A Simpler Undecidability Proof for System **F** Inhabitation

Andrej Dudenhefner[1] and Jakob Rehof[1]

Technical University of Dortmund, Dortmund, Germany
{andrej.dudenhefner, jakob.rehof}@cs.tu-dortmund.de

Polymorphic λ-calculus (also known as Girard's "system **F**" [3] or $\lambda 2$ [2]) is directly related to intuitionistic second-order propositional logic (IPC_2) via the Curry–Howard isomorphism (for an overview see [5]). In particular, provability in the implicational fragment of IPC_2 (is a given formula an IPC_2 theorem?) corresponds to inhabitation in system **F** (given a type, is there a term having that type in system **F**?).

Provability in IPC_2 was shown by Löb to be undecidable [4]. The proof itself is by reduction from provability in first-order predicate logic via a semantic argument. Since the original proof is heavily condensed (14 pages), Arts in collaboration with Dekkers provided a fully unfolded argument [1] (approx. 50 pages) reconstructing the original proof. Later, Sørensen and Urzyczyn developed a different, syntax oriented proof showing undecidability of inhabitation in system **F** [5, Section 11.6] (6 pages, moderately condensed).

In order to show undecidability of provability in IPC_2, each of the above approaches embeds first-order predicate logic into IPC_2. However, if one is solely interested in a concise and rigorous proof (e.g. for formalization or didactics), then there is no need for a full embedding. In fact, we can pursue a different approach to show undecidability of inhabitation in system **F**. In this extended abstract, we sketch a reduction from solvability of Diophantine equations (is there an integer solution to $P(x_1, \ldots, x_n) = 0$ where P is a polynomial with integer coefficients?) to inhabitation in system **F**. We argue that, compared to the previous approaches, the sketched reduction is more accessible for formalization and more comprehensible for didactic purposes.

First, let us fix some notation. Let *type variables* be ranged over by $a, b, c, \ldots$, we define *polymorphic types* ranged over by $\sigma, \tau, \rho, \ldots$ as

$$\sigma, \tau, \rho ::= a \mid \sigma \to \tau \mid \forall a.\sigma$$

Let $M, N, \ldots$ be ranged over Church-style polymorphic λ-calculus terms defined as

$$M, N ::= x \mid (M\, N) \mid (\lambda x : \sigma.M) \mid (\Lambda a.M) \mid M\, \tau$$

Let $\Delta = \{x_1 : \sigma_1, \ldots, x_n : \sigma_n\}$ denote finite *type environments*. Typing rules of system **F** deriving *judgements* $\Delta \vdash M : \sigma$ are as usual [5, Section 11.2].

As a starting point, we use the following Problem 1, which is undecidable by reduction (routine polynomial decomposition) from solvability of Diophantine equations.

Problem 1. *Given a set* $\mathsf{A} = \{\mathfrak{e}_1, \ldots \mathfrak{e}_l\}$ *of constraints over* $\mathcal{V} = \{a_1, \ldots, a_n\}$ *where each* $\mathfrak{e} \in \mathsf{A}$ *is of shape either* $a \doteq 1$ *or* $a \doteq b + c$ *or* $a \doteq b \cdot c$ *for some* $a, b, c \in \mathcal{V}$*, does there exist a substitution* $\zeta : \mathcal{V} \to \mathbb{N}$ *that satisfies* A*?*

Reducing Problem 1 to inhabitation in system **F** it suffices to axiomatize natural number addition and multiplication. Let us fix an instance of A of Problem 1 over variables $\{a_1, \ldots, a_n\}$. In the remainder of this long abstract we sketch the construction of a type environment Δ^{A} and type τ^{A} such that A has a solution iff there exists a term M such that $\Delta^{\mathsf{A}} \vdash M : \tau^{\mathsf{A}}$.

To simplify notation, let us define the following types (where $\dagger, \mathbf{1}, \ldots$ are standard type variables)

$$\dagger\,\sigma = \sigma \to \dagger \qquad U(\sigma) = (\dagger\sigma \to \bullet_1) \to (\sigma \to \bullet_2) \to u$$
$$S(\sigma,\tau,\rho) = (\dagger\sigma \to \bullet_1) \to (\dagger\tau \to \bullet_2) \to (\dagger\rho \to \bullet_3) \to s$$
$$P(\sigma,\tau,\rho) = (\dagger\sigma \to \bullet_1) \to (\dagger\tau \to \bullet_2) \to (\dagger\rho \to \bullet_3) \to p$$
$$\overline{a \doteq 1} = P(\mathbf{1},\mathbf{1},a) \qquad \overline{a \doteq b + c} = S(b,c,a) \qquad \overline{a \doteq b \cdot c} = P(b,c,a)$$

Intuitively, the type variable $\mathbf{1}$ represents $1 \in \mathbb{N}$, the type $U(\sigma)$ signifies that σ is an element of a universe $\mathcal{U}$, and $S(\sigma,\tau,\rho)$ (resp. $P(\sigma,\tau,\rho)$) signifies that the sum (resp. product) of the two elements σ and τ is ρ. We axiomatize natural number arithmetic as follows

$$\Delta_{\mathbb{N}} = \{x_u : \forall a.\Big(U(a) \to \forall b.(U(b) \to S(a,\mathbf{1},b) \to P(b,\mathbf{1},b) \to \blacktriangle) \to \blacktriangle\Big),$$
$$x_s : \forall abcde.\Big(U(a) \to U(b) \to U(c) \to U(d) \to U(e) \to$$
$$S(a,b,c) \to S(b,\mathbf{1},d) \to S(c,\mathbf{1},e) \to (S(a,d,e) \to \blacktriangle) \to \blacktriangle\Big),$$
$$x_p : \forall abcde.\Big(U(a) \to U(b) \to U(c) \to U(d) \to U(e) \to$$
$$P(a,b,c) \to S(b,\mathbf{1},d) \to S(c,a,e) \to (P(a,d,e) \to \blacktriangle) \to \blacktriangle\Big), y_u^{U(\mathbf{1})} : U(\mathbf{1}), y_p^{P(\mathbf{1},\mathbf{1},\mathbf{1})} : P(\mathbf{1},\mathbf{1},\mathbf{1})\}$$

Type assumptions in $\Delta_{\mathbb{N}}$ encompass the following assertions about members of a universe $\mathcal{U}$

- $y_u^{U(\mathbf{1})}$ asserts that $\mathbf{1} \in \mathcal{U}$ and $y_p^{P(\mathbf{1},\mathbf{1},\mathbf{1})}$ asserts that $\mathbf{1} \cdot \mathbf{1} = \mathbf{1}$
- x_u asserts that for any $a \in \mathcal{U}$ there is $b \in \mathcal{U}$ such that $a + \mathbf{1} = b$ and $b \cdot \mathbf{1} = b$
- x_s asserts for $a,b,c,d,e \in \mathcal{U}$: if $a + b = c$, $b + \mathbf{1} = d$ and $c + \mathbf{1} = e$, then $a + d = e$
- x_p asserts for $a,b,c,d,e \in \mathcal{U}$: if $a \cdot b = c$, $b + \mathbf{1} = d$ and $c + a = e$, then $a \cdot d = e$

Let $\Delta^{\mathsf{A}} = \Delta_{\mathbb{N}} \cup \{x_{\mathsf{A}} : \forall a_1 \ldots a_n.\Big(U(a_1) \to \ldots \to U(a_n) \to \overline{\mathfrak{C}_1} \to \ldots \to \overline{\mathfrak{C}_l} \to \blacktriangle\Big)\}$ and $\tau^{\mathsf{A}} = \blacktriangle$. We are able to establish soundness (cf. Theorem 1) and completeness (cf. Theorem 2) of our encoding.

Theorem 1 (Soundness)**.** *If $\Delta^{\mathsf{A}} \vdash M : \tau^{\mathsf{A}}$ for some M, then A has a solution.*

Theorem 2 (Completeness)**.** *If A has a solution, then $\Delta^{\mathsf{A}} \vdash M : \tau^{\mathsf{A}}$ for some M.*

A rigorous proof of soundness by routine case analysis uses the key property of system **F** that any inhabited type is inhabited by some β-normal η-long Church-style term. The proof of completeness is by direct construction of an inhabitant for a given solution of A. A formalization of the above reduction is currently under development.

References

[1] T. Arts and W. Dekkers. Embedding first order predicate logic in second order propositional logic. *Master's thesis, University of Nijmegen*, 1992.

[2] H. Barendregt. Introduction to generalized type systems. *J. Funct. Program.*, 1(2):125–154, 1991.

[3] J. Girard. *Interprétation fonctionelle et élimination des coupures de l'arithmétique d'ordre supérieur*. PhD thesis, Université Paris VII, 1972.

[4] M. H. Löb. Embedding first order predicate logic in fragments of intuitionistic logic. *J. Symb. Log.*, 41(4):705–718, 1976.

[5] M. H. Sørensen and P. Urzyczyn. *Lectures on the Curry-Howard Isomorphism*, volume 149 of *Studies in Logic and the Foundations of Mathematics*. Elsevier, 2006.