Logical Methods in Computer Science
Vol. 3 (3:6) 2007, pp. 1–31
www.lmcs-online.org

Submitted Oct. 13, 2006
Published Aug. 6, 2007

A NORMALIZING INTUITIONISTIC SET THEORY WITH INACCESSIBLE SETS *

WOJCIECH MOCZYDŁOWSKI

Department of Computer Science, Cornell University, Ithaca, NY, 14853, USA
e-mail address: wojtek@cs.cornell.edu

Abstract. We propose a set theory strong enough to interpret powerful type theories underlying proof assistants such as LEGO and also possibly Coq, which at the same time enables program extraction from its constructive proofs. For this purpose, we axiomatize an impredicative constructive version of Zermelo-Fraenkel set theory IZF with Replacement and ω-many inaccessibles, which we call $\mathrm{IZF}_{R\omega}$. Our axiomatization utilizes set terms, an inductive definition of inaccessible sets and the mutually recursive nature of equality and membership relations. It allows us to define a weakly-normalizing typed lambda calculus corresponding to proofs in $\mathrm{IZF}_{R\omega}$ according to the Curry-Howard isomorphism principle. We use realizability to prove the normalization theorem, which provides a basis for program extraction capability.

1. Introduction

Since the advent of proofs-as-programs paradigm, also called propositions-as-types or Curry-Howard isomorphism, many systems with program extraction capability have been built. Lego [LP92], Agda/Alfa [Coq, Hal], Coq [The04], Nuprl [C+86], Minlog [BBS+98] — to name a few. Some are quite powerful — for example Coq can interpret an intuitionistic version of Zermelo's set theory [Wer97]. With such power at hand, these systems have the potential of becoming very useful tools.

There is, however, one problem they all share, namely their foundational basis. In order to use Coq or Nuprl, one has to master the ways of types, a setting quite different from the set theory, the standard framework for doing mathematics. A newcomer to this world, presented even with Π and Σ types emulating familiar universal and existential quantifiers, is likely to become confused. The fact that the consistency of the systems is usually justified by a normalization theorem in one form or other, does not make the matters easier. Even when set-theoretic semantics is provided, it does not help much, given that the translation of "the statement $\forall x : \mathrm{nat}, \phi(x)$ is provable" is "the set $\Pi_{n \in \mathbb{N}} [\![\phi[x := n]]\!]$ is inhabited", instead

2000 ACM Subject Classification: F.4.1.

Key words and phrases: Intuitionistic set theory, inaccessible sets, Curry-Howard isomorphism, normalization.

* A version of this work is also available as a technical report [Moc06b].

Partly supported by NSF grants DUE-0333526 and 0430161.

DOI:10.2168/LMCS-3 (3:6) 2007

of expected "for all $x \in \mathbb{N}$, $\phi(x)$ holds". The systems which are not based on type theory share the problem of unfamiliar foundations. This is a serious shortcoming preventing the systems from becoming widely used, as the initial barrier to cross is set quite high.

In [Moc06a] we have made the first step to provide a solution to this problem, by presenting a framework enabling extraction of programs from proofs, while using the standard, natural language of set theory. That framework was based on the intuitionistic set theory IZF with Replacement, called IZF_R. Roughly speaking, IZF_R is what remains from Zermelo-Fraenkel set theory ZF after carefully removing the excluded middle, while retaining the axioms of Power Set and unrestricted Separation. The detailed exposition can be found in Section 3. For more information on IZF and bibliography see [Š85, Bee85]. We have defined a lambda calculus λZ corresponding to proofs in an intensional version of IZF_R and using realizability we have shown that λZ weakly normalizes. By employing an inner model of extensional set theory, we have used the normalization result to show that IZF_R enjoys the standard properties of constructive theories — the disjunction, numerical existence, set existence and term existence properties (DP, NEP, SEP and TEP). These properties can be used to extract programs from proofs [CM06]. All of them, apart from SEP, are essential to the extraction process. However, even though IZF_R is quite powerful, it is unclear if it is as strong as type theories underlying the systems of Coq and LEGO, Calculus of Inductive Constructions (CIC) and Extended Calculus of Constructions (ECC), as all known set-theoretical interpretations use ω-many strongly inaccessible cardinals [Wer97, Acz99].

We therefore axiomatize IZF with Replacement and ω-many inaccessible sets, which we call $\mathrm{IZF}_{R\omega}$. Our axiomatization uses an inductive definition of inaccessible sets. $\mathrm{IZF}_{R\omega}$ extended with excluded middle is equivalent to ZF with ω-many strong inaccessible cardinals. By utilizing the mutually recursive nature of equality and membership relation, we avoid the need for the inner model and define a lambda calculus λZ_ω corresponding directly to proofs in $\mathrm{IZF}_{R\omega}$. We prove its normalization using realizability. As in [Moc06a], normalization can be used to show DP, NEP, SEP and TEP. While DP and NEP have been proved for even stronger theories in [FS84], our method is the first to provide the proof of TEP and SEP for intuitionistic set theory with inaccessible sets.

Inaccessible sets perform a similar function in a constructive setting to strongly inaccessible cardinals in the classical world and universes in type theories. They are "large" sets/types, closed under certain operations ensuring that they give rise to models of set/type theories. The closure conditions largely coincide in both worlds and an inaccessible can be used to provide a set-theoretic intepretation of a universe [Wer97, Acz99]. Both CIC and ECC have ω-many universes. By results of Aczel [Acz99], $\mathrm{IZF}_{R\omega}$ is strong enough to interpret ECC. It is reasonable to expect that CIC could be interpreted too, as the inductive types in CIC need to satisfy positivity conditions and sufficiently strong inductive definitions are available in $\mathrm{IZF}_{R\omega}$ due to the presence of the Power Set and unrestricted Separation axioms. Indeed, Werner's set-theoretic interpretation [Wer97] of a large fragment of CIC uses only the existence of inductively-defined sets in the set-theoretic universe to interpret inductively-defined types.

Our normalization result makes it possible to extract programs from proofs, using techniques described in [CM06]. Thus $\mathrm{IZF}_{R\omega}$ has all the proof-theoretic power of LEGO and likely Coq, uses familiar set-theoretic language and enables program extraction from proofs. This makes it an attractive basis for a powerful and easy to use theorem prover.

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. In section 2 we present the intuitionistic first-order logic. We axiomatize IZF with Replacement and ω-many inaccessibles in sections 3 and 4. In section 5 we define the calculus λZ_ω and prove its standard properties. Realizability is defined in section 6 and used to prove normalization in section 7. We describe related work in section 8.

2. Intuitionistic first-order logic

We start with a detailed presentation of the intuitionistic first-order logic (IFOL). We use a natural deduction style of proof rules. The terms will be denoted by letters t, s, u. The logical variables will be denoted by letters a, b, c, d, e, f. The notation $\vec{a}$ denotes a finite sequence, treated as a set when convenient. The i-th element of a sequence is denoted by a_i. We consider α-equivalent formulas equal. 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 $t[a_1, \ldots, a_n := s_1, \ldots, s_n]$ to denote the result of substituting simultaneously $s_1, \ldots, s_n$ for $a_1, \ldots, a_n$. Contexts, denoted by Γ, are sets of formulas. The 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:

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

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

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

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

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

Negation in IFOL is an abbreviation: $\neg\phi \equiv \phi \to \bot$. So is the symbol $\leftrightarrow$: $\phi \leftrightarrow \psi \equiv (\phi \to \psi \land \psi \to \phi)$. 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.

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. $\square$

3. $\mathrm{IZF}^-_{R\omega}$

In this section we introduce our first approximation to IZF_R, called $\mathrm{IZF}^-_{R\omega}$, which is IZF_R from [Moc06a] extended with the axioms postulating the existence of inaccessible sets. We start by presenting the axioms of IZF_R. It is a first-order theory. When extended with excluded middle, it is equivalent to ZF. The signature consists of two binary relational symbols $\in, =$ and function symbols used in the axioms below. The symbols 0 and $S(a)$ are abbreviations for $\emptyset$ and $\bigcup\{a, \{a, a\}\}$. Bounded quantifiers and the quantifier $\exists! a$ (there exists exactly one a) are also abbreviations defined in the standard way.

- (EXT) $\forall a, b.\ a = b \leftrightarrow \forall c.\ c \in a \leftrightarrow c \in b$
- (L_ϕ) $\forall a, b, \vec{f}.\ a = b \wedge \phi(a, \vec{f}) \to \phi(b, \vec{f})$
- (EMPTY) $\forall c.\ c \in \emptyset \leftrightarrow \bot$
- (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_ϕ) $\forall \vec{f} \forall a \forall c.\ c \in S_\phi(a, \vec{f}) \leftrightarrow c \in a \wedge \phi(c, \vec{f})$
- (UNION): $\forall a \forall c.\ c \in \bigcup a \leftrightarrow \exists b \in a.\ c \in b$
- (POWER) $\forall a \forall c.\ c \in P(a) \leftrightarrow \forall b.\ b \in c \to b \in a$
- (REPL_ϕ) $\forall \vec{f}, a \forall c.\ c \in R_\phi(a, \vec{f}) \leftrightarrow (\forall x \in a \exists! y.\ \phi(x, y, \vec{f})) \wedge (\exists x \in a.\ \phi(x, c, \vec{f}))$
- (IND_ϕ) $\forall \vec{f}.(\forall a.(\forall b \in a.\ \phi(b, \vec{f})) \to \phi(a, \vec{f})) \to \forall a.\ \phi(a, \vec{f})$

The axioms (SEP_ϕ), (REPL_ϕ), (IND_ϕ) and (L_ϕ) are axiom schemas — there is one axiom for each formula ϕ. Note that there are terms S_ϕ and R_ϕ for each instance of the Separation and Replacement axioms. Formally, terms and formulas are defined by mutual induction:

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

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 $\forall b.\ b \in c \to b \in a$. We reserve the notation t_A and ϕ_A to denote the term and the corresponding formula for the axiom (A).

The terms $S_\phi(t, \vec{t})$ and $R_\phi(t, \vec{t})$ could be displayed as $\{c \in t \mid \phi(c, \vec{t})\}$ and $\{c \mid (\forall x \in t \exists! y \phi(x, y, \vec{t})) \wedge (\exists x \in t.\ \phi(x, c, \vec{t}))\}$, respectively.

3.1. On the axioms of $\mathbf{IZF}_R$.

3.1.1. *The Leibniz axiom.* The Leibniz axiom (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.

3.1.2. *The Replacement axiom.* A more familiar formulation of Replacement could be: "For all $\vec{F}, A$, if for all $x \in A$ there is exactly one y such that $\phi(x, y, \vec{F})$ holds, then there is a set D such that $\forall x \in A \exists y \in D.\ \phi(x, y, \vec{F})$ and for all $d \in D$ there is $x \in A$ such that $\phi(x, d, \vec{F})$". Let this formulation of Replacement be called ($\mathrm{REPL0}_\phi$), let (R_ϕ) be the term-free statement of our Replacement axiom, that is:

$$(R_\phi) \equiv \forall \vec{f}, a \exists! d.\ \forall c.\ c \in d \leftrightarrow (\forall x \in a \exists! y.\ \phi(x, y, \vec{f})) \wedge (\exists x \in a.\ \phi(x, c, \vec{f}))$$

and let IZ denote IZF_R without the Replacement axiom and corresponding function symbols. To justify our definition of Replacement, we prove the following two lemmas:

Lemma 3.1. *IZ $\vdash$ (R_ϕ) $\to$($\mathit{REPL0}_\phi$).*

Proof. Assume (R_ϕ), take any $\vec{F}, A$ and suppose that for all $x \in A$ there is exactly one y such that $\phi(x, y, \vec{F})$. Let D be the set we get by applying (R_ϕ). Take any $x \in A$, then there is y such that $\phi(x, y, \vec{F})$, so $y \in D$. Moreover, if $d \in D$ then there is $x \in A$ such that $\phi(x, d, \vec{F})$. This shows ($\mathrm{REPL0}_\phi$). □

Lemma 3.2. *IZ* $\vdash$ *(REPL0$_\phi$) $\to$(R_ϕ).*

Proof. Assume ($\mathrm{REPL0}_\phi$), take any $\vec{F}, A$ and consider the set

$$B \equiv \{a \in A \mid \forall x \in A \exists ! y.\ \phi(x, y, \vec{F})\}.$$

Then for all $b \in B$ there is exactly one y such that $\phi(b, y, \vec{F})$. Use ($\mathrm{REPL0}_\phi$) to get a set D. Then D is the set we are looking for. Indeed, if $d \in D$, then there is $b \in B$ such that $\phi(b, d, \vec{F})$ and so by the definition of B, $\forall x \in A \exists ! y.\ \phi(x, y, \vec{F})$ and $b \in A$. On the other hand, take any d and suppose that $\forall x \in A \exists ! y.\ \phi(x, y, \vec{F})$ and there is $x \in A$ such that $\phi(x, d, \vec{F})$. Then $x \in B$, so there is $y' \in D$ such that $\phi(x, y', \vec{F})$. But y' must be equal to d, so $d \in D$. As it is trivial to see that D is unique, the claim follows. □

3.1.3. *The terms of IZF$_R$.* The original presentation of IZF with Replacement presented in [Myh73] is term-free. Let us call it IZF_{R0}. We will now show that IZF_R is a definitional extension of IZF_{R0}.

In IZF_{R0} for each axiom (A) among the Empty Set, Pairing, Infinity, Separation, Replacement, Union and Power Set axioms, we can derive $\forall \vec{a} \exists ! d \forall c.\ c \in d \leftrightarrow \phi_A(c, \vec{a})$, using Lemma 3.2 in case of the Replacement axiom. We therefore definitionally extend IZF_{R0}, by introducing for each such (A) the corresponding new function symbol $t_A(\vec{a})$ along with the defining axiom $\forall \vec{a} \forall c.\ c \in t_A(\vec{a}) \leftrightarrow \phi_A(c, \vec{a})$.

We then need to provide the Separation and Replacement function symbols R_ϕ and S_ϕ, where ϕ may contain the new terms. To fix our attention, consider the Separation axiom. For some function symbol S_ϕ, we need to have:

$$\forall \vec{f}, a \forall c.\ c \in S_\phi(a, \vec{f}) \leftrightarrow c \in a \wedge \phi(c, \vec{f})$$

As all terms present in ϕ were introduced via a definitional extension of IZF_{R0}, there is a term-free formula ϕ' equivalent to ϕ. We therefore have:

$$\forall \vec{f}, a \forall c.\ c \in S_{\phi'}(a, \vec{f}) \leftrightarrow c \in a \wedge \phi'(c, \vec{f})$$

and consequently:

$$\forall \vec{f}, a \forall c.\ c \in S_{\phi'}(a, \vec{f}) \leftrightarrow c \in a \wedge \phi(c, \vec{f})$$

We define S_ϕ to be $S_{\phi'}$. Similarly, we can define R_ϕ to be $R_{\phi'}$. After iterating this process ω-many times, we obtain all instances of terms and axioms (A) present in IZF_R.

It remains to derive the Leibniz and $\in$-Induction axioms for formulas with terms. For the Leibniz axiom, take any $A, B, \vec{F}$ and suppose $A = B$ and $\phi(A, \vec{F})$. Then there is a term-free formula ϕ' equivalent to ϕ, so also $\phi'(A, \vec{F})$. By the Leibniz axiom in IZF_{R0}, $\phi'(B, \vec{F})$, so also $\phi(B, \vec{F})$.

For the $\in$-Induction axiom, take any $\vec{F}$ and suppose:

$$\forall a.\ (\forall b \in a.\ \phi(b, \vec{F})) \to \phi(a, \vec{F})$$

Taking ϕ' to be the term-free formula equivalent to ϕ, we get:

$$\forall a.\ (\forall b \in a.\ \phi'(b, \vec{F})) \to \phi'(a, \vec{F})$$

By $\in$-Induction in IZF_{R0}, we get $\forall a.\ \phi'(a, \vec{F})$, thus also $\forall a.\ \phi(a, \vec{F})$.

3.2. **Inaccessible sets.** To extend IZF_R with inaccessible sets, we add a family of axioms (INAC_i) for $i > 0$. We call the resulting theory $\mathrm{IZF}^-_{R\omega}$. The axiom (INAC_i) asserts the existence of the i-th inaccessible set, denoted by a new constant symbol V_i, and is defined as follows:

$$(\mathrm{INAC}_i)\ \forall c.\ c \in V_i \leftrightarrow \phi^i_1(c, V_i) \wedge \forall d.\ \phi^i_2(d) \to c \in d$$

Following the conventions set up for IZF_R, $\phi_{INAC_i}(c)$ is $\phi^i_1(c, V_i) \wedge \forall d.\ \phi^i_2(d) \to c \in d$. The formula $\phi^i_1(c, d)$ intuitively sets up conditions for c being a member of V_i, while $\phi^i_2(d)$ says what it means for d to be inaccessible. To streamline the definition, we set V_0 to abbreviate ω.

Definition 3.3. The formula $\phi^i_1(c, V_i)$ for $i > 0$ is a disjunction of the following five clauses:
(1) $c = V_{i-1}$
(2) there is $a \in V_i$ such that $c \in a$.
(3) there is $a \in V_i$ such that c is a union of a.
(4) there is $a \in V_i$ such that c is a power set of a.
(5) there is $a \in V_i$ such that c is a function from a to V_i.

Definition 3.4. The formula $\phi^i_2(d)$ for $i > 0$ is a conjunction of the following five clauses:
(1) $V_{i-1} \in d$.
(2) $\forall e, f.\ e \in d \wedge f \in e \to f \in d$.
(3) $\forall e \in d.\ \bigcup e \in d$.
(4) $\forall e \in d.\ P(e) \in d$.
(5) $\forall e \in d.\ \forall f \in e \to d.\ f \in d$, where $e \to d$ denotes the set of all functions from e to d.

Briefly, the i-th inaccessible set is the smallest transitive set containing V_{i-1} and closed under unions, power sets and taking functions from its elements into itself. It is easy to see that $\mathrm{IZF}^-_{R\omega}$+ EM is equivalent to ZF with ω-many strongly inaccessible cardinals. For a theory T, let $M(T)$ denote a sentence "T has a model". To show that the set V_i defined by (INAC_i) behaves as an inaccessible set in $\mathrm{IZF}^-_{R\omega}$ we prove:

Theorem 3.5 ($\mathrm{IZF}^-_{R\omega}$)**.** *For all $i > 0$, $V_i \models \mathrm{IZF}_R$+ $M(\mathrm{IZF}_R)$ + $M(\mathrm{IZF}_R$+ $M(\mathrm{IZF}_R))$ + ... (i times).*

Proof. By Clause 2 in the Definition 3.3, V_1 is transitive, so the equality and membership relations are absolute. Clause 1 gives us $\omega \in V_1$ and since its definition is Δ_0, $V_1 \models$(INF). Clauses 3 and 4 provide the (UNION) and (POWER) axioms. Transitivity then gives (SEP) and (PAIR), while Clause 5, thanks to Lemma 3.2, gives (REPL_ϕ). The existence of the empty set follows by (INF) and (SEP). For the Induction axiom, we need to show:

$$\forall \vec{f} \in V_i.\ (\forall a \in V_i.\ (\forall b \in V_i.\ b \in a \to \phi^{V_i}(b, \vec{f})) \to \phi^{V_i}(a, \vec{f})) \to \forall a \in V_i. \phi^{V_i}(a, \vec{f})$$

Take any $\vec{F} \in V_i$. It suffices to show that:

$$(\forall a.\ a \in V_i \to (\forall b.\ b \in V_i \to b \in a \to \phi^{V_i}(b, \vec{F})) \to \phi^{V_i}(a, \vec{F})) \to \forall a.\ a \in V_i \to \phi^{V_i}(a, \vec{F})$$

This is equivalent to:

$$(\forall a.\ (\forall b.\ b \in a \to b \in V_i \to \phi^{V_i}(b, \vec{F})) \to a \in V_i \to \phi^{V_i}(a, \vec{F})) \to \forall a.\ a \in V_i \to \phi^{V_i}(a, \vec{F})$$

But this is the instance of the induction axiom for the formula $a \in V_i \to \phi^{V_i}(a, \vec{f})$.

Thus $V_1 \models$IZF$_R$. Since $V_1 \in V_2$, $V_2 \models$ IZF$_R$+ M(IZF$_R$). Since $V_2 \in V_3$, $V_3 \models$IZF$_R$+ M(IZF$_R$+ M(IZF$_R$)). Proceeding in this manner by induction we get the claim. □

4. IZF$_{R\omega}$

We now present our final axiomatization of IZF with Replacement and inaccessible sets, which we call IZF$_{R\omega}$. The advantage of this axiomatization over the previous one is that equality and membership are defined in terms of each other, instead of being taken for granted and axiomatized with Extensionality and Leibniz axioms. This trick, which amounts to interpreting an extensional set theory in an intensional one, has already been used by Friedman in [Fri73]. As we shall see later, this makes it possible to prove a normalization theorem directly for the theory, thus avoiding the need for the detour via the class of transitively-L-stable sets used in [Moc06a].

The signature of IZF$_{R\omega}$ consists of three relational symbols: $\in_I, \in, =$ and terms of IZF$^-_{R\omega}$. The axioms of IZF$_{R\omega}$ are as follows:

- (IN) $\forall a, b.\ a \in b \leftrightarrow \exists c.\ c \in_I b \land a = c$
- (EQ) $\forall a, b.\ a = b \leftrightarrow \forall d.\ (d \in_I a \to d \in b) \land (d \in_I b \to d \in a)$
- (IND$_\phi$) $\forall \vec{f}.(\forall a.(\forall b \in_I a.\phi(b, \vec{f})) \to \phi(a, \vec{f})) \to \forall a.\phi(a, \vec{f})$
- (A) $\forall \vec{a}.\ \forall c.\ c \in_I t_A(\vec{a}) \leftrightarrow \phi_A(c, \vec{a})$, for (A) being one of (EMPTY), (PAIR), (INF), (SEP$_\phi$), (UNION), (POWER), (REPL$_\phi$), (INAC$_i$). For example, the Power Set axiom has a form: $\forall a \forall c.\ c \in_I P(a) \leftrightarrow \forall b.\ b \in c \to b \in a$.

The extra relational symbol $\in_I$ intuitively denotes the intensional membership relation. Note that neither the Leibniz axiom (L$_\phi$) nor the extensionality axiom are present. We will show, however, that they can be derived and that this axiomatization is as good as IZF$^-_{R\omega}$. From now on in this section, we work in IZF$_{R\omega}$. The following sequence of lemmas establishes that equality and membership behave in the correct way. Statements similar in spirit are also proved in the context of Boolean-valued models. Our treatment slightly simplifies the standard presentation by avoiding the need for mutual induction.

Lemma 4.1. *For all a, $a = a$.*

Proof. By $\in$-induction on a. Take any $b \in_I a$. By the inductive hypothesis, $b = b$, so also $b \in a$. □

Corollary 4.2. *If $a \in_I b$, then $a \in b$.*

Lemma 4.3. *For all a, b, if $a = b$, then $b = a$.*

Proof. Straighforward. □

Lemma 4.4. *For all b, a, c, if $a = b$ and $b = c$, then $a = c$.*

Proof. By $\in$-induction on b. First take any $d \in_I a$. By $a = b$, $d \in b$, so there is $e \in_I b$ such that $d = e$. By $b = c$, $e \in c$, so there is $f \in_I c$ such that $e = f$. By the inductive hypothesis for e, $d = f$, so $d \in c$.

The other direction is symmetric and proceeds from c to a. Take any $d \in_I c$. By $b = c$, $d \in b$, so there is $e \in_I b$ such that $d = e$. By $a = b$, $e \in a$, so there is $f \in_I a$ such that $e = f$. The inductive hypothesis gives the claim. $\square$

Lemma 4.5. *For all a, b, c, if $a \in c$ and $a = b$, then $b \in c$.*

Proof. Since $a \in c$, there is $d \in_I c$ such that $a = d$. By previous lemmas we also have $b = d$, so $b \in c$. $\square$

Lemma 4.6. *For all a, b, d, if $a = b$ and $d \in a$, then $d \in b$.*

Proof. Suppose $d \in a$, then there is e such that $e \in_I a$ and $d = e$. By $a = b$, $e \in b$. By Lemma 4.5, $d \in b$. $\square$

Lemma 4.7 (Extensionality)**.** *If for all d, $d \in a$ iff $d \in b$, then $a = b$.*

Proof. Take any $d \in_I a$. By Corollary 4.2 $d \in a$, so by Lemma 4.6 also $d \in b$. The other direction is symmetric. $\square$

We would like to mention that all the lemmas above have been verified by the computer, by a toy prover we wrote to experiment with $\mathrm{IZF}_{R\omega}$.

Lemma 4.8 (The Leibniz axiom)**.** *For any term $t(a, \vec{f})$ and formula $\phi(a, \vec{f})$ not containing $\in_I$, if $a = b$, then $t(a, \vec{f}) = t(b, \vec{f})$ and $\phi(a, \vec{f}) \leftrightarrow \phi(b, \vec{f})$.*

Proof. Straightforward mutual induction on generation of t and ϕ. We show some representative cases. Case t or ϕ of:

- $\bigcup t_1(a)$. If $c \in_I \bigcup t_1(a)$, then for some d, $c \in d \in t_1(a)$. By the inductive hypothesis $t_!(a) = t_1(b)$, so by Lemma 4.6 $d \in t_1(b)$, so $c \in_I \bigcup t_1(b)$ and by Corollary 4.2 also $c \in \bigcup t_1(b)$. The other direction is symmetric and by the (EQ) axiom we get $t(a) = t(b)$.
- $S_\phi(t_1(a), \vec{u}(a))$. If $c \in_I S_\phi(t_1(a), \vec{u}(a))$, then $c \in t_1(a)$ and $\phi(c, \vec{u}(a))$. By the inductive hypothesis, $t_1(a) = t_1(b)$, $\vec{u}(a) = \vec{u}(b)$, and thus $\phi(c, \vec{u}(b))$ and $c \in t_1(b)$, so $c \in_I S_\phi(t_1(b), \vec{u}(b))$ and also $c \in S_\phi(t_1(b), \vec{u}(b))$.
- $t(a) \in s(a)$. By the inductive hypothesis, $t(a) = t(b)$ and $s(a) = s(b)$. Thus by Lemma 4.6 $t(a) \in s(b)$ and by Lemma 4.5 $t(b) \in s(b)$.
- $\forall c.\ \phi(c, a, \vec{f})$. Take any c, we have $\phi(c, a, \vec{f})$, so by inductive hypothesis $\phi(c, b, \vec{f})$, so $\forall c.\ \phi(c, b, \vec{f})$. $\square$

Lemma 4.9. *For any term $t_A(\vec{a})$, $c \in t_A(\vec{a})$ iff $\phi_A(c, \vec{a})$.*

Proof. The right-to-left direction follows immediately by Corollary 4.2. For the left-to-right direction, suppose $c \in t_A(\vec{a})$. Then there is d such that $d \in_I t_A(\vec{a})$ and $c = d$. Therefore $\phi_A(d, \vec{a})$ holds and by the Leibniz axiom we also get $\phi_A(c, \vec{a})$. $\square$

Lemma 4.10. *For any axiom A of* $IZF^-_{R\omega}$, $IZF_{R\omega} \vdash A$.

Proof. Lemmas 4.7, 4.8 and 4.9 show the claim for all the axioms apart from (IND_ϕ). So suppose $\forall a.\ (\forall b \in a.\ \phi(b, \vec{f})) \to \phi(a, \vec{f})$. We need to show $\forall a.\ \phi(a, \vec{f})$. We proceed by $\in_I$-induction on a. It suffices to show $\forall c.\ (\forall d \in_I c.\ \phi(d, \vec{f})) \to \phi(c, \vec{f})$. Take any c and suppose $\forall d \in_I c.\ \phi(d, \vec{f})$. We need to show $\phi(c, \vec{f})$. Take a to be c in the assumption, so it suffices to show that $\forall b \in c.\ \phi(b, \vec{f})$. Take any $b \in c$. Then there is $e \in_I c$ such that $e = b$. By the inductive hypothesis $\phi(e, \vec{f})$ holds and hence by the Leibniz axiom we get $\phi(b, \vec{f})$, which shows the claim. $\square$

Corollary 4.11. *If* $IZF^-_{R\omega} \vdash \phi$, *then* $IZF_{R\omega} \vdash \phi$.

Lemma 4.12. *If* $IZF_{R\omega} \vdash \phi$ *and* ϕ *does not contain* $\in_I$, *then* $IZF^-_{R\omega} \vdash \phi$.

Proof. Working in $\mathrm{IZF}^-_{R\omega}$ simply interpret $\in_I$ as $\in$ to see that all axioms of $\mathrm{IZF}_{R\omega}$ are valid and that if $\mathrm{IZF}_{R\omega} \vdash \phi$, then $\mathrm{IZF}^-_{R\omega} \vdash \phi[\in_I := \in]$. $\square$

Therefore $\mathrm{IZF}_{R\omega}$ is a legitimate axiomatization of IZF with Replacement and inaccessible sets. From now on the names of the axioms refer to the axiomatization of $\mathrm{IZF}_{R\omega}$.

5. The λZ_ω calculus

We now introduce a lambda calculus λZ_ω for $\mathrm{IZF}_{R\omega}$, based on the Curry-Howard isomorphism principle. The part of λZ_ω corresponding to the first-order logic is essentially λP_1 from [SU06]. The rest of the calculus, apart from clauses corresponding to (IN), (EQ) and (INAC_i) axioms, is identical to λZ from [Moc06a].

5.1. **The terms of λZ_ω.** The lambda terms in λZ_ω will be denoted by letters M, N, O, P. There are two kinds of lambda abstraction in λZ_ω, one corresponding to the proofs of implication, the other to the proofs of universal quantification. We use separate sets of variables for these abstractions and call them propositional and first-order variables, respectively. Letters x, y, z will be used for the propositional variables and letters a, b, c for the first-order variables. Letters t, s, u are reserved for $\mathrm{IZF}_{R\omega}$ terms. The types in the system are $\mathrm{IZF}_{R\omega}$ formulas. The terms are generated by the following abstract grammar:

$$M ::= x \mid M\ N \mid \lambda a.\ M \mid \lambda x : \phi.\ M \mid \mathrm{inl}(M) \mid \mathrm{inr}(M) \mid \mathrm{fst}(M) \mid \mathrm{snd}(M)$$
$$[t, M] \mid M\ t \mid \langle M, N \rangle \mid \mathrm{case}(M, x : \phi.\ N, x : \psi.\ O) \mid \mathrm{magic}(M) \mid \mathrm{let}\ [a, x : \phi] := M\ \mathrm{in}\ N$$
$$\mathrm{ind}_{\phi(a,\vec{b})}(M, \vec{t}) \mid \mathrm{inac}_i\mathrm{Prop}(t, M) \mid \mathrm{inac}_i\mathrm{Rep}(t, M)$$
$$\mathrm{inProp}(t, u, M) \mid \mathrm{inRep}(t, u, M) \mid \mathrm{eqProp}(t, u, M) \mid \mathrm{eqRep}(t, u, M)$$
$$\mathrm{pairProp}(t, u_1, u_2, M) \mid \mathrm{pairRep}(t, u_1, u_2, M) \mid \mathrm{unionProp}(t, u, M) \mid \mathrm{unionRep}(t, u, M)$$
$$\mathrm{sep}_{\phi(a,\vec{f})}\mathrm{Prop}(t, u, \vec{u}, M) \mid \mathrm{sep}_{\phi(a,\vec{f})}\mathrm{Rep}(t, u, \vec{u}, M) \mid \mathrm{powerProp}(t, u, M) \mid \mathrm{powerRep}(t, u, M)$$
$$\mathrm{infProp}(t, M) \mid \mathrm{infRep}(t, M) \mid \mathrm{repl}_{\phi(a,b,\vec{f})}\mathrm{Prop}(t, u, \vec{u}, M) \mid \mathrm{repl}_{\phi(a,b,\vec{f})}\mathrm{Rep}(t, u, \vec{u}, M)$$

The ind terms correspond to the (IND) axiom, Prop and Rep terms correspond to the respective axioms of $\mathrm{IZF}^-_{R\omega}$ and the rest of the terms corresponds to the rules of IFOL. The exact nature of the correspondence will become clear in Section 5.3. To avoid listing all of them repeatedly, we adopt a convention of using axRep and axProp terms to tacitly mean all Rep and Prop terms, for ax being one of in, eq, pair, union, sep, power, inf, repl and $\mathrm{inac_i}$, unless we list some of them separately. With this convention in mind, we can summarize the definition of the Prop and Rep terms as:

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

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 all free variables of a term M by $FV(M)$ and 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.

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

$$(\lambda x : \phi.\ M)N \to M[x := N] \qquad (\lambda a.\ M)t \to M[a := t]$$
$$\mathrm{fst}(\langle M, N\rangle) \to M \qquad \mathrm{snd}(\langle M, N\rangle) \to N$$
$$\mathrm{case}(\mathrm{inl}(M), x : \phi.\ N, x : \psi.\ O) \to N[x := M] \qquad \mathrm{case}(\mathrm{inr}(M), x : \phi.\ N, x : \psi.\ O) \to O[x := M]$$
$$\mathrm{let}\ [a, x : \phi] := [t, M]\ \mathrm{in}\ N \to N[a := t][x := M]$$
$$\mathrm{axProp}(t, \vec{u}, \mathrm{axRep}(t, \vec{u}, M)) \to M$$
$$\mathrm{ind}_\phi(M, \overline{t}) \to \lambda c.\ M\ c\ (\lambda b.\lambda x : b \in_I c.\ \mathrm{ind}_\phi(M, \overline{t})\ b)$$

In the reduction rules for ind terms, the variable x is new.

The evaluation contexts describe call-by-need (lazy) evaluation order:

$$[\circ] ::= \mathrm{fst}([\circ]) \mid \mathrm{snd}([\circ]) \mid \mathrm{case}([\circ], x.N, x.O)$$
$$\mathrm{axProp}(t, \vec{u}, [\circ]) \mid \mathrm{let}\ [a, x : \phi] := [\circ]\ \mathrm{in}\ N \mid [\circ]\ M \mid \mathrm{magic}([\circ])$$

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

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

Definition 5.1. We write $M \downarrow$ if the reduction sequence starting from M terminates. In this situation we also say that M *normalizes*. We write $M \downarrow v$ if we want to state that v is the term at which this reduction sequence terminates. We write $M \to^* M'$ if M reduces to M' in some number of steps.

5.3. **The types of λZ_ω.** The type system for λZ_ω is constructed according to the principle of the Curry-Howard isomorphism for $\mathrm{IZF}_{R\omega}$. Types are $\mathrm{IZF}_{R\omega}$ formulas, and terms are λZ_ω terms. Contexts Γ are finite sets of pairs (x_i, ϕ_i). The first set of rules corresponds to first-order logic.

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

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

$$\frac{\Gamma \vdash M : \phi}{\Gamma \vdash \mathrm{inl}(M) : \phi \vee \psi} \qquad \frac{\Gamma \vdash M : \psi}{\Gamma \vdash \mathrm{inr}(M) : \phi \vee \psi}$$

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

$$\frac{\Gamma \vdash M : \phi}{\Gamma \vdash \lambda a.\ M : \forall a.\ \phi}\ a \notin FV_F(\Gamma) \qquad \frac{\Gamma \vdash M : \forall a.\ \phi}{\Gamma \vdash M\ t : \phi[a := t]} \qquad \frac{\Gamma \vdash M : \phi[a := t]}{\Gamma \vdash [t, M] : \exists a.\ \phi}$$

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

The rest of the rules correspond to $\mathrm{IZF}_{R\omega}$ axioms:

$$\frac{\Gamma \vdash M : \forall d.\ (d \in_I t \to d \in u) \wedge (d \in_I u \to d \in t)}{\Gamma \vdash \mathrm{eqRep}(t, u, M) : t = u}$$

$$\frac{\Gamma \vdash M : t = u}{\Gamma \vdash \mathrm{eqProp}(t, u, M) : \forall d.\ (d \in_I t \to d \in u) \wedge (d \in_I u \to d \in t)}$$

$$\frac{\Gamma \vdash M : \exists c.\ c \in_I u \wedge t = c}{\Gamma \vdash \mathrm{inRep}(t, u, M) : t \in u} \qquad \frac{\Gamma \vdash t \in u}{\Gamma \vdash \mathrm{inProp}(t, u, M) : \exists c.\ c \in_I u \wedge t = c}$$

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

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

5.4. **The properties of λZ_ω.** We now proceed with a standard sequence of lemmas for λZ_ω.

Lemma 5.2 (Canonical Forms)**.** *Suppose M is a value and $\vdash M : \vartheta$. Then:*

- $\vartheta = t \in_I t_A(\vec{u})$ *iff* $M = \mathrm{axRep}(t, \vec{u}, N)$ *and* $\vdash N : \phi_A(t, \vec{u})$.
- $\vartheta = \phi \vee \psi$ *iff* ($M = \mathrm{inl}(N)$ *and* $\vdash N : \phi$) *or* ($M = \mathrm{inr}(N)$ *and* $\vdash N : \psi$).
- $\vartheta = \phi \wedge \psi$ *iff* $M = \langle N, O\rangle$, $\vdash N : \phi$ *and* $\vdash O : \psi$.
- $\vartheta = \phi \to \psi$ *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* $\vdash N : \phi[a := t]$.
- $\vartheta = \bot$ *never happens.*

Proof. Immediate from the typing rules and the definition of values. □

Lemma 5.3 (Weakening)**.** *If* $\Gamma \vdash M : \phi$ *and* $FV(\psi) \cup \{x\}$ *are fresh to the proof tree* $\Gamma \vdash M : \phi$*, then* $\Gamma, x : \psi \vdash M : \phi$*.*

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

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_ω corresponding to $\mathrm{IZF}_{R\omega}$ axioms do not interact with substitutions in a significant way, the proofs are routine.

Lemma 5.4. *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.

- $\psi = \psi_1 \to \psi_2$, $M = \lambda y : \psi_1.\ O$. 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:
$$\frac{\Gamma, x : \phi, y : \psi_1 \vdash O : \psi_2}{\Gamma, x : \phi \vdash \lambda y : \psi_1.\ O : \psi_1 \to \psi_2}$$
By the inductive hypothesis, $\Gamma, y : \psi_1 \vdash O[x := N] : \psi_2$, so $\Gamma \vdash \lambda y : \psi_1.\ O[x := N] : \psi_1 \to \psi_2$. By the choice of y, $\Gamma \vdash (\lambda y : \psi_1.\ O)[x := N] : \psi_1 \to \psi_2$.
- $\psi = \psi_2, M = \mathrm{let}\ [a, y : \psi_1] := M_1\ \mathrm{in}\ M_2$. The proof tree ends with:
$$\frac{\Gamma, x : \phi \vdash M_1 : \exists a.\ \psi_1 \quad \Gamma, x : \phi, y : \psi_1 \vdash M_2 : \psi_2}{\Gamma, x : \phi \vdash \mathrm{let}\ [a, y : \psi_1] := M_1\ \mathrm{in}\ M_2 : \psi_2}$$
Choose a and y to be fresh. By the inductive hypothesis, $\Gamma \vdash M_1[x := N] : \exists a.\ \psi_1$ and $\Gamma, y : \psi_1 \vdash M_2[x := N] : \psi_2$. Thus $\Gamma \vdash \mathrm{let}\ [a, y : \psi_1] := M_1[x := N]\ \mathrm{in}\ M_2[x := N] : \psi_2$. By a and y fresh, $\Gamma \vdash (\mathrm{let}\ [a, y : \psi_1] := M_1\ \mathrm{in}\ M_2)[x := N] : \psi_2$ which is what we want. ◻

Lemma 5.5. *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 will show the proof just for two of them which do.

- $\phi = \forall b.\ \phi_1$, $M = \lambda b.\ M_1$. The proof tree ends with:
$$\frac{\Gamma \vdash M_1 : \phi_1}{\Gamma \vdash \lambda b.\ M_1 : \forall b.\ \phi_1}\ b \notin FV_F(\Gamma)$$
Without loss of generality we can assume that $b \notin FV(t) \cup \{a\}$. By the inductive 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, $\Gamma[a := t] \vdash (\lambda b.\ M_1)[a := t] \vdash (\forall b.\ \phi_1)[a := t]$.
- $\phi = \phi_1[b := u]$, $M = M_1\ u$ 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 inductive 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 $\Gamma[a := t] \vdash (M_1\ u)[a := t] : \phi_1[b := u][a := t]$. ◻

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

Lemma 5.6 (Subject Reduction, Preservation)**.** *If* $\Gamma \vdash M : \phi$ *and* $M \to N$*, then* $\Gamma \vdash N : \phi$*.*

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

- $(\lambda x : \phi_1.\ M_1)\ M_2 \to M_1[x := M_2]$. The proof tree $\Gamma \vdash M : \phi$ must end with:
$$\dfrac{\dfrac{\Gamma, x : \phi_1 \vdash M_1 : \phi}{\Gamma \vdash \lambda x : \phi_1.\ M_1 : \phi_1 \to \phi} \quad \Gamma \vdash M_2 : \phi_1}{\Gamma \vdash (\lambda x : \phi_1.\ M_1)\ M_2 : \phi}$$
By Lemma 5.4, $\Gamma \vdash M_1[x := M_2] : \phi_1$.
- let $[a, x : \phi_1] := [t, M_1]$ in $M_2 \to M_2[a := t][x := M_1]$. The proof tree $\Gamma \vdash M : \phi$ must end with:
$$\dfrac{\dfrac{\Gamma \vdash M_1 : \phi_1[a := t]}{\Gamma \vdash [t, M_1] : \exists a.\ \phi_1} \quad \Gamma, x : \phi_1 \vdash M_2 : \phi}{\Gamma \vdash \text{let } [a, x : \phi_1] := [t, M_1] \text{ in } M_2 : \phi}$$
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 5.5 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 5.4, we get $\Gamma \vdash M_2[a := t][x := M_1] : \phi$.
- $\text{axProp}(t, \vec{u}, \text{axRep}(t, \vec{u}, M_1)) \to M_1$. The proof tree must end with:
$$\dfrac{\dfrac{\Gamma \vdash M_1 : \phi_A(t, \vec{u})}{\Gamma \vdash \text{axRep}(t, \vec{u}, M_1)) : t \in_I t_A(\vec{u})}}{\Gamma \vdash \text{axProp}(t, \vec{u}, \text{axRep}(t, \vec{u}, M_1)) : \phi_A(t, \vec{u})}$$
The claim follows immediately.
- $\text{ind}_{\psi(a,\vec{f})}(M_1, \vec{t}) \to \lambda c.\ M_1\ c\ (\lambda b.\lambda x : b \in_I c.\ \text{ind}_{\psi(a,\vec{b})}(M_1, \vec{t})\ b)$. The proof tree must end with:
$$\dfrac{\Gamma \vdash M_1 : \forall c.\ (\forall b.\ b \in_I c \to \psi(b, \vec{t})) \to \psi(c, \vec{t})}{\Gamma \vdash \text{ind}_{\psi(a,\vec{f})}(M_1, \vec{t}) : \forall a.\ \psi(a, \vec{t})}$$
We choose b, c, x to be fresh. By applying α-conversion we can also obtain a proof tree of $\Gamma \vdash M_1 : \forall e.\ (\forall d.\ d \in_I e \to \psi(d, \vec{t})) \to \psi(e, \vec{t})$, where $\{d, e\} \cap \{b, c\} = \emptyset$. Then by Weakening we get $\Gamma, x : b \in_I c \vdash M_1 : \forall e.\ (\forall d.\ d \in_I e \to \psi(d, \vec{t})) \to \psi(e, \vec{t})$, so also $\Gamma, x : b \in_I c \vdash \text{ind}_{\psi(a,\vec{b})}(M_1, \vec{t}) : \forall a.\ \psi(a, \vec{t})$. Let the proof tree T be defined as:
$$\dfrac{\dfrac{\dfrac{\Gamma, x : b \in_I c \vdash \text{ind}_{\psi(a,\vec{b})}(M_1, \vec{t}) : \forall a.\ \psi(a, \vec{t})}{\Gamma, x : b \in_I c \vdash \text{ind}_{\psi(a,\vec{b})}(M_1, \vec{t})\ b : \psi(b, \vec{t})}}{\Gamma \vdash \lambda x : b \in_I c.\ \text{ind}_{\psi(a,\vec{b})}(M_1, \vec{t})\ b : b \in_I c \to \psi(b, \vec{t})}}{\Gamma \vdash \lambda b.\lambda x : b \in_I c.\ \text{ind}_{\psi(a,\vec{b})}(M_1, \vec{t})\ b : \forall b.\ b \in_I c \to \psi(b, \vec{t})}$$
Then the following proof tree shows the claim:
$$\dfrac{\dfrac{\dfrac{\Gamma \vdash M_1 : \forall c.\ (\forall b.\ b \in_I c \to \psi(b, \vec{t})) \to \psi(c, \vec{t})}{\Gamma \vdash M_1\ c : (\forall b.\ b \in_I c \to \psi(b, \vec{t})) \to \psi(c, \vec{t})} \quad T}{\Gamma \vdash M_1\ c\ (\lambda b.\lambda x : b \in_I c.\ \text{ind}_{\psi(a,\vec{b})}(M_1, \vec{t})\ b) : \psi(c, \vec{t})}}{\Gamma \vdash \lambda c.\ M_1\ c\ (\lambda b.\lambda x : b \in_I c.\ \text{ind}_{\psi(a,\vec{b})}(M_1, \vec{t})\ b) : \forall c.\ \psi(c, \vec{t})}$$

□

Lemma 5.7 (Progress). *If* $\vdash M : \phi$*, then either* M *is a value or there is* N *such that* $M \to N$*.*

Proof. Straightforward induction on the length of M. The proof proceeds by case analysis of M. We show several cases:

- It is easy to see that the case $M = x$ cannot happen.
- If $M = \lambda x : \phi.\ N$, then M is a value.
- If $M = N\ O$, then for some ψ, the proof must end with:

$$\frac{\vdash N : \psi \to \phi \quad \vdash O : \psi}{\vdash N\ O : \phi}$$

  By the inductive hypothesis, either N is a value or there is N' such that $N \to N'$. In the former case, by Canonical Forms for some P we have $N = \lambda x : \psi.\ P$, so $N\ O \to P[x := O]$. In the latter case, $N\ O \to N'\ O$.
- If $M = \mathrm{axRep}(t, \vec{u}, M)$, then M is a value.
- If $M = \mathrm{axProp}(t, \vec{u}, O)$, then we have the following proof tree:

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

  By the inductive hypothesis, either O is a value or there is O_1 such that $O \to O_1$. In the former case, by Canonical Forms, $O = \mathrm{axRep}(t, \vec{u}, P)$ and $M \to P$. In the latter, by the evaluation rules $\mathrm{axProp}(t, \vec{u}, O) \to \mathrm{axProp}(t, \vec{u}, O_1)$.
- The cases corresponding to the equality and membership axioms work in the same way.
- The ind terms always reduce. □

Corollary 5.8. *If* $\vdash M : \phi$ *and* $M \downarrow v$*, then* $\vdash v : \phi$ *and* v *is a value.*

Corollary 5.9. *If* $\vdash M : \bot$*, then* M *does not normalize.*

Proof. If M normalized, then by Corollary 5.8 we would have a value of type $\bot$, which by Canonical Forms is impossible. □

Finally, we state the formal correspondence between λZ_ω and $\mathrm{IZF}_{R\omega}$:

Lemma 5.10 (Curry-Howard isomorphism). *If* $\Gamma \vdash O : \phi$ *then* $IZF_{R\omega} + rg(\Gamma) \vdash \phi$*, where* $rg(\Gamma) = \{\phi \mid (x, \phi) \in \Gamma\}$*. If* $IZF_{R\omega} + \Gamma \vdash \phi$*, then there exists a term* M *such that* $\vec{\Gamma} \vdash M : \phi$*, where* $\vec{\Gamma} = \{(x_\phi, \phi) \mid \phi \in \Gamma\}$*.*

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 $\mathrm{IZF}_{R\omega}$ axioms:

- Let ϕ be one of the $\mathrm{IZF}_{R\omega}$ axioms apart from $\in$-Induction. Then $\phi = \forall \vec{a}.\ \forall c.\ c \in_I t_A(\vec{a}) \leftrightarrow \phi_A(c, \vec{a})$ for the axiom (A) (incorporating axioms (IN) and (EQ) in this case in the obvious way). Recall that $\phi_1 \leftrightarrow \phi_2$ is an abbreviation for $(\phi_1 \to \phi_2) \land (\phi_2 \to \phi_1)$. Let T be the following proof tree:

$$\frac{\dfrac{\Gamma, x : \phi_A(c, \vec{a}) \vdash x : \phi_A(c, \vec{a})}{\Gamma, x : \phi_A(c, \vec{a}) \vdash \mathrm{axRep}(c, \vec{a}, x) : c \in_I t_A(\vec{a})}}{\Gamma \vdash \lambda x : \phi_A(c, \vec{a}).\ \mathrm{axRep}(c, \vec{a}, x) : \phi_A(c, \vec{a}) \to c \in_I t_A(\vec{a})}$$

Let $M_1 = \lambda x : c \in_I t_A(\vec{a}).\ \mathrm{axProp}(c, \vec{a}, x)$ and let $M_2 = \lambda x : \phi_A(c, \vec{a}).\ \mathrm{axRep}(c, \vec{a}, x)$. Then the following proof tree shows the claim:

$$\dfrac{\dfrac{\dfrac{\dfrac{\Gamma, x : c \in_I t_A(\vec{a}) \vdash x : c \in_I t_A(\vec{a})}{\Gamma, x : c \in_I t_A(\vec{a}) \vdash \mathrm{axProp}(c, \vec{a}, x) : \phi_A(c, \vec{a})}}{\Gamma \vdash M_1 : c \in_I t_A(\vec{a}) \to \phi_A(c, \vec{a})} \quad T}{\Gamma \vdash \langle M_1, M_2 \rangle : c \in_I t_A(\vec{a}) \leftrightarrow \phi_A(c, \vec{a})}}{\Gamma \vdash \lambda \vec{a} \lambda c.\ \langle M_1, M_2 \rangle : \forall \vec{a}.\ \forall c.\ c \in_I t_A(\vec{a}) \leftrightarrow \phi_A(c, \vec{a})}$$

- Let ϕ be the $\in$-induction axiom. Let
$$M = \lambda \vec{f} \lambda x : (\forall a.(\forall b.\ b \in_I a \to \psi(b, \vec{f})) \to \psi(a, \vec{f})).\ \mathrm{ind}(x, \vec{f}).$$
The following proof tree shows the claim:
$$\dfrac{\dfrac{\Gamma, x : \forall a.(\forall b.\ b \in_I a \to \psi(b, \vec{f})) \to \psi(a, \vec{f}) \vdash x : \forall a.(\forall b.\ b \in_I a \to \psi(b, \vec{f})) \to \psi(a, \vec{f})}{\Gamma, x : \forall a.(\forall b.\ b \in_I a \to \phi(b, \vec{f})) \to \psi(a, \vec{f}) \vdash \mathrm{ind}_{\psi(a, \vec{f})}(x, \vec{f}) : \forall a.\ \psi(a, \vec{f})}}{\Gamma \vdash M : \forall \vec{f}.(\forall a.(\forall b.\ b \in_I a \to \psi(b, \vec{f})) \to \psi(a, \vec{f})) \to \forall a.\ \psi(a, \vec{f})}$$

□

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 5.9, normalization of λZ_ω entails consistency of $\mathrm{IZF}_{R\omega}$, which easily interprets Heyting Arithmetic. Therefore a normalization proof must utilize much stronger means, which we introduce in the following section.

6. Realizability for $\mathrm{IZF}_{R\omega}$

In this section we work in ZF with ω-many strongly inaccessible cardinals. We denote the i-th strongly inaccessible by Γ_i and choose them so that $\Gamma_i \in \Gamma_{i+1}$. It is likely that IZF with Collection and ω-many inaccessible sets 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].

6.1. **Realizers.** Our realizers are essentially terms of λZ_ω. For convenience, wherever possible, we erase logic terms and formulas from parameters of axRep, axProp, ind and case terms. We call the resulting calculus $\lambda \overline{Z_\omega}$. More formally, $\lambda \overline{Z_\omega}$ arises as an image of an erasure map $\overline{M}$, which takes as its argument a λZ_ω-term. This map is defined by structural induction on M and induced by the following cases:

$$\overline{\mathrm{axRep}(t, \vec{u}, M)} = \mathrm{axRep}(\overline{M}) \qquad \overline{\mathrm{axProp}(t, \vec{u}, M)} = \mathrm{axProp}(\overline{M}) \qquad \overline{\mathrm{ind}_\phi(M, \vec{t})} = \mathrm{ind}(\overline{M})$$
$$\overline{\lambda x : \phi.\ M} = \lambda x.\ \overline{M} \qquad \overline{\mathrm{let}\ [a, x : \phi] := M\ \mathrm{in}\ N} = \mathrm{let}\ [a, x] := \overline{M}\ \mathrm{in}\ \overline{N}$$
$$\overline{\mathrm{case}(M, x : \phi.\ N, x : \psi.\ O)} = \mathrm{case}(\overline{M}, x.\overline{N}, x.\overline{O})$$

The erasure on the rest of terms is defined in a natural way, for example $\overline{\langle M, N \rangle} = \langle \overline{M}, \overline{N} \rangle$, $\overline{[t, M]} = [t, \overline{M}]$ and $\overline{M\ t} = \overline{M}\ t$. The reduction rules and values in $\lambda \overline{Z_\omega}$ are induced from

λZ_ω in an obvious way. The set of $\lambda\overline{Z_\omega}$ terms will be denoted by $\Lambda_{\overline{Z\omega}}$ and the set of $\lambda\overline{Z_\omega}$ values will be denoted by $\lambda\overline{Z_{\omega v}}$.

Lemma 6.1. *If $\overline{M}$ normalizes, so does M.*

Proof. Straightforward — the erased information does not affect the reductions. ☐

The fact that logic terms do not play any role in the reductions is crucial for the normalization argument to work.

This definition of the erasure map and $\lambda\overline{Z_\omega}$ fixes a small mistake in the presentation in [Moc06a], where a bit too much information was erased.

6.2. **Realizability relation.** Having defined realizers, we proceed to define the realizability relation. Our definition was inspired by McCarty's [McC84]. From now on, the letter T denotes the set of all $\mathrm{IZF}_{R\omega}$ terms.

Definition 6.2. A set A is a λ-name iff A is a set of pairs (v, B) such that $v \in \lambda\overline{Z_{\omega v}}$ and B is a λ-name.

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

Definition 6.3. The class of λ-names is denoted by V^λ.

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

$$V^\lambda_\alpha = \bigcup_{\beta<\alpha} P(\lambda\overline{Z_{\omega v}} \times V^\lambda_\beta) \qquad V^\lambda = \bigcup_{\alpha\in\mathrm{ORD}} V^\lambda_\alpha$$

Definition 6.4. The λ-*rank* of a λ-name A, denoted by $\lambda rk(A)$, is the smallest α such that $A \in V^\lambda_\alpha$.

We now define three auxiliary relations between $\lambda\overline{Z_\omega}$ terms and pairs of sets in V^λ, which we write as $M \Vdash A \in_I B$, $M \Vdash A \in B$, $M \Vdash A = B$. These relations are a prelude to the definition of realizability.

$$\begin{array}{lcl}
M \Vdash A \in_I B & \equiv & M \downarrow v \wedge (v, A) \in B \\
M \Vdash A \in B & \equiv & M \downarrow \mathrm{inRep}(N) \wedge N \downarrow [u, O] \wedge \exists C \in V^\lambda.\ O \downarrow \langle O_1, O_2\rangle \wedge \\
 & & O_1 \Vdash C \in_I B \wedge O_2 \Vdash A = C \\
M \Vdash A = B & \equiv & M \downarrow \mathrm{eqRep}(M_0) \wedge M_0 \downarrow \lambda a.\ M_1 \wedge \forall t \in T, \forall D \in V^\lambda.\ M_1[a := t] \downarrow \langle O, P\rangle \wedge \\
 & & O \downarrow \lambda x.\ O_1 \wedge \forall N.\ (N \Vdash D \in_I A) \to O_1[x := N] \Vdash D \in B \wedge \\
 & & P \downarrow \lambda x.\ P_1 \wedge \forall N.\ (N \Vdash D \in_I B) \to P_1[x := N] \Vdash D \in A
\end{array}$$

The relations $M \Vdash A \in B$ and $M \Vdash A = B$ are defined together in a standard way by transfinite recursion. See for example [Rat05] for more details.

Definition 6.5. For any set $C \in V^\lambda$, C^+ denotes $\{(M, A) \mid M \Vdash A \in C\}$.

Definition 6.6. A (class-sized) first-order language L arises from enriching the $\mathrm{IZF}_{R\omega}$ signature with constants for all λ-names.

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

Definition 6.7. 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 induction a realizability relation $M \Vdash_\rho \phi$ in an environment ρ and a meaning of a term $[\![t]\!]_\rho$ in an environment ρ:

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

  Note that if $(M, B) \in \omega'^+$, then there is a finite ordinal α such that $B \in V^\lambda_\alpha$.
(4) $[\![V_i]\!]_\rho \equiv U_i$. We will define U_i below.
(5) $[\![t_A(\vec{u})]\!]_\rho \equiv \{(\mathrm{axRep}(N), B) \in \lambda\overline{Z_{\omega v}} \times V^\lambda_\gamma \mid N \Vdash_\rho \phi_A(B, \overrightarrow{[\![u]\!]_\rho})\}$. The ordinal γ will be defined below.
(6) $M \Vdash_\rho \bot \equiv \bot$
(7) $M \Vdash_\rho t \in_I s \equiv M \Vdash [\![t]\!]_\rho \in_I [\![s]\!]_\rho$
(8) $M \Vdash_\rho t \in s \equiv M \Vdash [\![t]\!]_\rho \in [\![s]\!]_\rho$
(9) $M \Vdash_\rho t = s \equiv M \Vdash [\![t]\!]_\rho = [\![s]\!]_\rho$
(10) $M \Vdash_\rho \phi \land \psi \equiv M \downarrow \langle M_1, M_2\rangle \land (M_1 \Vdash_\rho \phi) \land (M_2 \Vdash_\rho \psi)$
(11) $M \Vdash_\rho \phi \lor \psi \equiv (M \downarrow \mathrm{inl}(M_1) \land M_1 \Vdash_\rho \phi) \lor (M \downarrow \mathrm{inr}(M_1) \land M_1 \Vdash_\rho \psi)$
(12) $M \Vdash_\rho \phi \to \psi \equiv (M \downarrow \lambda x.\ M_1) \land \forall N.\ (N \Vdash_\rho \phi) \to (M_1[x := N] \Vdash_\rho \psi)$
(13) $M \Vdash_\rho \exists a.\ \phi \equiv M \downarrow [t, N] \land \exists A \in V^\lambda.\ N \Vdash_\rho \phi[a := A]$
(14) $M \Vdash_\rho \forall a.\ \phi \equiv M \downarrow \lambda a.\ N \land \forall A \in V^\lambda, \forall t \in T.\ N[a := t] \Vdash_\rho \phi[a := A]$

To define U_i, first recall that the axiom (INAC_i) has the following form:

$$(\mathrm{INAC}_i)\ \forall c.\ c \in V_i \leftrightarrow \phi^i_1(c, V_i) \land \forall d.\ \phi^i_2(d) \to c \in d.$$

We define a monotonic operator F on sets as:

$$F(A) = A \cup \{(\mathrm{inac}_i\mathrm{Rep}(N), C) \in \lambda\overline{Z_{\omega v}} \times V^\lambda_{\Gamma_i} \mid N \Vdash_\rho \phi^i_1(C, A) \land \forall d.\ \phi^i_2(d) \to C \in d\}.$$

We set U_i to be the smallest fixpoint of F. Formally, U_i is generated by transfinite inductive definition on ordinals:

$$U_{i,\gamma} = F(\bigcup_{\beta<\gamma} U_{i,\beta}) \qquad U_i = \bigcup_{\gamma \in \mathrm{ORD}} U_{i,\gamma}$$

Since F adds only elements from $\lambda\overline{Z_{\omega v}} \times V^\lambda_{\Gamma_i}$, any element of U_i is in $\lambda\overline{Z_{\omega v}} \times V^\lambda_{\Gamma_i}$, so $U_i \in V^\lambda_{\Gamma_{i+1}}$.

The definition of the ordinal γ in item 5 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 6.31 can be proved. Let $\vec{\alpha} = \overrightarrow{\lambda rk([\![u]\!]_\rho)}$. Case $t_A(\vec{u})$ of:

- $\{u_1, u_2\}$ — $\gamma = max(\alpha_1, \alpha_2)$
- $P(u)$ — $\gamma = \alpha + 1$.
- $\bigcup u$ — $\gamma = \alpha$.
- $S_{\phi(a,\vec{f})}(u, \vec{u})$ — $\gamma = \alpha_1$.
- $R_{\phi(a,b,\vec{f})}(u, \vec{u})$. This case is more complicated. The names are chosen to match the corresponding clause in the proof of Lemma 6.31. Let $G = \{(N_1, (N_{21}, B)) \in \Lambda_{\overline{Z\omega}} \times [\![u]\!]^+_\rho \mid \exists d \in V^\lambda.\ \psi(N_1, N_{21}, B, d)\}$, where $\psi(N_1, N_{21}, B, d) \equiv (N_1 \downarrow \lambda a.\ N_{11}) \land (N_{11} \downarrow$

$\lambda x.\ O) \wedge (O[x := N_{21}] \Vdash_\rho \phi(B, d, \overrightarrow{[\![u]\!]_\rho}) \wedge \forall e.\ \phi(B, e, \overrightarrow{[\![u]\!]_\rho}) \to e = d)$. 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 $D \in V^\lambda_\beta$ and $(N_1, (N_{21}, B))$ such that $g = (N_1, (N_{21}, B))$ and $\psi(N_1, N_{21}, B, D)$ holds. Set $\gamma = \beta + 1$.

At this point it is not clear yet that the realizability definition makes sense — a priori it might be circular. We will now show that it is not the case.

Definition 6.8. For any closed term s, we define number of occurences of s in any term t and formula ϕ, denoted by $Occ(s, t)$ and $Occ(s, \phi)$, respectively, by induction on the definition of terms and formulas. We show representative clauses of the definition:

- $Occ(s, s) = 1$.
- $Occ(s, a) = 0$, where a is a variable.
- $Occ(s, t_A(\vec{u})) = Occ(s, u_1) + \ldots + Occ(s, u_n)$.
- $Occ(s, S_\phi(t, \vec{u})) = Occ(s, \phi) + Occ(s, t) + Occ(s, u_1) + \ldots + Occ(s, u_n)$.
- $Occ(s, t \in u) = Occ(s, t) + Occ(s, u)$.
- $Occ(s, \phi \wedge \psi) = Occ(s, \phi) + Occ(s, \psi)$.

In a similar manner we define the number of function symbols FS in a term and formula.

Definition 6.9. Let $M(\mathbb{N})$ denote the set of all multisets over $\mathbb{N}$ with the standard well-founded ordering. Formally, a member A of $M(\mathbb{N})$ is a function from $\mathbb{N}$ to $\mathbb{N}$, returning for any n the number of copies of n in A. We define a function V taking terms and formulas into $M(\mathbb{N})$: $V(x)$ for any number i returns $Occ(V_i, x)$, for x being either a term or a formula.

Lemma 6.10. *The definition of realizability is well-founded.*

Proof. Use the measure function m which takes a clause in the definition and returns an element of $M(\mathbb{N}) \times \mathbb{N}^3$ with the lexicographical order:

$$\begin{aligned} m(M \Vdash_\rho \phi) &= (V(\phi), Occ(\omega, \phi), FS(\phi), \text{“structural complexity of } \phi\text{”}) \\ m([\![t]\!]_\rho) &= (V(t), Occ(\omega, t), FS(t), 0) \end{aligned}$$

Then the measure of the definiendum is always greater than the measure of the definiens — in the clauses for formulas the structural complexity goes down, while the rest of parameters do not grow larger. In the definition of $[\![V_i]\!]_\rho$, one V_i disappears replaced by two V_{i-1}'s. In the definition of $[\![\omega]\!]_\rho$, one ω disappears. Finally, in the definition of $[\![t_A(\vec{u})]\!]_\rho$, the topmost t_A disappears, while no new V_i's and ω's appear. □

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

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

- A — then $[\![t[a := s]]\!]_\rho = [\![t[a := [\![s]\!]_\rho]]\!]_\rho = [\![t]\!]_{\rho[a:=[\![s]\!]_\rho]} = A$.
- a — then $[\![t[a := s]]\!]_\rho = [\![s]\!]_\rho$, $[\![t[a := [\![s]\!]_\rho]]\!]_\rho = [\![[\![s]\!]_\rho]\!]_\rho = [\![s]\!]_\rho$ and also $[\![t]\!]_{\rho[a:=[\![s]\!]_\rho]} = [\![s]\!]_\rho$.

- $t_A(\vec{u})$. Then $[\![t[a := s]]\!]_\rho = \{(\mathrm{axRep}(N), A) \mid N \Vdash_\rho \phi_A(A, \vec{u}[a := s])\}$. By the inductive hypothesis, this is equal to $\{(\mathrm{axRep}(N), A) \mid N \Vdash_{\rho[a:=[\![s]\!]_\rho]} \phi_A(A, \vec{u})\} = [\![t]\!]_{\rho[a:=[\![s]\!]_\rho]}$ and also to $\{(\mathrm{axRep}(N), A) \mid N \Vdash_\rho \phi_A(A, \vec{u}[a := [\![s]\!]_\rho])\}$ and thus to $[\![t[a := [\![s]\!]_\rho]]\!]_\rho$.

For formulas, the atomic cases follow by the proof above and the non-atomic cases follow immediately by the application of the inductive hypothesis. □

Lemma 6.12. *If $(M \Vdash_\rho \phi)$ then $M \downarrow$.*

Proof. Straightforward from the definition of realizability — in every case the definition starts with the clause assuring normalization of M. □

Lemma 6.13. *If $M \to^* M'$ 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. □

Lemma 6.14. *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. □

Lemma 6.15. *If $M \Vdash_\rho \phi \to \psi$ and $N \Vdash_\rho \phi$, then $M\ N \Vdash \psi$.*

Proof. Suppose $M \Vdash_\rho \phi \to \psi$. Then $M \downarrow (\lambda x.\ O)$ and for all $P \Vdash \phi$, $O[x := P] \Vdash \psi$. Now, $M\ N \to^* (\lambda x.\ O)\ N \to O[x := N]$. Lemma 6.13 gives us the claim. □

6.3. **Properties of realizability.** We now establish several properties of the realizability relation, which mostly state that the truth in the realizability universe is not far from the truth in the real world, as far as ranks of sets are concerned.

Several lemmas mirror similar facts from McCarty's thesis [McC84]. We cannot, however, simply point to these lemmas and say that essentially they prove the same thing, as our realizability behaves a bit differently from his.

Lemma 6.16. *If $A \in V^\lambda_\alpha$, then there is $\beta < \alpha$ such that for all B, if $M \Vdash_\rho B \in A$, then $B \in V^\lambda_\beta$. If $M \Vdash_\rho B = A$, then $B \in V^\lambda_\alpha$. If $M \Vdash_\rho B \in_I A$, then $\lambda rk(B) < \lambda rk(A)$.*

Proof. By induction on α. Take any $A \in V^\lambda_\alpha$. By the definition of V^λ_α, there is $\beta < \alpha$ such that $A \subseteq \lambda\overline{Z_{\omega v}} \times V^\lambda_\beta$. Suppose $M \Vdash_\rho B \in A$. Then $M \downarrow \mathrm{inRep}(N)$, $N \downarrow [u, O]$, $O \downarrow \langle O_1, O_2\rangle$ and there is C such that $O_1 \Vdash C \in_I A$ and $O_2 \Vdash B = C$. Therefore, $O_1 \downarrow v$ and $(v, C) \in A$. Thus $C \in V^\lambda_\beta$, so by the inductive hypothesis also $B \in V^\lambda_\beta$ and we get the claim of the first part of the lemma.

For the second part, suppose $M \Vdash_\rho B = A$. This means that $M \downarrow \mathrm{eqRep}(M_0)$, $M_0 \downarrow \lambda a.\ M_1$ and for all $t \in T, D$, $M_1[a := t] \downarrow \langle O, P\rangle$. Moreover, $O \downarrow \lambda x.\ O_1$ and for all $N \Vdash_\rho D \in_I B$ we have $O_1[x := N] \Vdash_\rho D \in A$. In particular, if $(v, D) \in B$, then $O_1[x := v] \Vdash_\rho D \in A$. By the first part of the lemma, any such D is in V^λ_β for some $\beta < \alpha$, so $B \in V^\lambda_\alpha$.

The third part is trivial. □

Lemma 6.17. *$M \Vdash_\rho A = B$ iff $M \downarrow \mathrm{eqRep}(N)$ and $N \Vdash_\rho \forall d.\ (d \in_I A \to d \in B) \wedge (d \in_I B \to d \in A)$. Also, $M \Vdash_\rho A \in B$ iff $M \downarrow \mathrm{inRep}(N)$ and $N \Vdash_\rho \exists c.\ c \in_I B \wedge A = c$.*

Proof. Simply expand what it means for M to realize respective formulas. □

We now exhibit realizers corresponding to proofs of Lemmas 4.1-4.5. Their existence and corresponding properties will follow immediately from Theorem 7.4 once it is proved; however, we need them for the proof of Lemma 6.27. Since Lemma 6.27 only needs to be used for a set theory with inaccessibles, an alternative to tedious proofs below could be to prove normalization for the theory without inaccessibles first, and take realizers from that normalization theorem.

Lemma 6.18. *There is a term* eqRefl *such that* eqRefl $\Vdash_\rho \forall a.\ a = a$.

Proof. Take the term eqRefl $\equiv \mathrm{ind}(M)$, where $M = \lambda c.\ \lambda x.\ \mathrm{eqRep}(\lambda d.\ \langle N, N\rangle)$ and $N = \lambda y.\ \mathrm{inRep}([d, \langle y, x\ d\ y\rangle])$. Then eqRefl $\to \lambda a.\ M\ a\ (\lambda e.\ \lambda z.\ \mathrm{ind}(M)\ e)$. It suffices to show that for any A, t, $M\ t\ (\lambda e.\ \lambda z.\ \mathrm{ind}(M)\ e) \Vdash_\rho A = A$. We proceed by induction on λ-rank of A. We have $M\ t\ (\lambda e.\ \lambda z.\ \mathrm{ind}(M)\ e) \downarrow \mathrm{eqRep}(\lambda d.\ \langle N, N\rangle[x := \lambda e.\ \lambda z.\ \mathrm{ind}(M)\ e])$. It suffices to show that for all $s \in T, D \in V^\lambda$, for all $O \Vdash_\rho D \in_I A$, $\mathrm{inRep}([s, [O, (\lambda e.\ \lambda z.\ \mathrm{ind}(M)\ e)\ s\ O\rangle]) \Vdash_\rho D \in A$. Take any s, D and $O \Vdash_\rho D \in_I A$. By Lemma 6.16, $\lambda rk(D) < \lambda rk(A)$. We need to show the existence of C such that $O \Vdash_\rho C \in_I A$ and $(\lambda e.\ \lambda z.\ \mathrm{ind}(M)\ e)\ s\ O \Vdash_\rho D = C$. Taking $C \equiv D$, the first part follows trivially. Since $(\lambda e.\ \lambda z.\ \mathrm{ind}(M)\ e)\ s\ O \to^* \mathrm{ind}(M)\ s \to M\ s\ (\lambda e.\ \lambda z.\ \mathrm{ind}(M)\ s)$, we get the claim by Lemma 6.13 and the inductive hypothesis. □

Lemma 6.19. *There is a term* eqSymm *such that* eqSymm $\Vdash_\rho \forall a, b.\ a = b \to b = a$.

Proof. Take

$$\mathrm{eqSymm} \equiv \lambda a, b.\ \lambda x.\ N,\ \text{ where } N = \mathrm{eqRep}(\lambda d.\ \langle \mathrm{snd}(\mathrm{eqProp}(x)\ d), \mathrm{fst}(\mathrm{eqProp}(x)\ d)\rangle).$$

To show that eqSymm $\Vdash_\rho \forall a, b.\ a = b \to b = a$, it suffices to show that for any A, B, t, u, M, if $M \Vdash_\rho A = B$ then $N[x := M] \Vdash_\rho B = A$. Take any A, B, t, u, M. The claim follows if for all $s \in T, C$ we can show:

- There is M_1 such that $\mathrm{snd}(\mathrm{eqProp}(M)\ s) \downarrow \lambda x.\ M_1$ and for all $N_1 \Vdash_\rho C \in_I B$, $M_1[x := N_1] \Vdash_\rho C \in A$.
- There is M_2 such that $\mathrm{fst}(\mathrm{eqProp}(M)\ s) \downarrow \lambda x.\ M_2$ and for all $N_2 \Vdash_\rho C \in_I A$, $M_2[x := N_2] \Vdash_\rho C \in B$.

Since $M \Vdash_\rho A = B$, then there is O such that $M \downarrow \mathrm{eqRep}(O)$, so $\mathrm{fst}(\mathrm{eqProp}(M)\ s) \to^* \mathrm{fst}(O\ s)$. Moreover, for some O_1, O_2 we have $O\ s \downarrow \langle O_1, O_2\rangle$, where $O_1 \Vdash_\rho C \in_I A \to C \in B$ and $O_2 \Vdash_\rho C \in_I B \to C \in A$. Therefore, $\mathrm{fst}(\mathrm{eqProp}(M)\ s) \to^* O_1$ and similarly $\mathrm{snd}(\mathrm{eqProp}(M)\ s) \to^* O_2$. We also know that there are some P_1, P_2 such that $O_1 \downarrow \lambda x.\ P_1$, $O_2 \downarrow \lambda x.\ P_2$, $P_1[x := N_2] \Vdash_\rho C \in B$ and $P_2[x := N_1] \Vdash_\rho C \in A$. Taking $M_1 = P_2$ and $M_2 = P_1$, we get the claim by Lemma 6.13. □

Lemma 6.20. *There is a term* eqTrans *such that* eqTrans $\Vdash_\rho \forall b, a, c.\ a = b \wedge b = c \to a = c$.

Proof. The proof and the realizers mirror closely the proof of Lemma 4.4. Set:

$$\begin{aligned}
\mathrm{eqTrans} &= \mathrm{ind}(M_0)\\
M_0 &= \lambda b, x_1, a_1, c, x_2.\ \mathrm{eqRep}(\lambda f.\ \langle N, O\rangle)\\
N &= \lambda x_3.\ \mathrm{let}\ [a_2, x_4] := \mathrm{inProp}(\mathrm{fst}(\mathrm{eqProp}(\mathrm{fst}(x_2))\ f)\ x_3)\ \mathrm{in}\ N_1\\
N_1 &= \mathrm{let}\ [a_3, x_5] := \mathrm{inProp}(\mathrm{fst}(\mathrm{eqProp}(\mathrm{snd}(x_2))\ a_2)\ \mathrm{fst}(x_4))\ \mathrm{in}\ N_2\\
N_2 &= \mathrm{inRep}([a_3, \langle \mathrm{fst}(x_5), x_1\ a_2\ \mathrm{fst}(x_4)\ f\ a_3\ \langle \mathrm{snd}(x_4), \mathrm{snd}(x_5)\rangle\rangle])\\
O &= \lambda x_3.\ \mathrm{let}\ [a_2, x_4] := \mathrm{inProp}(\mathrm{snd}(\mathrm{eqProp}(\mathrm{snd}(x_2))\ f)\ x_3)\ \mathrm{in}\ O_1\\
O_1 &= \mathrm{let}\ [a_3, x_5] := \mathrm{inProp}(\mathrm{snd}(\mathrm{eqProp}(\mathrm{fst}(x_2))\ a_2)\ \mathrm{fst}(x_4))\ \mathrm{in}\ O_2\\
O_2 &= \mathrm{inRep}([a_3, \langle \mathrm{fst}(x_5), x_1\ a_2\ \mathrm{fst}(x_4)\ f\ a_3\ \langle \mathrm{snd}(x_4), \mathrm{snd}(x_5)\rangle\rangle]).
\end{aligned}$$

We will show that for all B, eqTrans $\downarrow \lambda b.\ R$ for some term R such that for any term t, $R[b := t] \Vdash_\rho \forall a, c.\ a = B \wedge B = c \to a = c$, which trivially implies the claim. We proceed by induction on λ-rank of B.

We have eqTrans $\to \lambda e.\ M_0\ e\ M_1$, where $M_1 = \lambda g.\ \lambda x.\ \mathrm{eqTrans}\ g$. Thus it suffices to show that for all t_1, $M_0\ t_1\ M_1 \Vdash_\rho \forall a, c.\ a = B \wedge B = c \to a = c$. Since $M_0\ t_1\ M_1 \downarrow \lambda a_1, c, x_2.\ \mathrm{eqRep}(\lambda f.\ \langle N, O\rangle[x_1 := M_1])$, it suffices to show that for all A, C, M_2 such that $M_2 \Vdash_\rho A = B \wedge B = C$ we have $\mathrm{eqRep}(\lambda f.\ \langle N, O\rangle[x_1, x_2 := M_1, M_2]) \Vdash_\rho A = C$. By Lemma 6.17, it suffices to show that for all F, u we have $N[x_1, x_2, f := M_1, M_2, u] \Vdash_\rho F \in_I A \to F \in C$ and $O[x_1, x_2, f := M_1, M_2, u] \Vdash_\rho F \in_I C \to F \in A$.

For the proof of the first claim, we have $N[x_1, x_2, f := M_1, M_2, u] \downarrow \lambda x_3. \ldots$. Take any $M_3 \Vdash_\rho F \in_I A$. We need to show that:

$$\begin{array}{rcl} \text{let } [a_2, x_4] & := & \mathrm{inProp}(\mathrm{fst}(\mathrm{eqProp}(\mathrm{fst}(M_2))\ u)\ M_3) \\ & \text{in} & N_1[x_1, x_2, x_3, f := M_1, M_2, M_3, u] \Vdash_\rho F \in C. \end{array}$$

We have $\mathrm{fst}(M_2) \Vdash_\rho A = B$, so $\mathrm{eqProp}(\mathrm{fst}(M_2)) \Vdash_\rho \forall f.\ (f \in_I A \to f \in B) \wedge (f \in_I B \to f \in A)$, so by Lemma 6.15 $\mathrm{fst}(\mathrm{eqProp}(\mathrm{fst}(M_2)\ u))\ M_3 \Vdash_\rho F \in B$. Therefore, $\mathrm{fst}(\mathrm{eqProp}(\mathrm{fst}(M_2)\ u))\ M_3 \downarrow \mathrm{inRep}(P)$ and $P \downarrow [t_2, M_4]$ for some P, A_2, t_2, M_4 such that $M_4 \Vdash_\rho A_2 \in_I B \wedge F = A_2$. Thus our term let $[a_2, x_4] := \ldots$ reduces to[1] $N_1[x_1, x_2, x_4, a_2, f := M_1, M_2, M_4, t_2, u]$.

Since $\mathrm{snd}(M_2) \Vdash_\rho B = C$, we similarly have $\mathrm{fst}(\mathrm{eqProp}(\mathrm{snd}(M_2))\ t_2)\ \mathrm{fst}(M_4) \Vdash_\rho A_2 \in C$, so $\mathrm{fst}(\mathrm{eqProp}(\mathrm{snd}(M_2))\ t_2)\ \mathrm{fst}(M_4) \downarrow \mathrm{inRep}(Q)$ and for some A_3, $Q \downarrow [t_3, M_5]$, $M_5 \Vdash_\rho A_3 \in_I C \wedge A_2 = A_3$. Therefore

$$N_1[\ldots] \downarrow \mathrm{inRep}([t_3, \langle \mathrm{fst}(M_5), M_1\ t_2\ \mathrm{fst}(M_4)\ u\ t_3\ \langle \mathrm{snd}(M_4), \mathrm{snd}(M_5)\rangle\rangle])$$

and by Lemma 6.13 it suffices to show that

$$\mathrm{inRep}([t_3, \langle \mathrm{fst}(M_5), M_1\ t_2\ \mathrm{fst}(M_4)\ u\ t_3\ \langle \mathrm{snd}(M_4), \mathrm{snd}(M_5)\rangle\rangle]) \Vdash_\rho F \in C$$

For this purpose, we need to show that $\mathrm{fst}(M_5) \Vdash_\rho A_3 \in_I C$, which is trivial, and that

$$M_1\ t_2\ \mathrm{fst}(M_4)\ u\ t_3\ \langle \mathrm{snd}(M_4), \mathrm{snd}(M_5)\rangle \Vdash_\rho F = A_3.$$

Since $M_1 = \lambda g.\ \lambda x.\ \mathrm{eqTrans}\ g$, $\mathrm{snd}(M_4) \Vdash_\rho F = A_2$ and $\mathrm{snd}(M_5) \Vdash_\rho A_2 = A_3$, all we need to have is that eqTrans $t_2 \Vdash_\rho \forall a, c.\ a = A_2 \wedge A_2 = c \to a = c$. Since $\mathrm{fst}(M_4) \Vdash_\rho A_2 \in_I B$, $\lambda rk(A_2) < \lambda rk(B)$ and we get the claim by the inductive hypothesis.

The proof of the second claim proceeds in a very similar fashion. The only thing which differs O and O_1 from N and N_1 is the exchange of fst and snd which corresponds to using the information that $\forall f.\ f \in_I C \to f \in B$ and $\forall f.\ f \in_I B \to f \in A$ and proceeding from C to A in the second part of the proof of Lemma 4.4. □

Lemma 6.21. *There is a term* lei *such that* lei $\Vdash_\rho \forall a, b, c.\ a \in c \wedge a = b \to b \in c$.

Proof. Take

$$\begin{array}{rcl} \mathrm{lei} & = & \lambda a, b, c, x.\ \text{let } [d, y] := \mathrm{inProp}(\mathrm{fst}(\mathrm{x}))\ \text{in} \\ & & \mathrm{inRep}([d, \langle \mathrm{fst}(y), \mathrm{eqTrans}\ a\ b\ c\ \langle \mathrm{eqSymm}\ a\ b\ \mathrm{snd}(x), \mathrm{snd}(y)\rangle\rangle]). \end{array}$$

We need to show that for any $t_1, t_2, t_3 \in T$, A, B, C, for any $M \Vdash_\rho A \in C \wedge A = B$, we have

$$\begin{array}{rcl} \text{let } [d, y] & := & \mathrm{inProp}(\mathrm{fst}(\mathrm{M}))\ \text{in} \\ & & \mathrm{inRep}([d, \langle \mathrm{fst}(y), \mathrm{eqTrans}\ t_1\ t_2\ t_3\ \langle \mathrm{eqSymm}\ t_1\ t_2\ \mathrm{snd}(M), \mathrm{snd}(y)\rangle\rangle]) \Vdash_\rho B \in C. \end{array}$$

[1] Since x_3 does not occur in N_1 and N_2, we omit it from the substitution.

We have $M \downarrow \langle M_1, M_2\rangle$, $M_1 \Vdash_\rho A \in C$, $M_2 \Vdash_\rho A = B$. Therefore $M_1 \downarrow \mathrm{inRep(N)}$, $N \downarrow [u, O]$, $O \downarrow \langle O_1, O_2\rangle$ and there is D such that $O_1 \Vdash_\rho D \in_I C$, $O_2 \Vdash_\rho A = D$. Therefore $\mathrm{inProp}(\mathrm{fst}(M)) \downarrow [u, O]$, so it suffices to show that

$$\mathrm{inRep}([u, \langle \mathrm{fst}(O), \mathrm{eqTrans}\ t_1\ t_2\ t_3\ \langle \mathrm{eqSymm}\ t_1\ t_2\ \mathrm{snd}(M), (\mathrm{snd}(O))\rangle\rangle]) \Vdash_\rho B \in C.$$

This follows if we can find some E such that $O_1 \Vdash_\rho E \in_I C$ and

$$\mathrm{eqTrans}\ t_1\ t_2\ t_3\ \langle \mathrm{eqSymm}\ t_1\ t_2\ \mathrm{snd}(M), \mathrm{snd}(O)\rangle \Vdash_\rho B = E.$$

Take E to be D. Since we have $\mathrm{eqSymm}\ t_1\ t_2\ \mathrm{snd}(M) \Vdash_\rho B = A$ and $\mathrm{snd}(O) \Vdash_\rho A = E$, the claim follows by Lemma 6.20. $\square$

The following two lemmas will be used for the treatment of ω in Lemma 6.31.

Lemma 6.22. *If $A, B \in V^\lambda_\alpha$, then $[\![\{A, B\}]\!]_\rho \in V^\lambda_{\alpha+1}$.*

Proof. Take any $(M, C) \in [\![\{A, B\}]\!]_\rho$. By the definition of $[\![\{A, B\}]\!]_\rho$, any such C is in V^λ_α, so $[\![\{A, B\}]\!]_\rho \in V^\lambda_{\alpha+1}$. $\square$

Lemma 6.23. *If $A \in V^\lambda_\alpha$ and $M \Vdash_\rho B = S(A)$, then $B \in V^\lambda_{\alpha+3}$.*

Proof. $M \Vdash_\rho B = S(A)$ means $M \Vdash_\rho B = \bigcup\{A, \{A, A\}\}$. By Lemma 6.16, it suffices to show that $[\![\bigcup\{A, \{A, A\}\}]\!]_\rho \in V^\lambda_{\alpha+3}$. Applying Lemma 6.22 twice, we find that $[\![\{A, \{A, A\}\}]\!]_\rho \in V^\lambda_{\alpha+2}$. By the definition of $[\![\bigcup\{A, \{A, A\}\}]\!]_\rho$, if $(M, C) \in [\![\bigcup\{A, \{A, A\}\}]\!]_\rho$, then $C \in V_{\lambda rk([\![\bigcup\{A, \{A, A\}\}]\!]_\rho)}$, so $C \in V^\lambda_{\alpha+2}$. Therefore $[\![\bigcup\{A, \{A, A\}\}]\!]_\rho \in V^\lambda_{\alpha+3}$ which shows the claim. $\square$

Lemma 6.24. *If $A, B \in V^\lambda_\alpha$ and $M \Vdash_\rho C = (A, B)$, then $C \in V^\lambda_{\alpha+2}$.*

Proof. Similar to the proof of Lemma 6.23, utilizing Lemmas 6.22 and 6.16. $\square$

Lemma 6.25. $\lambda rk(C) \leq rk(C^+) + \omega$.

Proof. If $(M, A) \in C$, then $M \Vdash_\rho A \in_I C$. We have $\mathrm{inRep}([a, \langle M, \mathrm{eqRefl}\ a\rangle]) \Vdash_\rho A \in C$, so $(\mathrm{inRep}([a, \langle M, \mathrm{eqRefl}\ a\rangle]), A) \in C^+$. The extra ω is there to deal with possible difficulties with finite C's, as we do not know a priori the rank of set-theoretic encoding of $\mathrm{inRep}([a, \langle M, \mathrm{eqRefl}\ a\rangle]$. $\square$

Lemma 6.26. *If $N \Vdash_\rho \forall x \in A.\ \phi$ then for all $(O, X) \in A^+$, $N \downarrow \lambda a.\ N_1$ and $N_1 \downarrow \lambda x.\ N_2$ and $N_2[x := O] \Vdash_\rho \phi[x := X]$. Also, if $N \Vdash_\rho \exists x \in A.\ \phi$ then there is $(O, X) \in A^+$ such that $N \downarrow [t, N_1]$, $N_1 \downarrow \langle O, N_2\rangle$ and $N_2 \Vdash_\rho \phi[x := X]$.*

Proof. If $N \Vdash_\rho \forall x \in A.\ \phi$ then $N \downarrow \lambda a.\ N_1$ and for all t, X, $N_1[a := t] \Vdash_\rho X \in A \to \phi$. In particular, taking $t = a$, we get $N_1 \downarrow \lambda x.\ N_2$ and for all O such that $O \Vdash_\rho X \in A$, $N_2[x := O] \Vdash_\rho \phi[x := X]$. This implies that for all X, for all O, if $O \Vdash_\rho X \in A$, then $N \downarrow \lambda a.\ N_1$, $N_1 \downarrow \lambda x.\ N_2$ and $N_2[x := O] \Vdash_\rho \phi[x := X]$, which proves the first part of the claim.

If $N \Vdash_\rho \exists x \in A.\ \phi$, then $N \downarrow [t, N_1]$ and there is X such that $N_1 \downarrow \langle O, N_2\rangle$, $O \Vdash_\rho X \in A$ and $N_2 \Vdash_\rho \phi[x := X]$, so there is $(O, X) \in A^+$ such that $N \downarrow [t, N_1]$, $N_1 \downarrow \langle O, N_2\rangle$ and $N_2 \Vdash_\rho \phi[x := X]$. $\square$

With our lemmas in hand, we can now prove:

Lemma 6.27. *Suppose $A \in U_i$ and $N \Vdash_\rho$"C is a function from A into V_i". Then $C \in V^\lambda_{\Gamma_i}$.*

Proof. First let us write formally the statement "C is a function from A into V_i". This means "for all $x \in A$ there is exactly one $y \in V_i$ such that $(x, y) \in C$ and for all $z \in C$ there is $x \in A$ and $y \in V_i$ such that $z = (x, y)$". Thus $N \downarrow \langle N_1, N_2\rangle$, $N_1 \Vdash_\rho \forall x \in A \exists! y \in V_i.\ (x, y) \in C$ and $N_2 \Vdash_\rho \forall z \in C \exists x \in A \exists y \in V_i.\ z = (x, y)$. So $N_1 \Vdash_\rho \forall x \in A \exists y \in V_i.\ (x, y) \in C \land \forall z.\ (x, z) \in C \to z = y$. By Lemma 6.26, for all $(O, X) \in A^+$ there is $(P, Y) \in U_i^+$ such that $\phi(O, X, P, Y)$ holds, where $\phi(O, X, P, Y)$ is defined as:

$$\begin{array}{rcl}\phi(O, X, P, Y) & \equiv & (N_1 \downarrow \lambda a.\ N_{11}) \land (N_{11} \downarrow \lambda x.\ N_{12}) \land (N_{12}[x := O] \downarrow [t, N_{13}]) \land \\ & & (N_{13} \downarrow \langle P, Q\rangle) \land (Q \downarrow \langle Q_1, Q_2\rangle) \land \\ & & (Q_1 \Vdash_\rho (X, Y) \in C) \land (Q_2 \Vdash_\rho \forall z.\ (X, z) \in C \to z = Y)\end{array}$$

Let $\psi(O, X, P, Y)$ be defined as:

$$\psi(O, X, P, Y) \equiv \exists Q_1, Q_2.\ (Q_1 \Vdash_\rho (X, Y) \in C) \land (Q_2 \Vdash_\rho \forall z.\ (X, z) \in C \to z = Y)$$

Obviously, if $\phi(O, X, P, Y)$ then $\psi(O, X, P, Y)$. So for all $(O, X) \in A^+$ there is $(P, Y) \in U_i^+$ such that $\psi(O, X, P, Y)$ holds.

Define a function F which takes $(O, X) \in A^+$ and returns $\{(P, Y) \in U_i^+ \mid \psi(O, X, P, Y)\}$. Suppose $(P_1, Y_1), (P_2, Y_2) \in F((O, X))$. Then there are Q_{11}, Q_{12}, Q_{21} such that $Q_{11} \Vdash_\rho (X, Y_1) \in C$, $Q_{12} \Vdash_\rho \forall z.\ (X, z) \in C \to z = Y_1$, $Q_{21} \Vdash_\rho (X, Y_2) \in C$. By Lemma 6.26, $Q_{12} \downarrow \lambda a.\ R_1$, $R_1 \downarrow \lambda x.\ R_2$ and $R_2[x := Q_{21}] \Vdash_\rho Y_2 = Y_1$. Since eqSymm a a $R_2[x := Q_{21}] \Vdash_\rho Y_1 = Y_2$, by Lemma 6.16 the λ-ranks of Y_1, Y_2 are the same and, since any such (P, Y) is a member of U_i^+, they are smaller than Γ_i. Also, for any $(O, X) \in A^+$, $F(O, X)$ is inhabited.

Furthermore, define a function G from A^+ to Γ_i, which takes $(O, X) \in A^+$ and returns $\bigcup\{\lambda rk((P, Y)) \mid (P, Y) \in F(O, X) \land \psi(O, X, P, Y)\}$. Then for any $(O, X) \in A^+$, $G(O, X)$ is an ordinal smaller than Γ_i and if $(P, Y) \in U_i^+$ and $\psi(O, X, P, Y)$, then $(P, Y) \in V^\lambda_{G(O,X)}$. Moreover, as Γ_i is inaccessible, $G \in R(\Gamma_i)$, where $R(\Gamma_i)$ denotes the Γ_i-th element of the standard cumulative hierarchy. Therefore $\bigcup ran(G)$ is also an ordinal smaller than Γ_i. We define an ordinal β to be $\max(\lambda rk(A), \bigcup ran(G))$.

Now take any $(M, B) \in C^+$, so $M \Vdash_\rho B \in C$. Then, by the definition of N_2 and Lemma 6.26 there is $(O, X) \in A^+$ and $(O_1, Z) \in U_i^+$ such that $N_2 \downarrow \lambda a.\ N_{21}$, $N_{21} \downarrow \lambda x.\ N_{22}$, $N_{22}[x := M] \downarrow [t, N_{23}]$, $N_{23} \downarrow \langle O, N_{24}\rangle$, $N_{24} \downarrow [t, N_{25}]$, $N_{25} \downarrow \langle O_1, R\rangle$ and $R \Vdash_\rho B = (X, Z)$. Let $M_1 =$ lei a a a $\langle M, R\rangle$, then $M_1 \Vdash_\rho (X, Z) \in C$. Take any element $(P, Y) \in F(O, X)$ and accompanying Q_1, Q_2. Then $Q_2 \downarrow \lambda a.\ Q_3$, $Q_3 \downarrow \lambda x.\ Q_4$ and $Q_4[x := M_1] \Vdash_\rho Z = Y$. By Lemma 6.16, $\lambda rk(Z) \le \lambda rk(Y)$ and thus $\lambda rk(Z) \le \beta$. Since $(O, X) \in A^+$, $\lambda rk(X) \le \beta$, too. By Lemma 6.24, $\lambda rk(B) \le \beta + 2$. By Lemma 6.25, $rk(B) \le \beta + \omega$, so $rk(C^+) \le \beta + \omega + 1$. By Lemma 6.25 again, $\lambda rk(C) \le \beta + 2\omega$. Since $\beta + 2\omega$ is still smaller than Γ_i, we get the claim. □

Lemma 6.28. *If $M \Vdash_\rho A \in U_{i,\gamma}$, then $M \Vdash_\rho A \in V_i$.*

Proof. If $M \Vdash_\rho A \in U_{i,\gamma}$, then $M \downarrow \mathrm{inRep}(N)$, $N \downarrow [t, O]$, $O \downarrow \langle O_1, O_2\rangle$ and there is C such that $O_1 \downarrow v$, $(v, C) \in U_{i,\gamma}$, $O_2 \Vdash_\rho C = A$. Then also $(v, C) \in U_i$, so $O_1 \Vdash_\rho C \in_I V_i$, so also $M \Vdash_\rho A \in V_i$. □

Lemma 6.29. *If $N \Vdash_\rho \psi_i(C, U_{i,\gamma})$, where ψ_i is one of the five clauses defining $\phi_1^i(C, U_{i,\gamma})$ in the Definition 3.3, then $N \Vdash_\rho \psi_i(C, V_i)$.*

Proof. There are five cases to consider:

- $N \Vdash_\rho C = V_{i-1}$. This case is trivial.
- $N \Vdash_\rho \exists a.\ a \in U_{i,\gamma} \wedge c \in a$. Then there is A such that $N \downarrow [t, O]$, $O \downarrow \langle O_1, O_2\rangle$, $O_1 \Vdash_\rho A \in U_{i,\gamma}$, $O_2 \Vdash_\rho C \in A$. By Lemma 6.28, $O_1 \Vdash_\rho A \in V_i$, so also $N \Vdash_\rho \exists a.\ a \in V_i \wedge c \in a$.
- $N \Vdash_\rho \exists a.\ a \in U_{i,\gamma} \wedge c = \bigcup a$. Then there is A such that $N \downarrow [t, O]$, $O \downarrow \langle O_1, O_2\rangle$, $O_1 \Vdash_\rho A \in U_{i,\gamma}$, $O_2 \Vdash_\rho C = \bigcup A$. Thus by Lemma 6.28 $O_1 \Vdash_\rho A \in V_i$ and we get the claim in the same way as in the previous case.
- $N \Vdash_\rho \exists a.\ a \in U_{i,\gamma} \wedge C = P(a)$. Similar to the previous case.
- $N \Vdash_\rho \exists a.\ a \in U_{i,\gamma} \wedge C \in a \to U_{i,\gamma}$. Then there is A such that $N \downarrow [t, O]$, $O \downarrow \langle O_1, O_2\rangle$, $O_1 \Vdash_\rho A \in U_{i,\gamma}$, $O_2 \Vdash_\rho$ "C is a function from A into $U_{i,\gamma}$". By Lemma 6.28, $O_1 \Vdash_\rho A \in V_i$. Expanding the second part, we have $O_2 \downarrow \langle P_1, P_2\rangle$, $P_1 \Vdash_\rho \forall x \in A \exists! y \in U_{i,\gamma}.\ (x, y) \in C$ and $P_2 \Vdash_\rho \forall z \in C \exists x \in A \exists y \in U_{i,\gamma}.\ z = (x, y)$. We will tackle P_1 and P_2 separately.
  - For P_1, we have for all X, t, $P_1 \downarrow \lambda a.\ P_{11}$, $P_{11}[a := t] \downarrow \lambda x.Q$ and for all $R \Vdash_\rho X \in A$ there is Y such that $Q[x := R] \downarrow [t_1, Q_0]$, $Q_0 \downarrow \langle Q_1, Q_2\rangle$, $Q_1 \Vdash_\rho Y \in U_{i,\gamma}$ and $Q_2 \Vdash_\rho (X, Y) \in C \wedge \forall z.\ (X, z) \in C \to z = Y$. By Lemma 6.28 we also have $Q_1 \Vdash_\rho Y \in V_i$, so also $P_1 \Vdash_\rho \forall x \in a \exists! y.\ y \in V_i \wedge (x, y) \in C$.
  - For P_2, we have for all Z, t, $P_2 \downarrow \lambda a.\ P_{11}$, $P_{11}[a := t] \downarrow \lambda x.Q$ and for all $R \Vdash_\rho Z \in C$ there are X, Y such that $Q[x := R] \downarrow [t_1, Q_0]$, $Q_0 \downarrow \langle Q_1, Q_2\rangle$ and $Q_1 \Vdash_\rho X \in A$. Moreover, $Q_2 \downarrow [t_2, S_0]$, $S_0 \downarrow \langle S_1, S_2\rangle$ and $S_1 \Vdash_\rho Y \in U_{i,\gamma}$. By Lemma 6.28 we also have $S_1 \Vdash_\rho Y \in V_i$, so also $P_2 \Vdash_\rho \forall z \in C \to \exists x \in A \exists y \in V_i.\ z = (x, y)$.

  Therefore also $O_2 \Vdash_\rho$ "C is a function from A into V_i" and in the end $N \Vdash_\rho \exists a.\ a \in V_i \wedge C \in a \to V_i$. $\square$

Corollary 6.30. *If $M \Vdash_\rho \phi_1^i(C, U_{i,\gamma})$, then $M \Vdash_\rho \phi_1^i(C, V_i)$.*

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

Lemma 6.31. $(M, C) \in [\![t_A(\vec{u})]\!]_\rho$ *iff* $M = \mathrm{axRep}(N)$ *and* $N \Vdash_\rho \phi_A(C, \overrightarrow{[\![u]\!]_\rho})$.

Proof. The proof proceeds by case analysis on $t_A(\vec{u})$. We first do the proof for all terms apart from ω and V_i, then we show the claim for ω and finally for V_i.

For all terms, save ω and V_i, the left-to-right direction is immediate. For the right-to-left direction, suppose $N \Vdash_\rho \phi_A(C, \overrightarrow{[\![u]\!]_\rho})$ and $M = \mathrm{axRep}(N)$. To show that $(M, C) \in [\![t_A(\vec{u})]\!]_\rho$, we need to show that $C \in V_\gamma^\lambda$. Let $\vec{\alpha} = \overrightarrow{rank([\![u]\!]_\rho)}$. Case $t_A(\vec{u})$ of:

- $\{u_1, u_2\}$. Suppose that $N \Vdash_\rho C = [\![u_1]\!]_\rho \vee C = [\![u_2]\!]_\rho$. Then either $N \downarrow \mathrm{inl}(N_1) \wedge N_1 \Vdash_\rho C = [\![u_1]\!]_\rho$ or $N \downarrow \mathrm{inr}(N_1) \wedge N_1 \Vdash_\rho C = [\![u_2]\!]_\rho$. By Lemma 6.16, in the former case $C \in V_{\alpha_1}^\lambda$, in the latter $C \in V_{\alpha_2}^\lambda$, so $C \in V_{max(\alpha_1,\alpha_2)}^\lambda$.
- $P(u)$. Suppose that $N \Vdash_\rho \forall d.\ d \in C \to d \in [\![u]\!]_\rho$. Then $N \downarrow \lambda a.\ N_1$ and for any t, $\forall D.\ N_1[a := t] \Vdash_\rho D \in C \to D \in [\![u]\!]_\rho$, so $\forall D, t.\ N_1[a := t] \downarrow \lambda x.\ N_2$ and for all O, if $O \Vdash D \in C$ then $N_2[x := O] \Vdash_\rho D \in [\![u]\!]_\rho$. Take any $(v, B) \in C$. Then $\mathrm{inRep}([a, \langle v, \mathrm{eqRefl\ a}\rangle]) \Vdash_\rho B \in C$, so $N_2[x := \mathrm{inRep}([a, \langle v, \mathrm{eqRefl\ a}\rangle]] \Vdash_\rho B \in [\![u]\!]_\rho$. Thus by Lemma 6.16 any such B is in V_α^λ, so $C \in V_{\alpha+1}^\lambda$.
- $\bigcup u$. Suppose $N \Vdash_\rho \exists c.\ c \in [\![u]\!]_\rho \wedge C \in c$. Then $N \downarrow [t, N_1]$ and there is B such that $N_1 \Vdash_\rho B \in [\![u]\!]_\rho \wedge C \in B$. Thus $N_1 \downarrow \langle N_1, N_2\rangle$, $N_1 \Vdash_\rho B \in [\![u]\!]_\rho$, $N_2 \Vdash_\rho C \in B$. By Lemma 6.16, any such B is in V_α^λ, so also $C \in V_\alpha^\lambda$.

- $S_{\phi(a,\vec{f})}(u,\vec{u})$. Suppose $N \Vdash_\rho C \in [\![u]\!]_\rho \land \phi(C, \overrightarrow{[\![u]\!]_\rho})$. Then $N \downarrow \langle N_1, N_2\rangle$ and $N_1 \Vdash_\rho C \in [\![u]\!]_\rho$. Thus $C \in V^\lambda_{\alpha_1}$.
- $R_{\phi(a,\vec{f})}(u,\vec{u})$. Suppose $N \Vdash_\rho (\forall x \in [\![u]\!]_\rho \exists! y.\ \phi(x,y,\overrightarrow{[\![u]\!]_\rho})) \land \exists x \in [\![u]\!]_\rho.\ \phi(x, C, \overrightarrow{[\![u]\!]_\rho})$. Then $N \downarrow \langle N_1, N_2\rangle$ and $N_2 \Vdash_\rho \exists x \in [\![u]\!]_\rho.\ \phi(x, C, \overrightarrow{[\![u]\!]_\rho})$. Thus $N_2 \downarrow [t, N_{20}]$, $N_{20} \downarrow \langle N_{21}, N_{22}\rangle$ and there is B such that $N_{21} \Vdash_\rho B \in [\![u]\!]_\rho$ and $N_{22} \Vdash_\rho \phi(B, C, \overrightarrow{[\![u]\!]_\rho})$. We also have $N_1 \Vdash_\rho \forall x \in [\![u]\!]_\rho \exists! y.\ \phi(x,y,\overrightarrow{[\![u]\!]_\rho})$, so $N_1 \downarrow \lambda a.\ N_{11}$ and for all C, $N_{11} \downarrow \lambda x.\ O$ and for all $P \Vdash_\rho C \in [\![u]\!]_\rho$, $O[x := P] \Vdash_\rho \exists! y.\ \phi(C, y, \overrightarrow{[\![u]\!]_\rho})$. So taking $C = B$ and $P = N_{21}$, there is D such that $N_1 \downarrow \lambda a.\ N_{11}$, $N_{11} \downarrow \lambda x.\ O$ and $O[x := N_{21}] \downarrow [s, O_1]$ and $O_1 \Vdash_\rho \phi(B, D, \overrightarrow{[\![u]\!]_\rho}) \land \forall e.\ \phi(B, e, \overrightarrow{[\![u]\!]_\rho}) \to e = D$. Therefore $(N_1, (N_{21}, B)) \in G$ from the definition of γ, so there is $D \in V^\lambda_\gamma$ such that $N_1 \downarrow \lambda a.\ N_{11}$, $N_{11} \downarrow \lambda x. O$, $O[x := N_{21}] \downarrow [s, O_1]$ and $O_1 \Vdash_\rho \phi(B, D, \overrightarrow{[\![u]\!]_\rho}) \land \forall e.\ \phi(B, e, \overrightarrow{[\![u]\!]_\rho}) \to e = D$. So $O_1 \downarrow \langle O_{11}, O_{12}\rangle$ and $O_{12} \Vdash_\rho \forall e.\ \phi(B, e, \overrightarrow{[\![u]\!]_\rho}) \to e = D$. Therefore, $O_{12} \downarrow \lambda a.\ Q$, $Q \downarrow \lambda x.\ Q_1$ and $Q_1[x := N_{22}] \Vdash_\rho C = D$. By Lemma 6.16, $C \in V^\lambda_\gamma$.

Now we tackle ω. For the left-to-right direction, obviously $M = \text{infRep}(N)$. 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 $N \Vdash_\rho A = 0 \lor \exists y \in \omega'.\ A = S(y)$.
- 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 $[t, O] \Vdash_\rho \exists y.\ y \in \omega' \land A = S(y)$, so $N \Vdash_\rho A = 0 \lor \exists y \in \omega'.\ A = S(y)$.

For the right-to-left direction, suppose $N \Vdash_\rho A = 0 \lor (\exists y.\ y \in \omega' \land A = S(y))$. Then either $N \downarrow \text{inl}(N_1)$ or $N \downarrow \text{inr}(N_1)$. In the former case, $N_1 \Vdash_\rho A = 0$, so by Lemma 6.16 $A \in V^\lambda_\omega$. In the latter, $N_1 \Vdash_\rho \exists y.\ y \in \omega' \land A = S(y)$. Thus $N_1 \downarrow [t, O]$ and there is B such that $O \Vdash_\rho B \in \omega' \land A = S(B)$. So $O \downarrow \langle M', P\rangle$, $(M', B) \in \omega'^+$ and $P \Vdash_\rho A = S(B)$. This is exactly the inductive step of the definition of ω', so it remains to show that $A \in V^\lambda_\omega$. Since $(M', B) \in \omega'^+$, there is a finite ordinal α such that $B \in V^\lambda_\alpha$. By Lemma 6.23, $A \in V^\lambda_{\alpha+3}$, so also $A \in V^\lambda_\omega$ and we get the claim.

Finally, we take care of V_i. We first show the left-to-right direction. Suppose $(M, A) \in U_i$, then $M = \text{inac}_\text{i}\text{Rep}(N)$. We must have $N \Vdash_\rho \phi^i_1(A, U_{i,\gamma}) \land \forall d.\ \phi^i_2(d) \to A \in d$ for some ordinal γ. Then $N \downarrow \langle N_1, N_2\rangle$, $N_1 \Vdash_\rho \phi^i_1(A, U_{i,\gamma})$, $N_2 \Vdash_\rho \forall d.\ \phi^i_2(d) \to A \in d$. Corollary 6.30 gives us $N_1 \Vdash_\rho \phi^i_1(A, V_i)$, so $N \Vdash_\rho \phi^i_1(A, V_i) \land \forall d.\ \phi^i_2(d) \to A \in d$, which is what we want.

For the right-to-left direction, suppose $N \Vdash_\rho \phi^i_1(C, V_i) \land \forall d.\ \phi^i_2(d) \to C \in d$. We need to show that $(\text{inac}_\text{i}\text{Rep}(\text{N}), C) \in U_i$. By the definition of U_i it suffices to show that $C \in V_{\Gamma_i}$. We have $N \downarrow \langle N_1, N_2\rangle$ and $N_1 \Vdash_\rho$ "C is equal to V_{i-1} or there is $A \in V_i$ such that C is a powerset/union/member of A, or C is a function from A into V_i.". The proof splits into corresponding five cases. The first four are easy to prove using Lemma 6.16 and the definition of the ordinal γ in the clause 5 in the definition of realizability. The last one follows by Lemma 6.27. □

7. Normalization

In this section, environments ρ are finite partial functions mapping propositional variables to terms of $\lambda\overline{Z_\omega}$ and first-order variables to pairs (t, A), where $t \in T$ and $A \in V^\lambda$. Therefore, $\rho : Var \cup FVar \to \Lambda_{\overline{Z\omega}} \cup (T \times V^\lambda)$, where Var denotes the set of propositional variables and $FVar$ denotes the set of first-order variables. Note that any ρ can be used as a realizability environment by considering only the mapping of first-order variables to V^λ. Therefore we will be using the notation $\Vdash_\rho$ also for these environments ρ.

Definition 7.1. For a sequent $\Gamma \vdash M : \phi$, $\rho \models \Gamma \vdash M : \phi$ 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, $[\![t]\!]_\rho$ is defined and so is the realizability relation $M \Vdash_\rho \phi$.

Definition 7.2. For a sequent $\Gamma \vdash M : \phi$, if $\rho \models \Gamma \vdash M : \phi$ then $M[\rho]$ is $M[x_1 := \rho(x_1), \ldots, x_n := \rho(x_n), a_1 := \rho_T(a_1), \ldots, a_k := \rho_T(a_k)]$, where $FV(M) = \{x_1, \ldots, x_n\}$, $FV_F(M) = \{a_1, \ldots, a_k\}$ and ρ_T denotes the restriction of ρ to the mapping from first-order variables into terms: $\rho_T = \lambda a \in FVar.\ \pi_1(\rho(a))$.

Lemma 7.3. *$M[\rho][x := N] = M[\rho[x := N]]$. Also $M[\rho][a := t] = M[\rho[a := (t, A)]]$.*

Proof. Straightforward structural induction on M. □

Theorem 7.4 (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_ω 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.
- $$\frac{\Gamma \vdash M : \phi \to \psi \quad \Gamma \vdash N : \phi}{\Gamma \vdash M\ N : \psi}$$
  By the inductive hypothesis, $M' \Vdash_\rho \phi \to \psi$ and $N' \Vdash_\rho \phi$. Lemma 6.15 gives the claim.
- $$\frac{\Gamma, x : \phi \vdash M : \psi}{\Gamma \vdash \lambda x : \phi.\ M : \phi \to \psi}$$
  We need to show that for any $N \Vdash_\rho \phi$, $M'[x := N] \Vdash_\rho \psi$. Take any such N. Let $\rho' = \rho[x := N]$. Then $\rho' \models \Gamma, x : \phi \vdash M : \psi$, so by the inductive hypothesis $\overline{M}[\rho'] \Vdash_{\rho'} \psi$. By Lemma 7.3 $\overline{M}[\rho'] = \overline{M}[\rho][x := N] = M'[x := N]$, so $M'[x := N] \Vdash_{\rho'} \psi$. Since ρ' agrees with ρ on logic variables, by Lemma 6.14 we get $M'[x := N] \Vdash_\rho \psi$.
- $$\frac{\Gamma \vdash M : \bot}{\Gamma \vdash \mathrm{magic}(M) : \phi}$$
  By the inductive hypothesis, $M' \Vdash_\rho \bot$, which is not the case, so anything holds, in particular $\mathrm{magic}(M') \Vdash_\rho \phi$.
- $$\frac{\Gamma \vdash M : \phi \land \psi}{\Gamma \vdash \mathrm{fst}(M) : \phi}$$
  By the inductive hypothesis, $M' \Vdash_\rho \phi \land \psi$, so $M' \downarrow \langle M_1, M_2 \rangle$ and $M_1 \Vdash_\rho \phi$. Therefore $\mathrm{fst}(M) \to^* \mathrm{fst}(\langle M_1, M_2 \rangle) \to M_1$. Lemma 6.13 gives the claim.
- $$\frac{\Gamma \vdash M : \phi \land \psi}{\Gamma \vdash \mathrm{snd}(M) : \psi}$$
  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 inductive hypothesis.
- $$\frac{\Gamma \vdash M : \phi}{\Gamma \vdash \mathrm{inl}(M) : \phi \vee \psi}$$
  We need to show that $M' \Vdash_\rho \phi$, which we get from the inductive hypothesis.
- $$\frac{\Gamma \vdash M : \psi}{\Gamma \vdash \mathrm{inr}(M) : \phi \vee \psi}$$
  Symmetric to the previous case.
- $$\frac{\Gamma \vdash M : \phi \vee \psi \quad \Gamma, x : \phi \vdash N : \vartheta \quad \Gamma, x : \psi \vdash O : \vartheta}{\Gamma \vdash \mathrm{case}(M, x : \phi.\ N, x : \psi.\ O) : \vartheta}$$
  By the inductive hypothesis, $M' \Vdash_\rho \phi \vee \psi$. Therefore either $M' \downarrow \mathrm{inl}(M_1)$ and $M_1 \Vdash_\rho \phi$ or $M' \downarrow \mathrm{inr}(M_2)$ 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 inductive hypothesis we get $\overline{N}[\rho[x := M_1]] \Vdash_\rho \vartheta$. We also have $\mathrm{case}(M, x.\overline{N}, x.\overline{O}) \to^* \mathrm{case}(\mathrm{inl}(M_1), x.\overline{N}, x.\overline{O}) \to \overline{N}[x := M_1]$. By Lemma 7.3, $\overline{N}[x := M_1] = \overline{N}[\rho[x := M_1]]$, so Lemma 6.13 gives us the claim.
- $$\frac{\Gamma \vdash M : \phi}{\Gamma \vdash \lambda a.\ M : \forall a.\ \phi}$$
  By the inductive hypothesis, for all $\rho \models \Gamma \vdash M : \phi$, $\overline{M}[\rho] \Vdash \phi$. We need to show that for all $\rho \models \Gamma \vdash \lambda a.\ M : \forall a.\ \phi$, $\overline{(\lambda a.\ M)}[\rho] \Vdash_\rho \forall a.\ \phi$. This is equivalent to $\lambda a.\ \overline{M}[\rho] \Vdash_\rho \forall a.\ \phi$. Take any such ρ. We need to show that $\forall A, t.\ \overline{M}[\rho][a := t] \Vdash_\rho \phi[a := A]$. Take any A and t. Since $\rho[a := (t, A)] \models \Gamma \vdash M : \phi$ and by Lemma 7.3 $\overline{M}[\rho][a := t] = \overline{M}[\rho[a := (t, A)]]$, we get the claim by the inductive hypothesis.
- $$\frac{\Gamma \vdash M : \forall a.\ \phi}{\Gamma \vdash M\ t : \phi[a := t]}$$
  By the inductive 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 $N[a := t[\rho]] \Vdash_\rho \phi[a := [\![t]\!]_\rho]$. By Lemma 6.11, $N[a := t[\rho]] \Vdash_\rho \phi[a := t]$. Since $M'\ (t[\rho]) \to^* (\lambda a.\ N)\ t[\rho] \to N[a := t[\rho]]$, Lemma 6.13 gives us the claim.
- $$\frac{\Gamma \vdash M : \phi[a := t]}{\Gamma \vdash [t, M] : \exists a.\ \phi}$$
  By the inductive hypothesis, $M' \Vdash_\rho \phi[a := t]$, so by Lemma 6.11, $M' \Vdash_\rho \phi[a := [\![t]\!]_\rho]$. Thus, there is a lambda-name A, namely $[\![t]\!]_\rho$, such that $M' \Vdash_\rho \phi[a := A]$. Thus, $\overline{[t, M]}[\rho] = [t[\rho], M'] \Vdash_\rho \exists a.\ \phi$ which is what we want.
- $$\frac{\Gamma \vdash M : \exists a.\ \phi \quad \Gamma, x : \phi \vdash N : \psi}{\Gamma \vdash \mathrm{let}\ [a, x : \phi] := M \text{ in } N : \psi}\ a \notin FV(\Gamma, \psi)$$
  Let $\rho \models \Gamma \vdash \mathrm{let}\ [a, x : \phi] := M \text{ in } N : \psi$. We need to show $\overline{\mathrm{let}\ [a, x : \phi] := M \text{ in } N}[\rho] = \mathrm{let}\ [a, x] := M' \text{ in } \overline{N}[\rho] \Vdash_\rho \psi$. By the inductive 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 inductive 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 6.14 $\overline{N}[\rho'] \Vdash_\rho \psi$. Now, let $[a, x : \phi] := M'$ in $\overline{N}[\rho] \to^*$ let $[a, x] := [t, M_1]$ in $\overline{N}[\rho] \to \overline{N}[\rho][a := t][x := M_1] = \overline{N}[\rho']$. Lemma 6.13 gives us the claim.

- $$\frac{\Gamma \vdash M : \forall d.\ (d \in_I t \to d \in u) \land (d \in_I u \to d \in t)}{\Gamma \vdash \mathrm{eqRep}(t, u, M) : t = u}$$
  By the inductive hypothesis, $M' \Vdash_\rho \forall d.\ (d \in_I t \to d \in u) \land (d \in_I u \to d \in t)$. By Lemma 6.11, $M' \Vdash_\rho \forall d.\ (d \in_I [\![t]\!]_\rho \to d \in [\![u]\!]_\rho) \land (d \in_I [\![u]\!]_\rho \to d \in [\![t]\!]_\rho)$. By Lemma 6.17, $\mathrm{eqRep}(M') \Vdash_\rho [\![t]\!]_\rho = [\![u]\!]_\rho$. Lemma 6.11 applied again gives us the claim.
  $$\frac{\Gamma \vdash M : t = u}{\Gamma \vdash \mathrm{eqProp}(t, u, M) : \forall d.\ (d \in_I t \to d \in u) \land (d \in_I u \to d \in t)}$$
  By the inductive hypothesis, $M' \Vdash_\rho t = u$. By Lemma 6.11, $M' \Vdash_\rho [\![t]\!]_\rho = [\![u]\!]_\rho$. By Lemma 6.17, $M' \downarrow \mathrm{eqRep}(N)$ and $N \Vdash_\rho \forall d.\ (d \in_I [\![t]\!]_\rho \to d \in [\![u]\!]_\rho) \land (d \in_I [\![u]\!]_\rho \to d \in [\![t]\!]_\rho)$. Since $\overline{\mathrm{eqProp}(t, u, M)} = \mathrm{eqProp}(M') \to^* \mathrm{eqProp}(\mathrm{eqRep}(N)) \to N$, by Lemma 6.13 $\overline{\mathrm{eqProp}(t, u, M)} \Vdash_\rho \forall d.\ (d \in_I [\![t]\!]_\rho \to d \in [\![u]\!]_\rho) \land (d \in_I [\![u]\!]_\rho \to d \in [\![t]\!]_\rho)$. Lemma 6.11 applied once again gives us the claim.
- For inProp and inRep, the proof is similar to the two previous cases.
- $$\frac{\Gamma \vdash M : \phi_A(t, \vec{u})}{\Gamma \vdash \mathrm{axRep}(t, \vec{u}, M) : t \in_I t_A(\vec{u})}$$
  By the inductive hypothesis, $M' \Vdash_\rho \phi_A(t, \vec{u})$. By Lemma 6.11 this is equivalent to $M' \Vdash_\rho \phi_A([\![t]\!]_\rho, \overrightarrow{[\![u]\!]_\rho})$. By Lemma 6.31 $(\mathrm{axRep}(M'), [\![t]\!]_\rho) \in [\![t_A(\vec{u})]\!]_\rho$, so $\mathrm{axRep}(M') \Vdash_\rho t \in_I t_A(\vec{u})$.
- $$\frac{\Gamma \vdash M : t \in_I t_A(\vec{u})}{\Gamma \vdash \mathrm{axProp}(t, \vec{u}, M) : \phi_A(t, \vec{u})}$$
  By the inductive hypothesis, $M' \Vdash_\rho t \in_I t_A(\vec{u})$. This means that $M' \downarrow v$ and $(v, [\![t]\!]_\rho) \in [\![t_A(\vec{u})]\!]_\rho$. By Lemma 6.31, $v = \mathrm{axRep}(N)$ and $N \Vdash_\rho \phi_A([\![t]\!]_\rho, \overrightarrow{[\![u]\!]_\rho})$. By Lemma 6.11, $N \Vdash_\rho \phi_A(t, \vec{u})$. Moreover, $\overline{\mathrm{axProp}(t, \vec{u}, M)} = \mathrm{axProp}(M') \to^* \mathrm{axProp}(\mathrm{axRep}(N)) \to N$. Lemma 6.13 gives us the claim.
- $$\frac{\Gamma \vdash M : \forall c.\ (\forall b.\ b \in_I c \to \phi(b, \vec{t})) \to \phi(c, \vec{t})}{\Gamma \vdash \mathrm{ind}(M, \vec{t}) : \forall a.\ \phi(a, \vec{t})}$$
  Since $\mathrm{ind}(M')$ reduces to $\lambda c.\ M'\ c\ (\lambda b.\ \lambda x.\ \mathrm{ind}(M')\ b)$, by Lemma 6.13 it suffices to show that for all C, t, $M'\ t\ (\lambda b.\ \lambda x.\ \mathrm{ind}(M')\ b) \Vdash_\rho \phi(C, \vec{t})$. We proceed by induction on λ-rank of C. Take any C, t. By the inductive hypothesis, $M' \Vdash_\rho \forall c.\ (\forall b.\ b \in_I c \to \phi(b, \vec{t})) \to \phi(c, \vec{t})$, so $M' \downarrow \lambda c.\ N$ and $N[c := t] \Vdash_\rho \forall b.\ b \in_I C \to \phi(b, \vec{t})$. By Lemma 6.15, it suffices to show that $\lambda b.\ \lambda x.\ \mathrm{ind}(M')\ b \Vdash_\rho \forall b.\ b \in_I C \to \phi(b, \vec{t})$. Take any B, u, $O \Vdash_\rho B \in_I C$, we need to show that $\mathrm{ind}(M')[x := O]\ u \Vdash_\rho \phi(B, \vec{t})$. As $x \notin FV(M')$, it suffices to show that $\mathrm{ind}(M')\ u \Vdash_\rho \phi(B, \vec{t})$, which, by Lemma 6.13, is equivalent to $M'\ u\ (\lambda b.\ \lambda x.\ \mathrm{ind}(M')\ b) \Vdash_\rho \phi(B, \vec{t})$. As $O \Vdash_\rho B \in_I C$, the λ-rank of B is less than the λ-rank of C and we get the claim by the inductive hypothesis. □

Corollary 7.5 (Normalization)**.** *If* $\vdash M : \phi$*, then* $M \downarrow$*.*

Proof. Take ρ mapping all free propositional variables of M to themselves and all free first-order variables a of M to $(a, \emptyset)$. Then $\rho \models\vdash M : \phi$. By Theorem 7.4, $\overline{M}[\rho]$ normalizes. By the definition of ρ, $\overline{M}[\rho] = \overline{M}$. By Lemma 6.1, M normalizes. □

As the reduction system is deterministic, the distinction between strong and weak normalization does not exist. If the reduction system is extended to allow reductions anywhere inside the term, the Corollary 7.5 shows only weak normalization. The counterexamples from [Moc06a] adapted to λZ_ω show that $\mathrm{IZF}_{R\omega}$ does not strongly normalize and that non-well-founded version does not normalize at all.

Our method of carrying the normalization proof is very different from the standard approach, based on Girard's method of candidates [GTL89]. As the candidates method is usually used to show strong normalization of formal systems, it is unclear if it could be applied to $\mathrm{IZF}_{R\omega}$, given that it does not strongly normalize. Although it might be possible to restate the realizability relation in terms closer to the candidates method, we believe our account is easier to understand and closer to its roots [McC84]. We will show how to apply our method to show normalization of several weaker systems in the forthcoming [Moc07].

The normalization theorem immediately provides the standard properties of constructive set theories — the disjunction property, the term existence property, the set existence property and the numerical existence property. Proofs are the same as in [Moc06a]; we only show the proofs of TEP and SEP.

Corollary 7.6 (Term Existence Property)**.** *If* $IZF_{R\omega} \vdash \exists x.\ \phi(x)$*, then there is a term* t *such that* $IZF_{R\omega} \vdash \phi(t)$*.*

Proof. By the Curry-Howard isomorphism, there is a λZ_ω-term M such that $\vdash M : \exists x.\ \phi$. By Corollary 5.8, $M \downarrow v$ and $\vdash v : \exists x.\ \phi$. By Canonical Forms, there is a pair $[t, N]$ such that $\vdash N : \phi(t)$. Therefore, by the Curry-Howard isomorphism, $\mathrm{IZF}_{R\omega} \vdash \phi(t)$. □

Corollary 7.7 (Set Existence Property)**.** *If* $IZF_{R\omega} \vdash \exists x.\ \phi(x)$ *and* ϕ *is term-free, then there is a term-free formula* $\psi(x)$ *such that* $IZF_{R\omega} \vdash \exists! x.\ \phi(x) \land \psi(x)$*.*

Proof. By the previous corollary we have $\mathrm{IZF}_{R\omega} \vdash \phi(t)$ for some term t. Moreover, for any $\mathrm{IZF}_{R\omega}$ term s, there is a term-free defining formula $\psi_s(x)$ such that $\mathrm{IZF}_{R\omega} \vdash \psi_s(s) \land \exists! x.\ \psi_s(x)$. Therefore $\mathrm{IZF}_{R\omega} \vdash \exists! x.\ \phi(x) \land \psi_t(x)$. □

In [CM06] we have shown how to use DP, NEP and TEP for the purpose of program extraction. Thus our results establish $\mathrm{IZF}_{R\omega}$ as a valid basis for a prover based on set theory with inaccessibles with the capability of program extraction from constructive proofs.

8. Related work

Several normalization results for impredicative constructive set theories much weaker than IZF 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 PTS (Pure Type System) [Miq04], where he also showed strong normalization of the calculus. This result was later extended — Dowek and Miquel [DM06] interpreted a version of constructive Zermelo set theory in a strongly normalizing *deduction-modulo* system.

In [Miq03], Miquel interpreted IZF_C without the $\in$-induction axiom in a strongly-normalizing lambda calculus with types based on $F\omega.2$. It is unclear if Miquel's techniques could be used to prove any of DP, NEP, SEP and TEP for the theory or to provide interpretations of ECC or CIC.

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

The standard metamathematical properties of theories related to IZF are well investigated. Myhill [Myh73] showed DP, NEP, SEP and TEP for IZF with Replacement and non-recursive list of set terms. Friedman and Ŝĉedrov [FS83] showed SEP and TEP for an extension of that theory with countable choice axioms. Recently DP and NEP were shown for IZF with Collection extended with various choice principles by Rathjen [Rat06]. However, the technique does not seem to be strong enough to provide TEP and SEP.

Powerful large set axioms (including the existence of class-many inaccessibles) were added to IZF with Collection by Friedman and Ŝĉedrov [FS84]. The notion of an inaccessible set they use differs from ours, as their inaccessibles must also model the Collection axiom. We do not know if these two notions coincide. Both DP and NEP was shown for the resulting theories, but we do not think that SEP and TEP could be proved with their technique.

Inaccessible sets were also investigated in the context of weaker, predicative CZF (Constructive Zermelo-Fraenkel). Crosilla and Rathjen [CR02] showed that the power of inaccessible set axioms might be closely linked to the $\in$-induction axiom. They proved that inaccessible sets added to CZF with $\in$-induction taken away do not add any proof-theoretical power.

Acknowledgements

I would like to thank my advisor, Bob Constable, for comments and support, Richard Shore for helpful discussions, David Martin for commenting on the early stages of this research and anonymous referees for their comments.

References

[Acz99] Peter Aczel. On relating type theories and set theories. In *TYPES '98: Selected papers from the International Workshop on Types for Proofs and Programs*, pages 1–18, London, UK, 1999. Springer-Verlag.

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

[BBS+98] H. Benl, U. Berger, H. Schwichtenberg, et al. Proof theory at work: Program development in the Minlog system. In W. Bibel and P. G. Schmitt, editors, *Automated Deduction*, volume II. Kluwer, 1998.

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

[C+86] Robert L. Constable et al. *Implementing Mathematics with the Nuprl Proof Development System*. Prentice-Hall, NJ, 1986.

[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 *LNCS*, pages 162–176. Springer, 2006.

[Coq] Catarina Coquand. Agda. Available from http://www.cs.chalmers.se/~catarina/agda.

[CR02] L. Crosilla and Michael Rathjen. Inaccessible set axioms may have little consistency strength. *Ann. Pure Appl. Logic*, 115(1-3):33–70, 2002.

[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 Ŝĉedrov. Set existence property for intuitionistic theories with countable choice. *Annals of Pure and Applied Logic*, 25:129–140, 1983.

[FS84] Harvey Friedman and Andre Ŝĉedrov. Large sets in intuitionistic set theory. *Annals of Pure and Applied Logic*, 27:1–24, 1984.

[GTL89] J-Y. Girard, P. Taylor, and Y. Lafont. *Proofs and Types*, volume 7 of *Cambridge Tracts in Computer Science*. Cambridge University Press, 1989.

[Hal] Thomas Hallgren. Alfa. Available from http://www.cs.chalmers.se/~hallgren/Alfa.

[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.

[LP92] Z. Luo and R. Pollack. LEGO proof development system: User's manual. Technical Report ECS-LFCS-92-211, University of Edinburgh, 1992.

[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 *Proc. of 12th Ann. Conf. of the EACSL (CSL 2003)*, volume 2803 of *LNCS*, 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 IZF with Replacement. In *Proc. 15th Ann. Conf. of the EACSL (CSL 2006)*, volume 4207 of *Lecture Notes in Computer Science*. Springer, 2006.

[Moc06b] Wojciech Moczydłowski. A Normalizing Intuitionistic Set Theory with Inaccessible Sets. Technical Report TR2006-2051, Cornell University, 2006.

[Moc07] Wojciech Moczydłowski. *Investigations on Sets and Types*. PhD thesis, Cornell University, August 2007. To appear.

[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.

[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.

[The04] The Coq Development Team. *The Coq Proof Assistant Reference Manual – Version V8.0*, April 2004.

[Š85] Andre Ščedrov. Intuitionistic set theory. In *Harvey Friedman's Research on the Foundations of Mathematics*, pages 257–284. Elsevier, 1985.

[Wer97] Benjamin Werner. Sets in types, types in sets. In *TACS '97: Proc. of the 3rd Int. Symposium on Theoretical Aspects of Computer Software*, pages 530–546. Springer-Verlag, 1997.