A Simpler Undecidability Proof for System F Inhabitation

Andrej Dudenhefner
Technical University of Dortmund, Dortmund, Germany
andrej.dudenhefner@cs.tu-dortmund.de

Jakob Rehof
Technical University of Dortmund, Dortmund, Germany
jakob.rehof@cs.tu-dortmund.de

Abstract

Provability in the intuitionistic second-order propositional logic (resp. inhabitation in the polymorphic lambda-calculus) was shown by Löb to be undecidable in 1976. Since the original proof is heavily condensed, Arts in collaboration with Dekkers provided a fully unfolded argument in 1992 spanning approximately fifty pages. Later in 1997, Urzyczyn developed a different, syntax oriented proof. Each of the above approaches embeds (an undecidable fragment of) first-order predicate logic into second-order propositional logic.

In this work, we develop a simpler undecidability proof by 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?). Compared to the previous approaches, the given reduction is more accessible for formalization and more comprehensible for didactic purposes. Additionally, we formalize soundness and completeness of the reduction in the Coq proof assistant under the banner of "type theory inside type theory".

2012 ACM Subject Classification Theory of computation → Type theory

Keywords and phrases System F, Lambda Calculus, Inhabitation, Propositional Logic, Provability, Undecidability, Coq, Formalization

Digital Object Identifier 10.4230/LIPIcs.TYPES.2018.2

Supplement Material `https://github.com/mrhaandi/ipc2`

Acknowledgements We would like to thank Paweł Urzyczyn for sharing his insights on second order propositional logic provability, which helped to develop the presented results.

1 Introduction

Polymorphic λ-calculus (also known as Girard's system **F** [7] or $\lambda 2$ [2]) is directly related to intuitionistic second-order propositional logic (IPC_2) via the Curry–Howard isomorphism (for an overview see [11]). 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 [8] (see also [5] for an earlier approach by Gabbay in an extension of IPC_2). Löb's proof 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] (50 pages) reconstructing the original proof. Later, Urzyczyn developed a different, syntax oriented proof showing undecidability of inhabitation in system **F** [13] (6 pages, moderately condensed). Urzyczyn's proof is by reduction from two-counter automata to a fragment of first-order predicate logic to inhabitation in system **F**. In 2010 Sørensen and Urzyczyn [12] gave a general translation of intuitionistic first-order predicate logic, covering the full set of logical connectives, into intuitionistic second-order propositional logic.

In order to show undecidability of provability in IPC_2, each of the above approaches embeds (a fragment of) first-order predicate logic into IPC_2. However, if one is solely interested in a concise and rigorous undecidability proof (e.g. for formalization or didactics), then there is no need to represent an expressive logic.

In this work we provide 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**. Compared to the previous approaches, the described reduction is more accessible for formalization and more comprehensible for didactic purposes. Compared to Löb's proof, we separate IPC_2 proof normalization from the main argument. Compared to Urzyczyn's proof, we only need to axiomatize natural number addition and multiplication, instead of a fragment of first-order predicate logic.

Additionally, we formalize [3] soundness and completeness of the reduction in the Coq proof assistant under the banner of "type theory inside type theory".

Organization of the paper. The polymorphic λ-calculus (system **F**) is described in Section 2 together with the associated inhabitation problem (Problem 6). In Section 3 we reduce a decision problem (Problem 9), which is equivalent to solvability of Diophantine equations, to inhabitation in system **F**. Additionally, in Paragraph 3.3 we outline a formalization of soundness (Theorem 27) and completeness (Theorem 19) of the described reduction. We conclude the paper in Section 4.

2 Polymorphic Lambda-Calculus

The Polymorphic Lambda-Calculus (also known as Girard's system **F** [7] or $\lambda 2$ [2]) provides a concise proof notation for the implicational fragment of intuitionistic second-order propositional logic (IPC_2) under the Curry-Howard isomorphism. In this section we assemble necessary prerequisites in order to discuss inhabitation in system **F** (or equivalently provability in IPC_2).

We denote *polymorphic types* (Definition 1) by σ, τ, ρ, where *type variables* are denoted by a, b, c and drawn from the denumerable set $\mathbb{A}$. Conventionally, the operator $\to$ binds more strongly than $\forall$.

▶ **Definition 1** (Polymorphic Types, $\mathbb{T}$). $\mathbb{T} \ni \sigma, \tau, \rho ::= a \mid (\sigma \to \tau) \mid (\forall a.\sigma)$

Type variables that are not *bound* by the operator $\forall$ are *free*, and the set of free type variables in a type σ is denoted by $\mathrm{Var}(\sigma) = \{a \in \mathbb{A} \mid a \text{ is free in } \sigma\}$. A *substitution* of occurrences of a free type variable a in σ by τ is denoted by $\sigma[a := \tau]$.

We denote *Church-style polymorphic λ-terms* (Definition 2) by M, N, where *term variables* are denoted by x, y, z.

▶ **Definition 2** (Church-style Polymorphic λ-Terms).
$M, N ::= x \mid (M\ N) \mid (\lambda x : \sigma.M) \mid (\Lambda a.M) \mid (M\ \tau)$

A *type environment*, denoted by Δ, is a finite set of *type assumptions* having the shape $x : \sigma$ for distinct term variables.

▶ **Definition 3** (Type Environment). $\Delta ::= \{x_1 : \sigma_1, \ldots, x_n : \sigma_n\}$ *where* $x_i \neq x_j$ *for* $i \neq j$

We define the *domain*, the *erasure*, the *extension* of Δ, and the *free type variables* in Δ.

▶ **Definition 4** (Domain, Erasure, Extension, Free Type Variables).

$$\mathrm{dom}(\Delta) = \{x_1, \ldots, x_n\} \qquad |\Delta| = \{\sigma_1, \ldots, \sigma_n\}$$

$$\Delta, x : \sigma = \Delta \cup \{x : \sigma\} \text{ if } x \notin \mathrm{dom}(\Delta) \qquad \mathrm{Var}(\Delta) = \bigcup_{\sigma \in |\Delta|} \mathrm{Var}(\sigma)$$

The rules of the system **F** with *judgements* of shape $\Delta \vdash M : \sigma$ are given below (cf. [11, Section 12]). This system enjoys subject reduction and strong normalization properties.

▶ **Definition 5** (system **F**).

$$\frac{}{\Delta, x : \tau \vdash x : \tau}\ (\mathrm{Ax})$$

$$\frac{\Delta \vdash M : \sigma \to \tau \qquad \Delta \vdash N : \sigma}{\Delta \vdash M\ N : \tau}\ (\to\mathrm{E}) \qquad \frac{\Delta \vdash M : \forall a.\sigma}{\Delta \vdash M\ \tau : \sigma[a := \tau]}\ (\forall\mathrm{E})$$

$$\frac{\Delta, x : \sigma \vdash M : \tau}{\Delta \vdash \lambda x : \sigma.M : \sigma \to \tau}\ (\to\mathrm{I}) \qquad \frac{\Delta \vdash M : \tau \qquad a \notin \mathrm{Var}(\Delta)}{\Delta \vdash \Lambda a.M : \forall a.\tau}\ (\forall\mathrm{I})$$

We sometimes superscript types assigned to subterms in a derivation of a judgement, e.g.

$$\emptyset \vdash \Big(\lambda x : (\forall a.a \to a).\big((x\ (b \to b))^{(b\to b)\to(b\to b)}\ (x\ b)\big)^{b\to b}\Big)\ \Big(\Lambda a.\lambda y : a.y\Big)^{\forall a.a\to a} : b \to b$$

One core decision problem for any typing system is *inhabitation* (Problem 6).

▶ **Problem 6** (Inhabitation, $\Delta \vdash ? : \tau$). *Given a type environment Δ and a type τ, is there a term M such that $\Delta \vdash M : \tau$?*

Inhabitation in system **F** directly corresponds to provability in IPC_2 [11, Section 12] (Proposition 7).

▶ **Proposition 7.** *$\Delta \vdash M : \tau$ iff τ is derivable from $|\Delta|$ in the intuitionistic second-order propositional logic.*

Whenever the particular inhabitant M is immaterial, we write $|\Delta| \vdash \tau$ for $\Delta \vdash M : \tau$. A key property of system **F** is that given a type derivation $\Delta \vdash M : \tau$, there exists a term N^τ in β-normal η-*long* form such that $\Delta \vdash N : \tau$ [13, Lemma 4]. The property of η-longness (Definition 8, cf. *fully applied* in [13]) is defined inductively, taking into account types (ascribed in supersripts) which are assigned to individual subterms.

▶ **Definition 8** (η-longness). *A term M^τ is η-long if one of the following conditions is met*

- *$M^\tau = x^\sigma\ t_1 \ldots t_n$ and $\tau = a$ for some term variable x, type variable a and types or η-long terms $t_1, \ldots, t_n$*
- *$M^\tau = (\lambda x : \sigma.N^\rho)^{\sigma\to\rho}$ where N^ρ is η-long*
- *$M^\tau = (\Lambda a.N^\rho)^{\forall a.\rho}$ where N^ρ is η-long*

We say that N is a *long normal inhabitant* of τ in Δ, if $\Delta \vdash N : \tau$ and N^τ is in β-normal η-long form.

3 Undecidability of Inhabitation

In the remainder of this work we use $\mathbb{N}$ to denote the set of positive integers. As a starting point, we use the following Problem 9, which is undecidable by reduction from solvability of Diophantine equations (for an overview see [9]). In particular, solvability of Diophantine equations in integers is equivalent to solvability of Diophantine equations in $\mathbb{N}$, which by routine subterm decomposition is equivalent to Problem 9.

▶ **Problem 9.** *Given a set* $\mathsf{A} = \{\mathfrak{e}_1, \dots \mathfrak{e}_l\}$ *of constraints over variables* $\mathcal{V} = \{a_1, \dots, a_n\}$ *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*?*

▶ **Proposition 10.** *Problem 9 is undecidable.*

In order to reduce Problem 9 to inhabitation in system **F** it suffices to axiomatize natural number addition and multiplication. Let us fix an instance A of Problem 9 over variables $\mathcal{V} = \{a_1, \dots, a_n\}$. In the remainder of this section we construct the type environment Δ_{A} such that A has a solution iff there exists a term M such that $\Delta_{\mathsf{A}} \vdash M : \blacktriangle$.

For our construction let us fix the type variables $\dagger, u, s, p, \blacktriangle, \bullet_1, \bullet_2, \bullet_3$ and $\bar{i}$ for $i \in \mathbb{N}$. Additionally, for each variable $a_i \in \mathcal{V}$ let us fix the type variable a_i.

Similarly to [13, Section 7], we define the following types to represent particular predicates on natural numbers.

▶ **Definition 11** (Types $\dagger\sigma, U(\sigma), S(\sigma,\tau,\rho), P(\sigma,\tau,\rho)$)**.**

$$\begin{aligned}
\dagger\sigma &= \sigma \to \dagger \\
U(\sigma) &= (\dagger\sigma \to \bullet_1) \to (\sigma \to \bullet_2) \to u \\
S(\sigma,\tau,\rho) &= (\dagger\sigma \to \bullet_1) \to (\dagger\tau \to \bullet_2) \to (\dagger\rho \to \bullet_3) \to s \\
P(\sigma,\tau,\rho) &= (\dagger\sigma \to \bullet_1) \to (\dagger\tau \to \bullet_2) \to (\dagger\rho \to \bullet_3) \to p
\end{aligned}$$

Intuitively, the type $U(\sigma)$ is used to assert that σ represents a natural number, and $S(\sigma,\tau,\rho)$ (resp. $P(\sigma,\tau,\rho)$) is used to assert that the sum (resp. product) of natural numbers represented by σ and τ is represented by ρ. The motivation behind the above encoding (including types $\dagger\sigma$) is of technical nature, leading to convenient inversion lemmas.

Using above types, we represent constraints as follows

▶ **Definition 12** (Constraint Representation)**.**

$$\overline{a \doteq 1} = P(\overline{1}, \overline{1}, a) \qquad \overline{a \doteq b + c} = S(b, c, a) \qquad \overline{a \doteq b \cdot c} = P(b, c, a)$$

Next, we axiomatize finite fragments of natural number arithmetic as follows

▶ **Definition 13** (Type Environments $\Delta_{\mathbb{N}}, \Delta_{\overline{1}}$)**.**

$$\begin{aligned}
\Delta_{\mathbb{N}} = \Big\{ & x_u : \forall a.\Big(U(a) \to \forall b.(U(b) \to S(a,\overline{1},b) \to P(b,\overline{1},b) \to \blacktriangle) \to \blacktriangle\Big), \\
& x_s : \forall abcde.\Big(U(a) \to U(b) \to U(c) \to U(d) \to U(e) \to \\
& \qquad S(a,b,c) \to S(b,\overline{1},d) \to S(c,\overline{1},e) \to (S(a,d,e) \to \blacktriangle) \to \blacktriangle\Big), \\
& x_p : \forall abcde.\Big(U(a) \to U(b) \to U(c) \to U(d) \to U(e) \to \\
& \qquad P(a,b,c) \to S(b,\overline{1},d) \to S(c,a,e) \to (P(a,d,e) \to \blacktriangle) \to \blacktriangle\Big)\Big\} \\
\Delta_{\overline{1}} = \big\{ & y_{U(\overline{1})} : U(\overline{1}), y_{P(\overline{1},\overline{1},\overline{1})} : P(\overline{1},\overline{1},\overline{1})\big\}
\end{aligned}$$

As we will see in the subsequent development, type assumptions in $\Delta_{\mathbb{N}} \cup \Delta_{\overline{1}}$ encompass the following assertions about members of a universe $\mathcal{U}$ which represent natural numbers

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

The choice of $\Delta_{\mathbb{N}}$ is motivated by the fact that a solution of A is supported by an appropriately large finite fragment of natural number arithmetic and does not require the induction principle.

Let the type environment Δ_{A} (Definition 14) encompass the axiomatization of natural number arithmetic together with the assumption that the representation of a solution of A implies $\blacktriangle$. We will reduce solvability of A to $\Delta_{\mathsf{A}} \vdash ? : \blacktriangle$.

▶ **Definition 14** (Type Environments $\Delta_I, \Delta_{\mathsf{A}}$).

$$\Delta_I = \Delta_{\mathbb{N}} \cup \left\{ x_{\mathsf{A}} : \forall a_1 \dots a_n.\big(U(a_1) \to \dots \to U(a_n) \to \overline{\mathfrak{e}_{\overline{1}}} \to \dots \to \overline{\mathfrak{e}_{\overline{\mathsf{I}}}} \to \blacktriangle\big) \right\}$$

$$\Delta_{\mathsf{A}} = \Delta_I \cup \Delta_{\overline{1}}$$

In the above, the type variable $\blacktriangle$ assumes the role of the type variable **false** in [13]. Whereas [13] uses a positive description of first-order predicate logic, we (again, for technical convenience) use doubly-negated conclusions in $\Delta_{\mathbb{N}}$. Following this intuition, the type of x_u corresponds to $\forall a.U(a) \to \neg(\forall b.\neg(U(b) \wedge S(a, \overline{1}, b) \wedge P(b, \overline{1}, b)))$ (cf. list of assertions above). Possibly, we could have used a more natural second-order axiomatization of natural numbers with conventional negation ($\neg\sigma = \sigma \to \forall a.a$) and existential ($\exists a.\sigma = \forall b.((\forall a.(\sigma \to b)) \to b)$) representations. However, both introduce additional universal quantifiers that are neither necessary nor convenient in the proof.

In the remainder of this section we establish completeness (Theorem 19) and soundness (Theorem 27) of the reduction from solvability of A to $\Delta_{\mathsf{A}} \vdash ? : \blacktriangle$.

3.1 Completeness

In this paragraph we show that satisfiability of A implies $\Delta_{\mathsf{A}} \vdash M : \blacktriangle$ for some term M. Intuitively, we derive $|\Delta_{\mathsf{A}}| \vdash \blacktriangle$ in four steps by approaching the goal $\blacktriangle$ many times, each time adding new assumptions. Step 1 introduces representations $\overline{2}, \dots, \overline{\mathsf{N}}$ of natural numbers $2, \dots, \mathsf{N}$, where N is the maximal element in the codomain of some solution of A. Additionally, step 1 introduces assumptions $U(\bar{i})$, $S(\overline{i-1}, \overline{1}, \bar{i})$ and $P(\bar{i}, \overline{1}, \bar{i})$ for $i = 2 \dots \mathsf{N}$. Step 2 introduces information on addition for numbers $1, \dots, \mathsf{N}$, i.e. for $i+j = k \leq \mathsf{N}$ we introduce the assumption $S(\bar{i}, \bar{j}, \bar{k})$. Step 3 introduces information on multiplication for numbers $1, \dots, \mathsf{N}$, i.e. for $i \cdot j = k \leq \mathsf{N}$ we introduce the assumption $P(\bar{i}, \bar{j}, \bar{k})$. Finally, step 4 uses the introduced assumptions to derive $\blacktriangle$ using $x_{\mathsf{A}} : \forall a_1 \dots a_n.\big(U(a_1) \to \dots \to U(a_n) \to \overline{\mathfrak{e}_{\overline{1}}} \to \dots \to \overline{\mathfrak{e}_{\overline{\mathsf{I}}}} \to \blacktriangle\big)$.

For a more accessible presentation of the proof of completeness (Theorem 19), we define type environments $\Delta_U^m, \Delta_S^m, \Delta_P^m$ that contain assumptions for natural numbers up to a bound m that are introduced using x_u. Observe that $\Delta_{\overline{1}} = \Delta_U^1 \cup \Delta_S^1 \cup \Delta_P^1$.

▶ **Definition 15** (Type Environments $\Delta_U^m, \Delta_S^m, \Delta_P^m$). *For $m \in \mathbb{N}$ let*

$$\Delta_U^m = \{ y_{U(\bar{i})} : U(\bar{i}) \mid i = 1 \dots m \}$$

$$\Delta_S^m = \{ y_{S(\overline{i-1},\overline{1},\bar{i})} : S(\overline{i-1}, \overline{1}, \bar{i}) \mid i = 2 \dots m \}$$

$$\Delta_P^m = \{ y_{P(\bar{i},\overline{1},\bar{i})} : P(\bar{i}, \overline{1}, \bar{i}) \mid i = 1 \dots m \}$$

The following Lemmas 16, 17, and 18 each contain the inductive argument used in the outlined steps 1, 2, and 3. Specifically, these lemmas are used to introduce sufficient information on representations of natural numbers to verify a solution of A.

▶ **Lemma 16.** *Let $m \in \mathbb{N}$. If $\Delta_I \cup \Delta_U^{m+1} \cup \Delta_S^{m+1} \cup \Delta_P^{m+1} \vdash N : \blacktriangle$, then $\Delta_I \cup \Delta_U^m \cup \Delta_S^m \cup \Delta_P^m \vdash M : \blacktriangle$ for some M.*

Proof. Immediate using $M = x_u\ \overline{m}\ y_{U(\overline{m})}\ (\Lambda\overline{m+1}.M')$, where
$M' = \lambda y_{U(\overline{m+1})} : U(\overline{m+1}).\lambda y_{S(\overline{m},\overline{1},\overline{m+1})} : S(\overline{m}, \overline{1}, \overline{m+1}).\lambda y_{P(\overline{m+1},\overline{1},\overline{m+1})} : P(\overline{m+1}, \overline{1}, \overline{m+1}).N$. ◀

▶ **Lemma 17.** *Let $i,j,k,m \in \mathbb{N}$ be such that $i,j,k \leq m$ and let $\Delta_S \supseteq \Delta_S^m$ be a type environment such that $(y_{S(\bar{i},\bar{j},\bar{k})} : S(\bar{i},\bar{j},\bar{k})) \in \Delta_S$.*
If $\Delta_I \cup \Delta_U^m \cup \Delta_S \cup \{y_{S(\bar{i},\overline{j+1},\overline{k+1})} : S(\bar{i},\overline{j+1},\overline{k+1})\} \cup \Delta_P^m \vdash N : \blacktriangle$,
then $\Delta_I \cup \Delta_U^m \cup \Delta_S \cup \Delta_P^m \vdash M : \blacktriangle$ for some M.

Proof. Immediate using
$M = x_s\ \bar{i}\ \bar{j}\ \bar{k}\ \overline{j+1}\ \overline{k+1}\ y_{U(\bar{i})}\ y_{U(\bar{j})}\ y_{U(\bar{k})}\ y_{U(\overline{j+1})}\ y_{U(\overline{k+1})}\ y_{S(\bar{i},\bar{j},\bar{k})}\ y_{S(\bar{j},\bar{1},\overline{j+1})}\ y_{S(\bar{k},\bar{1},\overline{k+1})}\ M'$,
where $M' = \lambda y_{S(\bar{i},\overline{j+1},\overline{k+1})} : S(\bar{i},\overline{j+1},\overline{k+1}).N$. ◀

▶ **Lemma 18.** *Let $i,j,k,m \in \mathbb{N}$ be such that $i,j,k \leq m$, $\Delta_S \supseteq \Delta_S^m$ be such that $(y_{S(\bar{k},\bar{i},\overline{k+i})} : S(\bar{k},\bar{i},\overline{k+i})) \in \Delta_S$ and Δ_P be such that $(y_{P(\bar{i},\bar{j},\bar{k})} : P(\bar{i},\bar{j},\bar{k})) \in \Delta_P$.*
If $\Delta_I \cup \Delta_U^m \cup \Delta_S \cup \Delta_P \cup \{y_{P(\bar{i},\overline{j+1},\overline{k+i})} : P(\bar{i},\overline{j+1},\overline{k+i})\} \vdash N : \blacktriangle$,
then $\Delta_I \cup \Delta_U^m \cup \Delta_S \cup \Delta_P \vdash M : \blacktriangle$ for some M.

Proof. Immediate using
$M = x_p\ \bar{i}\ \bar{j}\ \bar{k}\ \overline{j+1}\ \overline{k+i}\ y_{U(\bar{i})}\ y_{U(\bar{j})}\ y_{U(\bar{k})}\ y_{U(\overline{j+1})}\ y_{U(\overline{k+i})}\ y_{P(\bar{i},\bar{j},\bar{k})}\ y_{S(\bar{j},\bar{1},\overline{j+1})}\ y_{S(\bar{k},\bar{i},\overline{k+i})}\ M'$,
where $M' = \lambda y_{P(\bar{i},\overline{j+1},\overline{k+i})} : P(\bar{i},\overline{j+1},\overline{k+i}).N$. ◀

By repeated application of the above Lemmas 16, 17, and 18 we show that a solution of A induces an inhabitant M such that $\Delta_{\mathsf{A}} \vdash M : \blacktriangle$.

▶ **Theorem 19** (Completeness)**.** *If A has a solution, then $\Delta_{\mathsf{A}} \vdash M : \blacktriangle$ for some M.*

Proof. Let $\zeta : \mathcal{V} \to \mathbb{N}$ solve A, and let $\mathsf{N} = \max\{\zeta(a) \mid a \in \mathcal{V}\}$. We derive $\Delta_{\mathsf{A}} \vdash M : \blacktriangle$ in four steps.

Step 1: By repeated application of Lemma 16, in order to derive $|\Delta_{\mathsf{A}}| \vdash \blacktriangle$, it suffices to derive $|\Delta_I \cup \Delta_U^{\mathsf{N}} \cup \Delta_S^{\mathsf{N}} \cup \Delta_P^{\mathsf{N}}| \vdash \blacktriangle$. Observe that

- For $S(\bar{i},\bar{j},\bar{k}) \in |\Delta_S^{\mathsf{N}}|$ we have $j = 1$ and $i + j = k$
- For $P(\bar{i},\bar{j},\bar{k}) \in |\Delta_P^{\mathsf{N}}|$ we have $j = 1$ and $i \cdot j = k$

Step 2: By repeated application of Lemma 17, in order to derive $|\Delta_I \cup \Delta_U^{\mathsf{N}} \cup \Delta_S^{\mathsf{N}} \cup \Delta_P^{\mathsf{N}}| \vdash \blacktriangle$, it suffices to derive $|\Delta_I \cup \Delta_U^{\mathsf{N}} \cup \Delta_S \cup \Delta_P^{\mathsf{N}}| \vdash \blacktriangle$,
where $\Delta_S = \{y_{S(\bar{i},\bar{j},\bar{k})} : S(\bar{i},\bar{j},\bar{k}) \mid i,j,k \in \mathbb{N} \text{ and } i + j = k \leq \mathsf{N}\}$.

Step 3: By repeated application of Lemma 18, in order to derive $|\Delta_I \cup \Delta_U^{\mathsf{N}} \cup \Delta_S \cup \Delta_P^{\mathsf{N}}| \vdash \blacktriangle$, it suffices to derive $|\Delta_I \cup \Delta_U^{\mathsf{N}} \cup \Delta_S \cup \Delta_P| \vdash \blacktriangle$,
where $\Delta_P = \{y_{P(\bar{i},\bar{j},\bar{k})} : P(\bar{i},\bar{j},\bar{k}) \mid i,j,k \in \mathbb{N} \text{ and } i \cdot j = k \leq \mathsf{N}\}$.

Step 4: Finally, the claim follows from the following judgement

$$\Delta_I \cup \Delta_U^{\mathsf{N}} \cup \Delta_S \cup \Delta_P \vdash x_{\mathsf{A}}\ \overline{\zeta(a_1)} \ldots \overline{\zeta(a_n)}\ y_{U(\overline{\zeta(a_1)})} \cdots y_{U(\overline{\zeta(a_n)})}\ y_{\overline{\mathfrak{e}_1}} \ldots y_{\overline{\mathfrak{e}_l}} : \blacktriangle$$

In particular, we have

- $\zeta(a_i) \leq \mathsf{N}$ implies $U(\overline{\zeta(a_i)}) \in |\Delta_U^{\mathsf{N}}|$ for $i = 1 \ldots n$
- $\zeta(a) = 1$ implies $\overline{\overline{\zeta(a)} \doteq 1} = P(\bar{1},\bar{1},\bar{1}) \in |\Delta_P|$
- $\zeta(a) = \zeta(b) + \zeta(c) \leq \mathsf{N}$ implies $\overline{\overline{\zeta(a)} \doteq \overline{\zeta(b)} + \overline{\zeta(c)}} = S(\overline{\zeta(b)},\overline{\zeta(c)},\overline{\zeta(a)}) \in |\Delta_S|$
- $\zeta(a) = \zeta(b) \cdot \zeta(c) \leq \mathsf{N}$ implies $\overline{\overline{\zeta(a)} \doteq \overline{\zeta(b)} \cdot \overline{\zeta(c)}} = P(\overline{\zeta(b)},\overline{\zeta(c)},\overline{\zeta(a)}) \in |\Delta_P|$ ◀

3.2 Soundness

In this paragraph we show that $\Delta_{\mathsf{A}} \vdash M : \blacktriangle$ implies satisfiability of A. Intuitively, we show that a derivation of $\Delta_{\mathsf{A}} \vdash M : \blacktriangle$, where M is β-normal and η-long, necessarily completes (parts of) the four steps described in Section 3.1, only adding sound assumptions wrt. addition and multiplication.

Let us define the set of types $\mathcal{C}$ (Definition 20), observing that $\dagger \notin \mathcal{C}$ and $\overline{1} \notin \mathcal{C}$.

▶ **Definition 20** (Set of Types $\mathcal{C}$). $\mathcal{C} = \{u, s, p, \blacktriangle, \bullet_1, \bullet_2, \bullet_3\}$.

We use $\mathcal{C}$, from which any formula in $|\Delta_{\mathsf{A}}|$ is derivable, to hide particular structure of Δ_{A} and identify certain types that are "logically equivalent" wrt. Δ_{A}.

▶ **Lemma 21.** *Let $a, b \in \mathbb{A} \setminus (\mathcal{C} \cup \{\dagger\})$ be type variables. If $\mathcal{C} \vdash \dagger a \to \dagger b$, then $a = b$.*

Proof. A long normal inhabitant M of $\dagger a \to \dagger b$ in $\mathcal{C}$ is necessarily of the shape $M = \lambda x : \dagger a.\lambda y : b.(x^{\dagger a}\ y^{b})^{\dagger}$, which implies $a = b$. ◀

▶ **Corollary 22.** *Let σ, τ be types and let $a, b \in \mathbb{A} \setminus (\mathcal{C} \cup \{\dagger\})$ be type variables. If $\mathcal{C} \vdash \dagger a \to \dagger\sigma$, $\mathcal{C} \vdash \dagger\sigma \to \dagger\tau$ and $\mathcal{C} \vdash \dagger\tau \to \dagger b$, then $a = b$.*

Using the above Corollary 22 we can lift functions with type variable domain to functions with type domain (Definition 23).

▶ **Definition 23.** *Given a map $[\![\cdot]\!] : \mathcal{U} \to \mathbb{N}$ for some finite set $\mathcal{U} \subseteq \mathbb{A} \setminus (\mathcal{C} \cup \{\dagger\})$ of type variables, we define $[\![\cdot]\!]^* : \mathbb{T} \to \mathbb{N}$ by* $[\![\sigma]\!]^* = \begin{cases} [\![a]\!] & \text{if } a \in \mathcal{U},\ \mathcal{C} \vdash \dagger a \to \dagger\sigma \text{ and } \mathcal{C} \vdash \dagger\sigma \to \dagger a \\ \text{undefined} & \text{otherwise, i.e. there is no such } a \end{cases}$

By Corollary 22 the partial map $[\![\cdot]\!]^* : \mathbb{T} \to \mathbb{N}$ is well-defined. Intuitively, the condition $\mathcal{C} \vdash \dagger a \to \dagger\sigma$ and $\mathcal{C} \vdash \dagger\sigma \to \dagger a$ identifies σ with a wrt. Δ_{A} in the sense of the following Lemma 24.

▶ **Lemma 24.** *Let $\sigma \in \mathbb{T}$ be a type and let $\mathcal{U} \subseteq \mathbb{A} \setminus (\mathcal{C} \cup \{\dagger\})$ be a finite set of type variables. If $\{s, p, \blacktriangle\} \cup \{U(a) \mid a \in \mathcal{U}\} \vdash U(\sigma)$, then $\mathcal{C} \vdash \dagger a \to \dagger\sigma$ and $\mathcal{C} \vdash \dagger\sigma \to \dagger a$ for some $a \in \mathcal{U}$.*

Proof. A long normal inhabitant M of $U(\sigma)$ is necessarily of the shape

$$M = \lambda x_1 : \dagger\sigma \to \bullet_1.\lambda x_2 : \sigma \to \bullet_2.z^{U(a)}\ (\lambda y_1 : \dagger a.x_1\ N_1^{\dagger\sigma})^{\dagger a \to \bullet_1}\ (\lambda y_2 : a.x_2\ N_2^{\sigma})^{a \to \bullet_2}$$

for some $a \in \mathcal{U}$. Therefore, for $\Gamma = \{s, p, \blacktriangle\} \cup \{U(a) \mid a \in \mathcal{U}\}$ we have

1. $\Gamma, \dagger\sigma \to \bullet_1, \sigma \to \bullet_2, \dagger a \vdash \dagger\sigma$ which implies $\mathcal{C} \vdash \dagger a \to \dagger\sigma$
2. $\Gamma, \dagger\sigma \to \bullet_1, \sigma \to \bullet_2, a \vdash \sigma$ which implies $\mathcal{C} \vdash a \to \sigma$, therefore $\mathcal{C} \vdash \dagger\sigma \to \dagger a$ ◀

▶ **Corollary 25.** *Let $\sigma \in \mathbb{T}$ be a type and let $[\![\cdot]\!] : \mathcal{U} \to \mathbb{N}$ be a map for some finite set $\mathcal{U} \subseteq \mathbb{A} \setminus (\mathcal{C} \cup \{\dagger\})$ of type variables. If $\{s, p, \blacktriangle\} \cup \{U(a) \mid a \in \mathcal{U}\} \vdash U(\sigma)$, then $[\![\sigma]\!]^* \in \mathbb{N}$.*

The above Corollary 25 establishes a correspondence between σ and some type variable $a \in \mathcal{U}$ via derivability of $U(\sigma)$. This will allow us to reason about arbitrary (impredicative) instances of types in Δ_{A}. The following Lemma 26 extends this correspondence to sums and products.

▶ **Lemma 26.** *Given a map* $[\![\cdot]\!] : \mathcal{U} \to \mathbb{N}$ *for some finite set* $\mathcal{U} \subseteq \mathbb{A} \setminus (\mathcal{C} \cup \{\dagger\})$ *of type variables, let* $\Gamma_S \subseteq \{S(\sigma_1, \sigma_2, \sigma_3) \mid [\![\sigma_1]\!]^* + [\![\sigma_2]\!]^* = [\![\sigma_3]\!]^* \in \mathbb{N}\}$ *and* $\Gamma_P \subseteq \{P(\sigma_1, \sigma_2, \sigma_3) \mid [\![\sigma_1]\!]^* \cdot [\![\sigma_2]\!]^* = [\![\sigma_3]\!]^* \in \mathbb{N}\}$.
For types $\tau_1, \tau_2, \tau_3 \in \mathbb{T}$ *such that* $[\![\tau_1]\!]^*, [\![\tau_2]\!]^*, [\![\tau_3]\!]^* \in \mathbb{N}$ *we have*
(*i*) *If* $\{u, p, \blacktriangle\} \cup \Gamma_S \vdash S(\tau_1, \tau_2, \tau_3)$, *then* $[\![\tau_1]\!]^* + [\![\tau_2]\!]^* = [\![\tau_3]\!]^* \in \mathbb{N}$.
(*ii*) *If* $\{u, s, \blacktriangle\} \cup \Gamma_P \vdash P(\tau_1, \tau_2, \tau_3)$, *then* $[\![\tau_1]\!]^* \cdot [\![\tau_2]\!]^* = [\![\tau_3]\!]^* \in \mathbb{N}$.

Proof. For (*i*), let $\Gamma = \{u, p, \blacktriangle\} \cup \Gamma_S$ and assume $\Gamma \vdash S(\tau_1, \tau_2, \tau_3)$. A long normal inhabitant M of $S(\tau_1, \tau_2, \tau_3)$ is necessarily of the shape

$$M = \lambda x_1 : \dagger\tau_1 \to \bullet_1 . \lambda x_2 : \dagger\tau_2 \to \bullet_2 . \lambda x_3 : \dagger\tau_3 \to \bullet_3 . z^{S(\sigma_1,\sigma_2,\sigma_3)}\ N_1^{\dagger\sigma_1 \to \bullet_1}\ N_2^{\dagger\sigma_2 \to \bullet_2}\ N_3^{\dagger\sigma_3 \to \bullet_3}$$

where $N_i = (\lambda y_i : \dagger\sigma_i . x_i\ L_i^{\dagger\tau_i})$ for $i = 1, 2, 3$ and $S(\sigma_1, \sigma_2, \sigma_3) \in \Gamma_S$.

Therefore, we have $\Gamma, \dagger\tau_1 \to \bullet_1, \dagger\tau_2 \to \bullet_2, \dagger\tau_3 \to \bullet_3 \vdash \dagger\sigma_i \to \dagger\tau_i$ for $i = 1, 2, 3$, which implies $\mathcal{C} \vdash \dagger\sigma_i \to \dagger\tau_i$ for $i = 1, 2, 3$. Additionally, by Definition 23 there exist type variables $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathcal{U}$ such that $\mathcal{C} \vdash \dagger a_i \to \dagger\sigma_i$ and $\mathcal{C} \vdash \dagger\tau_i \to \dagger b_i$ for $i = 1, 2, 3$. By Corollary 22, we obtain $[\![\sigma_i]\!]^* = [\![\tau_i]\!]^*$ for $i = 1, 2, 3$, which implies the claim.

The proof of (*ii*) is analogous to the proof of (*i*). ◀

Finally, we establish soundness of our reduction in the following Theorem 27.

▶ **Theorem 27** (Soundness). *If* $\Delta_{\mathsf{A}} \vdash M : \blacktriangle$ *for some* M, *then* A *has a solution.*

Proof. We show a more general claim. Given a map $[\![\cdot]\!] : \mathcal{U} \to \mathbb{N}$ for some finite set $\mathcal{U} \subseteq \mathbb{A} \setminus (\mathcal{C} \cup \{\dagger\})$ of type variables such that $\overline{1} \in \mathcal{U}$ and $[\![\overline{1}]\!] = 1$, let $\Delta = \Delta_I \cup \Delta_U \cup \Delta_S \cup \Delta_P$ such that

$$|\Delta_U| = \{U(a) \mid a \in \mathcal{U}\}$$
$$|\Delta_S| \subseteq \{S(\sigma_1, \sigma_2, \sigma_3) \mid [\![\sigma_1]\!]^* + [\![\sigma_2]\!]^* = [\![\sigma_3]\!]^* \in \mathbb{N}\}$$
$$|\Delta_P| \subseteq \{P(\sigma_1, \sigma_2, \sigma_3) \mid [\![\sigma_1]\!]^* \cdot [\![\sigma_2]\!]^* = [\![\sigma_3]\!]^* \in \mathbb{N}\}$$

We show that $|\Delta| \vdash \blacktriangle$ implies that A has a solution.

Assume $|\Delta| \vdash \blacktriangle$, then there exists a long normal form M such that $\Delta \vdash M : \blacktriangle$. We proceed by induction on the depth of M, which necessarily has one of the following shapes:

- $x_u \sigma N^{U(\sigma)} (\Lambda b . \lambda y_u : U(b) . \lambda y_s : S(\sigma, \overline{1}, b) . \lambda y_p : P(b, \overline{1}, b) . M_1^{\blacktriangle})$:
  Wlog. b, y_u, y_s, y_p are fresh. We have
  - $\Delta \vdash N : U(\sigma)$, therefore $[\![\sigma]\!]^* \in \mathbb{N}$ by Corollary 25.
  - $\Delta, y_u : U(b), y_s : S(\sigma, \overline{1}, b), y_p : P(b, \overline{1}, b) \vdash M_1 : \blacktriangle$.

  For $\mathcal{U}' = \mathcal{U} \cup \{b\}$ extending the domain of $[\![\cdot]\!]$ to b by $[\![b]\!] := [\![\sigma]\!]^* + 1$, $\Delta'_U = \Delta_U \cup \{y_u : U(b)\}$, $\Delta'_S = \Delta_S \cup \{y_s : S(\sigma, \overline{1}, b)\}$ and $\Delta'_P := \Delta_P \cup \{y_p : P(b, \overline{1}, b)\}$, we have that $\Delta_I \cup \Delta'_U \cup \Delta'_S \cup \Delta'_P \vdash M_1 : \blacktriangle$. Since $[\![b]\!]^* = [\![b]\!] = [\![\sigma]\!]^* + 1 = [\![\sigma]\!]^* + [\![\overline{1}]\!]$ and $[\![b]\!]^* = [\![b]\!]^* \cdot [\![\overline{1}]\!]^*$, by the induction hypothesis we obtain the claim.
- $x_s \sigma_1 \dots \sigma_5 N_1^{U(\sigma_1)} \dots N_5^{U(\sigma_5)} L_1^{S(\sigma_1,\sigma_2,\sigma_3)} L_2^{S(\sigma_2,\overline{1},\sigma_4)} L_3^{S(\sigma_3,\overline{1},\sigma_5)} (\lambda y_s : S(\sigma_1, \sigma_4, \sigma_5) . M_1^{\blacktriangle})$:
  Wlog. y_s is fresh. We have
  - $\Delta \vdash N_i : U(\sigma_i)$, therefore $[\![\sigma_i]\!]^* \in \mathbb{N}$ for $i = 1 \dots 5$ by Corollary 25.
  - $\Delta \vdash L_1 : S(\sigma_1, \sigma_2, \sigma_3)$, $\Delta \vdash L_2 : S(\sigma_2, \overline{1}, \sigma_4)$ and $\Delta \vdash L_3 : S(\sigma_3, \overline{1}, \sigma_5)$. Therefore, $[\![\sigma_1]\!]^* + [\![\sigma_2]\!]^* = [\![\sigma_3]\!]^*$, $[\![\sigma_2]\!]^* + [\![\overline{1}]\!]^* = [\![\sigma_4]\!]^*$ and $[\![\sigma_3]\!]^* + [\![\overline{1}]\!]^* = [\![\sigma_5]\!]^*$ by Lemma 26.
  - $\Delta, y_s : S(\sigma_1, \sigma_4, \sigma_5) \vdash M_1 : \blacktriangle$

  For $\Delta'_S = \Delta_S \cup \{y_s : S(\sigma_1, \sigma_4, \sigma_5)\}$ we have $\Delta_I \cup \Delta_U \cup \Delta'_S \cup \Delta_P \vdash M_1 : \blacktriangle$. Since $[\![\sigma_5]\!]^* = [\![\sigma_3]\!]^* + [\![\overline{1}]\!]^* = [\![\sigma_1]\!]^* + [\![\sigma_2]\!]^* + [\![\overline{1}]\!]^* = [\![\sigma_1]\!]^* + [\![\sigma_4]\!]^*$, by the induction hypothesis we obtain the claim.

- $x_p\sigma_1 \dots \sigma_5 N_1^{U(\sigma_1)} \dots N_5^{U(\sigma_5)} L_1^{P(\sigma_1,\sigma_2,\sigma_3)} L_2^{S(\sigma_2,\overline{1},\sigma_4)} L_3^{S(\sigma_3,\sigma_1,\sigma_5)} (\lambda y_p : P(\sigma_1,\sigma_4,\sigma_5).M_1^{\blacktriangle})$:
  Wlog. y_p is fresh. We have
  - $\Delta \vdash N_i : U(\sigma_i)$, therefore $[\![\sigma_i]\!]^* \in \mathbb{N}$ for $i = 1 \dots 5$ by Corollary 25.
  - $\Delta \vdash L_1 : P(\sigma_1,\sigma_2,\sigma_3)$, $\Delta \vdash L_2 : S(\sigma_2,\overline{1},\sigma_4)$ and $\Delta \vdash L_3 : S(\sigma_3,\sigma_1,\sigma_5)$. Therefore, $[\![\sigma_1]\!]^* \cdot [\![\sigma_2]\!]^* = [\![\sigma_3]\!]^*$, $[\![\sigma_2]\!]^* + [\![\overline{1}]\!]^* = [\![\sigma_4]\!]^*$ and $[\![\sigma_3]\!]^* + [\![\sigma_1]\!]^* = [\![\sigma_5]\!]^*$ by Lemma 26.
  - $\Delta, y_p : P(\sigma_1,\sigma_4,\sigma_5) \vdash M_1 : \blacktriangle$

  For $\Delta'_P = \Delta_P \cup \{y_p : P(\sigma_1,\sigma_4,\sigma_5)\}$ we have $\Delta_I \cup \Delta_U \cup \Delta_S \cup \Delta'_P \vdash M_1 : \blacktriangle$. Since $[\![\sigma_5]\!]^* = [\![\sigma_3]\!]^* + [\![\sigma_1]\!]^* = [\![\sigma_1]\!]^* \cdot [\![\sigma_2]\!]^* + [\![\sigma_1]\!]^* = [\![\sigma_1]\!]^* \cdot ([\![\sigma_2]\!]^* + [\![\overline{1}]\!]^*) = [\![\sigma_1]\!]^* \cdot [\![\sigma_4]\!]^*$, by the induction hypothesis we obtain the claim.
- $x_{\mathsf{A}}\sigma_1 \dots \sigma_n N_1^{U(\sigma_1)} \dots N_n^{U(\sigma_n)} L_1^{\overline{\mathfrak{e}}_1[a_i:=\sigma_i \mid i=1\dots n]} \dots L_l^{\overline{\mathfrak{e}}_l[a_i:=\sigma_i \mid i=1\dots n]}$:
  We have $\Delta \vdash N_i : U(\sigma_i)$, therefore $[\![\sigma_i]\!]^* \in \mathbb{N}$ for $i = 1 \dots n$ by Corollary 25. We show that the map $a_i \mapsto [\![\sigma_i]\!]^*$ satisfies each $\mathfrak{e}_j \in \mathsf{A}$ by distinguishing the following cases for $\mathfrak{e}_j$:
  Case $a_i \doteq 1$: We have $\overline{\mathfrak{e}_j}[a_i := \sigma_i \mid 1 = 1 \dots n] = P(\overline{1},\overline{1},\sigma_i)$. Since $\Delta \vdash L_j : P(\overline{1},\overline{1},\sigma_i)$, we have $[\![\sigma_i]\!]^* = [\![\overline{1}]\!]^* \cdot [\![\overline{1}]\!]^* = 1$ by Lemma 26.
  Case $a_{i_1} \doteq a_{i_2} + a_{i_3}$: We have $\overline{\mathfrak{e}_j}[a_i := \sigma_i \mid 1 = 1 \dots n] = S(\sigma_{i_2},\sigma_{i_3},\sigma_{i_1})$. Since $\Delta \vdash L_j : S(\sigma_{i_2},\sigma_{i_3},\sigma_{i_1})$, we have $[\![\sigma_{i_1}]\!]^* = [\![\sigma_{i_2}]\!]^* + [\![\sigma_{i_3}]\!]^*$ by Lemma 26.
  Case $a_{i_1} \doteq a_{i_2} \cdot a_{i_3}$: We have $\overline{\mathfrak{e}_j}[a_i := \sigma_i \mid 1 = 1 \dots n] = P(\sigma_{i_2},\sigma_{i_3},\sigma_{i_1})$. Since $\Delta \vdash L_j : P(\sigma_{i_2},\sigma_{i_3},\sigma_{i_1})$, we have $[\![\sigma_{i_1}]\!]^* = [\![\sigma_{i_2}]\!]^* \cdot [\![\sigma_{i_3}]\!]^*$ by Lemma 26. ◀

3.3 Formalization

In this paragraph we outline a formalization [3] of the above soundness (Theorem 27) and completeness (Theorem 19) results in Coq 8.8 using the SSReflect proof methodology. The formalization spans 4000 lines of code, of which three quarters is boilerplate.

The main result is formalized in `MainResult.v` as

```
Theorem correctness : ∀ (ds : list diophantine), Diophantine.solvable ds ↔
  derivation (ΓI ds ++ [U one; P one one one]) triangle.
```

In the above, constraints of shape either $a \doteq 1$ or $a \doteq b + c$ or $a \doteq b \cdot c$ that are used in Problem 9 are captured in `Diophantine.v` by the inductive type `Inductive diophantine : Set`. Derivability in system **F** (or rather IPC_2) is formalized in `Derivations.v` by the inductive type

```
Inductive derivation (Γ : list formula) : formula → Prop
```

The property of long normal inhabitation (reflecting Definition 8) is internalized in the definition of inductive type (also containing a bound on the depth of the derivation as the first parameter)

```
Inductive normal_derivation : nat → list formula → formula → Prop
```

For an in-depth analysis of type derivations in system **F** see [6]. Normalization of system **F** and existence of η-long inhabitants, i.e. completeness of `normal_derivation` wrt. `derivation` is (at the time of writing) not part of the formalization

```
Axiom normal_derivation_completeness : ∀ (Γ : list formula) (s: formula),
  derivation Γ s → ∃ (n : nat), normal_derivation n Γ s.
```

whereas soundness of `normal_derivation` wrt. `derivation` is shown by

```
Theorem normal_derivation_soundness : ∀ (n : nat) (Γ : list formula) (s: formula),
  normal_derivation n Γ s → derivation Γs.
```

The more general claim that is used in the proof of soundness (Theorem 27) is formalized in `Soundness.v` as

```
Theorem soundness : ∀ (n : nat) (ΓU ΓS ΓP : list formula),
  (∀ {s : formula}, In s ΓU → represents_nat s) →
  (∀ {s : formula}, In s ΓS → encodes_sum s) →
  (∀ {s : formula}, In s ΓP → encodes_prod s) →
  ∀ (ds : list diophantine),
  normal_derivation n ((Encoding.ΓI ds) ++ ΓU ++ ΓS ++ ΓP) Encoding.triangle →
  Diophantine.solvable ds.
```

Completeness (Theorem 19) is formalized in `Completeness.v` as

```
Lemma completeness : ∀ (ds : list diophantine), Diophantine.solvable ds →
  derivation (ΓI ds ++ [U one; P one one one]) triangle.
```

where the first three steps in the proof of Theorem 19 are formalized individually as `Theorem completeness_U`, `Theorem completeness_S`, and `Theorem completeness_P`.

At the time of writing, theorems `soundness` and `completeness` use only the above axiom `normal_derivation_completeness` as an assumption that is not formally proven.

Several aspects of the "informal" proof, at first glance, appear problematic and are clarified in the formal proof. In Definition 23 we partially define an interpretation $[\![\cdot]\!]^*$ of arbitrary types as natural numbers based on derivability in system **F**. Not only is derivability undecidable, but it is the actual subject of our analysis. The map $[\![\cdot]\!]^*$ is formalized in `Encoding.v` as

```
Inductive interpretation (s : formula) (n : nat) : Prop
```

and its well-definedness is shown in `Soundness.v` by

```
Lemma interpretation_soundness : ∀ (s : formula) (m1 m2 : nat),
  interpretation s m1 → interpretation s m2 → m1 = m2.
```

The absence of classical principles or the axiom of choice (resp. Hilbert's epsilon) as assumptions in our main result ensures that the whole argument is constructive.

Another aspect elaborated in the formal proof is the argumentation based on the necessary shape of long normal inhabitants. Clearly, a complete case analysis of all imaginable inhabitants would clutter an "informal" proof, that is supposed to focus on interesting cases. Luckily, the formal proof can utilize numerous tactics to deal with the trivial cases automatically. Most prominently, the tactic `decompose_USP` implemented in `Soundness.v` discovers and transforms suitable assumptions by full case analysis to apply Lemma 26.

4 Conclusion

This work contains the (as of yet) simplest, syntax oriented proof that inhabitation in system **F** (resp. provability in intuitionistic second-order propositional logic) is undecidable. The proof is by reduction from (a variant of) solvability of Diophantine equations. In spirit, the reduction can be considered an instance of Sørensen's and Urzyczyn's reduction from provability in first-order predicate logic to provability in second-order propositional logic. Additionally, we formalized soundness and completeness results in the Coq proof assistant.

The next step is to eliminate the axiom regarding existence of long normal inhabitants in system **F** by using existing work [10]. In near future, we envision to embed the formalization into the larger framework of computational reductions in Coq [4] already containing a collection of formalized reductions that are used in undecidability results.

References

1 T. Arts and W. Dekkers. Embedding first order predicate logic in second order propositional logic. *Technical report 93-02, Katholieke Universiteit Nijmegen*, 1993.

2 H. Barendregt. Introduction to Generalized Type Systems. *J. Funct. Program.*, 1(2):125–154, 1991.

3 A. Dudenhefner. Reduction from Diophantine equations to provability in IPC2 / System F. `https://github.com/mrhaandi/ipc2`. Accessed: 2018-09-18.

4 Y. Forster, E. Heiter, and G. Smolka. Verification of PCP-Related Computational Reductions in Coq. In *Interactive Theorem Proving - 9th International Conference, ITP 2018, Held as Part of the Federated Logic Conference, FloC 2018, Oxford, UK, July 9-12, 2018, Proceedings*, pages 253–269, 2018. `doi:10.1007/978-3-319-94821-8_15`.

5 D. M. Gabbay. On 2nd order intuitionistic propositional calculus with full comprehension. *Archive for Mathematical Logic*, 16(3):177–186, 1974.

6 P. Giannini and S. Ronchi Della Rocca. Characterization of typings in polymorphic type discipline. In *Proceedings of the Third Annual Symposium on Logic in Computer Science (LICS '88), Edinburgh, Scotland, UK, July 5-8, 1988*, pages 61–70, 1988. `doi:10.1109/LICS.1988.5101`.

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

8 M. H. Löb. Embedding First Order Predicate Logic in Fragments of Intuitionistic Logic. *J. Symb. Log.*, 41(4):705–718, 1976. `doi:10.2307/2272390`.

9 D. Martin. Hilbert's tenth problem is unsolvable. *The American Mathematical Monthly*, 80(3):233–269, 1973.

10 K. Sakaguchi. A Formalization of Typed and Untyped lambda-Calculi in SSReflect-Coq and Agda2. `https://github.com/pi8027/lambda-calculus`. Accessed: 2019-04-02.

11 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.

12 M. H. Sørensen and P. Urzyczyn. A Syntactic Embedding of Predicate Logic into Second-Order Propositional Logic. *Notre Dame Journal of Formal Logic*, 51(4):457–473, 2010. `doi:10.1215/00294527-2010-029`.

13 P. Urzyczyn. Inhabitation in Typed Lambda-Calculi (A Syntactic Approach). In *Typed Lambda Calculi and Applications, Third International Conference on Typed Lambda Calculi and Applications, TLCA '97, Nancy, France, April 2-4, 1997, Proceedings*, pages 373–389, 1997. `doi:10.1007/3-540-62688-3_47`.