. It is likely that IZF_C would be sufficient, as excluded middle is not used explicitly; however, arguments using ordinals and ranks would need to be done very carefully, as the notion of an ordinal in constructive set theories is problematic [Pow75, Tay96].

Our definition of realizability is inspired by McCarty's presentation in his Ph. D. thesis [McC84]. However, while he used it mainly to prove independence results for IZF_C and to carry out recursive mathematics, we use it to prove normalization of λZ .

The realizability relation \Vdash relates *realizers* with IZF_R^- formulas over an extended signature. The realizers are terms of λZ ; the signature is extended with class-many constants we call λ -names. We proceed with the formal definitions.

Definition 5.1. The set of all values in λZ is denoted by Λ_{val} .

Definition 5.2. A set A is a λ -name iff A is a set of pairs (v, B) such that $v \in \Lambda_{val}$ and B is a λ -name.

In other words, λ -names are sets hereditarily labelled by λZ values.

Definition 5.3. The class of λ -names is denoted by V^λ .

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

$$V_\alpha^\lambda = \bigcup_{\beta < \alpha} P(\Lambda_{val} \times V_\beta^\lambda) \quad V^\lambda = \bigcup_{\alpha \in ORD} V_\alpha^\lambda$$

The λ -rank of a λ -name A , denoted by $lrk(A)$, is the smallest α such that $A \in V_\alpha^\lambda$.

Definition 5.4. For any $A \in V^\lambda$, A^+ denotes $\{(M, B) \mid M \downarrow v \wedge (v, B) \in A\}$.

Definition 5.5. An *environment* is a finite partial function from first-order variables to V^λ .

We will use the letter ρ to denote *environments*.

The environments are used to store elements of V^λ . In order to smoothen the presentation and make the account closer to the standard accounts of realizability for constructive set theories [McC84, Rat05, Rat06], we make it possible for the formulas to mention constants from V^λ as well. Strictly speaking this is unnecessary and we could give the account of the realizability relation and the normalization theorem using only environments; the cost to pay would be some loss of clarity.

Formally, we extend the first-order language of IZF_R in the following way:

Definition 5.6. A (class-sized) first-order language L arises by enriching the IZF_R signature with constants for all λ -names.

From now on until the end of this section, the letters A, B, C range over λ -names.

Definition 5.7. 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 $\llbracket t \rrbracket_\rho$ in an environment ρ :

- (1) $\llbracket a \rrbracket_\rho \equiv \rho(a)$
- (2) $\llbracket A \rrbracket_\rho \equiv A$
- (3) $\llbracket \omega \rrbracket_\rho \equiv \omega'$, where ω' is defined by the means of inductive definition: ω' is the smallest set such that:
 - $(\text{infRep}(\emptyset, N), A) \in \omega'$ if $N \downarrow \text{inl}(O)$, $O \Vdash_\rho A = 0$ and $A \in V_\omega^\lambda$.
 - If $(M, B) \in \omega'^+$, then $(\text{infRep}(\emptyset, N), A) \in \omega'$ if $N \downarrow \text{inr}(N_1)$, $N_1 \downarrow [t, O]$, $O \downarrow \langle M, P \rangle$, $P \Vdash_\rho A = S(B)$, $A \in V_\omega^\lambda$.

Note that if $(M, B) \in \omega'^+$, then there is a finite ordinal α such that $B \in V_\alpha^\lambda$.

- (4) $\llbracket t_A(\vec{u}) \rrbracket_\rho \equiv \{(\text{axRep}(\emptyset, \vec{0}, N), B) \in \Lambda_{val} \times V_\gamma^\lambda \mid N \Vdash_\rho \phi_A(B, \overrightarrow{\llbracket u \rrbracket_\rho})\}$
- (5) $M \Vdash_\rho \perp \equiv \perp$
- (6) $M \Vdash_\rho t \in s \equiv M \downarrow v \wedge (v, \llbracket t \rrbracket_\rho) \in \llbracket s \rrbracket_\rho$
- (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) $M \Vdash_\rho \phi \vee \psi \equiv (M \downarrow \text{inl}(M_1) \wedge M_1 \Vdash_\rho \phi) \vee (M \downarrow \text{inr}(M_1) \wedge M_1 \Vdash_\rho \psi)$
- (9) $M \Vdash_\rho \phi \rightarrow \psi \equiv (M \downarrow \lambda x. M_1) \wedge \forall N. (N \Vdash_\rho \phi) \rightarrow (M_1[x := N] \Vdash_\rho \psi)$
- (10) $M \Vdash_\rho \forall a. \phi \equiv M \downarrow \lambda a. N \wedge \forall A \in V^\lambda, \forall t \in Tms. N[a := t] \Vdash_\rho \phi[a := A]$
- (11) $M \Vdash_\rho \exists a. \phi \equiv M \downarrow [t, N] \wedge \exists A \in V^\lambda. N \Vdash_\rho \phi[a := A]$

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

The definition of the ordinal γ in item 4 depends on $t_A(\vec{u})$. This ordinal is close to the rank of the set denoted by $t_A(\vec{u})$ and is chosen so that Lemma 5.18 can be proven. Let $\vec{\alpha} = \overrightarrow{\lambda rk(\llbracket u \rrbracket_\rho)}$. Case $t_A(\vec{u})$ of:

- \emptyset — $\gamma = \emptyset$.
- $\{u_1, u_2\}$ — $\gamma = \max(\alpha_1, \alpha_2)$.
- $P(u)$ — $\gamma = \alpha + 1$.
- $\bigcup u$ — $\gamma = \alpha$.
- $S_{\phi(a, \vec{f})}(u, \vec{u})$ — $\gamma = \alpha_1$.
- $R_{\phi(a, b, \vec{f})}(u, \vec{u})$. This case is more complicated. The names are chosen to match the corresponding clause in the proof of Lemma 5.18. Let $G = \{(N_1, (N_{21}, B)) \in \Lambda \times \llbracket u \rrbracket_\rho^+ \mid \exists d \in V^\lambda. \psi(N_1, N_{21}, B, d)\}$, where $\psi(N_1, N_{21}, B, d) \equiv (N_1 \downarrow \lambda a. N_{11}) \wedge (N_{11} \downarrow \lambda x. O) \wedge \exists s \in Tms. (O[x := N_{21}] \downarrow [s, O_1]) \wedge (O_1 \Vdash_\rho \phi(B, d, \llbracket u \rrbracket_\rho) \wedge \forall e. \phi(B, e, \llbracket u \rrbracket_\rho) \rightarrow e = d)$. Then for all $g \in G$ there is D and $(N_1, (N_{21}, B))$ such that $g = (N_1, (N_{21}, B))$ and $\psi(N_1, N_{21}, B, D)$. Use Collection to collect these D 's in one set H , so that for all $g \in G$ there is $D \in H$ such that the property holds. 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 $D \in H$, $\lambda rk(D) < \beta$. Therefore for all $g \in G$ there is $D \in V_\beta^\lambda$ and $(N_1, (N_{21}, B))$ such that $g = (N_1, (N_{21}, B))$ and $\psi(N_1, N_{21}, B, D)$ holds. Set $\gamma = \beta + 1$.

Lemma 5.8. 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 natural numbers:

- $m(M \Vdash_\rho \phi) = (\text{“number of constants } \omega \text{ in } \phi\text{”}, \text{“number of function symbols in } \phi\text{”}, \text{“structural complexity of } \phi\text{”})$
- $m(\llbracket t \rrbracket_\rho) = (\text{“number of constants } \omega \text{ in } t\text{”}, \text{“number of function symbols in } t\text{”}, 0)$

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 — the number of terms does not increase in the clauses for realizability and the 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 \mathbb{N}^3 with lexicographical order is well-founded, the claim follows. \square

Since the definition is well-founded, (metalevel) inductive proofs on the definition of realizability are justified, such as the proof of the following lemma:

Lemma 5.9. $\llbracket t[a := s] \rrbracket_\rho = \llbracket t[a := \llbracket s \rrbracket_\rho] \rrbracket_\rho = \llbracket t \rrbracket_{\rho[a := \llbracket s \rrbracket_\rho]}$ and $M \Vdash_\rho \phi[a := s]$ iff $M \Vdash_\rho \phi[a := \llbracket s \rrbracket_\rho]$ iff $M \Vdash_{\rho[a := \llbracket s \rrbracket_\rho]} \phi$.

Proof. Straightforward induction on the definition of realizability. We show representative cases. Case t of:

- A — then $\llbracket t[a := s] \rrbracket_\rho = \llbracket t[a := \llbracket s \rrbracket_\rho] \rrbracket_\rho = \llbracket t \rrbracket_{\rho[a := \llbracket s \rrbracket_\rho]} = A$.
- a — then $\llbracket t[a := s] \rrbracket_\rho = \llbracket s \rrbracket_\rho$, $\llbracket t[a := \llbracket s \rrbracket_\rho] \rrbracket_\rho = \llbracket \llbracket s \rrbracket_\rho \rrbracket_\rho = \llbracket s \rrbracket_\rho$ and also $\llbracket t \rrbracket_{\rho[a := \llbracket s \rrbracket_\rho]} = \llbracket s \rrbracket_\rho$.
- $t_A(\vec{u})$. Then $\llbracket t[a := s] \rrbracket_\rho = \{(\text{axRep}(\emptyset, \vec{\emptyset}, N), A) \mid N \Vdash_\rho \phi_A(A, \vec{u}[a := s])\}$. By the induction hypothesis, this set is equal to $\{(\text{axRep}(\emptyset, \vec{\emptyset}, N), A) \mid N \Vdash_\rho \phi_A(A, \vec{u}[a := \llbracket s \rrbracket_\rho])\} = \llbracket t[a := \llbracket s \rrbracket_\rho] \rrbracket_\rho$ and also to $\{(\text{axRep}(\emptyset, \vec{\emptyset}, N), A) \mid N \Vdash_{\rho[a := \llbracket s \rrbracket_\rho]} \phi_A(A, \vec{u})\}$ and thus to $\llbracket t \rrbracket_{\rho[a := \llbracket s \rrbracket_\rho]}$.

Case ϕ of:

- $t \in u$. We have $M \Vdash_\rho (t \in u)[a := s]$ iff $M \Vdash_\rho t[a := s] \in u[a := s]$ iff $M \Downarrow v$ and $(v, \llbracket t[a := s] \rrbracket_\rho) \in \llbracket u[a := s] \rrbracket_\rho$. By the induction hypothesis, this is equivalent to $(v, \llbracket t[a := \llbracket s \rrbracket_\rho] \rrbracket_\rho) \in \llbracket u[a := \llbracket s \rrbracket_\rho] \rrbracket_\rho$ and to $(v, \llbracket t \rrbracket_{\rho[a := \llbracket s \rrbracket_\rho]}) \in \llbracket u \rrbracket_{\rho[a := \llbracket s \rrbracket_\rho]}$, so also to $M \Vdash_\rho t[a := \llbracket s \rrbracket_\rho] \in u[a := \llbracket s \rrbracket_\rho]$ and to $M \Vdash_{\rho[a := \llbracket s \rrbracket_\rho]} t \in u$. This shows the claim.
- $\forall b. \phi$. We have $M \Vdash_\rho (\forall b. \phi)[a := s]$ iff (choosing b to be fresh) $M \Vdash_\rho \forall b. \phi[a := s]$ iff $M \Downarrow \lambda b. N$ and $\forall A \in V^\lambda, \forall u \in Tms. N[b := u] \Vdash_\rho \phi[a := s][b := A]$. By the choice of b , this is equivalent to $\forall A \in V^\lambda, \forall u \in Tms. N[b := u] \Vdash_\rho \phi[b := A][a := s]$. By the induction hypothesis, this is equivalent to $\forall A \in V^\lambda, \forall u \in Tms. N[b := u] \Vdash_\rho \phi[b := A][a := \llbracket s \rrbracket_\rho]$ and to $\forall A \in V^\lambda, \forall u \in Tms. N[b := u] \Vdash_{\rho[a := \llbracket s \rrbracket_\rho]} \phi[b := A]$, from which we easily recover the claim. \square

Lemma 5.10. If $(M \Vdash_\rho \phi)$ then $M \Downarrow$.

Proof. Straightforward from the definition of realizability. For $\phi = \perp$, the claim trivially follows and in every other case the definition starts with a clause assuring normalization of M . \square

Lemma 5.11. If $M \rightarrow^* M'$ then $M' \Vdash_\rho \phi$ iff $M \Vdash_\rho \phi$.

Proof. Whether $M \Vdash_\rho \phi$ or not depends only on the value of M , which does not change with reduction or expansion. \square

Lemma 5.12. If ρ agrees with ρ' on $FV(\phi)$, then $M \Vdash_\rho \phi$ iff $M \Vdash_{\rho'} \phi$. In particular, if $a \notin FV(\phi)$, then $M \Vdash_\rho \phi$ iff $M \Vdash_{\rho[a := A]} \phi$.

Proof. Straightforward induction on the definition of realizability — the environment is used only to provide the meaning of the free variables of terms in a formula. \square

Lemma 5.13. If $M \Vdash_\rho \phi \rightarrow \psi$ and $N \Vdash_\rho \phi$, then $M N \Vdash \psi$.

Proof. Suppose $M \Vdash_\rho \phi \rightarrow \psi$. Then $M \Downarrow (\lambda x. O)$ and for all $P \Vdash \phi$, $O[x := P] \Vdash \psi$. Now, $M N \rightarrow^* (\lambda x. O) N \rightarrow O[x := N]$. Lemma 5.11 gives us the claim. \square

We now prove a sequence of lemmas which culminates in Lemma 5.18, the keystone in the normalization proof.

Lemma 5.14. If $A \in V_\alpha^\lambda$ then there is $\beta < \alpha$ such that for all B , if $M \Vdash_\rho B \in A$, then $B \in V_\beta^\lambda$. Also, if $M \Vdash_\rho B = A$, then $B \in V_\alpha^\lambda$.

Proof. Take $A \in V_\alpha^\lambda$. Then there is $\beta < \alpha$ such that $A \in P(\Lambda_{val} \times V_\beta^\lambda)$. Take any B . If $M \Vdash_\rho B \in A$, then $M \Downarrow v$ and $(v, B) \in A$, so $B \in V_\beta^\lambda$.

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 $M \Downarrow \lambda c. N$ and for all $t \in Tms$, for all C , $N[c := t] \Vdash_\rho C \in A \leftrightarrow C \in B$, so $\forall t, C. N[c := t] \Downarrow \langle M_1, M_2 \rangle$, $M_1 \Vdash_\rho C \in A \rightarrow C \in B$ and $M_2 \Vdash_\rho C \in B \rightarrow C \in A$. Thus, for all t, C , $M_2 \Downarrow \lambda x. M_3$ and for all $M_4 \Vdash_\rho C \in B$, $M_3[x := M_4] \Vdash_\rho C \in A$. Take any element $(v, C) \in B$. Then $v \Vdash_\rho C \in B$, so $M_3[x := v] \Vdash_\rho C \in A$. Thus by the first part, $C \in V_\beta^\lambda$. Therefore $B \subseteq \Lambda_{val} \times V_\beta^\lambda$, so $B \in P(\Lambda_{val} \times V_\beta^\lambda) = V_{\beta+1}^\lambda$, so $B \in V_\alpha^\lambda$. \square

The following two lemmas will be used for the treatment of ω in Lemma 5.18.

Lemma 5.15. If $A, B \in V_\alpha^\lambda$, then $\llbracket \{A, B\} \rrbracket_\rho \in V_{\alpha+1}^\lambda$.

Proof. Take any $(M, C) \in \llbracket \{A, B\} \rrbracket_\rho$. By the definition of $\llbracket \{A, B\} \rrbracket_\rho$, any such C is in V_α^λ , so $\llbracket \{A, B\} \rrbracket_\rho \in V_{\alpha+1}^\lambda$. \square

Lemma 5.16. If $A \in V_\alpha^\lambda$ and $(M, C) \in \llbracket \bigcup A \rrbracket_\rho$, then $C \in V_\alpha^\lambda$.

Proof. By the definition of $\llbracket \bigcup A \rrbracket_\rho$, if $(M, C) \in \llbracket \bigcup A \rrbracket_\rho$ then $(M, C) \in V_{\lambda rk(A)}^\lambda$, so $C \in V_\alpha^\lambda$. \square

Lemma 5.17. If $A \in V_\alpha^\lambda$ and $M \Vdash_\rho B = S(A)$, then $B \in V_{\alpha+3}^\lambda$.

Proof. $M \Vdash_\rho B = S(A)$ means $M \Vdash_\rho B = \bigcup \{A, \{A, A\}\}$. By Lemma 5.14, it suffices to show that $\llbracket \bigcup \{A, \{A, A\}\} \rrbracket_\rho \in V_{\alpha+3}^\lambda$. Applying Lemma 5.15 twice, we find that $\llbracket \{A, \{A, A\}\} \rrbracket_\rho \in V_{\alpha+2}^\lambda$. By Lemma 5.16, if $(M, C) \in \llbracket \bigcup \{A, \{A, A\}\} \rrbracket_\rho$, then $C \in V_{\alpha+2}^\lambda$, which shows the claim. \square

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

Lemma 5.18. $(M, A) \in \llbracket t_A(\vec{u}) \rrbracket_\rho$ iff $M = \text{axRep}(\emptyset, \vec{\emptyset}, N)$ and $N \Vdash_\rho \phi_A(A, \overrightarrow{\llbracket u \rrbracket}_\rho)$.

Proof. For all terms apart from ω , the left-to-right part is immediate. For the right-to-left part, suppose $N \Vdash_\rho \phi_A(A, \overrightarrow{\llbracket u \rrbracket}_\rho)$ and $M = \text{axRep}(\emptyset, \vec{\emptyset}, N)$. To show that $(M, A) \in \llbracket t_A(\vec{u}) \rrbracket_\rho$, we need to show that $A \in V_\gamma^\lambda$. The proof proceeds by case analysis on $t_A(\vec{u})$. Let $\vec{\alpha} = \overrightarrow{\lambda rk(\llbracket u \rrbracket_\rho)}$. Case $t_A(\vec{u})$ of:

- \emptyset . If $N \Vdash_\rho \perp$ then anything holds, in particular $A \in \emptyset$.
- $\{u_1, u_2\}$. Suppose that $N \Vdash_\rho A = \llbracket u_1 \rrbracket_\rho \vee A = \llbracket u_2 \rrbracket_\rho$. Then either $N \downarrow \text{inl}(N_1) \wedge N_1 \Vdash_\rho A = \llbracket u_1 \rrbracket_\rho$ or $N \downarrow \text{inr}(N_1) \wedge N_1 \Vdash_\rho A = \llbracket u_2 \rrbracket_\rho$. By Lemma 5.14, in the former case $A \in V_{\alpha_1}^\lambda$, in the latter $A \in V_{\alpha_2}^\lambda$, so $A \in V_{\max(\alpha_1, \alpha_2)}^\lambda$.
- $P(u)$. Suppose that $N \Vdash_\rho \forall c. c \in A \rightarrow c \in \llbracket u \rrbracket_\rho$. Then $N \downarrow \lambda c. N_1$ and for all t, C , $N_1[c := t] \downarrow \lambda x. N_2$ and $\forall O. (O \Vdash C \in A) \Rightarrow N_2[x := O] \Vdash_\rho C \in \llbracket u \rrbracket_\rho$. Take any $(v, B) \in A$. Then $v \Vdash_\rho B \in A$. So $N_2[x := v] \Vdash_\rho B \in \llbracket u \rrbracket_\rho$. By Lemma 5.14 any such B is in V_α^λ , so $A \in V_{\alpha+1}^\lambda$.
- $\bigcup u$. Suppose $N \Vdash_\rho \exists c. c \in \llbracket u \rrbracket_\rho \wedge A \in c$. Then $N \downarrow [t, O]$ and there is C such that $O \downarrow \langle O_1, O_2 \rangle$, $O_1 \Vdash_\rho C \in \llbracket u \rrbracket_\rho$ and $O_2 \Vdash_\rho A \in C$. Two applications of Lemma 5.14 provide the claim.
- $S_{\phi(a, \vec{f})}(u, \vec{u})$. Suppose $N \Vdash_\rho A \in \llbracket u \rrbracket_\rho \wedge \phi(A, \overrightarrow{\llbracket u \rrbracket}_\rho)$. Then $N \downarrow \langle N_1, N_2 \rangle$ and $N_1 \Vdash_\rho A \in \llbracket u \rrbracket_\rho$. Lemma 5.14 shows the claim.
- $R_{\phi(a, b, \vec{f})}(u, \vec{u})$. Suppose $N \Vdash_\rho (\forall x \in \llbracket u \rrbracket_\rho \exists! y. \phi(x, y, \overrightarrow{\llbracket u \rrbracket}_\rho)) \wedge \exists x \in \llbracket u \rrbracket_\rho. \phi(x, A, \overrightarrow{\llbracket u \rrbracket}_\rho)$. Then $N \downarrow \langle N_1, N_2 \rangle$ and $N_2 \Vdash_\rho \exists x \in \llbracket u \rrbracket_\rho. \phi(x, A, \overrightarrow{\llbracket u \rrbracket}_\rho)$. Thus $N_2 \downarrow [t, N_{20}]$, $N_{20} \downarrow \langle N_{21}, N_{22} \rangle$ and there is B such that $N_{21} \Vdash_\rho B \in \llbracket u \rrbracket_\rho$ and $N_{22} \Vdash_\rho \phi(B, A, \overrightarrow{\llbracket u \rrbracket}_\rho)$. We also have $N_1 \Vdash_\rho \forall x \in \llbracket u \rrbracket_\rho \exists! y. \phi(x, y, \overrightarrow{\llbracket u \rrbracket}_\rho)$, so $N_1 \downarrow \lambda a. N_{11}$ and for all C, t , $N_{11}[a := t] \downarrow \lambda x. O$ and for all $P \Vdash_\rho C \in \llbracket u \rrbracket_\rho$, $O[x := P] \Vdash_\rho \exists! y. \phi(C, y, \overrightarrow{\llbracket u \rrbracket}_\rho)$. So taking $C = B$, $t = a$ and $P = N_{21}$, there is D such that $N_{11} \downarrow \lambda a. N_{11}$, $N_{11} \downarrow \lambda x. O$, $O[x := N_{21}] \downarrow [s, O_1]$ and $O_1 \Vdash_\rho \phi(B, D, \overrightarrow{\llbracket u \rrbracket}_\rho) \wedge \forall e. \phi(B, e, \overrightarrow{\llbracket u \rrbracket}_\rho) \rightarrow e = D$. Therefore $(N_1, (N_{21}, B)) \in G$ from the definition of γ , so there is $D \in V_\gamma^\lambda$ such that $N_1 \downarrow \lambda a. N_{11}$, $N_{11} \downarrow \lambda x. O$, $O[x := N_{21}] \downarrow [s, O_1]$ and $O_1 \Vdash_\rho \phi(B, D, \overrightarrow{\llbracket u \rrbracket}_\rho) \wedge \forall e. \phi(B, e, \overrightarrow{\llbracket u \rrbracket}_\rho) \rightarrow e = D$. So $O_1 \downarrow \langle O_{11}, O_{12} \rangle$ and $O_{12} \Vdash_\rho \forall e. \phi(B, e, \overrightarrow{\llbracket u \rrbracket}_\rho) \rightarrow e = D$. Therefore, $O_{12} \downarrow \lambda a. Q$, $Q \downarrow \lambda x. Q_1$ (since we can take again $t = a$ and $Q[a := a] = Q$) and $Q_1[x := N_{22}] \Vdash_\rho A = D$. By Lemma 5.14, $A \in V_\gamma^\lambda$.

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

- The base case. Then $N \downarrow \text{inl}(O)$ and $O \Vdash_\rho A = 0$, so $N \Vdash_\rho A = 0 \vee \exists y \in \omega'. A = S(y)$.

- The inductive step. Then $N \downarrow \text{inr}(N_1)$, $N_1 \downarrow [t, O]$, $O \downarrow \langle M', P \rangle$, $(M', B) \in \omega'^+$, $P \Vdash_\rho A = S(B)$. Therefore, there is C (namely B) such that $M' \Vdash_\rho C \in \omega'$ and $P \Vdash_\rho A = S(C)$. Thus $[t, O] \Vdash_\rho \exists y. y \in \omega' \wedge A = S(y)$, so $N \Vdash_\rho A = 0 \vee \exists y \in \omega'. A = S(y)$.

For the right-to-left direction, suppose $N \Vdash_\rho A = 0 \vee (\exists y. y \in \omega' \wedge A = S(y))$. Then either $N \downarrow \text{inl}(N_1)$ or $N \downarrow \text{inr}(N_1)$. In the former case, $N_1 \Vdash_\rho A = 0$, so by Lemma 5.14 $A \in V_\omega^\lambda$. In the latter, $N_1 \Vdash_\rho \exists y. y \in \omega' \wedge A = S(y)$. Thus $N_1 \downarrow [t, O]$ and there is B such that $O \Vdash_\rho B \in \omega' \wedge A = S(B)$. 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 $A \in V_\omega^\lambda$. Since $(M', B) \in \omega'^+$, there is a finite ordinal α such that $B \in V_\alpha^\lambda$. By Lemma 5.17, $A \in V_{\alpha+3}^\lambda$, so also $A \in V_\omega^\lambda$ and we get the claim. \square

6. NORMALIZATION

In this section, environments ρ are finite partial functions mapping proof variables to terms of λZ and first-order variables to pairs (t, A) , where $t \in Tms$ and $A \in V^\lambda$. Therefore, $\rho : Var \cup FVar \rightarrow \Lambda \cup (Tms \times V^\lambda)$, where Var denotes the set of proof variables and $FVar$ denotes the set of first-order variables. For any ρ , ρ_T denotes the restriction of ρ to the mapping from first-order variables into terms: $\rho_T = \lambda a \in FVar. \pi_1(\rho(a))$. Note that any ρ can be used as a realizability environment by considering only the mapping of first-order variables to V^λ .

We first define a reduction-preserving forgetting map $M \rightarrow \overline{M}$ on the terms of λZ . The map changes all first-order arguments of axRep and axProp terms to \emptyset . It is induced inductively in a natural way by the cases:

$$\overline{\text{axRep}(t, \vec{u}, M)} = \text{axRep}(\emptyset, \vec{\emptyset}, \overline{M}) \quad \overline{\text{axProp}(t, \vec{u}, M)} = \text{axProp}(\emptyset, \vec{\emptyset}, \overline{M})$$

So for example, $\overline{\lambda a. M} = \lambda a. \overline{M}$, $\overline{[t, M]} = [t, \overline{M}]$, $\overline{\langle M, N \rangle} = \langle \overline{M}, \overline{N} \rangle$ and so on. The reduction-preserving character of the map is captured by the following lemmas:

Lemma 6.1. If $M \rightarrow N$ then $\overline{M} \rightarrow \overline{N}$.

Proof. Straightforward. The first-order terms mapped to \emptyset do not play a role in reductions. \square

Lemma 6.2. If \overline{M} normalizes, then so does M .

Proof. By Lemma 6.1, an infinite reduction sequence starting from M would induce an infinite reduction sequence starting from \overline{M} . \square

Definition 6.3. For a sequent $\Gamma \vdash \phi$, $\rho \models \Gamma \vdash M : \phi$ means that ρ is defined on $FV(\Gamma, M, \phi)$ and for all $(x_i, \phi_i) \in \Gamma$, $\rho(x_i) \Vdash_\rho \phi_i$.

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

Definition 6.4. For a sequent $\Gamma \vdash M : \phi$, if $\rho \models \Gamma \vdash M : \phi$ then $M[\rho]$ is $M[x_1 := \rho(x_1), \dots, x_n := \rho(x_n), a_1 := \rho_T(a_1), \dots, a_k := \rho_T(a_k)]$, where $FV(M) = \{x_1, \dots, x_n\}$ and $FV_F(M) = \{a_1, \dots, a_k\}$. Similarly, if ρ is defined on the free variables a_1, \dots, a_k of t , then $t[\rho]$ denotes $t[a_1 := \rho_T(a_1), \dots, a_k := \rho_T(a_k)]$.

Lemma 6.5. If ρ is not defined on x , then $M[\rho][x := N] = M[\rho[x := N]]$. Also if ρ is not defined on a , then $M[a := t] = M[\rho[a := (t, A)]]$.

Proof. Straightforward structural induction on M . \square

Theorem 6.6 (Normalization). *If $\Gamma \vdash M : \vartheta$ then for all $\rho \models \Gamma \vdash M : \vartheta$, $\overline{M}[\rho] \Vdash_\rho \vartheta$.*

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

•

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

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

•

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

By the induction hypothesis, $M' \Vdash_\rho \phi \rightarrow \psi$ and $N' \Vdash_\rho \phi$. Lemma 5.13 gives the claim.

•

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

Take any $\rho \models \Gamma$ and fresh x . 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 $\rho' \models \Gamma, x : \phi \vdash M : \psi$, so by the induction hypothesis $\overline{M}[\rho'] \Vdash_{\rho'} \psi$. Since x is fresh, ρ is undefined on x , so by Lemma 6.5 $\overline{M}[\rho'] = \overline{M}[\rho][x := N] = M'[x := N]$. Therefore $M'[x := N] \Vdash_{\rho'} \psi$. Since ρ' agrees with ρ on logic variables, by Lemma 5.12 we get $M'[x := N] \Vdash_\rho \psi$.

•

$$\frac{\Gamma \vdash M : \perp}{\Gamma \vdash \text{magic}(M) : \phi}$$

By the induction hypothesis, $M' \Vdash_\rho \perp$, which is not the case, so anything holds, in particular $\text{magic}(M') \Vdash_\rho \phi$.

•

$$\frac{\Gamma \vdash M : \phi \wedge \psi}{\Gamma \vdash \text{fst}(M) : \phi}$$

By the induction hypothesis, $M' \Vdash_\rho \phi \wedge \psi$, so $M' \downarrow \langle M_1, M_2 \rangle$ and $M_1 \Vdash_\rho \phi$. Therefore $\text{fst}(M) \rightarrow^* \text{fst}(\langle M_1, M_2 \rangle) \rightarrow M_1$. Lemma 5.11 gives the claim.

•

$$\frac{\Gamma \vdash M : \phi \wedge \psi}{\Gamma \vdash \text{snd}(M) : \psi}$$

Symmetric to the previous case.

•

$$\frac{\Gamma \vdash M : \phi \quad \Gamma \vdash N : \psi}{\Gamma \vdash \langle M, N \rangle : \phi \wedge \psi}$$

All we need to show is $M' \Vdash_\rho \phi$ and $N' \Vdash_\rho \psi$, which we get from the induction hypothesis.

•

$$\frac{\Gamma \vdash M : \phi}{\Gamma \vdash \text{inl}(M) : \phi \vee \psi}$$

We need to show that $M' \Vdash_\rho \phi$, which we get from the induction hypothesis.

•

$$\frac{\Gamma \vdash M : \psi}{\Gamma \vdash \text{inr}(M) : \phi \vee \psi}$$

Symmetric to the previous case.

$$\frac{\Gamma \vdash M : \phi \vee \psi \quad \Gamma, x : \phi \vdash N : \vartheta \quad \Gamma, x : \psi \vdash O : \vartheta}{\Gamma \vdash \text{case}(M, x : \phi. N, x : \psi. O) : \vartheta}$$

By the induction hypothesis, $M' \Vdash_{\rho} \phi \vee \psi$. Take x fresh, so that ρ is undefined on x . Therefore either $M' \downarrow \text{inl}(M_1)$ and $M_1 \Vdash_{\rho} \phi$ or $M' \downarrow \text{inr}(M_2)$ and $M_2 \Vdash_{\rho} \psi$. We only treat the former case, the latter is symmetric. Since $\rho[x := M_1] \Vdash_{\rho} \Gamma, x : \phi \vdash N : \vartheta$, by the induction hypothesis we get $\overline{N}[\rho[x := M_1]] \Vdash_{\rho} \vartheta$. We also have $\text{case}(M, x : \phi. \overline{N}, x : \psi. \overline{O}) \rightarrow^* \text{case}(\text{inl}(M_1), x : \phi. \overline{N}, x : \psi. \overline{O}) \rightarrow \overline{N}[x := M_1]$. By Lemma 6.5, $\overline{N}[x := M_1] = \overline{N}[\rho[x := M_1]]$, so Lemma 5.11 gives us the claim.

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

By the induction hypothesis, for all $\rho' \models \Gamma \vdash M : \phi$, $M[\rho'] \Vdash_{\rho'} \phi$. We need to show that for all $\rho \models \Gamma \vdash \lambda a. M : \forall a. \phi$, $(\lambda a. M)[\rho] \Vdash_{\rho} \forall a. \phi$. Take any such ρ . Using α -conversion we can assure that ρ is not defined on a , so it suffices to show that $\lambda a. \overline{M}[\rho] \Vdash_{\rho} \forall a. \phi$, which is equivalent to $\forall A, t. \overline{M}[\rho][a := t] \Vdash_{\rho} \phi[a := A]$. Take any A and t . By Lemma 5.9 it suffices to show that $\overline{M}[\rho][a := t] \Vdash_{\rho[a := A]} \phi$. Since $\rho[a := (t, A)] \models \Gamma \vdash M : \phi$, by the induction hypothesis we get $\overline{M}[\rho[a := (t, A)]] \Vdash_{\rho[a := A]} \phi$. By Lemma 6.5 $\overline{M}[\rho][a := t] = \overline{M}[\rho[a := (t, A)]]$, which shows the claim.

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

By the induction hypothesis, $M' \Vdash_{\rho} \forall a. \phi$, so $M' \downarrow \lambda a. N$ and $\forall A, u. N[a := u] \Vdash_{\rho} \phi[a := A]$. In particular $N[a := t[\rho]] \Vdash_{\rho} \phi[a := \llbracket t \rrbracket_{\rho}]$. By Lemma 5.9, $N[a := t[\rho]] \Vdash_{\rho} \phi[a := t]$. Since $\overline{M} t[\rho] = M' (t[\rho]) \rightarrow^* (\lambda a. N) t[\rho] \rightarrow N[a := t[\rho]]$, Lemma 5.11 gives us the claim.

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

By the induction hypothesis, $M' \Vdash_{\rho} \phi[a := t]$, so by Lemma 5.9, $M' \Vdash_{\rho} \phi[a := \llbracket t \rrbracket_{\rho}]$. Thus, there is a λ -name A , namely $\llbracket t \rrbracket_{\rho}$, such that $M' \Vdash_{\rho} \phi[a := A]$. Thus, $[t, M][\rho] = [t[\rho], M'] \Vdash_{\rho} \exists a. \phi$, which is what we want.

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

Let $\rho \models \Gamma \vdash \text{let } [a, x : \phi] := M \text{ in } N : \psi$. Choose x, a so that ρ is undefined on these variables. We need to show $(\text{let } [a, x : \phi] := M \text{ in } N)[\rho] = \text{let } [a, x : \phi] := M' \text{ in } \overline{N}[\rho] \Vdash_{\rho} \psi$. By the induction hypothesis, $M' \Vdash_{\rho} \exists a. \phi$, so $M' \downarrow [t, M_1]$ and for some $A, M_1 \Vdash_{\rho} \phi[a := A]$. By the induction hypothesis again, for any $\rho' \models \Gamma, x : \phi \vdash N : \psi$ we have $\overline{N}[\rho'] \Vdash_{\rho'} \psi$. Take $\rho' = \rho[x := M_1, a := (t, A)]$. Since $a \notin FV(\psi)$, by Lemma 5.12 $\overline{N}[\rho'] \Vdash_{\rho} \psi$. Now, let $[a, x : \phi] := M' \text{ in } \overline{N}[\rho] \rightarrow^* \text{let } [a, x : \phi] := [t, M_1] \text{ in } \overline{N}[\rho] \rightarrow \overline{N}[\rho][a := t][x := M_1] = \overline{N}[\rho']$. Lemma 5.11 gives us the claim.

$$\frac{\Gamma \vdash M : \phi_A(t, \vec{u})}{\Gamma \vdash \text{axRep}(t, \vec{u}, M) : t \in t_A(\vec{u})}$$

By the induction hypothesis, $M' \Vdash_\rho \phi_A(t, \vec{u})$. By Lemma 5.9 this is equivalent to $M' \Vdash_\rho \phi_A(\llbracket t \rrbracket_\rho, \overline{\llbracket u \rrbracket_\rho})$. By Lemma 5.18, $(\text{axRep}(\emptyset, \vec{\emptyset}, M'), \llbracket t \rrbracket_\rho) \in \llbracket t_A(\vec{u}) \rrbracket_\rho$, so $\text{axRep}(t, \vec{u}, M) \Vdash_\rho t \in t_A(\vec{u})$.

•

$$\frac{\Gamma \vdash M : t \in t_A(\vec{u})}{\Gamma \vdash \text{axProp}(t, \vec{u}, M) : \phi_A(t, \vec{u})}$$

By the induction hypothesis, $M' \Vdash_\rho t \in t_A(\vec{u})$. This means that $M' \downarrow v$ and $(v, \llbracket t \rrbracket_\rho) \in \llbracket t_A(\vec{u}) \rrbracket_\rho$. By Lemma 5.18, $v = \text{axRep}(\emptyset, \vec{\emptyset}, N)$ and $N \Vdash_\rho \phi_A(\llbracket t \rrbracket_\rho, \overline{\llbracket u \rrbracket_\rho})$. By Lemma 5.9, $N \Vdash_\rho \phi_A(t, \vec{u})$. Moreover,

$$\overline{\text{axProp}(t, \vec{u}, M)[\rho]} = \text{axProp}(\emptyset, \vec{\emptyset}, M') \rightarrow^* \text{axProp}(\emptyset, \vec{\emptyset}, \text{axRep}(\emptyset, \vec{\emptyset}, N)) \rightarrow N.$$

Lemma 5.11 gives us the claim.

•

$$\frac{\Gamma \vdash M : \forall c. (\forall b. b \in c \rightarrow \phi(b, \vec{t})) \rightarrow \phi(c, \vec{t})}{\Gamma \vdash \text{ind}_{\phi(a, \vec{f})}(\vec{t}, M) : \forall a. \phi(a, \vec{t})}$$

Since $\text{ind}_{\phi(a, \vec{f})}(\vec{t}, M')$ reduces to $\lambda c. M' c (\lambda b. \lambda x. \text{ind}_{\phi(a, \vec{f})}(\vec{t}, M') b)$, by Lemma 5.11 it suffices to show that for all C, t , $M' t (\lambda b. \lambda x. \text{ind}_{\phi(a, \vec{f})}(\vec{t}, M') b) \Vdash_\rho \phi(C, \vec{t})$. We proceed by induction on λ -rank of C . Take any C, t . By the induction hypothesis, $M' \Vdash_\rho \forall c. (\forall b. b \in c \rightarrow \phi(b, \vec{t})) \rightarrow \phi(c, \vec{t})$, so $M' \downarrow \lambda c. N$ and $N[c := t] \Vdash_\rho (\forall b. b \in C \rightarrow \phi(b, \vec{t})) \rightarrow \phi(C, \vec{t})$. By Lemma 5.11, $M' t \Vdash_\rho (\forall b. b \in C \rightarrow \phi(b, \vec{t})) \rightarrow \phi(C, \vec{t})$, so by Lemma 5.13, it suffices to show that $\lambda b. \lambda x. \text{ind}_{\phi(a, \vec{f})}(\vec{t}, M') b \Vdash_\rho \forall b. b \in C \rightarrow \phi(b, \vec{t})$. Take any B, u , $O \Vdash_\rho B \in C$, we need to show that $\text{ind}_{\phi(a, \vec{f})}(\vec{t}, M')[x := O] u \Vdash_\rho \phi(B, \vec{t})$. As $x \notin FV(M')$, it suffices to show that $\text{ind}_{\phi(a, \vec{f})}(\vec{t}, M') u \Vdash_\rho \phi(B, \vec{t})$, which, by Lemma 5.11, is equivalent to $M' u (\lambda b. \lambda x. \text{ind}_{\phi(a, \vec{f})}(\vec{t}, M') b) \Vdash_\rho \phi(B, \vec{t})$. As $O \Vdash_\rho B \in C$, the λ -rank of B is less than the λ -rank of C and we get the claim by the induction hypothesis. \square

Corollary 6.7 (Normalization). If $\vdash M : \phi$, then $M \downarrow$.

Proof. Take ρ mapping all free proof variables of M to themselves and all free first-order variables a of M to (a, \emptyset) . Then $\rho \Vdash M : \phi$. By Theorem 6.6, $\overline{M[\rho]}$ normalizes. By the definition of ρ , $\overline{M[\rho]} = \overline{M}$. By Lemma 6.2, M normalizes. \square

Recall that in non-deterministic reduction systems, strong normalization means that for any term M , all reduction paths starting from M terminate, while weak normalization means that for any term M there is a terminating reduction path starting from M . Our reduction system for λZ can be viewed as selecting a call-by-need reduction strategy in a non-deterministic reduction system, where a reduction can be applied anywhere inside of the term. In this view, our results show only weak normalization of the calculus. 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 M. Crabbé and adapted to our framework shows:

Theorem 6.8 (Crabbé's counterexample). *There is a formula ϕ and a term M such that $\vdash M : \phi$ and M does not strongly normalize.*

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

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

We first show that these terms can be typed. Let T denote the following proof tree, showing that $\vdash N : t \in t \rightarrow \perp$:

$$\frac{\frac{\frac{\frac{y : t \in t \vdash y : t \in \{x \in 0 \mid x \in x \rightarrow \perp\}}{y : t \in t \vdash \text{sepProp}(t, 0, y)} : t \in 0 \wedge t \in t \rightarrow \perp}}{y : t \in t \vdash \text{snd}(\text{sepProp}(t, 0, y)) : t \in t \rightarrow \perp}}{y : t \in t \vdash y : t \in t}}{y : t \in t \vdash \text{snd}(\text{sepProp}(t, 0, y)) \quad y : \perp}}{\vdash \lambda y : t \in t. \text{snd}(\text{sepProp}(t, 0, y)) \quad y : t \in t \rightarrow \perp}$$

By Weakening, we can also obtain a tree T_1 showing that $x : t \in 0 \vdash N : t \in t \rightarrow \perp$. The following proof tree shows that $\vdash M : t \in 0 \rightarrow \perp$:

$$\frac{\frac{\frac{\frac{\frac{\frac{T_1}{x : t \in 0 \vdash N : t \in t \rightarrow \perp}}{x : t \in 0 \vdash \langle x, N \rangle : t \in 0 \wedge t \in t \rightarrow \perp}}{x : t \in 0 \vdash \text{sepRep}(t, 0, \langle x, N \rangle) : t \in t}}{x : t \in 0 \vdash N (\text{sepRep}(t, 0, \langle x, N \rangle)) : \perp}}{x : t \in 0 \vdash x : t \in 0} \quad \frac{\frac{T_1}{x : t \in 0 \vdash N : t \in t \rightarrow \perp}}{x : t \in 0 \vdash N (\text{sepRep}(t, 0, \langle x, N \rangle)) : \perp}}{\vdash \lambda x : t \in 0. N (\text{sepRep}(t, 0, \langle x, N \rangle)) : t \in 0 \rightarrow \perp}$$

We now exhibit an infinite reduction sequence starting from M :

$$\begin{aligned} M &= \lambda x : t \in 0. N (\text{sepRep}(t, 0, \langle x, N \rangle)) && = \\ &\lambda x : t \in 0. (\lambda y : t \in t. \text{snd}(\text{sepProp}(t, 0, y)) \quad y) (\text{sepRep}(t, 0, \langle x, N \rangle)) && \rightarrow \\ &\lambda x : t \in 0. \text{snd}(\text{sepProp}(t, 0, (\text{sepRep}(t, 0, \langle x, N \rangle))) (\text{sepRep}(t, 0, \langle x, N \rangle))) && \rightarrow \\ &\lambda x : t \in 0. \text{snd}(\langle x, N \rangle) (\text{sepRep}(t, 0, \langle x, N \rangle)) && \rightarrow \\ &\lambda x : t \in 0. N (\text{sepRep}(t, 0, \langle x, N \rangle)) = M && \rightarrow \dots \end{aligned}$$

□

Note that the counterexample also shows that the weak normalization of λZ is really weak — although $\vdash M : \phi$ entails weak normalization of M , $\Gamma \vdash M : \phi$ does not, as there is a context Γ such that $\Gamma \vdash M : \phi$ and M does not 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) $\forall a. a \in d \leftrightarrow a \in c \wedge a \in a \rightarrow a \in a$.

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

Lemma 6.9. $T \vdash d \in c$

Proof. It suffices to show that $d = c$. Take any $e \in d$, then $e \in c$. On the other hand, suppose $e \in c$. Since obviously $e \in e \rightarrow e \in e$, we also get $e \in d$.

Proof.

Theorem 6.10. *There is a formula ϕ and a term M such that $\vdash_T M : \phi$ and M does not weakly normalize.*

Proof. Let N be the lambda term corresponding to the proof of Lemma 6.9 along with the proof tree T_N . Take $\phi = d \in d \rightarrow d \in d$. Consider the terms:

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

Again, we first show that these terms are typable. Let S be the following proof tree, showing that $\vdash O : d \in d \rightarrow d \in d$:

$$\frac{\frac{\frac{x : d \in d \vdash x : d \in d}{x : d \in d \vdash \text{dProp}(d, c, x) : d \in c \wedge d \in d \rightarrow d \in d}}{x : d \in d \vdash \text{snd}(\text{dProp}(d, c, x)) : d \in d \rightarrow d \in d} \quad \frac{}{x : d \in d \vdash x : d \in d}}{x : d \in d \vdash \text{snd}(\text{dProp}(d, c, x)) \quad x : d \in d}}{\vdash \lambda x : d \in d. \text{snd}(\text{dProp}(d, c, x)) \quad x : d \in d \rightarrow d \in d}$$

Then the following proof tree shows that M is typable:

$$\frac{\frac{S}{\vdash O : d \in d \rightarrow d \in d} \quad \frac{\frac{\frac{T_N}{\vdash N : d \in c} \quad \frac{S}{\vdash O : d \in d \rightarrow d \in d}}{\vdash \langle N, O \rangle : d \in c \wedge d \in d \rightarrow d \in d}}{\vdash \text{dRep}(d, c, \langle N, O \rangle) : d \in d}}{\vdash O (\text{dRep}(d, c, \langle N, O \rangle)) : d \in d}$$

Finally, we exhibit the only reduction sequence starting from M :

$$\begin{aligned} M &= O (\text{dRep}(d, c, \langle N, O \rangle)) && = \\ &(\lambda x : d \in d. \text{snd}(\text{dProp}(d, c, x)) \quad x) (\text{dRep}(d, c, \langle N, O \rangle)) && \rightarrow \\ &\text{snd}(\text{dProp}(d, c, \text{dRep}(d, c, \langle N, O \rangle))) (\text{dRep}(d, c, \langle N, O \rangle)) && \rightarrow \\ &\text{snd}(\langle N, O \rangle) (\text{dRep}(d, c, \langle N, O \rangle)) && \rightarrow \\ &O (\text{dRep}(d, c, \langle N, O \rangle)) = M && \rightarrow \dots \end{aligned}$$

□

These counterexamples to normalization properties can also be presented in a cleaner way in the framework of higher-order rewriting [Moc06a].

7. APPLICATIONS

The normalization theorem immediately provides several results.

Corollary 7.1 (Disjunction Property). If $\text{IZF}_R^- \vdash \phi \vee \psi$, then $\text{IZF}_R^- \vdash \phi$ or $\text{IZF}_R^- \vdash \psi$.

Proof. Suppose $\text{IZF}_R^- \vdash \phi \vee \psi$. By the Curry-Howard isomorphism, there is a λZ term M such that $\vdash M : \phi \vee \psi$. By Corollary 4.8, $M \downarrow v$ and $\vdash v : \phi \vee \psi$. By Canonical Forms, either $v = \text{inl}(N)$ and $\vdash N : \phi$ or $v = \text{inr}(N)$ and $\vdash N : \psi$. By applying the other direction of the Curry-Howard isomorphism we get the claim. □

Corollary 7.2 (Term Existence Property). If $\text{IZF}_R^- \vdash \exists x. \phi(x)$, then there is a closed term t such that $\text{IZF}_R^- \vdash \phi(t)$.

Proof. By the 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 the Curry-Howard isomorphism $\text{IZF}_R^- \vdash \phi(t)$. If t is not closed already, then let $\vec{a} = FV(t)$. We have $\text{IZF}_R^- \vdash \forall \vec{a}. \phi(t)$, so also $\phi(t[\vec{a} := \vec{\emptyset}])$. \square

To show NEP, 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 $\text{natRep}(t, N)$. By Canonical Forms, $\vdash N : t = 0 \vee \exists y \in \omega. t = S(y)$. F then normalizes N to either $\text{inl}(O)$ or $\text{inr}(O)$. 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 obtains 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 t, t_1, t_2, \dots of terms obtained throughout the execution of F . We have $\text{IZF}_R^- \vdash t \in \omega$, $\text{IZF}_R^- \vdash t = S(t_1)$, $\text{IZF}_R^- \vdash t_1 = S(t_2)$ and so on. The length of the sequence is therefore exactly the natural number denoted by t .

Corollary 7.3 (Numerical Existence Property). If $\text{IZF}_R^- \vdash \exists x \in \omega. \phi(x)$, then there is a natural number n and term t such that $\text{IZF}_R^- \vdash \phi(t) \wedge t = \bar{n}$.

Proof. As before, use the Curry-Howard isomorphism to get a value $[t, M]$ such that $\vdash [t, M] : \exists x. x \in \omega \wedge \phi(x)$. Thus $\vdash M : t \in \omega \wedge \phi(t)$, so $M \downarrow \langle M_1, M_2 \rangle$ and $\vdash M_1 : t \in \omega$. Take $n = F(\vdash M_1 : t \in \omega)$. By patching together the proofs $\text{IZF}_R^- \vdash t = S(t_1)$, $\text{IZF}_R^- \vdash t_1 = S(t_2)$, \dots , $\text{IZF}_R^- \vdash t_n = 0$ obtained throughout the execution of F , we get $\text{IZF}_R^- \vdash t = \bar{n}$. \square

This version of NEP differs from the one usually found in the literature, where in the end $\phi(\bar{n})$ 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. More specifically, we conjecture that there is a term t and formula ϕ such that $\text{IZF}_R^- \vdash \phi(t) \wedge t = \bar{n}$ and IZF_R^- does not prove $\phi(\bar{n})$.

8. EXTENSIONAL IZF_R

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

Lemma 8.1. Equality is an equivalence relation.

Proof. Straightforward. \square

Definition 8.2. A set C is *L-stable*, if $A \in C$ and $A = B$ implies $B \in C$.

Thus, L-stable sets are well-behaved as far as the atomic version of the Leibniz axiom ($\forall a, b, c. a \in c \wedge a = b \rightarrow b \in c$) is concerned.

Definition 8.3. A set C is *transitively L-stable* (we say that $\text{TLS}(C)$ holds) 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 e.g. in [AR01]. We denote the class of transitively L-stable sets by T . The statement $V = T$ stands for $\forall A. \text{TLS}(A)$. The class T in IZF_R^- plays a similar role to the class of well-founded sets in ZF without Foundation.

Lemma 8.4. $\text{IZF}_R \vdash V = T$.

Proof. Straightforward \in -induction. \square

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

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

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

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

Lemma 8.5. T is transitive.

Proof. Take any A in T and suppose $a \in A$. Then by the definition of T , $a \in T$ as well. \square

Lemma 8.6. If $A = C$ and $A \in T$, then $C \in T$.

Proof. This is *not* obvious, as there is no Leibniz axiom in the logic. Suppose $a \in C$ and $a = b$. Since $A = C$, $a \in A$. Since A is L-stable, $b \in A$, so also $b \in C$. Thus C is L-stable.

If $a \in C$, then $a \in A$. Since $A \in T$ and T is transitive, $a \in T$. Thus C is transitively L-stable. \square

Lemma 8.7. Equality is absolute for T .

Proof. Take any $a, b \in T$. Suppose $(a = b)^T$. This means that for all $c \in T$, $c \in a \leftrightarrow c \in b$. As T is transitive, this is equivalent to for all c , $c \in a \leftrightarrow c \in b$, so also $a = b$ in the real world. On the other hand, if $\forall c. c \in a \leftrightarrow c \in b$, then obviously also $\forall c \in T. c \in a \leftrightarrow c \in b$. \square

The following three lemmas are essentially used to show that T is closed under the axioms of IZF_R .

Lemma 8.8. $0 \in T$. If $A \in T$, then $S(A) \in T$.

Proof. That $0 \in T$ is obvious. Take any $A \in T$. To show that $A \cup \{A\} \in T$, suppose $a \in A \cup \{A\}$ and $a = b$. If $a \in A$, then by $A \in T$ we have $b \in A$ and $a \in T$. If $a \in \{A\}$, then $a = A$, so also $b = A$ and by Lemma 8.6 $a \in T$. In both cases $b \in A \cup \{A\}$ which shows the claim. \square

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

Lemma 8.9. For any term $t(a, \vec{f})$, $\forall a, b, \vec{f} \in T. (a = b \rightarrow t^T(a, \vec{f}) = t^T(b, \vec{f})) \wedge t^T(a, \vec{f}) \in T$.

Proof. Case $t(a, \vec{f})$ of:

- a, f_i, \emptyset . The claim is trivial.
- ω . It suffices to show that $\omega \in T$. We show by \in -induction on a that $\forall a. a \in \omega \rightarrow a \in T \wedge \forall b. a = b \rightarrow b \in \omega$. Take any $a \in \omega$. Then either $a = 0$ or there is $y \in \omega$ such that $a = S(y)$. Take any b such that $a = b$. In the former case $b = 0$, so $b \in \omega$ and by Lemmas 8.6 and 8.8 we get $a \in T$. In the latter case, take this y . We have $b = S(y)$, so $b \in \omega$. By $a = S(y)$, $y \in a$, so by the induction hypothesis $y \in T$, thus by Lemma 8.8 we also get $a \in T$.

- $\{t_1(a, \vec{f}), t_2(a, \vec{f})\}$. By the induction hypothesis, $t_1^T(a, \vec{f}) = t_1^T(b, \vec{f})$ and $t_2^T(a, \vec{f}) = t_2^T(b, \vec{f})$. In order to show that $\{t_1(a, \vec{f}), t_2(a, \vec{f})\}^T = \{t_1(b, \vec{f}), t_2(b, \vec{f})\}^T$, take any $A \in \{t_1^T(a, \vec{f}), t_2^T(a, \vec{f})\}$. Then either $A = t_1^T(a, \vec{f})$ or $A = t_2^T(a, \vec{f})$, so either $A = t_1^T(b, \vec{f})$ or $A = t_2^T(b, \vec{f})$, in both cases $A \in \{t_1(b, \vec{f}), t_2(b, \vec{f})\}^T$. The other direction is symmetric and we get $\{t_1(a, \vec{f}), t_2(a, \vec{f})\}^T = \{t_1(b, \vec{f}), t_2(b, \vec{f})\}^T$.

Furthermore, by the induction hypothesis, $t_1^T(a, \vec{f}) \in T$ and $t_2^T(a, \vec{f}) \in T$. Thus in both cases by Lemma 8.6, $A \in T$. Suppose $A = B$. Then either $B = t_1^T(a, \vec{f})$, or $B = t_2^T(a, \vec{f})$. In both cases $B \in \{t_1(a, \vec{f}), t_2(a, \vec{f})\}^T$. Thus we have shown that $\{t_1(a, \vec{f}), t_2(a, \vec{f})\}^T \in T$.

- $\bigcup t(a, \vec{f})$. Take any $A \in (\bigcup t(a, \vec{f}))^T = \bigcup t^T(a, \vec{f})$. By the induction hypothesis, $t^T(a, \vec{f}) = t^T(b, \vec{f})$. Thus there is $B \in t^T(a, \vec{f})$ such that $A \in B$. Thus also $B \in t^T(b, \vec{f})$, so $A \in \bigcup t^T(b, \vec{f})$. The other direction is symmetric and we get $(\bigcup t(a, \vec{f}))^T = (\bigcup t(b, \vec{f}))^T$.

Furthermore, by the induction hypothesis, $t^T(a, \vec{f}) \in T$, so by transitivity of T , $B \in T$ and also $A \in T$. Finally, suppose that $C = A$. Then since $B \in T$, $C \in B$, so $C \in \bigcup t^T(a, \vec{f})$. This shows the claim.

- $P(t(a, \vec{f}))$. By the induction hypothesis, $t^T(a, \vec{f}) = t^T(b, \vec{f})$. Suppose $A \in (P(t(a, \vec{f})))^T$. Then $A \subseteq t^T(a, \vec{f})$ and $A \in T$. Thus also $A \subseteq t^T(b, \vec{f})$, so $A \in (P(t(b, \vec{f})))^T$. The other direction is symmetric and we get $(P(t(a, \vec{f})))^T = (P(t(b, \vec{f})))^T$.

Suppose $A = B$. Since $A \in T$, by Lemma 8.6 $B \in T$. It is easy to see that also $B \subseteq t^T(a, \vec{f})$, so $B \in P(t^T(a, \vec{f})) \cap T = (P(t(a, \vec{f})))^T$.

- $S_{\phi(a, \vec{f})}(t(a, \vec{f}), t(a, \vec{f}))$. Suppose $A \in (S_{\phi(a, \vec{f})}(t(a, \vec{f}), t(a, \vec{f})))^T$. Then $A \in t^T(a, \vec{f}) \wedge \phi^T(A, t^T(a, \vec{f}))$. By the induction hypothesis, $t^T(a, \vec{f}) \in T$ and $\overline{t^T(a, \vec{f})} \in T$. Thus, by transitivity of T , $A \in T$. Moreover, by the induction hypothesis, $\overline{t^T(a, \vec{f})} = \overline{t^T(b, \vec{f})}$ and $\overline{t^T(a, \vec{f})} = \overline{t^T(b, \vec{f})}$. Therefore $A \in \overline{t^T(b, \vec{f})}$. By Lemma 8.10 we get $\phi^T(A, \overline{t^T(b, \vec{f})})$. This shows that $A \in (S_{\phi(a, \vec{f})}(t(b, \vec{f}), t(b, \vec{f})))^T$. The other direction is symmetric and we get $(S_{\phi(a, \vec{f})}(t(a, \vec{f}), t(a, \vec{f})))^T = (S_{\phi(a, \vec{f})}(t(b, \vec{f}), t(b, \vec{f})))^T$.

Suppose $A = B$. By Lemma 8.6, $B \in T$. Since $\overline{t^T(a, \vec{f})} \in T$, $B \in \overline{t^T(a, \vec{f})}$. By Lemma 8.10, $\phi^T(B, \overline{t^T(a, \vec{f})})$ holds. Thus $(S_{\phi(a, \vec{f})}(t(a, \vec{f}), t(a, \vec{f})))^T \in T$.

- $R_{\phi(a, b, \vec{f})}(a, \vec{f})$. Suppose $A \in (R_{\phi(a, b, \vec{f})}(t(a, \vec{f}), u(a, \vec{f})))^T$ and $A = B$. This means that:
 - $\forall x \in t^T(a, \vec{f}) \exists! y \in T. \phi^T(x, y, u^T(a, \vec{f}))$. Take any $x \in t^T(b, \vec{f})$. By the induction hypothesis, $x \in t^T(a, \vec{f})$. Thus there is $y \in T$ such that $\phi^T(x, y, u^T(a, \vec{f}))$ and $\forall z \in T. \phi^T(x, z, u^T(a, \vec{f})) \rightarrow z = y$. We will now show that there is exactly one $y' \in T$ such that $\phi^T(x, y', u^T(b, \vec{f}))$. Take $y' = y$. By the induction hypothesis, $\overline{u^T(a, \vec{f})} = \overline{u^T(b, \vec{f})}$. By Lemma 8.10, $\phi^T(x, y', \overline{u^T(b, \vec{f})})$. Take any $z' \in T$ and assume $\phi^T(x, z', \overline{u^T(b, \vec{f})})$. By Lemma 8.10, $\phi(x, z', \overline{u^T(a, \vec{f})})$, so $z' = y'$. Thus we have shown that $\forall x \in t^T(b, \vec{f}) \exists! y \in T. \phi^T(x, y, \overline{u^T(b, \vec{f})})$.

– $\exists x \in t^T(a, \vec{f})$. $A \in T \wedge \overrightarrow{\phi^T(x, A, u^T(a, \vec{f}))}$. Take this x . By Lemma 8.6, $B \in T$, so by Lemma 8.10, $\overrightarrow{\phi^T(x, B, u^T(a, \vec{f}))}$. Moreover, by Lemma 8.10, $\overrightarrow{\phi^T(x, A, u^T(b, \vec{f}))}$. Thus there is $x \in t^T(b, \vec{f})$ such that $\overrightarrow{\phi^T(x, A, u^T(b, \vec{f}))}$.
Altogether, this shows that $A \in (R_{\phi(a, b, \vec{f})}(t(b, \vec{f}), u(b, \vec{f})))^T$. The other direction is symmetric and we get $(R_{\phi(a, b, \vec{f})}(t(a, \vec{f}), u(a, \vec{f})))^T = (R_{\phi(a, b, \vec{f})}(t(b, \vec{f}), u(b, \vec{f})))^T$. We have also shown that $(R_{\phi(a, b, \vec{f})}(t(a, \vec{f}), u(a, \vec{f})))^T \in T$, so the proof is complete. \square

Lemma 8.10. $T \models L_{\phi(a, \vec{f})}$. In other words, $\forall a, b, \vec{f} \in T. a = b \rightarrow \phi^T(a, \vec{f}) \rightarrow \phi^T(b, \vec{f})$.

Proof. We show representative cases. Case ϕ of:

- $t(a, \vec{f}) \in s(a, \vec{f})$ for some terms t, s . We need to show that if $A, B, \vec{F} \in T$, $A = B$ and $t^T(A, \vec{F}) \in s^T(A, \vec{F})$, then $t^T(B, \vec{F}) \in s^T(B, \vec{F})$. By Lemma 8.9, $t^T(A, \vec{F}) = t^T(B, \vec{F})$, $s^T(A, \vec{F}) = s^T(B, \vec{F})$ and $s^T(A, \vec{F}) \in T$. Therefore $t^T(B, \vec{F}) \in s^T(A, \vec{F})$, which entails $t^T(B, \vec{F}) \in s^T(B, \vec{F})$.
- $\phi_1(a, \vec{f}) \rightarrow \phi_2(a, \vec{f})$. Take any $A, B, \vec{F} \in T$, assume $A = B$, $\phi_1^T(A, \vec{F}) \rightarrow \phi_2^T(A, \vec{F})$ and $\phi_1^T(B, \vec{F})$. By the induction hypothesis for ϕ_1 , $\phi_1^T(A, \vec{F})$. Using the assumption we obtain $\phi_2^T(A, \vec{F})$. By the induction hypothesis for ϕ_2 we get $\phi_2^T(B, \vec{F})$.
- $\exists c. \phi_1(a, \vec{f}, c)$. Take any $A, B, \vec{F} \in T$, assume $A = B$ and $\exists c \in T. \phi_1^T(A, \vec{F}, c)$. Then there is a set $C \in T$ such that $\phi_1^T(A, \vec{F}, C)$ holds. By the induction hypothesis, merging \vec{f} with c , we get $\phi_1^T(B, \vec{F}, C)$, so also $\exists c. \phi_1^T(B, \vec{F}, c)$. \square

Theorem 8.11. $T \models IZF_R$. In other words, T is an inner model of IZF_R .

Proof. We proceed axiom by axiom.

- (EMPTY) Straightforward.
- (PAIR) Take any $A, B \in T$. That $\{A, B\}$ satisfies the (PAIR) axiom in T follows by absoluteness of equality.
- (UNION) Take any $A \in T$. Suppose $C \in \bigcup A$. Then there is some B such that $C \in B \in A$. Since A is transitive, $B \in T$. On the other hand, if there is $B \in T$ such that $C \in B \in A$, then obviously $C \in \bigcup A$.
- (INF) Suppose $C \in \omega$. Then either $C = 0$ or there is $y \in \omega$ such that $C = S(y)$. We need to show that either $C = 0$ or there is $y \in T$ such that $y \in \omega^T$ and $C = S^T(y)$. If $C = 0$, the claim is trivial. Otherwise, suppose there is $y \in \omega$ such that $C = S(y)$. Then $y \in C$, so by transitivity of T , $y \in T$. We also know that $\omega^T = \omega$ and $S^T(y) = S(y)$. The claim follows.

On the other hand, suppose $C = 0$ or there is $y \in T$ such that $y \in \omega$ and $C = S^T(y)$. In both cases, C is trivially in ω .

- (POWER) Take any $A, C \in T$. Suppose $C \in P^T(A)$. Then $\forall D \in C. D \in A$, so also for all $D \in T, D \in C \rightarrow D \in A$. On the other hand, suppose that for all $D \in T, D \in C \rightarrow D \in A$. To show that $C \in P^T(A)$, we need to show that $C \in T$ and for all $D \in C, D \in A$. We already have the former. To show the latter, note that by transitivity of T , any $D \in C$ is also in T , so by the assumption in A . This shows the claim.

- (SEP $_{\phi(a,\vec{f})}$) Take any $A, \vec{F} \in T$ and suppose $C \in \{x \in A \mid \phi(x, \vec{F})\}^T$. Then $C \in A$ and $\phi^T(C, \vec{F})$, which is what we need. On the other hand, if $C \in A$ and $\phi^T(C, \vec{F})$, then also $C \in \{x \in A \mid \phi^T(x, \vec{F})\} = \{x \in A \mid \phi(x, \vec{F})\}^T$.
- (REPL $_{\phi(a,b,\vec{f})}$) Take any $A, \vec{F}, C \in T$ such that $C \in \{z \mid (\forall x \in A \exists! y. \phi(x, y, \vec{F})) \wedge \exists x \in A. \phi(x, z, \vec{F})\}^T$. This is equivalent to $(\forall x \in A \exists! y. y \in T \wedge \phi^T(x, y, \vec{F})) \wedge \exists x \in A. C \in T \wedge \phi^T(x, C, \vec{F})$. Since $A \in T$ and T is closed under equality, it is also equivalent to $(\forall x \in T. x \in A \rightarrow \exists y. y \in T \wedge \phi^T(x, y, \vec{F}) \wedge \forall z. z \in T \rightarrow z = y \rightarrow \phi^T(x, z, \vec{f})) \wedge \exists x \in T. x \in A \wedge C \in T \wedge \phi^T(x, C, \vec{F})$, which is what we want.
- (IND $_{\phi(a,\vec{f})}$) Take $\vec{F} \in T$ and suppose that $\forall x \in T. (\forall y \in T. y \in x \rightarrow \phi^T(y, \vec{F})) \rightarrow \phi^T(x, \vec{F})$. We have to show that $\forall a. a \in T \rightarrow \phi^T(a, \vec{F})$. We proceed by \in -induction on a . Take any $A \in T$. By the assumption instantiated with A , $(\forall y \in T. y \in A \rightarrow \phi^T(y, \vec{F})) \rightarrow \phi^T(A, \vec{F})$. We have to show that $\phi^T(A, \vec{F})$. It suffices to show that $\forall y \in T. y \in A \rightarrow \phi^T(y, \vec{F})$. Take any $y \in T \cap A$. By the induction hypothesis for y , we get $\phi^T(y, \vec{F})$ and the claim.
- (L $_{\phi(a,\vec{f})}$) Follows by Lemma 8.10. \square

Lemma 8.12. For any term $t(\vec{a})$ and any formula $\phi(\vec{a})$, $\text{IZF}_R \vdash \forall \vec{a}. t^T(\vec{a}) = t(\vec{a}) \wedge \phi^T(\vec{a}) \leftrightarrow \phi(\vec{a})$.

Proof. By induction on the generation of terms and formulas. Case t of:

- a, ω, \emptyset . The proof is obvious.
- $\{t_1, t_2\}$. By the induction hypothesis, $t_1^T = t_1$ and $t_2^T = t_2$. So if $a \in \{t_1^T, t_2^T\}$, then $a = t_1$ or $a = t_2$, so $a \in \{t_1, t_2\}$. The other direction is symmetric.
- $\bigcup t_1$. By the induction hypothesis, $t_1^T = t_1$. If $a \in \bigcup t_1^T$, then there is b such that $a \in b \in t_1^T$, so $b \in t_1$ and $a \in \bigcup t_1$. The other direction is symmetric.
- $P(t_1)$. By the induction hypothesis, $t_1^T = t_1$. If $a \in P(t_1^T) \cap T$, then $a \subseteq t_1^T$, so also $a \subseteq t_1$ and consequently $a \in P(t_1)$. On the other hand, if $a \in P(t_1)$, then by $V = T$ we also get $a \in T$, so $a \in (P(t_1))^T$.
- $\{x \in t_1 \mid \phi(x, \vec{u})\}$. By the induction hypothesis, $t_1^T = t_1, \vec{u}^T = \vec{u}$. Suppose $a \in \{x \in t_1^T \mid \phi^T(x, \vec{u}^T)\}$. Then $a \in t_1^T$, so $a \in t_1$. Since $\phi^T(a, \vec{u}^T)$ and we work in IZF_R , $\phi^T(a, \vec{u})$. By the induction hypothesis, $\phi(a, \vec{u})$, so $a \in \{x \in t_1 \mid \phi(x, \vec{u})\}$. The other direction is symmetric.
- $\{y \mid \forall x \in t_1 \exists! y. \phi(x, y, \vec{u}) \wedge \exists x \in t_1. \phi(x, y, \vec{u})\}$. By the induction hypothesis, $t_1^T = t_1$ and $\vec{u}^T = \vec{u}$. Suppose $a \in \{y \mid \forall x \in t_1 \exists! y. \phi(x, y, \vec{u}) \wedge \exists x \in t_1. \phi(x, y, \vec{u})\}^T$. Then:
 - For all $x \in t_1^T$ there is exactly one $y \in T$ such that $\phi^T(x, y, \vec{u}^T)$. By the induction hypothesis and $V = T$, we also have for all $x \in t_1$ there is exactly one y such that $\phi(x, y, \vec{u})$.
 - There is $x \in t_1^T$ such that $a \in T$ and $\phi^T(x, a, \vec{u}^T)$. Then also there is $x \in t_1$ such that $\phi(x, a, \vec{u})$.
Altogether, $a \in \{y \mid \forall x \in t_1 \exists! y. \phi(x, y, \vec{u}) \wedge \exists x \in t_1. \phi(x, y, \vec{u})\}$. The other direction is similar.

For the formulas, we show representative cases. Case ϕ of:

- $t \in s$. By the induction hypothesis, $t^T = t$ and $s^T = s$, so by the Leibniz axiom $t^T \in s^T$ is equivalent to $t \in s$.
- $\forall a. \phi_1$. Suppose $\forall a. \phi_1$, then since $V = T$ we have $\forall a \in T. \phi_1$. By the induction hypothesis, $\forall a \in T. \phi_1^T$. The other direction is similar. \square

Lemma 8.13. $\text{IZF}_R \vdash \phi$ iff $\text{IZF}_R^- \vdash \phi^T$.

Proof. The left-to-right direction follows by Theorem 8.11. For the right-to-left direction, if $\text{IZF}_R^- \vdash \phi^T$, then also $\text{IZF}_R \vdash \phi^T$ and Lemma 8.12 shows the claim.

Proof.

Corollary 8.14. IZF_R satisfies DP, NEP and TEP.

Proof. For DP, suppose $\text{IZF}_R \vdash \phi \vee \psi$. By Lemma 8.13, $\text{IZF}_R^- \vdash \phi^T \vee \psi^T$. By DP for IZF_R^- , either $\text{IZF}_R^- \vdash \phi^T$ or $\text{IZF}_R^- \vdash \psi^T$. Using Lemma 8.13 again we get either $\text{IZF}_R \vdash \phi$ or $\text{IZF}_R \vdash \psi$.

For NEP, suppose $\text{IZF}_R \vdash \exists x. x \in \omega \wedge \phi(x)$. By Lemma 8.13, $\text{IZF}_R^- \vdash \exists x. x \in T \wedge x \in \omega^T. \phi^T(x)$, so $\text{IZF}_R^- \vdash \exists x \in \omega^T. x \in T \wedge \phi^T(x)$. Since $\omega^T = \omega$, using NEP for IZF_R^- we get a natural number n such that $\text{IZF}_R^- \vdash \exists x \in \omega. x \in T \wedge \phi^T(x) \wedge x = \bar{n}$, thus also $\text{IZF}_R^- \vdash \exists x \in T. x \in \omega^T \wedge \phi^T(x) \wedge x = \bar{n}$. By Lemma 8.13 and $\bar{n} = \bar{n}^T$, we get $\text{IZF}_R \vdash \exists x. \phi(x) \wedge x = \bar{n}$. By the Leibniz axiom, $\text{IZF}_R \vdash \phi(\bar{n})$.

For TEP, suppose $\text{IZF}_R \vdash \exists x. \phi(x)$. By Lemma 8.13, $\text{IZF}_R^- \vdash \exists x \in T. \phi^T(x)$. By TEP for IZF_R^- , there is a term t such that $\text{IZF}_R^- \vdash \phi^T(t)$. This implies $\text{IZF}_R \vdash \phi^T(t)$. By Lemma 8.12, $t^T = t$, so by the Leibniz axiom in IZF_R we get $\text{IZF}_R \vdash \phi^T(t^T)$. Since $\phi^T(t^T) = \phi(t)^T$, by Lemma 8.12 we get $\text{IZF}_R \vdash \phi(t)$. \square

Corollary 8.15 (Set Existence Property). If $\text{IZF}_R \vdash \exists x. \phi(x)$ and $\phi(x)$ is term-free, then there is a term-free formula $\psi(x)$ such that $\text{IZF}_R \vdash \exists! x. \phi(x) \wedge \psi(x)$.

Proof. Take the closed t from Term Existence Property, so that $\text{IZF}_R \vdash \phi(t)$. By Corollary 3.2 there is a term-free formula $\psi(x)$ defining t , so that $\text{IZF}_R \vdash (\exists! x. \psi(x)) \wedge \psi(t)$. Then $\text{IZF}_R \vdash \exists! x. \phi(x) \wedge \psi(x)$ can be easily derived. \square

A different technique to tackle the problem of Leibniz axiom, used by Friedman in [Fri73], is to define new membership (\in^*) and equality (\sim) relations in an intensional universe from scratch, so that (V, \in^*, \sim) interprets his intuitionistic set theory along with Leibniz axiom. Our T , on the other hand, utilizes existing $\in, =$ relations. We present an alternative normalization proof, where the method to tackle Leibniz axiom is closer to Friedman's ideas, in [Moc06b].

9. RELATED WORK

Several normalization results for impredicative constructive set theories much weaker than IZF_R exist. Bailin [Bai88] proved strong normalization of a constructive set theory without the induction and replacement axioms. Miquel interpreted a theory of similar strength in a Pure Type System [Miq04]. In [Miq03] he also defined a strongly normalizing lambda calculus with types based on $F\omega.2$, capable of interpreting IZF_C without the \in -induction axiom. This result was later extended — Dowek and Miquel [DM06] interpreted a version of constructive Zermelo set theory in a strongly normalizing deduction-modulo system.

Krivine [LK01] defined realizability using lambda calculus for classical set theory conservative over ZF. The types for the calculus were defined. However, it seems that the types correspond more to the truth in the realizability model than to provable statements in the theory. Moreover, the calculus does not even weakly normalize.

The standard metamathematical properties of theories related to IZF_R are well investigated. Myhill [Myh73] showed DP, NEP, SEP and TEP for IZF with Replacement and

non-recursive list of set terms. Friedman and Šćedrov [FS83] showed SEP and TEP for an extension of that theory with countable choice axioms. Recently DP and NEP were shown for IZF_C extended with various choice principles by Rathjen [Rat06]. However, the technique does not seem to be strong enough to provide TEP and SEP.

In [Moc06b], we show normalization of IZF_R extended with ω -many inaccessible sets.

ACKNOWLEDGMENTS

I would like to thank my advisor, Bob Constable, for support and for giving me the idea for λZ and this research, Richard Shore for helpful discussions, David Martin for commenting on my ideas, Daria Walukiewicz-Chrząszcz for the higher-order rewriting counterexample, thanks to which I could prove Theorem 6.10 and anonymous referees for helpful comments.

REFERENCES

- [AR01] Peter Aczel and Michael Rathjen. Notes on constructive set theory. Technical Report 40, Institut Mittag-Leffler (The Royal Swedish Academy of Sciences), 2000/2001.
- [Bai88] Sidney C. Bailin. A normalization theorem for set theory. *J. Symb. Log.*, 53(3):673–695, 1988.
- [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. In *Proc. 3rd Int. Joint Conf. on Automated Reasoning (IJCAR 2006)*, volume 4130 of *Lecture Notes in Computer Science*, pages 162–176. Springer, 2006.
- [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.
- [FS83] Harvey Friedman and Andre Šćedrov. Set existence property for intuitionistic theories with countable choice. *Annals of Pure and Applied Logic*, 25:129–140, 1983.
- [FS85] Harvey Friedman and Andre Šćedrov. The lack of definable witnesses and provably recursive functions in intuitionistic set theories. *Advances in Mathematics*, 57:1–13, 1985.
- [Kun80] Kenneth Kunen. *Set theory: an introduction to independence proofs*. Elsevier, 1980.
- [LK01] Jean Louis Krivine. Typed lambda-calculus in classical Zermelo-Fraenkel set theory. *Archive for Mathematical Logic*, 40(3):189–205, 2001.
- [LP99] Leslie Lamport and Lawrence C. Paulson. Should your specification language be typed? *ACM-TOPLAS: ACM Transactions on Programming Languages and Systems*, 21, 1999.
- [Lub02] Robert S. Lubarsky. IKP and Friends. *J. Symb. Log.*, 67(4):1295–1322, 2002.
- [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 Matthias Baaz and Johann A. Makowsky, editors, *Proceedings of 12th Annual Conference of the EACSL (CSL 2003)*, volume 2803 of *Lecture Notes in Computer Science*, pages 441–454. Springer, 2003.
- [Miq04] Alexandre Miquel. Lambda-Z: Zermelo’s Set Theory as a PTS with 4 Sorts. In Jean-Christophe Filliâtre, Christine Paulin-Mohring, and Benjamin Werner, editors, *TYPES*, volume 3839 of *Lecture Notes in Computer Science*, pages 232–251. Springer, 2004.
- [Moc06a] Wojciech Moczydłowski. Normalization of intuitionistic set theories. In Alfons Geser and Harald Sondergaard, editors, *Extended Abstracts of the 8th International Workshop on Termination, WST’06*, August 2006.
- [Moc06b] Wojciech Moczydłowski. A Normalizing Intuitionistic Set Theory with Inaccessible Sets. Technical Report 2006-2051, Computer Science Department, Cornell University, October 2006. In submission.

- [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.
- [Pie02] Benjamin C. Pierce. *Types and Programming Languages*. MIT Press, 2002.
- [Pow75] William Powell. Extending Gödel’s negative interpretation to ZF. *Journal of Symbolic Logic*, 40:221–229, 1975.
- [Rat05] Michael Rathjen. The disjunction and related properties for constructive Zermelo-Fraenkel set theory. *Journal of Symbolic Logic*, 70:1233–1254, 2005.
- [Rat06] Michael Rathjen. Metamathematical properties of intuitionistic set theories with choice principles. 2006. Manuscript, available from the web page of the author.
- [Š85] Andre Šcedrov. Intuitionistic set theory. In *Harvey Friedman’s Research on the Foundations of Mathematics*, pages 257–284. Elsevier, 1985.
- [SU06] M.H.B. Sørensen and P. Urzyczyn. *Lectures on the Curry-Howard Isomorphism*. Elsevier, 2006.
- [Tay96] Paul Taylor. Intuitionistic sets and ordinals. *Journal of Symbolic Logic*, 61(3):705–744, 1996.