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 \(\omega\)-many inaccessibles, which we call 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 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 \(\Pi\) and \(\Sigma\) 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 \(\forall x : \text{nat}, \phi(x)\) 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.
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 [885, Bee85]. We have defined a lambda calculus $\lambda Z$ corresponding to proofs in an intensional version of IZF$_R$ and using realizability we have shown that $\lambda Z$ 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 $\omega$-many strongly inaccessible cardinals [Wer97, Acz99].

We therefore axiomatize IZF with Replacement and $\omega$-many inaccessible sets, which we call IZF$_{R\omega}$. Our axiomatization uses an inductive definition of inaccessible sets. IZF$_{R\omega}$ extended with excluded middle is equivalent to ZF with $\omega$-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 $\lambda Z_{\omega}$ corresponding directly to proofs in 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 interpretation of a universe [Wer97, Acz99]. Both CIC and ECC have $\omega$-many universes. By results of Aczel [Acz99], 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 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 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 \( \omega \)-many inaccessibles in sections 3 and 4. In section 5 we define the calculus \( \lambda Z_\omega \) 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 \( \alpha \)-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 \( t[a_1, ..., a_n := s_1, ..., s_n] \) to denote the result of substituting simultaneously \( s_1, ..., s_n \) for \( a_1, ..., a_n \).

Contexts, denoted by \( \Gamma \), are sets of formulas. The free variables of a formula \( \phi \), denoted by \( \text{FV}(\phi) \), are defined as usual. The free variables of a context \( \Gamma \), denoted by \( \text{FV}(\Gamma) \), are the free variables of all formulas in \( \Gamma \). The notation \( \phi(\vec{a}) \) means that all free variables of \( \phi \) are among \( \vec{a} \). The proof rules are as follows:

- \( \Gamma, \phi \vdash \psi \rightarrow \phi \rightarrow \psi \)
- \( \Gamma \vdash \phi \rightarrow \psi \rightarrow \Gamma \vdash \phi \rightarrow \psi \)
- \( \Gamma \vdash \phi \land \psi \rightarrow \phi \land \psi \rightarrow \Gamma \vdash \phi \land \psi \)
- \( \Gamma \vdash \phi \lor \psi \rightarrow \phi \lor \psi \rightarrow \Gamma \vdash \phi \lor \psi \)
- \( \Gamma \vdash \phi \rightarrow \psi \rightarrow \Gamma, \phi \vdash \psi \rightarrow \Gamma, \psi \vdash \psi \)
- \( \Gamma \vdash \forall a. \phi \rightarrow a \notin \text{FV}(\Gamma) \rightarrow \Gamma \vdash \forall a. \phi \rightarrow \Gamma \vdash \phi \)
- \( \Gamma \vdash \exists a. \phi \rightarrow a \notin \text{FV}(\Gamma) \rightarrow \Gamma \vdash \exists a. \phi \rightarrow \Gamma \vdash \phi \)

Negation in IFOL is an abbreviation: \( \neg \phi \equiv \phi \rightarrow \bot \). So is the symbol \( \leftrightarrow : \phi \leftrightarrow \psi \equiv (\phi \rightarrow \psi \land \psi \rightarrow \phi) \). Note that IFOL does not contain equality. The excluded middle rule added to IFOL makes it equivalent to the classical first-order logic without equality.

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

Proof. Straightforward structural induction on \( \phi \). \( \square \)

3. IZF_{\text{Rω}}^-

In this section we introduce our first approximation to IZF\(_R\), called IZF\(_R^\omega\), which is IZF\(_R\) from \[\text{Moc06a}\] 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) \( \forall a, b. a = b \iff \forall c. c \in a \leftrightarrow c \in b \)
• (L_\phi) \( \forall a, b, \vec{f}. a = b \land \phi(a, \vec{f}) \rightarrow \phi(b, \vec{f}) \)
• (EMPTY) \( \forall c. c \in \emptyset \leftrightarrow \bot \)
• (PAIR) \( \forall a, b \forall c. c \in \{a, b\} \leftrightarrow c = a \lor c = b \)
• (INF) \( \forall c. c \in \omega \leftrightarrow c = 0 \lor \exists b \in \omega. c = S(b) \)
• (SEP_\phi) \( \forall \vec{f} \forall a \forall c. c \in S_\phi(a, \vec{f}) \leftrightarrow c \in a \land \phi(c, \vec{f}) \)
• (UNION): \( \forall a \forall c. c \in \bigcup a \leftrightarrow \exists b \in a. c \in b \)
• (POWER) \( \forall a \forall c. c \in P(a) \leftrightarrow \forall b. b \in c \rightarrow b \in a \)
• (REPL_\phi) \( \forall \vec{f}, a \forall c. c \in R_\phi(a, \vec{f}) \leftrightarrow (\forall x \in a \exists! y. \phi(x, y, \vec{f})) \land (\exists x \in a. \phi(x, c, \vec{f})) \)
• (IND_\phi) \( \forall \vec{f}. (\forall b. (\forall x \in a. \phi(b, \vec{f})) \rightarrow \phi(a, \vec{f})) \rightarrow \forall a. \phi(a, \vec{f}) \)

The axioms (SEP_\phi), (REPL_\phi), (IND_\phi) and (L_\phi) are axiom schemes — there is one axiom for each formula \( \phi \). Note that there are terms \( S_\phi \) and \( R_\phi \) for each instance of the Separation and Replacement axioms. Formally, terms and formulas are defined by mutual induction:

\[
\phi ::= t \in t \mid t = t \mid \ldots \\
\text{t ::= a } \mid \{t, t\} \mid S_\phi(t, \vec{t}) \mid R_\phi(t, \vec{t}) \mid \ldots
\]

The axioms (EMPTY), (PAIR), (INF), (SEP_\phi), (UNION), (POWER) and (REPL_\phi) all assert the existence of certain classes and have the same form: \( \forall \vec{a} \forall c. c \in t_\phi(\vec{a}) \leftrightarrow \phi_\phi(c, \vec{a}) \), where \( t_\phi \) is a function symbol and \( \phi_\phi \) a corresponding formula for the axiom (A). For example, for (POWER), \( t_\text{POWER} \) is \( P \) and \( \phi_\text{POWER} \) is \( \forall b. b \in c \rightarrow b \in a \). We reserve the notation \( t_\phi \) and \( \phi_\phi \) 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 \( \{c \mid (\forall x \in t \exists! y. \phi(x, y, \vec{t})) \land (\exists x \in t. \phi(x, c, \vec{t}))\} \), respectively.

3.1. On the axioms of IZF_R.

3.1.1. The Leibniz axiom. The Leibniz axiom (L_\phi) 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_\phi) 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 (REPL_0_\phi), let \( (R_\phi) \) be the term-free statement of our Replacement axiom, that is:

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

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_\phi) \rightarrow (REPL_0_\phi).
Proof. Assume \((R_\phi)\), 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 \((R_\phi)\). 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 \((\text{REPL0}_\phi)\).

Lemma 3.2. \(\text{IZF} \vdash (\\text{REPL0}_\phi) \rightarrow (R_\phi)\).

Proof. Assume \((\text{REPL0}_\phi)\), 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 \((\text{REPL0}_\phi)\) 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 \(\forall a \exists! d \forall c. c \in d \leftrightarrow \phi_A(c, a)\), 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 \(\forall a \forall c. c \in t_{A}(\vec{a}) \leftrightarrow \phi_A(c, \vec{a})\).

We then need to provide the Separation and Replacement function symbols \(R_\phi\) and \(S_\phi\), where \(\phi\) may contain the new terms. To fix our attention, consider the Separation axiom. For some function symbol \(S_\phi\), we need to have:

\[ \forall \vec{f}, \forall c. c \in S_\phi(a, \vec{f}) \Leftrightarrow c \in a \land \phi(c, \vec{f}) \]

As all terms present in \(\phi\) were introduced via a definitional extension of IZF\(_R0\), there is a term-free formula \(\phi'\) equivalent to \(\phi\). We therefore have:

\[ \forall \vec{f}, \forall c. c \in S_\phi'(a, \vec{f}) \Leftrightarrow c \in a \land \phi'(c, \vec{f}) \]

and consequently:

\[ \forall \vec{f}, \forall c. c \in S_{\phi'}(a, \vec{f}) \Leftrightarrow c \in a \land \phi(c, \vec{f}) \]

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

It remains to derive the Leibniz and \(\varepsilon\)-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 \(\phi'\) equivalent to \(\phi\), 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 \(\varepsilon\)-Induction axiom, take any \(\vec{F}\) and suppose:

\[ \forall a. (\forall b \in a. \phi(b, \vec{F})) \rightarrow \phi(a, \vec{F}) \]
Taking $\phi'$ to be the term-free formula equivalent to $\phi$, we get:

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

By $\in$-Induction in $\text{IZF}_R\omega$, we get $\forall a. \phi'(a, \vec{F})$, thus also $\forall a. \phi(a, \vec{F})$.

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

$$(\text{INAC}_i) \forall c. c \in V_i \leftrightarrow \phi_1^i(c, V_i) \land \forall d. \phi_2^i(d) \rightarrow c \in d$$

Following the conventions set up for $\text{IZF}_R$, $\phi_{\text{INAC}_i}(c)$ is $\phi_1^i(c, V_i) \land \forall d. \phi_2^i(d) \rightarrow c \in d$. The formula $\phi_1^i(c, d)$ intuitively sets up conditions for $c$ being a member of $V_i$, while $\phi_2^i(d)$ says what it means for $d$ to be inaccessible. To streamline the definition, we set $V_0$ to abbreviate $\omega$.

**Definition 3.3.** The formula $\phi_1^i(c, V_i)$ 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 $\phi_2^i(d)$ for $i > 0$ is a conjunction of the following five clauses:

1. $V_{i-1} \in d$.
2. $\forall e, f. e \in d \land f \in e \rightarrow f \in d$.
3. $\forall e \in d. \bigcup e \in d$.
4. $\forall e \in d. P(e) \in d$.
5. $\forall e \in d. \forall f \in e \rightarrow f \in d. f \in d$, where $e \rightarrow d$ 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 $\text{IZF}_R^- \cup \text{EM}$ is equivalent to $\text{ZF}$ with $\omega$-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 $(\text{INAC}_i)$ behaves as an inaccessible set in $\text{IZF}_{R\omega}^-$ we prove:

**Theorem 3.5 (IZF_{R\omega}^-).** For all $i > 0$, $V_i \models \text{IZF}_R + M(\text{IZF}_R) + M(\text{IZF}_R + M(\text{IZF}_R)) + \ldots$ (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 $\Delta_0$, $V_1 \models (\text{INF})$. 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_\phi). The existence of the empty set follows by (INF) and (SEP). For the Induction axiom, we need to show:

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

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

$$\forall a. a \in V_i \rightarrow (\forall b. b \in V_i \rightarrow b \in a \rightarrow \phi^{V_i}(b, \vec{F})) \rightarrow \phi^{V_i}(a, \vec{F})) \rightarrow \forall a. a \in V_i \rightarrow \phi^{V_i}(a, \vec{F})$$
This is equivalent to:
\[(\forall a. (\forall b. b \in a \rightarrow b \in V_i \rightarrow \phi^{V_i}(b, \vec{F})) \rightarrow a \in V_i \rightarrow \phi^{V_i}(a, \vec{F})) \rightarrow \forall a. a \in V_i \rightarrow \phi^{V_i}(a, \vec{F})\]
But this is the instance of the induction axiom for the formula \(a \in V_i \rightarrow \phi^{V_i}(a, \vec{F})\).

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

4. \(\text{IZF}_{R\omega}\)

We now present our final axiomatization of IZF with Replacement and inaccessible sets, which we call \(\text{IZF}_{R\omega}\). 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 \(\text{IZF}_{R\omega}\) consists of three relational symbols: \(\in_I, \in, =\) and terms of \(\text{IZF}_{R\omega}\). The axioms of \(\text{IZF}_{R\omega}\) are as follows:

- (IN) \(\forall a, b. a \in b \leftrightarrow \exists c. c \in_I b \land a = c\)
- (EQ) \(\forall a, b. a = b \leftrightarrow \forall d. (d \in_I a \rightarrow d \in b) \land (d \in_I b \rightarrow d \in a)\)
- (IND_\phi) \(\forall \vec{F}, \forall a. (\forall b. b \in I a \rightarrow \phi(a, \vec{F})) \rightarrow \phi(a, \vec{F}) \rightarrow \forall a. \phi(a, \vec{F})\)
- (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: \(\forall a. \forall c. c \in_I P(a) \leftrightarrow \forall b. b \in c \rightarrow b \in a\).

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 \(\text{IZF}_{R\omega}\). From now on in this section, we work in \(\text{IZF}_{R\omega}\). 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 \(b \in a\). \(\square\)

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. Straightforward. \(\square\)
Lemma 4.4. For all $b, a, c$, if $a = b$ and $b = c$, then $a = c$.

Proof. By $\epsilon$-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 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 $\phi$. We show some representative cases. Case $t$ or $\phi$ 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 $t_1(a) = t_1(b)$, so by Lemma 4.6, $d \in_t b$, so $c \in_I t_1(b)$ 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 $c \in S_\phi(t_1(b), \vec{u}(b))$ 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 $\phi(c, \vec{f})$, 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_ω}, IZF_{Rω} ⊨ A.

Proof. Lemmas 4.7, 4.8 and 4.9 show the claim for all the axioms apart from (IND). Lemma 4.10. For any axiom
suppose that \( \forall a. (\forall b \in a. \phi(b, \tilde{f})) \rightarrow \phi(a, \tilde{f}) \). We need to show \( \forall a. \phi(a, \tilde{f}) \). We proceed by \( \in_I \)-induction on a. It suffices to show \( \forall c. (\forall d \in_I c. \phi(d, \tilde{f})) \rightarrow \phi(c, \tilde{f}) \). Take any c and suppose \( \forall d \in_I c. \phi(d, \tilde{f}) \). We need to show \( \phi(c, \tilde{f}) \). Take a to be c in the assumption, so it suffices to show that \( \forall b \in c. \phi(b, \tilde{f}) \). Take any b ∈ c. Then there is e ∈ I c such that e = b. By the inductive hypothesis \( \phi(e, \tilde{f}) \) holds and hence by the Leibniz axiom we get \( \phi(b, \tilde{f}) \), which shows the claim. \( \square \)

Corollary 4.11. If IZF_{R_ω} ⊨ \phi, then IZF_{Rω} ⊨ \phi.

Lemma 4.12. If IZF_{Rω} ⊨ \phi and \( \phi \) does not contain \( \in_I \), then IZF_{Rω} ⊨ \phi.

Proof. Working in IZF_{Rω}, simply interpret \( \in_I \) as \( \in \) to see that all axioms of IZF_{Rω} are valid and that if IZF_{Rω} ⊨ \phi, then IZF_{Rω} ⊨ \phi(\in_I := \in). \( \square \)

Therefore IZF_{Rω} is a legitimate axiomatization of IZF with Replacement and inaccessible sets. From now on the names of the axioms refer to the axiomatization of IZF_{Rω}.

5. The \( \lambda Z_\omega \) calculus

We now introduce a lambda calculus \( \lambda Z_\omega \) for IZF_{R_ω}, based on the Curry-Howard isomorphism principle. The part of \( \lambda Z_\omega \) corresponding to the first-order logic is essentially \( \lambda P_1 \) from SU06. The rest of the calculus, apart from clauses corresponding to (IN), (EQ) and (INAC_i) axioms, is identical to \( \lambda Z \) from Moc06.

5.1. The terms of \( \lambda Z_\omega \). The lambda terms in \( \lambda Z_\omega \) will be denoted by letters \( M, N, O, P \). There are two kinds of lambda abstraction in \( \lambda Z_\omega \), 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 IZF_{Rω} terms. The types in the system are IZF_{Rω} formulas. The terms are generated by the following abstract grammar:

\[
M ::= x \mid M \ N \mid \lambda a. M \mid \lambda x : \phi. M \mid \text{in}(M) \mid \text{inr}(M) \mid \text{fst}(M) \mid \text{snd}(M) \mid t, M \mid \langle M, N \rangle \mid \text{case}(M, x : \phi. N, x : \psi. O) \mid \text{magic}(M) \mid \text{let } [a, x : \phi] := M \text{ in } N \\
\text{ind}_{\phi(a, \tilde{g})}(M, \tilde{f}) \mid \text{inac}_r \text{Prop}(t, M) \mid \text{inac}_r \text{Rep}(t, M) \\
\text{pairProp}(t, u_1, u_2, M) \mid \text{eqProp}(t, u_1, M) \mid \text{eqProp}(t, u_1, M) \\
\text{powerProp}(t, u, M) \mid \text{powerProp}(t, u_1, u_2, M) \mid \text{unionProp}(t, u_1, M) \mid \text{unionRep}(t, u_1, M) \\
\text{sep}_{\phi(a, \tilde{f})} \text{Prop}(t, u, \tilde{u}, M) \mid \text{sep}_{\phi(a, \tilde{f})} \text{Prop}(t, u, \tilde{u}, M) \mid \text{powerProp}(t, u, M) \mid \text{powerRep}(t, u, M) \\
\text{inProp}(t, M) \mid \text{inRep}(t, M) \mid \text{repl}_{\phi(a, \tilde{f})} \text{Prop}(t, u, \tilde{u}, M) \mid \text{repl}_{\phi(a, \tilde{f})} \text{Rep}(t, u, \tilde{u}, M)
\]

The \( \text{ind} \) terms correspond to the (IND) axiom, Prop and Rep terms correspond to the respective axioms of IZF_{Rω} 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 \text{axRep} and \text{axProp} terms to tacitly
mean all Rep and Prop terms, for ax being one of in, eq, pair, union, sep, power, inf, repl and inac, unless we list some of them separately. With this convention in mind, we can summarize the definition of the Prop and Rep terms as:

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

where the number of terms in the sequence \( \vec{u} \) depends on the particular axiom.

The free variables of a lambda term are defined as usual, taking into account that variables in \( \lambda \), case and let terms bind respective terms. The relation of \( \alpha \)-equivalence is defined taking this information into account. We consider \( \alpha \)-equivalent terms equal. We denote all free variables of a term \( M \) by \( \text{FV}(M) \) and the free first-order variables of a term by \( \text{FV}_F(M) \). The free (first-order) variables of a context \( \Gamma \) are denoted by \( \text{FV}(\Gamma) \) and defined in a natural way.

5.2. The reduction relation. The deterministic reduction relation \( \rightarrow \) arises from the following reduction rules and evaluation contexts:

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

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

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

\[
\begin{align*}
\langle c \rangle & := \text{fst}(\langle c \rangle) \mid \text{snd}(\langle c \rangle) \mid \text{case}(\langle c \rangle, x.N, x.O) \\
\text{axProp}(t, \vec{u}, \langle c \rangle) \mid \text{let } [a, x : \phi] := [c] \text{ in } N \mid \langle c \rangle \ M \mid \text{magic}(\langle c \rangle)
\end{align*}
\]

We distinguish certain \( \lambda Z_\omega \) 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.

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

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 \( M \rightarrow^* M' \) if \( M \) reduces to \( M' \) in some number of steps.
5.3. The types of $\lambda Z_\omega$. The type system for $\lambda Z_\omega$ is constructed according to the principle of the Curry-Howard isomorphism for IZF$_{R\omega}$. Types are IZF$_{R\omega}$ formulas, and terms are $\lambda Z_\omega$ terms. Contexts $\Gamma$ are finite sets of pairs $(x_i,\phi_i)$. The first set of rules corresponds to first-order logic.

\[
\begin{array}{llll}
\Gamma, x : \phi \vdash x : \phi & \Gamma \vdash M : \phi \rightarrow \psi & \Gamma \vdash N : \phi & \Gamma, x : \phi \vdash M : \psi \\
\hline
\Gamma \vdash M : \phi & \Gamma \vdash N : \psi & \Gamma \vdash M : \phi \land \psi & \Gamma \vdash \lambda x : \phi. M : \phi \rightarrow \psi \\
\Gamma \vdash \langle M, N \rangle : \phi \land \psi & \Gamma \vdash \text{fst}(M) : \phi & \Gamma \vdash \text{snd}(M) : \psi & \\
\Gamma \vdash M : \phi & \Gamma \vdash M : \psi & \\
\Gamma \vdash \text{inl}(M) : \phi \lor \psi & \Gamma \vdash \text{inr}(M) : \phi \lor \psi & \\
\Gamma \vdash M : \phi \lor \psi & \Gamma, x : \phi \vdash N : \phi & \Gamma, x : \psi \vdash O : \phi & \\
\Gamma \vdash \text{case}(M, x : \phi, N, x : \psi, O) : \phi \\
\end{array}
\]

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

\[
\begin{array}{llll}
\Gamma \vdash M : \forall d. (d \in I t \rightarrow d \in u) \land (d \in I u \rightarrow d \in t) & \\
\Gamma \vdash \text{eqRep}(t, u, M) : t = u & \Gamma \vdash M : t = u \\
\Gamma \vdash \text{eqProp}(t, u, M) : \forall d. (d \in I t \rightarrow d \in u) \land (d \in I u \rightarrow d \in t) & \Gamma \vdash t \in u \\
\Gamma \vdash \text{inRep}(t, u, M) : t \in u & \Gamma \vdash \text{inProp}(t, u, M) : \exists c. c \in I u \land t = c \\
\Gamma \vdash M : \phi(t, \bar{u}) & \Gamma \vdash M : t \in I t_A(\bar{u}) & \\
\Gamma \vdash \text{axRep}(t, \bar{u}, M) : t \in I t_A(\bar{u}) & \Gamma \vdash \text{axProp}(t, \bar{u}, M) : \phi_A(t, \bar{u}) & \\
\Gamma \vdash M : \forall c. (\forall b. b \in I c \rightarrow \phi(b, \bar{t}) \rightarrow \phi(c, \bar{t}) & \Gamma \vdash \text{ind}_{\phi(a, \bar{t})}(M, \bar{t}) : \forall a. \phi(a, \bar{t}) \\
\end{array}
\]

5.4. The properties of $\lambda Z_\omega$. We now proceed with a standard sequence of lemmas for $\lambda Z_\omega$.

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

- $\varnothing = t \in I t_A(\bar{u})$ iff $M = \text{axRep}(t, \bar{u}, N)$ and $\vdash N : \phi_A(t, \bar{u})$.
- $\varnothing = \phi \lor \psi$ iff $(M = \text{inl}(N)$ and $\vdash N : \phi)$ or $(M = \text{inr}(N)$ and $\vdash N : \psi)$.
- $\varnothing = \phi \land \psi$ iff $M = \langle N, O \rangle$, $\vdash N : \phi$ and $\vdash O : \psi$.
- $\varnothing = \phi \rightarrow \psi$ iff $M = \lambda x : \phi. N$ and $\vdash x : \phi$.
- $\varnothing = \forall a. \phi$ iff $M = \lambda a. N$ and $\vdash N : \phi$.
- $\varnothing = \exists a. \phi$ iff $M = [t, N]$ and $\vdash N : \phi[a := t]$.
- $\varnothing = \bot$ never happens.

**Proof.** Immediate from the typing rules and the definition of values. \qed
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 $\lambda Z_\omega$ corresponding to $IZF_{R\omega}$ 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. 

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

\[
\begin{array}{c}
\Gamma, x : \phi, y : \psi_1 \vdash O : \psi_2 \\
\hline
\Gamma, x : \phi \vdash \lambda y : \psi_1. O : \psi_1 \rightarrow \psi_2
\end{array}
\]

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

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

\[
\begin{array}{c}
\Gamma, x : \phi \vdash M_1 : \exists a. \psi_1 \\
\Gamma, x : \phi, y : \psi_1 \vdash M_2 : \psi_2 \\
\hline
\Gamma, x : \phi \vdash \text{let } [a, y : \psi_1] := M_1 \text{ in } M_2 : \psi_2
\end{array}
\]

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 $\Gamma \vdash \text{let } [a, y : \psi_1] := M_1[x := N] \text{ in } M_2[x := N] : \psi_2$. By $a$ and $y$ fresh, $\Gamma \vdash (\text{let } [a, y : \psi_1] := M_1 \text{ in } M_2)[x := N] : \psi_2$ which is what we want. 

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:

\[
\begin{array}{c}
\Gamma \vdash M_1 : \phi_1 \\
\hline
\Gamma \vdash \lambda b. M_1 : \forall b. \phi_1 \quad b \notin FV(\Gamma)
\end{array}
\]

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 $b$, $\Gamma[a := t] \vdash (\lambda b. M_1)[a := t] : (\forall b. \phi_1)[a := t]$.

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

\[
\begin{array}{c}
\Gamma \vdash M_1 : \forall b. \phi_1 \\
\hline
\Gamma \vdash M_1 u : \phi_1[b := u]
\end{array}
\]

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 2.4 and $b \notin FV(t)$, we get $\Gamma[a := t] \vdash (M_1 u)[a := t] : \phi_1[b := u][a := t]$. 

\[
\Box
\]
With the lemmas at hand, Progress and Preservation follow easily:

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

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

- $(\lambda x : \phi_1, M_1) M_2 \rightarrow M_1[x := M_2]$. The proof tree $\Gamma \vdash M : \phi$ must end with:

  $\Gamma, x : \phi_1 \vdash M_1 : \phi$

  $\Gamma \vdash \lambda x : \phi_1, M_1 : \phi_1 \rightarrow \phi$

  $\Gamma \vdash M_2 : \phi_1$

  $\Gamma \vdash (\lambda x : \phi_1, M_1) M_2 : \phi$

By Lemma 5.4, $\Gamma \vdash M_1[x := M_2] : \phi_1$.

- let $[a, x : \phi_1] := [t, M_1]$ in $M_2 \rightarrow M_2[a := t|x := M_1]$. The proof tree $\Gamma \vdash M : \phi$ must end with:

  $\Gamma \vdash M_1 : \phi_1[a := t]

  \Gamma \vdash [t, M_1] : \exists a. \phi_1$

  $\Gamma, x : \phi_1 \vdash M_2 : \phi$

  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, $a \notin \text{FV}(\phi)$, 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 $\Gamma \vdash M_2[a := t][x := M_1] : \phi$.

- $\text{axProp}(t, \vec{u}, \text{axRep}(t, \vec{u}, M_1)) \rightarrow M_1$. The proof tree must end with:

  $\Gamma \vdash M_1 : \phi_A(t, \vec{u})$

  $\Gamma \vdash \text{axRep}(t, \vec{u}, M_1) : t \in_I t_A(\vec{u})$

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

The claim follows immediately.

- $\text{ind}_{\psi(a, \vec{f})}(M_1, \vec{t}) \rightarrow \lambda c. M_1 c (\lambda b. \lambda x : b \in_I c. \text{ind}_{\psi(a, \vec{b})}(M_1, \vec{t}) b)$. The proof tree must end with:

  $\Gamma \vdash M_1 : \forall c. (\forall b. b \in_I c \rightarrow \psi(b, \vec{t})) \rightarrow \psi(c, \vec{t})$

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

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

$\Gamma, x : b \in_I c \vdash \text{ind}_{\psi(a, \vec{b})}(M_1, \vec{t}) b : \psi(b, \vec{t})$

Then the following proof tree shows the claim:

$\Gamma \vdash M_1 : \forall c. (\forall b. b \in_I c \rightarrow \psi(b, \vec{t})) \rightarrow \psi(c, \vec{t})$

$\Gamma \vdash M_1 c : (\forall b. b \in_I c \rightarrow \psi(b, \vec{t})) \rightarrow \psi(c, \vec{t})$

$\Gamma \vdash M_1 c (\lambda b. \lambda x : b \in_I c. \text{ind}_{\psi(a, \vec{b})}(M_1, \vec{t}) b) : \psi(c, \vec{t})$

$\Gamma \vdash \lambda c. M_1 c (\lambda b. \lambda x : b \in_I c. \text{ind}_{\psi(a, \vec{b})}(M_1, \vec{t}) b) : \forall c. \psi(c, \vec{t})$
Lemma 5.7 (Progress). If $\vdash M : \phi$, then either $M$ is a value or there is $N$ such that $M \rightarrow N$.

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 $M = NO$, then for some $\psi$, the proof must end with:
  \[ \vdash N : \psi \vdash O : \psi \]
  \[ \vdash NO : \phi \]
  By the inductive hypothesis, either $N$ is a value or there is $N'$ such that $N \rightarrow N'$. In the former case, by Canonical Forms for some $P$ we have $N = \lambda x : \psi. P$, so $NO \rightarrow P[x := O]$. In the latter case, $NO \rightarrow N'O$.
- If $M = axRep(t, u, M)$, then $M$ is a value.
- If $M = axProp(t, u, O)$, then we have the following proof tree:
  \[ \vdash O : t \in_I t_A(u) \]
  \[ \vdash axProp(t, u, O) : \phi_A(t, u) \]
  By the inductive hypothesis, either $O$ is a value or there is $O_1$ such that $O \rightarrow O_1$. In the former case, by Canonical Forms, $O = axRep(t, u, P)$ and $M \rightarrow P$. In the latter, by the evaluation rules $axProp(t, u, O) \rightarrow axProp(t, u, O_1)$.
- The cases corresponding to the equality and membership axioms work in the same way.
- The $\text{ind}$ terms always reduce. \qed

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. \qed

Finally, we state the formal correspondence between $\lambda Z\omega$ and 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 $\Gamma \vdash M : \phi$, where $\Gamma = \{(x_\phi, \phi) \mid \phi \in \Gamma \}$.

Proof. Both parts follow by easy induction on the proof. The first part is straightforward, to get the claim simply erase the lambda terms from the proof tree. For the second part, we show terms and trees corresponding to IZF$_R$$_\omega$ axioms:

- Let $\phi$ be one of the IZF$_R$$_\omega$ axioms apart from $\in$-Induction. Then $\phi = \forall \bar{u}. \forall c. c \in_I t_A(\bar{a}) \leftrightarrow \phi_A(c, \bar{a})$ 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 $(\phi_1 \rightarrow \phi_2) \land (\phi_2 \rightarrow \phi_1)$. Let $T$ be the following proof tree:
  \[ \Gamma, x : \phi_A(c, \bar{a}) \vdash x : \phi_A(c, \bar{a}) \]
  \[ \Gamma, x : \phi_A(c, \bar{a}) \vdash axRep(c, \bar{a}, x) : c \in_I t_A(\bar{a}) \]
  \[ \Gamma \vdash \lambda x : \phi_A(c, \bar{a}). axRep(c, \bar{a}, x) : \phi_A(c, \bar{a}) \rightarrow c \in_I t_A(\bar{a}) \]
Let $M_1 = \lambda x : c \in I t_A(\bar{a}) \cdot axProp(c, \bar{a}, x)$ and let $M_2 = \lambda x : \phi_A(c, \bar{a}) \cdot axRep(c, \bar{a}, x)$. Then the following proof tree shows the claim:

\[
\Gamma, x : c \in I t_A(\bar{a}) \vdash x : c \in I t_A(\bar{a})
\]

Then the following proof tree shows the claim:

\[
\Gamma, x : c \in I t_A(\bar{a}) \vdash axProp(c, \bar{a}, x) : \phi_A(c, \bar{a})
\]

\[
\Gamma \vdash M_1 : c \in I t_A(\bar{a}) \Rightarrow \phi_A(c, \bar{a})
\]

\[
\Gamma \vdash M_1, M_2 : c \in I t_A(\bar{a}) \Leftrightarrow \phi_A(c, \bar{a})
\]

- Let $\phi$ be the $\varepsilon$-induction axiom. Let

\[
M = \lambda \bar{f} \lambda x : (\forall a. (\forall b \in I a \rightarrow \psi(b, \bar{f})) \rightarrow \psi(a, \bar{f})) \cdot \text{ind}(x, \bar{f}).
\]

The following proof tree shows the claim:

\[
\Gamma, x : \forall a. (\forall b \in I a \rightarrow \psi(b, \bar{f})) \rightarrow \psi(a, \bar{f}) \vdash x : \forall a. (\forall b \in I a \rightarrow \psi(b, \bar{f})) \rightarrow \psi(a, \bar{f})
\]

\[
\Gamma, x : \forall a. (\forall b \in I a \rightarrow \psi(b, \bar{f})) \rightarrow \psi(a, \bar{f}) \vdash \text{ind}(\psi(a, \bar{f}), x, \bar{f}) : \forall a. \psi(a, \bar{f})
\]

\[
\Gamma \vdash M : \forall \bar{f}. (\forall a. (\forall b \in I a \rightarrow \psi(b, \bar{f})) \rightarrow \psi(a, \bar{f})) \rightarrow \forall a. \psi(a, \bar{f})
\]

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

6. Realizability for $\text{IZF}_{R_\omega}$

In this section we work in $\text{ZF}$ with $\omega$-many strongly inaccessible cardinals. We denote the $i$-th strongly inaccessible by $\Gamma_i$ and choose them so that $\Gamma_i \in \Gamma_{i+1}$. It is likely that $\text{IZF}$ with Collection and $\omega$-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 $\lambda Z_\omega$. For convenience, wherever possible, we erase logic terms and formulas from parameters of axRep, axProp, ind and case terms. We call the resulting calculus $\lambda Z_\omega$. More formally, $\lambda Z_\omega$ arises as an image of an erasure map $\lambda M$, which takes as its argument a $\lambda Z_\omega$-term. This map is defined by structural induction on $M$ and induced by the following cases:

\[
\lambda z : \phi. M = \lambda z. [M]
\]

\[
\lambda x : \phi. M = \lambda x. [M]
\]

\[
\text{let } a, x : \phi \text{ } := M \text{ in } N = \text{let } [a, x] := [M] \text { in } [N]
\]

\[
\text{case}(M, x : \phi. N, x : \psi. O) = \text{case}([M], x : [N], x : [O])
\]

The erasure on the rest of terms is defined in a natural way, for example $\langle M, N \rangle = [M, N]$, $[t, M] = [t, M]$ and $M t = M t$. The reduction rules and values in $\lambda Z_\omega$ are induced from
λZω in an obvious way. The set of λZω terms will be denoted by ΛZω and the set of λZω values will be denoted by λZωv.

**Lemma 6.1.** If 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 λZω 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 IZF Rω terms.

**Definition 6.2.** A set A is a λ-name iff A is a set of pairs (v, B) such that v ∈ λZωv and B is a λ-name.

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

**Definition 6.3.** The class of λ-names is denoted by Vλ.

Formally, Vλ is generated by the following transfinite inductive definition on ordinals:

\[ V^λ_0 = \emptyset \]

\[ V^λ_\alpha = \bigcup_{\beta < \alpha} P(\lambda Zωv \times V^λ_\beta) \quad V^λ = \bigcup_{\alpha \in \text{ORD}} V^λ_\alpha \]

**Definition 6.4.** The λ-rank of a λ-name A, denoted by λrk(A), is the smallest \( \alpha \) such that A ∈ Vα.

We now define three auxiliary relations between λZω terms and pairs of sets in Vλ, which we write as M ⊩ A ∈ I B, M ⊩ A ∈ B, M ⊩ A = B. These relations are a prelude to the definition of realizability.

\[ M ⊩ A ∈ I B \equiv M \downarrow v \land (v, A) ∈ B \]

\[ M ⊩ A ∈ B \equiv M \downarrow \text{inRep}(N) \land N \downarrow [u, O] \land \exists C ∈ V^λ. O \downarrow \{O_1, O_2\} \land O_1 \uparrow C \land B \land O_2 \uparrow A = C \]

\[ M ⊩ A = B \equiv M \downarrow \text{eqRep}(M_0) \land M_0 \downarrow \lambda a. M_1 \land \forall t ∈ T, \forall D ∈ V^λ. M_1[a := t] \downarrow \{O, P\} \land O \downarrow \lambda x. O_1 \land \forall N. (N \uparrow D \in I A) \rightarrow O_1[x := N] \uparrow D \in B \land P \downarrow \lambda x. P_1 \land \forall N. (N \uparrow D \in I B) \rightarrow P_1[x := N] \uparrow D \in A \]

The relations M ⊩ A ∈ B and M ⊩ 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 ∈ Vλ, C+ denotes \{ (M, A) | M ⊩ A ∈ C \}.

**Definition 6.6.** A (class-sized) first-order language L arises from enriching the IZF Rω signature with constants for all λ-names.

From now on until the end of this section, symbols M, N, O, P range exclusively over λZω-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 Vλ. We call such functions environments.
Definition 6.7. For any formula $\phi$ of $L$, any term $t$ of $L$ and $\rho$ defined on all free variables of $\phi$ and $t$, we define by metalevel induction a realizability relation $M \models_\rho \phi$ in an environment $\rho$ and a meaning of a term $\lfloor t \rfloor_\rho$ in an environment $\rho$:

1. $\lfloor a \rfloor_\rho \equiv \rho(a)$
2. $\lfloor A \rfloor_\rho \equiv A$
3. $\lfloor \omega \rfloor_\rho \equiv \omega'$, where $\omega'$ is defined by the means of inductive definition: $\omega'$ is the smallest set such that:
   - if $(\text{infRep}(N), A) \in \omega'$ if $N \downarrow \text{lin}(O), O \models_\rho A = 0$ and $A \in V_\omega^\lambda$.
   - if $(M, B) \in \omega'$, then $(\text{infRep}(N), A) \in \omega'$ if $N \downarrow \text{lin}(N_1), N_1 \downarrow \lfloor t, O \rfloor, O \downarrow \langle M, P \rangle$, $P \models_\rho A = S(B)$ and $A \in V_\omega^\alpha$.

4. $\lfloor V_1 \rfloor_\rho \equiv U_i$. We will define $U_i$ below.
5. $\lfloor \lambda x \rho(a) \rfloor_\rho \equiv \{(a x \text{Rep}(N), B) \in \lambda Z_{\omega v} \times V_\gamma^\lambda \mid N \models_\rho \phi_A(B, \lfloor u \rfloor_\rho^\gamma)\}$. The ordinal $\gamma$ will be defined below.
6. $M \models_\rho \bot \equiv \bot$
7. $M \models_\rho t \in s \equiv M \models_\rho \lfloor t \rfloor_\rho \in \lfloor s \rfloor_\rho$
8. $M \models_\rho t \equiv s \equiv M \models_\rho \lfloor t \rfloor_\rho = \lfloor s \rfloor_\rho$
9. $M \models_\rho t \in s \equiv M \models_\rho \lfloor t \rfloor_\rho \in \lfloor s \rfloor_\rho$
10. $M \models_\rho (\phi \land \psi) \equiv M \downarrow \langle M_1, M_2 \rangle \land (M_1 \models_\rho \phi) \land (M_2 \models_\rho \psi)$
11. $M \models_\rho (\phi \lor \psi) \equiv (M \downarrow \text{lin}(M_1) \land M_1 \models_\rho \phi) \lor (M \downarrow \text{lin}(M_1) \land M_1 \models_\rho \psi)$
12. $M \models_\rho \phi \rightarrow \psi \equiv (M \downarrow \lambda x. M_1) \land \forall N. (N \models_\rho \phi \rightarrow (M_1[x := N] \models_\rho \psi))$
13. $M \models_\rho \exists a. \phi \equiv M \downarrow \{t, N \} \land \exists A \in V_\lambda^\gamma. N \models_\rho \phi[a := A]$.
14. $M \models_\rho \forall a. \phi \equiv M \downarrow \lambda a. N \land \forall A \in V_\lambda^\gamma, \forall t \in T. N[a := t] \models_\rho \phi[a := A]$

To define $U_i$, first recall that the axiom $(\text{INAC}_i)$ has the following form:

$$(\text{INAC}_i) \forall c. c \in V_i \leftrightarrow \phi^1_1(c, V_i) \land \forall d. \phi^2_2(d) \rightarrow c \in d.$$ 

We define a monotonic operator $F$ on sets as:

$$F(A) = A \cup \{(\text{inac}_i \text{Rep}(N), C) \in \lambda Z_{\omega v} \times V_\lambda^\gamma \mid N \models_\rho \phi^1_1(C, A) \land \forall d. \phi^2_2(d) \rightarrow C \in d\}.$$ 

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

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

Since $F$ adds only elements from $\lambda Z_{\omega v} \times V_\lambda^\gamma$, any element of $U_i$ is in $\lambda Z_{\omega v} \times V_\lambda^\gamma$, so $U_i \in V_{\alpha + 1}^\lambda$.

The definition of the ordinal $\gamma$ in item 5 depends on $t_A(\bar{u})$. This ordinal is close to the rank of the set denoted by $t_A(\bar{u})$ and is chosen so that Lemma 6.31 can be proved. Let $\bar{\alpha} = \lambda x k(\lfloor u \rfloor_\rho^\gamma)$. Case $t_A(\bar{u})$ of:

- $\{u_1, u_2\} \rightarrow \alpha = \max(\alpha_1, \alpha_2)$
- $P(u) \rightarrow \gamma = \alpha + 1$.
- $\bigcup u \rightarrow \gamma = \alpha$.
- $S_{\phi(a, \bar{f})}(u, \bar{u}) \rightarrow \gamma = \alpha_1$.
- $R_{\phi(a, b, \bar{f})}(u, \bar{u})$. This case is more complicated. The names are chosen to match the corresponding clause in the proof of Lemma 6.31. Let $G = \{(N_1, (N_{21}, B)) \in \lambda Z_{\omega} \times \lfloor u \rfloor_\rho^\gamma \mid \exists d \in V_\lambda. \psi(N_1, N_{21}, B, d)\}$, where $\psi(N_1, N_{21}, B, d) \equiv (N_1 \downarrow \lambda a. N_{11} \land (N_{11} \downarrow \ldots \alpha$.
\[ \lambda x. O \land (O[x := N_{21}] \models_\rho \phi(B, d, [u^1_\rho]) \land \forall e. \phi(B, e, [u^1_\rho]) \rightarrow e = d) \].

Then for all \( g \in G \) there is \( D \) and \( (N_1, (N_{21}, B)) \) such that \( g = (N_1, (N_{21}, B)) \) and \( \psi(N_1, N_{21}, B, D) \). Use Collection to collect these \( D \)'s in one set \( H \), so that for all \( g \in G \) there is \( D \in H \) such that the property holds. Apply Replacement to \( H \) to get the set of \( \lambda \)-ranks of sets in \( H \). Then \( \beta \equiv \bigcup H \) is an ordinal and for any \( D \in H \), \( \lambdark(D) < \beta \). Therefore for all \( g \in G \) there is \( D \in V_\beta^A \) 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 occurrences of \( s \) in any term \( t \) and formula \( \phi \), 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.
- \( Occ(s, t_A(\vec{u})) = Occ(s, u_1) + \ldots + Occ(s, u_n) \).
- \( Occ(s, S_\Delta(t, \vec{u})) = Occ(s, \phi) + Occ(s, t) + Occ(s, u_1) + \ldots + Occ(s, u_n) \).
- \( Occ(s, t \in u) = Occ(s, t) + Occ(s, u) \).
- \( Occ(s, \phi \land \psi) = Occ(s, \phi) + Occ(s, \psi) \).

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:

\[
m(M \models_\rho \phi) = (V(\phi), Occ(\omega, \phi), FS(\phi), "\text{structural complexity of } \phi"")
\]

\[
m([t]_\rho) = (V(t), Occ(\omega, t), FS(t), 0)
\]

Then the measure of the definendum is always greater than the measure of the definens — 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 \( \omega \) disappears. Finally, in the definition of \( [t_A(\vec{u})]_\rho \), the topmost \( t_A \) disappears, while no new \( V_i \)'s and \( \omega \)'s appear. \( \square \)

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

**Lemma 6.11.** \( [t[a := s]] = [t[a := s]]_\rho = [t[a := s]]_\rho = [t[a := s]]_\rho \) and \( M \models_\rho \phi[a := s] \iff M \models_\rho \phi[a := s] \).

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

- Case \( A \) then \( [t[a := s]]_\rho = [t[a := s]]_\rho = [t[a := s]]_\rho = A \).
- Case \( a \) then \( [t[a := s]]_\rho = [s]_\rho, [t[a := s]]_\rho = [s]_\rho, [s]_\rho = [s]_\rho \) and also \( [t[a := s]]_\rho = [s]_\rho \).
• $t_A(\bar{u})$. Then $[t[a := s]]_\rho = \{(axRep(N), A) \mid N \vdash_\rho \phi_A(A, \bar{u}[a := s])\}$. By the inductive hypothesis, this is equal to $\{(axRep(N), A) \mid N \vdash_\rho[a := [s]_\rho] \phi_A(A, \bar{u})\} = [t[a := [s]_\rho]]_\rho$ and also to $\{(axRep(N), A) \mid N \vdash_\rho \phi_A(A, \bar{u}[a := [s]_\rho])\}$ 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 $M \rightarrow^* M'$ then $M' \vdash_\rho \phi$ iff $M \vdash_\rho \phi$.

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

**Lemma 6.14.** If $\rho$ agrees with $\rho'$ 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 $M \vdash_\rho \phi \rightarrow \psi$ and $N \vdash_\rho \phi$, then $M N \vdash \psi$.

*Proof.* Suppose $M \vdash_\rho \phi \rightarrow \psi$. Then $M \downarrow (\lambda x. O)$ and for all $P \vdash \phi$, $O[x := P] \vdash \psi$. Now, $M N \rightarrow^* (\lambda x. O) N \rightarrow O[x := N]$. Lemma 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 $M \vdash_\rho B \in I$, then $\lambda r k(B) < \lambda r k(A)$.

*Proof.* By induction on $\alpha$. Take any $A \in V^\lambda_{\alpha}$. By the definition of $V^\lambda_{\alpha}$, there is $\beta < \alpha$ such that $A \subseteq \lambda \in \omega \times V^\lambda_{\beta}$. Suppose $M \vdash_\rho B \in A$. Then $M \downarrow \text{inRep}(N)$, $N \downarrow [u, O]$, $O \downarrow (O_1, O_2)$ and there is $C$ such that $O_1 \vdash C \in I$ 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 $M \downarrow \text{eqRep}(M_0)$, $M_0 \downarrow \lambda a. M_1$ and for all $t \in T, D$, $M_1[a := t] \downarrow (O, P)$. Moreover, $O \downarrow \lambda x. O_1$ and for all $N \vdash_\rho D \in I$ 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 $V^\lambda_{\beta}$ for some $\beta < \alpha$, so $B \in V^\lambda_{\alpha}$.

The third part is trivial.

**Lemma 6.17.** $M \vdash_\rho A = B$ iff $M \downarrow \text{eqRep}(N)$ and $N \vdash_\rho \forall d. (d \in I A \rightarrow d \in B) \land (d \in I B \rightarrow d \in A)$. Also, $M \vdash_\rho A \in B$ iff $M \downarrow \text{inRep}(N)$ and $N \vdash_\rho \exists c. c \in I B \land A = c$.

*Proof.* Simply expand what it means for $M$ to realize respective formulas.
We now exhibit realizers corresponding to proofs of Lemmas 6.18-6.20. 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 ⪰ ρ ∀a. a = a.

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

**Lemma 6.19.** There is a term eqSymm such that eqSymm ⪰ ρ ∀a, b. a = b → b = a.

**Proof.** Take

\[
\text{eqSymm} \equiv \lambda a, b. \lambda x. \lambda y. \, N
\]

where \( N = \text{eqRep}(\lambda d. \langle \text{snd(eqProp}(x) \, d), \text{fst(eqProp}(x) \, d) \rangle) \).

To show that eqSymm ⪰ ρ ∀a, b. a = b → b = a, it suffices to show that for any \( A, B, t, u, M \), if \( M \parallel ρ A = B \) then \( N|x := M| \parallel ρ B = A \). 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 \( \text{snd(eqProp}(M) \, s) \downarrow \lambda x. \, M_1 \) and for all \( N_1 \parallel ρ C \in_I B, M_1|x := N_1| \parallel ρ C \in A \).
- There is \( M_2 \) such that \( \text{fst(eqProp}(M) \, s) \downarrow \lambda x. \, M_2 \) and for all \( N_2 \parallel ρ C \in_I A, M_2|x := N_2| \parallel ρ C \in B \).

Since \( M \parallel ρ A = B \), then there is \( O \) such that \( M \downarrow \text{eqRep}(O) \), so \( \text{fst(eqProp}(M) \, s) \rightarrow^* \text{fst}(O \, s) \). Moreover, for some \( O_1, O_2 \) we have \( O \downarrow \langle O_1, O_2 \rangle \), where \( O_1 \parallel ρ C \in_I A \rightarrow C \in B \) and \( O_2 \parallel ρ C \in_I B \rightarrow C \in A \). Therefore, \( \text{fst(eqProp}(M) \, s) \rightarrow^* O_1 \) and similarly \( \text{snd(eqProp}(M) \, s) \rightarrow^* O_2 \). We also know that there are some \( P_1, P_2 \) such that \( O_1 \downarrow \lambda x. \, P_1, O_2 \downarrow \lambda x. \, P_2, P_1|x := N_2| \parallel ρ C \in B \) and \( P_2|x := N_1| \parallel ρ C \in A \). 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 ⪰ ρ ∀b, a, c. a = b \& b = c \rightarrow a = c.

**Proof.** The proof and the realizers mirror closely the proof of Lemma 6.4. Set:

\[
eq \text{eqTrans} = \text{ind}(M_0)
\]

\[
M_0 = \lambda b, x_1, a_1, c, x_2. \text{eqRep}(\lambda f. \langle N, O \rangle)
\]

\[
N = \lambda x_3. \text{let } [a_2, x_4] := \text{inProp}(\text{fst(eqProp(fst(x_2)) f) x_3}) \, \text{in } N_1
\]

\[
N_1 = \text{let } [a_3, x_5] := \text{inProp}(\text{fst(eqProp(snd(x_2)) a_2 f(x_3)}) \, \text{in } N_2
\]

\[
N_2 = \text{inRep}([a_3, \langle \text{fst(x_5)}, x_1 a_2 \text{fst(x_4)} f a_3 \langle \text{snd(x_4)}, \text{snd(x_5)}\rangle\rangle])
\]

\[
O = \lambda x_3. \text{let } [a_2, x_4] := \text{inProp}(\text{snd(eqProp(snd(x_2)) f) x_3}) \, \text{in } O_1
\]

\[
O_1 = \text{let } [a_3, x_5] := \text{inProp}(\text{eqProp(fst(x_2)) a_2 f(x_4)}) \, \text{in } O_2
\]

\[
O_2 = \text{inRep}([a_3, \langle \text{fst(x_5)}, x_1 a_2 \text{fst(x_4)} f a_3 \langle \text{snd(x_4)}, \text{snd(x_5)}\rangle\rangle])
\]
We will show that for all \( B \), \( \text{eqTrans} \downarrow \lambda b. R \) for some term \( R \) such that for any term \( t \), \( R[t := t] \models \rho \forall a, c. a = B \land B = c \rightarrow a = c \), which trivially implies the claim. We proceed by induction on \( \lambda\text{rk} \) of \( B \).

We have \( \text{eqTrans} \rightarrow \lambda e. M_0 e M_1 \), where \( M_1 = \lambda g. \lambda x. \text{eqTrans} \ g \). Thus it suffices to show that for all \( t_1, M_0 t_1 M_1 \models \rho \forall a, c. a = B \land B = c \rightarrow a = c \). Since \( M_0 t_1 M_1 \downarrow \lambda \alpha_1, c, x_2. \text{eqRep} (\lambda f. \langle N, O \rangle [x_1 := M_1]) \), it suffices to show that for all \( A, C, M_2 \) such that \( M_2 \models \rho \ A = B \land B = C \) we have \( \text{eqRep} (\lambda f. \langle N, O \rangle [x_1, x_2 := M_1, M_2]) \models \rho \ A = C \). By Lemma 6.17 it suffices to show that for all \( F, u \) we have \( N[x_1, x_2, f := M_1, M_2, u] \models \rho \ F \in I \rightarrow F \in C \) and \( O[x_1, x_2, f := M_1, M_2, u] \models \rho \ F \in I \rightarrow F \in A \).

For the proof of the first claim, we have \( N[x_1, x_2, f := M_1, M_2, u] \downarrow \lambda x_3 \). Take any \( M_3 \models \rho \ F \in I \). We need to show that:

\[
\begin{align*}
&\text{let } [a_2, x_4] := \text{inProp}(\text{fst}(\text{eqProp}(\text{fst}(M_2)) \ u) \ M_3) \\
&\text{in } N_1[x_1, x_2, x_3, f := M_1, M_2, M_5, u] \models \rho \ F \in C.
\end{align*}
\]

We have \( \text{fst}(M_2) \models \rho A = B \), so \( \text{eqProp}(\text{fst}(M_2)) \models \rho \forall f. (f \in I \rightarrow f \in B) \land (f \in I B \rightarrow f \in A) \), so by Lemma 6.15 \( \text{fst}(\text{eqProp}(\text{fst}(M_2)) u) \ M_3 \models \rho \ F \in B \). Therefore, \( \text{fst}(\text{eqProp}(\text{fst}(M_2)) u) \ M_3 \downarrow \text{inRep}(P) \) and \( P \downarrow \{t_2, M_4\} \) for some \( P, A_2, t_2, M_4 \) such that \( M_1 \models \rho \ A_2 \in I \ B \land F = A_2 \). Thus our term let \( [a_2, x_4] := \ldots \text{reduces to} \{\ldots \text{inRep}(\{t_3, \text{fst}(M_5), t_1, t_2 \text{fst}(M_4) \ u \ t_3 \text{snd}(M_4), \text{snd}(M_5)\})\} \)

and by Lemma 6.13 it suffices to show that

\[
\text{inRep}(\{t_3, \text{fst}(M_5), t_1, t_2 \text{fst}(M_4) \ u \ t_3 \text{snd}(M_4), \text{snd}(M_5)\}) \models \rho \ F \in C
\]

For this purpose, we need to show that \( \text{fst}(M_5) \models \rho \ A_3 \in I \ C \), which is trivial, and that

\[
M_1 \ t_2 \text{fst}(M_4) \ u \ t_3 \text{snd}(M_4), \text{snd}(M_5) \models \rho \ F = A_3.
\]

Since \( M_1 = \lambda g. \lambda x. \text{eqTrans} \ g \), \( \text{snd}(M_4) \models \rho \ F = A_2 \) and \( \text{snd}(M_5) \models \rho \ A_2 = A_3 \), all we need to have is that \( \text{eqTrans} \ t_2 \models \rho \forall a, c. a = A_2 \land A_2 = c \rightarrow a = c \). Since \( \text{fst}(M_4) \models \rho \ A_2 \in I \ B \), \( \lambda \text{rk}(A_2) < \lambda \text{rk}(B) \) 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 \( N_1 \) is the exchange of \( \text{fst} \) and \( \text{snd} \) which corresponds to using the information that \( \forall f. f \in I \ C \rightarrow f \in B \) and \( \forall f. f \in I \ B \rightarrow f \in A \) and proceeding from \( C \) to \( A \) in the second part of the proof of Lemma 4.4.

\begin{lemma}
There is a term \( lei \) such that \( \text{let } [d, y] := \text{inProp}(\text{fst}(x)) \text{ in } \text{inRep}([d, (\text{fst}(y), \text{eqTrans} \ a \ b \ c \ \langle \text{eqSymm} \ a \ b \ \text{snd}(x), \text{snd}(y)\rangle])]. \)
\end{lemma}

\begin{proof}
Take \( \text{let } [d, y] := \text{inProp}(\text{fst}(M)) \text{ in } \text{inRep}([d, (\text{fst}(y), \text{eqTrans} \ t_1, t_2, t_3 \ \langle \text{eqSymm} \ t_1, t_2 \ \text{snd}(M), \text{snd}(y)\rangle]) \models \rho \ B \in C. \)
\end{proof}

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

$$\inRep([u, (f^\rho \rho)(O, \text{EqTrans} t_1 t_2 t_3 \langle \text{EqSymm} t_1 t_2 \text{snd}(M), (\text{snd}(O)) \rangle)] \Vdash_\rho B \in C.$$ 

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

$$\text{EqTrans} t_1 t_2 t_3 \langle \text{EqSymm} t_1 t_2 \text{snd}(M), \text{snd}(O) \rangle \Vdash_\rho B = E.$$ 

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

The following two lemmas will be used for the treatment of $\omega$ in Lemma [6.31].

**Lemma 6.22.** If $A, B \in V_\alpha^\lambda$, then $\{\{A, B\}\}_\rho \in V_{\alpha+1}^\lambda$.

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

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

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

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

**Proof.** Similar to the proof of Lemma [6.23] utilizing Lemmas [6.22] and [6.16].

**Lemma 6.25.** $\lambda r k(C) \leq r k(C^+) + \omega$.

**Proof.** If $(M, A) \in C$, then $M \Vdash_\rho A \in I \subset C$. We have $\inRep([a, (M, \text{EqRefl} a)]) \Vdash_\rho A \in C$, so $(\inRep([a, (M, \text{EqRefl} a)]), A) \in C^+$. The extra $\omega$ 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 $\inRep([a, (M, \text{EqRefl} a)])$.

**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 $N \downarrow [t, N_1], N_1 \downarrow (O, N_2)$ 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 $t, X$, $N_1[a := t] \Vdash_\rho X \in A \rightarrow \phi$. 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 $N_1 \downarrow (O, N_2), O \Vdash_\rho X \in A$ and $N_2 \Vdash_\rho \phi[x := X]$, so there is $(O, X) \in A^+$ such that $N \downarrow [t, N_1], N_1 \downarrow (O, N_2)$ and $N_2 \Vdash_\rho \phi[x := X]$. 


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 \( C \in V_{1^A}^i \).

**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 \( N \downarrow (N_1, N_2), N_1 \vDash \rho \forall x \in A \exists ! y \in V_i. (x, y) \in C \) and \( N_2 \vDash \rho \forall z \in C \exists x \in A \exists y \in V_i. z = (x, y) \). So \( N_1 \vDash \rho \forall x \in A \exists y \in V_i. (x, y) \in C \wedge \forall z. (x, z) \in C \to z = y \). 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:

\[
\phi(O, X, P, Y) \equiv (N_1 \downarrow \lambda a. N_{11}) \wedge (N_11 \downarrow \lambda x. N_{12}) \wedge (N_{12}[x := O] \downarrow [t, N_{13}]) \wedge (N_{13} \downarrow (P, Q)) \wedge (Q \downarrow (Q_1, Q_2)) \wedge (Q_1 \vDash \rho (X, Y) \in C) \wedge (Q_2 \vDash \rho \forall z. (x, z) \in C \to z = Y)
\]

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

\[
\psi(O, X, P, Y) \equiv \exists Q_1, Q_2. (Q_1 \vDash \rho (X, Y) \in C) \wedge (Q_2 \vDash \rho \forall z. (x, z) \in C \to z = Y)
\]

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 \( \lambda \)-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 \( \Gamma_i \). Also, for any \( (O, X) \in A^+ \), \( F(O(X)) \) is inhabited.

Furthermore, define a function \( G \) from \( A^+ \) to \( \Gamma_i \), which takes \( (O, X) \in A^+ \) and returns \( \bigcup \{ \lambda rk((P, Y)) \mid (P, Y) \in F(O(X) \wedge \psi(O, X, P, Y)) \} \). Then for any \( (O, X) \in A^+ \), \( G(O(X)) \) is an ordinal smaller than \( \Gamma_i \) and if \( (P, Y) \in U_i^+ \) and \( \psi(O, X, P, Y) \), then \( (P, Y) \in V_{1^A}^i \). Moreover, as \( \Gamma_i \) is inaccessible, \( G \in R(\Gamma_i) \), where \( R(\Gamma_i) \) denotes the \( \Gamma_i \)-th element of the standard cumulative hierarchy. Therefore \( \bigcup \text{ran}(G) \) is also an ordinal smaller than \( \Gamma_i \). We define an ordinal \( \beta \) to be \( \max(\lambda rk(A), \bigcup \text{ran}(G)) \).

Now take any \((M, B) \in C^+\), so \( M \vDash \rho B \in C \). Then, by the definition of \( N \) and Lemma \[6.26\] there is \((O, X) \in A^+ \) and \((O_1, Z) \in U_i^+ \) such that \( N_2 \downarrow \lambda a. N_{21}, N_{21} \downarrow \lambda x. N_{22}, N_{22}[x := M] \downarrow [t, N_{23}], N_{23} \downarrow (O, N_{24}), N_{24} \downarrow [t, N_{25}], N_{25} \downarrow (O_1, R) \) and \( R \vDash \rho B = (X, Z) \). Let \( M_1 = i \varepsilon a a \varepsilon M, R \), 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 \[6.16\] \( \lambda rk(Z) \leq \lambda rk(Y) \) and thus \( \lambda rk(Z) \leq \beta \). Since \( (O, X) \in A^+ \), \( \lambda rk(X) \leq \beta \), too. By Lemma \[6.24\] \( \lambda rk(B) \leq \beta + 2 \). By Lemma \[6.24\] \( rk(B) \leq \beta + \omega \), so \( rk(C^+) \leq \beta + \omega + 1 \). By Lemma \[6.25\] again, \( \lambda rk(C) \leq \beta + 2 \omega \). Since \( \beta + 2 \omega \) is still smaller than \( \Gamma_i \), 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 \( M \downarrow \text{inRep}(N), N \downarrow [t, O], O \downarrow (O_1, O_2) \) and there is \( C \) such that \( O_1 \downarrow v_1, (v, C) \in U_{i, \gamma}, O_2 \vDash \rho C = A \). Then also \((v, C) \in U_i \), so \( O_1 \vDash \rho C \in I \), so also \( M \vDash \rho A \in V_i \).
Lemma 6.29. If $N \models \psi_1(C, U_{i, \gamma})$, where $\psi_1$ is one of the five clauses defining $\phi_1(C, U_{i, \gamma})$ in the Definition 3.3, then $N \models \psi_1(C, V_i)$.

Proof. There are five cases to consider:

- $N \models \exists a. a \in U_{i, \gamma} \land c \in a$. Then there is $A$ such that $N \downarrow [t, O], O \downarrow \langle O_1, O_2 \rangle, O_1 \models a \in U_{i, \gamma}, O_2 \models C \in A$. By Lemma 6.28, $O_1 \models a \in V_i$, so also $N \models \exists a. a \in V_i \land c \in a$.

- $N \models \exists a. a \in U_{i, \gamma} \land c = \bigcup a$. Then there is $A$ such that $N \downarrow [t, O], O \downarrow \langle O_1, O_2 \rangle, O_1 \models a \in U_{i, \gamma}, O_2 \models C = \bigcup A$. Thus by Lemma 6.28, $O_1 \models a \in V_i$ and we get the claim in the same way as in the previous case.

- $N \models \exists a. a \in U_{i, \gamma} \land C = P(a)$. Similar to the previous case.

- $N \models \exists a. a \in U_{i, \gamma} \land C \rightarrow U_{i, \gamma}$. Then there is $A$ such that $N \downarrow [t, O], O \downarrow \langle O_1, O_2 \rangle, O_1 \models a \in U_{i, \gamma}, O_2 \models C \rightarrow a$ is a function from $A$ into $U_{i, \gamma}$”. By Lemma 6.28, $O_1 \models a \in V_i$. Expanding the second part, we have $O_2 \downarrow \langle P_1, P_2 \rangle$, $P_1 \models \forall x \in A \exists y \in U_{i, \gamma}, (x, y) \in C$ and $P_2 \models \forall z \in C \exists x \in A \exists y \in U_{i, \gamma}, z = (x, y)$. We will tackle $P_1$ and $P_2$ separately.

- For $P_1$, we have for all $X, t, P_1 \downarrow \lambda a. P_1[a := t] \downarrow \lambda x. X$. For all $R \models X \in A$ there is $Y$ such that $Q[x := R] \downarrow \langle t_1, Q_0 \rangle, Q_0 \downarrow \langle Q_1, Q_2 \rangle, Q_1 \models Y \in U_{i, \gamma}$ and $Q_2 \models (X, Y) \in C \land \forall z. (x, z) \in C \rightarrow z = Y$. By Lemma 6.28, we also have $Q_1 \models Y \in V_i$, so also $P_1 \models \forall x \in a \exists y \in (x, y) \in C$.

- For $P_2$, we have for all $Z, t, P_2 \downarrow \lambda a. P_2[a := t] \downarrow \lambda x. X$. For all $R \models Z \in C$ there are $X, Y$ such that $Q[x := R] \downarrow \langle t_1, Q_0 \rangle, Q_0 \downarrow \langle Q_1, Q_2 \rangle$ and $Q_1 \models X \in A$. Moreover, $Q_2 \downarrow \langle t_1, S_0 \rangle, S_0 \downarrow \langle S_1, S_2 \rangle$ and $S_1 \models Y \in U_{i, \gamma}$. By Lemma 6.28, we also have $S_1 \models Y \in V_i$, so also $P_2 \models \forall z \in C \rightarrow \exists y \in A \exists y \in V_i, z = (x, y)$. Therefore also $P_2 \models C \rightarrow A$ is a function from $A$ into $V_i$” and in the end $N \models \exists a. a \in V_i \rightarrow V_i$. }

Corollary 6.30. If $M \models \phi_1(C, U_{i, \gamma})$, then $M \models \phi_1(C, V_i)$.

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

Lemma 6.31. $(M, C) \in [t_A(\bar{u})]_\rho$ iff $M = \text{axRep}(N)$ and $N \models \phi_A(C, \overline{\text{Rep}(\langle u \rangle)\rho})$.

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

For all terms, save $\omega$ and $V_i$, the left-to-right direction is immediate. For the right-to-left direction, suppose $N \models \phi_A(C, \overline{\text{Rep}(\langle u \rangle)\rho})$ and $M = \text{axRep}(N)$. To show that $(M, C) \in [t_A(\bar{u})]_\rho$, we need to show that $C \in V_{\lambda}^\gamma$. Let $\lambda = \text{rank}(\overline{\langle u \rangle})$. Case $t_A(\bar{u})$ of:

- $\{u_1, u_2\}$. Suppose that $N \models \exists a. a \in U_{i, \gamma} \land C \models u_2 \rho$. Then either $N \downarrow \text{inl}(N_1) \land N_1 \models C = \overline{u_1 \rho}$ or $N \downarrow \text{inr}(N_1) \land N_1 \models C = \overline{u_2 \rho}$. By Lemma 6.16, in the former case $C \in V_{\alpha_1}^{\lambda}$, in the latter $C \in V_{\alpha_2}^{\lambda}$, so $C \in V_{\alpha_2}^{\lambda}$.

- $P(u)$. Suppose that $N \models \forall d. d \in C \rightarrow d \in \overline{u \rho}$. Then $N \downarrow \lambda a. N_1$ and for any $t, \forall D, N_1[a := t] \models D \in [u \rho]$, so $\forall D, t, N_1[a := t] \downarrow \lambda x. N_2$ and for all $O$, if $O \models D \in C$ then $N_2[x := O] \models D \in \overline{u \rho}$. Take any $(v, B) \in C$. Then $\text{inRep}[(a, \langle v, \text{eqRef}\langle a \rangle \rangle)] \models B \in C$, so $N_2[x := \text{inRep}[(a, \langle v, \text{eqRef}\langle a \rangle \rangle)] \models B \in \overline{u \rho}$. Thus by Lemma 6.16, any such $B$ is in $V_{\alpha_1}^{\lambda}$, so $C \in V_{\alpha_1}^{\lambda}$.

- $\overline{\text{Rep}(\langle u \rangle)\rho}$. Suppose that $N \models \exists c. c \in \overline{u \rho} \land C \in c$. Then $N \downarrow \langle t, N_1 \rangle$ and there is $B$ such that $N_1 \models B \in \overline{u \rho} \land C \in B$. Thus $N_1 \downarrow \langle N_1, N_2 \rangle, N_1 \models B \in \overline{u \rho}, N_2 \models C \in B$. By Lemma 6.16, any such $B$ is in $V_{\alpha_1}^{\lambda}$, so $C \in V_{\alpha_1}^{\lambda}$. 

• $S_{\phi(a,\bar{y})}(u, \bar{u})$. Suppose $N \models_{\rho} C \in [u]_\rho \land \phi(C, [\bar{u}]_\rho)$. Then $N \downarrow \langle N_1, N_2 \rangle$ and $N_1 \models_{\rho} C \in [u]_\rho$. Thus $C \in V^\lambda_1$.

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

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

• The base case. Then $N \downarrow \text{in}(O) \land O \models_{\rho} A = 0$, so $N \models_{\rho} A = 0 \lor \exists y \in \omega'. A = S(y)$.

• Inductive step. Then $N \downarrow \text{inr}(N_1), N_1 \downarrow [t, O], O \downarrow \langle M', P \rangle, (M', B) \in \omega'^+, P \models_{\rho} A = S(B)$. Therefore, there is $C$ (namely $B$) such that $M' \models_{\rho} C \in \omega'$ and $P \models_{\rho} A = S(C)$.

Thus $[t, O] \models_{\rho} \exists y. y \in \omega' \land A = S(y)$, so $N \models_{\rho} A = 0 \lor \exists y \in \omega'. A = S(y)$.

For the right-to-left direction, suppose $N \models_{\rho} A = 0 \lor \exists y \in \omega' \land A = S(y))$. Then either $N \downarrow \text{in}(N_1)$ or $N \downarrow \text{inr}(N_1)$. In the former case, $N_1 \models_{\rho} A = 0$, so by Lemma 6.16, $A \in V^\lambda_\omega$. In the latter, $N_1 \models_{\rho} \exists y. y \in \omega' \land A = S(y)$. Thus $N_1 \downarrow [t, O]$ and there is $B$ such that $O \models_{\rho} B \in \omega' \land A = S(B)$. So $O \downarrow \langle M', P \rangle, (M', B) \in \omega'^+$ and $P \models_{\rho} A = S(B)$. This is exactly the inductive step of the definition of $\omega'$, so it remains to show that $A \in V^\lambda_\omega$. Since $(M', B) \in \omega'^+$, there is a finite ordinal $\alpha$ 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 $M = \text{inac}_i\text{Rep}(N)$. We must have $N \models_{\rho} \phi_1(A, U_{i, \gamma}) \land \forall d. \phi_2(d) \rightarrow A \in d$ for some ordinal $\gamma$. Then $N \downarrow \langle N_1, N_2 \rangle$, $N_1 \models_{\rho} \phi_1(A, U_{i, \gamma})$, $N_2 \models_{\rho} \forall d. \phi_2(d) \rightarrow A \in d$. Corollary 6.30 gives us $N_1 \models_{\rho} \phi_1(A, V_i)$, so $N \models_{\rho} \phi_1(A, V_i) \land \forall d. \phi_2(d) \rightarrow A \in d$, which is what we want.

For the right-to-left direction, suppose $N \models_{\rho} \phi_1(C, V_i) \land \forall d. \phi_2(d) \rightarrow C \in d$. We need to show that $(\text{inac}_i\text{Rep}(N), C) \in U_i$. By the definition of $U_i$ it suffices to show that $C \in V_{i, 1}$. We have $N \downarrow \langle N_1, N_{20} \rangle$ and $N_1 \models_{\rho} \text{“}C\text{” 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 $\gamma$ in the clause 5 in the definition of realizability. The last one follows by Lemma 6.27.

7. Normalization

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

**Definition 7.1.** For a sequent $\Gamma \vdash M : \phi$, $\rho \models \Gamma \vdash M : \phi$ means that $\rho$ is defined on $FV(\Gamma, M, \phi)$ and for all $(x_i, \phi_i) \in \Gamma$, $\rho(x_i) \models_\rho \phi_i$.

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

**Definition 7.2.** For a sequent $\Gamma \vdash M : \phi$, $\rho \models \Gamma \vdash M : \phi$ 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 $FV(M) = \{x_1, \ldots, x_n\}$, $FV_T(M) = \{a_1, \ldots, a_k\}$ and $\rho_T$ denotes the restriction of $\rho$ 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 $\Gamma \vdash M : \emptyset$ then for all $\rho \models \Gamma \vdash M : \emptyset$, $M[\rho] \models_\rho \emptyset$.

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

- $\Gamma, x : \phi \vdash x : \phi$

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

- $\Gamma \vdash M : \phi \rightarrow \psi$ \quad $\Gamma \vdash N : \phi$

$$\Gamma \vdash M \mid N : \psi$$

By the inductive hypothesis, $M' \models_\rho \phi \rightarrow \psi$ and $N' \models_\rho \phi$. Lemma 6.15 gives the claim.

- $\Gamma, x : \phi \vdash M : \psi$

$$\Gamma \vdash \lambda x : \phi. \quad M : \phi \rightarrow \psi$$

We need to show that for any $N \models_\rho \phi$, $M'[x := N] \models_\rho \psi$. Take any such $N$. Let $\rho' = \rho[x := N]$. Then $\rho' \models \Gamma, x : \phi \vdash M : \psi$, so by the inductive hypothesis $\overline{M[\rho']} \models_{\rho'} \psi$. By Lemma 7.3 $M[\rho'] = \overline{M[\rho][x := N]} = M'[x := N]$, so $M'[x := N] \models_{\rho'} \psi$. Since $\rho'$ agrees with $\rho$ on logic variables, by Lemma 6.14 we get $M'[x := N] \models_\rho \psi$.

- $\Gamma \vdash M : \bot$

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

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

- $\Gamma \vdash M : \phi \land \psi$

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

By the inductive hypothesis, $M' \models_\rho \phi \land \psi$, so $M' \downarrow (M_1, M_2)$ and $M_1 \models_\rho \phi$. Therefore $\text{fst}(M) \rightarrow^* \text{fst}((M_1, M_2)) \rightarrow M_1$. Lemma 6.13 gives the claim.

- $\Gamma \vdash M : \phi \land \psi$

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

Symmetric to the previous case.
\[
\Gamma \vdash M : \phi \quad \Gamma \vdash N : \psi
\]
\[
\Gamma \vdash \langle M, N \rangle : \phi \land \psi
\]
All we need to show is \(M' \vdash_{\sigma} \phi\) and \(N' \vdash_{\sigma} \psi\), which we get from the inductive hypothesis.

\[
\Gamma \vdash M : \phi
\]
\[
\Gamma \vdash \text{inl}(M) : \phi \lor \psi
\]
We need to show that \(M' \vdash_{\sigma} \phi\), which we get from the inductive hypothesis.

\[
\Gamma \vdash M : \psi
\]
\[
\Gamma \vdash \text{inr}(M) : \phi \lor \psi
\]
Symmetric to the previous case.

\[
\Gamma \vdash M : \phi \lor \psi \quad \Gamma, x : \phi \vdash N : \emptyset \quad \Gamma, x : \psi \vdash O : \emptyset
\]
\[
\Gamma \vdash \text{case}(M, x : \phi, N, x : \psi, O) : \emptyset
\]
By the inductive hypothesis, \(M' \vdash_{\sigma} \phi \lor \psi\). Therefore either \(M' \downarrow \text{inl}(M_1)\) and \(M_1 \vdash_{\sigma} \phi\) or \(M' \downarrow \text{inr}(M_2)\) and \(M_2 \vdash_{\sigma} \psi\). We only treat the former case, the latter is symmetric. Since \(\rho[x := M_1] \vdash_{\sigma} \rho, \Gamma, x : \phi \vdash N : \emptyset\), by the inductive hypothesis we get \(\overline{N}[\rho[x := M_1]] \vdash_{\sigma} \emptyset\). We also have \(\text{case}(M, x, \overline{N}, x, \overline{O}) \to^* \text{case}(\text{inl}(M_1), x, \overline{N}, x, \overline{O}) \to \overline{N}[x := M_1]\). By Lemma 7.3, \(\overline{N}[x := M_1] = \overline{N}[\rho[x := M_1]]\), so Lemma 6.13 gives us the claim.

\[
\Gamma \vdash M : \phi
\]
\[
\Gamma \vdash \lambda a. M : \forall a. \phi
\]
By the inductive hypothesis, for all \(\sigma \models \Gamma \vdash M : \phi\), \(\overline{M}[\rho] \vdash_{\sigma} \phi\). We need to show that for all \(\sigma \models \Gamma \vdash \lambda a. M : \forall a. \phi\), \(\overline{M}[\rho] \vdash_{\sigma} \forall a. \phi\). This is equivalent to \(\lambda a. \overline{M}[\rho] \vdash_{\sigma} \forall a. \phi\). Take any such \(\sigma\). We need to show that \(\forall A, t. \overline{M}[\rho][a := t] \vdash_{\sigma} \phi[a := A]\). Take any \(A\) and \(t\). Since \(\sigma[a := (t, A)] \models \Gamma \vdash M : \phi\) and by Lemma 7.3, \(\overline{M}[\rho][a := t] = \overline{M}[\rho[a := (t, A)]\), we get the claim by the inductive hypothesis.

\[
\Gamma \vdash M : \forall a. \phi
\]
\[
\Gamma \vdash M t : \phi[a := t]
\]
By the inductive hypothesis, \(M' \vdash_{\sigma} \forall a. \phi\), so \(M' \downarrow \lambda a. N\). \(\forall A, u. N[a := u] \vdash_{\sigma} \phi[a := A]\). In particular \(N[a := t]\rho] \vdash_{\sigma} \phi[a := [t]\rho]\). By Lemma 6.11, \(N[a := t]\rho] \vdash_{\sigma} \phi[a := t]\). Since \(M' \uparrow \phi[t]\rho]) \to^* (\lambda a. N) t\rho] \to N[a := t]\rho]\), Lemma 6.13 gives us the claim.

\[
\Gamma \vdash M : \phi[a := t]
\]
\[
\Gamma \vdash [t, M] : \exists a. \phi
\]
By the inductive hypothesis, \(M' \vdash_{\sigma} \phi[a := t]\), so by Lemma 6.11, \(M' \vdash_{\sigma} \phi[a := [t]\rho]\). Thus, there is a lambda-name \(A\), namely \([t]\rho\), such that \(M' \vdash_{\sigma} \phi[a := A]\). Thus, \(\overline{[t, M]\rho]} = [t]\rho]\), so \([t, M] \vdash_{\sigma} \exists a. \phi\) which is what we want.

\[
\Gamma \vdash M : \exists a. \phi \quad \Gamma, x : \psi \vdash N : \psi
\]
\[
\Gamma \vdash \text{let } [a, x : \phi] := M \text{ in } N : \psi
\]
Let \(\sigma \models \Gamma \vdash [a, x : \phi] := M \text{ in } N : \psi\). We need to show \(\text{let } [a, x] := M' \text{ in } \overline{N}[\rho] \vdash_{\sigma} \psi\). By the inductive hypothesis, \(M' \vdash_{\sigma} \exists a. \phi\), so \(M' \downarrow [t, M_1]\) and for some \(A, M_1 \vdash_{\sigma} \phi[a := A]\). By the inductive hypothesis again, for any
\[ \rho' \models \Gamma, x : \phi \vdash N : \psi \] we have \( \overline{\psi} \models \rho' \psi. \) Take \( \rho' = \rho[x \mapsto M_1, a := (t, A)]. \) Since \( a \notin \text{FV}(\psi), \) by Lemma 6.14 \( \overline{\psi} \models \rho \psi. \) Now, let \( [a, x : \phi] := M' \) in \( \overline{\psi} \models \rho \rightarrow \psi \) let \( [a, x] := [t, M_1] \) in \( \overline{\psi} \models [a := t][x := M_1] = \overline{\psi} \). Lemma 6.13 gives us the claim.

- By the inductive hypothesis, \( \forall \lambda \cdot \lambda_b. \lambda x. \text{ind}(\lambda c. \lambda_x. \text{ind}(M') b), \) by Lemma 6.13 it suffices to show that for all \( C, t, M' \) \( \lambda b. \lambda x. \text{ind}(M') b \models \rho \phi(C, \overline{t}). \) We proceed by induction on \( \lambda \text{-rank of} C. \) Take any \( C, t. \) By the inductive hypothesis, \( M' \models \rho \forall \lambda c. \lambda b. \lambda x. \text{ind}(M') b \models \rho \phi(c, \overline{t}). \) So \( M' \models \rho \forall \lambda c. \lambda b. \lambda x. \text{ind}(M') b \models \rho \phi(c, \overline{t}). \) By Lemma 6.13 it suffices to show that \( \lambda b. \lambda x. \text{ind}(M') b \models \rho \phi(b, \overline{t}). \) Take any \( B, u, \) \( O \models \rho B \models \lambda x. \text{ind}(M') \lambda b. \lambda x. \text{ind}(M') b \models \rho \phi(B, \overline{t}). \) As \( x \notin \text{FV}(M'), \) it suffices to show that \( \lambda b. \lambda x. \text{ind}(M') b \models \rho \phi(B, \overline{t}). \) As \( O \models \rho B \models \lambda x. \text{ind}(M') \lambda b. \lambda x. \text{ind}(M') b \models \rho \phi(b, \overline{t}). \)
Corollary 7.5 (Normalization). If $\vdash M : \phi$, then $M \downarrow$.

Proof. Take $\rho$ mapping all free propositional variables of $M$ to themselves and all free first-order variables $a$ of $M$ to $(a, \emptyset)$. Then $\rho \vdash M : \phi$. By Theorem 7.4, $\overline{M}[\rho]$ normalizes. By the definition of $\rho$, $\overline{M}[\rho] = M$. 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 $\lambda Z_\omega$ show that 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 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 $\lambda Z_\omega$-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, IZF$_{R\omega} \vdash \phi(t)$. □

Corollary 7.7 (Set Existence Property). If IZF$_{R\omega} \vdash \exists x. \phi(x)$ and $\phi$ 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 IZF$_{R\omega} \vdash \phi(t)$ for some term $t$. Moreover, for any IZF$_{R\omega}$ term $s$, there is a term-free defining formula $\psi_s(x)$ such that IZF$_{R\omega} \vdash \psi_s(s) \land \exists! x. \psi_s(x)$. Therefore IZF$_{R\omega} \vdash \exists! x. \phi(x) \land \psi_l(x)$. □

In [CM06] we have shown how to use DP, NEP and TEP for the purpose of program extraction. Thus our results establish 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 Ščedrov [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 Ščedrov [FS83]. 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


