Normalization of intuitionistic set theories

Wojciech Moczydłowski *

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

Abstract. IZF is a well-investigated impredicative constructive counterpart of Zermelo-Fraenkel set theory. We define a weakly-normalizing lambda calculus λZ corresponding to proofs in an intensional version of IZF with Replacement according to the Curry-Howard isomorphism principle. By adapting a counterexample invented by M. Crabbé, we show that λZ does not strongly normalize. Moreover, we prove that the calculus corresponding to a non-well-founded IZF does not even weakly normalize. Thus λZ and IZF are positioned on the fine line between weak, strong and lack of normalization.

1 Introduction

There are various lambda calculi corresponding to constructive theories via the propositions-as-types principle, also called the Curry-Howard isomorphism. Some famous examples are Girard's System F for second-order intuitionistic logic and F_ω for higher-order intuitionistic logic. Many powerful calculi exist which do not correspond to the existing theory, instead providing it implicitly. Prominent examples are Martin-Löf's type theory with extensions, Coquand and Huet's Calculus of Constructions and Luo's Extended Calculus of Constructions implemented in Nuprl, Coq and Lego, respectively.

Normalization of a calculus, weak or strong, is a standard tool used to justify its consistency and to provide program extraction capabilities. The more powerful the system is, the more difficult it is to prove its normalization. Girard's proof for System F cannot be formalized in the first-order arithmetic. Calculus of Inductive Constructions requires at least the proof-theoretical power of Zermelo's set theory for its normalization.

The gap between weak and strong normalization for the calculi we mentioned seems minimal. Apart from Martin-Löf's type theory, all of them strongly normalize. Many of them can be specified in the framework of Pure Type Systems and it's been conjectured by Barendregt, Geuvers and Klop that for Pure Type Systems, weak normalization entails strong normalization. Reasonable calculi have also the property that their inconsistency implies the existence of a non-normalizing term, which violates even weak normalization of the calculus.

One natural class of constructive theories for which no propositions-as-types interpretation has been known until recently ([4]) are constructive set theories. They have been investigated thoroughly. Results and bibliography concerning predicative CZF (Constructive Zermelo-Fraenkel) with variants can be found in [1] and on the authors' webpages. More powerful, impredicative IZF (Intuitionistic Zermelo-Fraenkel) has been investigated mainly before 1990 and information can be found in [5] and [2].

We introduce a lambda calculus λZ corresponding to proofs in IZF_R^-, an impredicative intensional version of IZF containing in particular the Power Set, unrestricted Separation and Replacement axioms. λZ has several interesting properties:

* Partly supported by NSF grants DUE-0333526 and 0430161.

- It corresponds to a natural constructive theory.
- It weakly normalizes. The proof method combines realizability with reduction-preserving erasure map and uses all proof-theoretic power of ZF set theory.
- It does not strongly normalize. A very small fragment of a theory suffices to exhibit the counterexample to the strong normalization property.
- A slight semantic modification to IZF_R^-, namely making it non-well-founded, makes the calculus not even weakly normalizing.

Therefore λZ and IZF_R^- are positioned on the fine line between weak, strong and lack of normalization.

Normalization of λZ makes it possible to extract programs from proofs in IZF_R^-. We describe program extraction from IZF proofs in details in [3]. More detailed proofs of our results can be found in [4].

2 $\mathbf{IZF}_R$

Intuitionistic set theory IZF_R is a first-order theory, equivalent to ZF when extended with excluded middle. The signature consists of one binary relational symbol $\in$ and function symbols used in the axioms below. The relational symbol $t = u$ is an abbreviation for $\forall z.\ z \in t \leftrightarrow z \in u$. Function symbols 0 and $S(t)$ are abbreviations for $\{x \in \omega \mid \bot\}$ and $\bigcup\{t, \{t, t\}\}$. Bounded quantifiers and the quantifier $\exists! a$ (there exists exactly one a) are also abbreviations defined in the standard way.

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

These axioms correspond very closely to the standard axiomatization of Zermelo-Fraenkel set theory ZF. The Separation axiom schema ($\mathrm{SEP}_{\phi(a,\overline{f})}$) asserts, for a given set a, the existence of the set $\{c \in a \mid \phi(c, \overline{f})\}$. Our Replacement axiom schema ($\mathrm{REPL}_{\phi(a,b,\overline{f})}$) is equivalent to the more standard formulation: "If for all $x \in a$ there is exactly one y such that $\phi(x, y, \overline{f})$ holds, then there is a set D such that $\forall x \in a \exists y.\ y \in D \wedge \phi(x, y, \overline{f})$ and for all $c \in D$ there is $x \in a$ such that $\phi(x, c, \overline{f})$". The Induction axiom schema ($\mathrm{IND}_{\phi(a,\overline{f})}$) states the principle of $\in$-induction, which in ZF follows from the fact that the membership relation $\in$ is well-founded. The Leibniz axiom schema ($\mathrm{L}_{\phi(a,\overline{f})}$) is usually present in the logic as a proof rule. However, as there is no clear way to assign a computational meaning to the rule, we instead make it a part of the axiom system.

The intensional version, which we call IZF_R^-, arises by removing the Leibniz axiom ($\mathrm{L}_{\phi(a,\overline{f})}$). It is also possible to define a normalizing lambda calculus for full, extensional IZF_R, but the presentation becomes less clear.

3 λZ

The lambda terms in λZ will be denoted by letters M, N, O, P. Letters x, y, z and a, b, c will be used for lambda variables. There are two kinds of lambda abstractions, one used for proofs of implications, the other for proofs of universal quantification. Letters t, s, u are reserved for IZF_R^- terms. The types in the system are IZF_R formulas.

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

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

$$\mathrm{ind}_{\phi(a,\overline{b})}(M, \overline{t}) \mid \mathrm{pairProp}(t, u_1, u_2, M) \mid \mathrm{pairRep}(t, u_1, u_2, M)$$

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

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

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

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

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

The rest of terms correspond to the rules of the first-order logic. The nature of the correspondence is expressed by the typing system in Section 3.1.

The deterministic call-by-need reduction relation $\to$ arises from the following reduction rules and evaluation contexts. In the reduction rules for ind terms, the variable x is new.

$$(\lambda x : \phi.\ M)N \to M[x := N] \quad (\lambda a.\ M)t \to M[a := t] \quad \mathrm{fst}(\langle M, N\rangle) \to M \quad \mathrm{snd}(\langle M, N\rangle) \to N$$

$$\mathrm{case}(\mathrm{inl}(M), x.N, x.O) \to N[x := M] \qquad \mathrm{case}(\mathrm{inr}(M), x.N, x.O) \to O[x := M]$$

$$\mathrm{let}\ [a, x : \phi] = [t, M]\ \mathrm{in}\ N \to N[a := t][x := M] \qquad \mathrm{axProp}(t, \overline{u}, \mathrm{axRep}(t, \overline{u}, M)) \to M$$

$$\mathrm{ind}_{\phi(a,\overline{b})}(M, \overline{t}) \to \lambda c.\ M\ c\ (\lambda b.\lambda x : b \in c.\ \mathrm{ind}_{\phi(a,\overline{b})}(M, \overline{t})\ b)$$

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

3.1 Types

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

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

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

$$\frac{\Gamma \vdash M : \phi \vee \psi \quad \Gamma, x : \phi \vdash N : \vartheta \quad \Gamma, x : \psi \vdash O : \vartheta}{\Gamma \vdash \mathrm{case}(M, x.N, x.O) : \vartheta} \qquad \frac{\Gamma \vdash M : \phi}{\Gamma \vdash \lambda a.\ M : \forall a.\ \phi}\ a \notin FV_L(\Gamma)$$

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

$$\frac{\Gamma \vdash M : \phi_A(t, \overline{u})}{\Gamma \vdash \mathrm{axRep}(t, \overline{u}, M) : t \in t_A(\overline{u})} \qquad \frac{\Gamma \vdash M : t \in t_A(\overline{u})}{\Gamma \vdash \mathrm{axProp}(t, \overline{u}, M) : \phi_A(t, \overline{u})} \qquad \frac{\Gamma \vdash M : \forall a.\ \phi}{\Gamma \vdash M\ t : \phi[a := t]}$$

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

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

Progress and Preservation (Subject Reduction) can be proved for λZ in a standard way.

4 Normalization

Theorem 1 (Normalization of λZ). *If $\vdash M : \phi$, then M normalizes.*

Proof (Sketch). First, a first-order erasure map $M \to \overline{M}$ is defined from terms of λZ to untyped lambda terms. It erases all information regarding quantifiers, logic variables and terms, while preserving computational behavior. For example, $\overline{\lambda a.M} = \overline{M}$, and $\overline{[t, M]} = \overline{M}$. One can prove, in a standard way, that if $\overline{M}$ normalizes, then so does M. Second, a realizability relation $M \Vdash \phi$ is defined in such a way that the following properties hold:

- If $M \Vdash \phi$, then M normalizes.
- If $\vdash M : \phi$, then $\overline{M} \Vdash \phi$.

By combining these definitions and facts, the theorem can be proved.

If the reduction system is extended to allow reductions anywhere in terms, Theorem 1 shows only weak normalization — the existence of a terminating reduction sequence. Strong normalization (every reduction sequence terminates) does not hold. Only a weak form of the separation axiom is needed for this effect to arise:

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

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

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

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

This counterexample can be presented in a simpler way using higher-order rewriting on top of simply-typed lambda calculus. Consider lambda calculus with simple types, two type constants A, B, corresponding to $t \in t$ and $t \in 0$, two typed constants:

$$\text{prop} : A \to (B \wedge (A \to \bot)) \qquad \text{rep} : (B \wedge (A \to \bot)) \to A$$

and a higher-order rewriting rule $\text{prop}(\text{rep}(x)) \to x$. Let $N = \lambda y : A.\ \text{snd}(\text{prop}(y))\ y$, $M = \lambda x : B.\ N\ (\text{rep}(\langle x, N\rangle))$. Then the infinite reduction sequence is exhibited by:

$$M = \lambda x : B.\ N\ (\text{rep}(\langle x, N\rangle)) = \lambda x : B.\ (\lambda y : A.\ \text{snd}(\text{prop}(y))\ y)\ \text{rep}(\langle x, N\rangle) \to$$

$$\to \lambda x : B.\ \text{snd}(\text{prop}(\text{rep}(\langle x, N\rangle)))\ \text{rep}(\langle x, N\rangle) \to \lambda x : B.\ \text{snd}(\langle x, N\rangle)\ \text{rep}(\langle x, N\rangle) \to M$$

This is essentially the computational behavior of $\lambda x.\ \Omega$, where $\Omega = (\lambda y.\ y\ y)(\lambda y.\ y\ y)$. Modulo extra type B, the constants rep and prop along with the rewriting rule establish isomorphism of A and $A \to \bot$, which makes it less surprising, as in a type system where $A = A \to \bot$ even Ω can be typed along the same lines.

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

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

The axiom (C) introduces the constant c, which denotes a non-well-founded set. The axiom (D) is an instance of the Separation axiom, the set d introduced is $\{a \in c \mid a \in a \to a \in a\}$. The lambda calculus corresponding to T is defined just as for IZF_R^-.

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

Proof. It is relatively easy to find a term O such that $\vdash_T O : d \in c$. Take $\phi = d \in d \to d \in d$. The term M below proves the claim.

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

Again, putting this counterexample in the framework of higher-order rewriting we have:

$$\text{prop} : A \to (B \wedge (A \to A)) \qquad \text{rep} : (B \wedge (A \to A)) \to A \qquad \text{prop}(\text{rep}(x)) \to x$$

The term M now behaves exactly as Ω, as this time the term O of type B can be produced.

Acknowledgments

I would like to thank anonymous referees for helpful comments.

References

1. Peter Aczel and Michael Rathjen. Notes on constructive set theory. Technical Report 40, Institut Mittag-Leffler (The Royal Swedish Academy of Sciences), 2000/2001.
2. Michael Beeson. *Foundations of Constructive Mathematics*. Springer-Verlag, 1985.
3. Robert Constable and Wojciech Moczydłowski. Extracting Programs from Constructive HOL Proofs via IZF Set-Theoretic Semantics. In *Proceedings of 3rd International Joint Conference on Automated Reasoning (IJCAR 2006)*. Springer, 2006. To appear.
4. Wojciech Moczydłowski. Normalization of IZF with Replacement. In *Proceedings of 15th Annual Conference of the EACSL (CSL 2006)*. Springer, 2006. To appear.
5. Andre Ŝĉedrov. Intuitionistic set theory. In *Harvey Friedman's Research on the Foundations of Mathematics*, pages 257–284. Elsevier, 1985.