Formalising the Undecidability of Higher-Order Unification

Simon Spies

Advisor — Yannick Forster

Supervisor — Gert Smolka

Saarland University

Programming Systems Lab.

12th April 2019

Bachelor Talk

Motivation — $\forall n.\ n + 0 = n$

natind.v

```
Lemma plus_zero: ∀ n, n + 0 = n.
Proof.
  Check ℕ_ind.
  apply ℕ_ind with (P ≔ λ n ⇒ n + 0 = n).
  reflexivity.
  cbn; now intros ? →.
Qed.
```

```
❶  * 153 natind.v   Coq                u   unix | 5: 0   All
2 subgoals (ID 8)


  0 + 0 = 0

subgoal 2 (ID 9) is:
 ∀ n : ℕ, n + 0 = n → S n + 0 = S n
~
❷  % 130 *goals*   Coq Goals   Utoks©e®    utf-8 | 4: 0   All
```

Motivation — $\forall n.\ n + 0 = n$

Overview

Higher-Order — $\mathbf{U}$

following Dowek (2001)

Nth-Order — $\mathbf{U}_n$

$\mathbf{U}_n \subseteq \mathbf{U}$

Third-Order — $\mathbf{U}_3$

following Huet (1973)

Second-Order — $\mathbf{U}_2$

following Goldfarb (1981)

Example

$$\Gamma \vdash \lambda xy.fx \stackrel{?}{=} \lambda xy.fy : A$$

where $\Gamma = (f : \alpha \to \alpha)$ and $A = \alpha \to \alpha \to \alpha$.

Solution

$$\sigma f = \lambda\_.z$$
$$\sigma x = x \qquad \text{othw.}$$
in $\Delta = (z : \alpha)$

Proof

$$(\lambda xy.fx)[\sigma] \equiv \lambda xy.z$$
$$\equiv (\lambda xy.fy)[\sigma]$$

Higher-Order Unification — **U**

$$\mathbf{U}\ (\Gamma \vdash s \stackrel{?}{=} t : A) :=$$
$$\exists \sigma \Delta.\ \Delta \vdash \sigma : \Gamma \quad \text{and} \quad s[\sigma] \equiv t[\sigma]$$

$\boxed{\Delta \vdash \sigma : \Gamma}$

$$\frac{\forall (x : A) \in \Gamma.\ \Delta \vdash \sigma x : A}{\Delta \vdash \sigma : \Gamma}$$

$\boxed{s \equiv t}$

$$\frac{s \succ^* v \qquad t \succ^* v}{s \equiv t}$$

Undecidability

$$\textbf{H10} \quad \preceq \quad \textbf{SU} \quad \preceq \quad \textbf{U}$$

$$\textbf{SU}\ (\{\Gamma \vdash s_i \stackrel{?}{=} t_i : A_i \mid i = 1, \ldots, n\}) :=$$
$$\exists \sigma \Delta.\ \Delta \vdash \sigma : \Gamma \quad \text{and} \quad \forall i.\ s_i[\sigma] \equiv t_i[\sigma]$$

Hilbert's tenth problem — **H10**

Example $x \doteq 42$ $y \doteq x \cdot y$ $z \doteq z + z$

Solution $\theta x = 42$ $\theta y = \theta z = 0$

$$\boxed{\theta \vDash d}$$

$$\begin{aligned} \theta \vDash x \doteq c \quad &\text{iff} \quad \theta x = c \\ \theta \vDash x + y \doteq z \quad &\text{iff} \quad \theta y + \theta y = \theta z \\ \theta \vDash x \cdot y \doteq z \quad &\text{iff} \quad \theta y \cdot \theta y = \theta z \end{aligned}$$

$$\mathbf{H10}(D) := \exists \theta . \forall d \in D.\ \theta \vDash d$$

Church Numerals

$$\boxed{[\![n]\!]}$$

$$[\![n]\!] := \lambda af.f^n\ a$$

Operations

$$\text{add}\ s\ t := \lambda af.s\ (t\ a\ f)\ f \qquad \text{mul}\ s\ t := \lambda af.s\ a\ (\lambda b.t\ b\ f)$$

Characteristic Equation $f^n(fa) = f(f^n a)$ Let s be a normal.

$$\lambda af.s\ (f\ a)\ f \equiv \lambda af.f\ (s\ a\ f) \quad \text{iff} \quad s = [\![n]\!] \quad \text{for some } n : \mathbb{N}$$

H10 $\preceq$ SU

$$\textbf{H10}(D) \quad \text{iff} \quad \textbf{SU}(\overline{D})$$

Proof.

Pick $\overline{D}$:

$$\overline{x \doteq c} := x \stackrel{?}{=} [\![c]\!] \qquad \overline{x + y \doteq z} := \mathsf{add}\ x\ y \stackrel{?}{=} z$$

$$\overline{x \cdot y \doteq z} := \mathsf{mul}\ x\ y \stackrel{?}{=} z$$

$$\overline{x} := \lambda af.x\ (f\ a)\ f \stackrel{?}{=} \lambda af.f\ (x\ a\ f)$$

Overview

Higher-Order — U

following Dowek (2001)

Nth-Order — $\mathbf{U}_n$

$\mathbf{U}_n \subseteq \mathbf{U}$

Third-Order — $\mathbf{U}_3$

following Huet (1973)

Second-Order — $\mathbf{U}_2$

following Goldfarb (1981)

Order

$$\boxed{\text{ord } A}$$

$$\text{ord } \alpha = 1 \qquad \text{ord } (A \to B) = \max\{\text{ord } A + 1, \text{ord } B\}$$

First-Order

$$\alpha \qquad \beta \qquad \gamma \qquad \delta \qquad \cdots$$

Second-Order

$$\alpha \to \alpha \qquad \beta \to \alpha \qquad \alpha \to \beta \to \gamma$$

Third-Order

$$(\alpha \to \alpha) \to \alpha \qquad (\alpha \to \beta \to \alpha) \to \beta \qquad (\beta \to \alpha) \to (\beta \to \alpha) \to \gamma$$

Nth-Order Fragment

$$\boxed{\Gamma \vdash_n s : A}$$

Let Ω be a signature.

$$\frac{(x : A) \in \Gamma \quad \text{ord } A \leq n}{\Gamma \vdash_n x : A} \qquad \frac{\text{ord } (\Omega c) \leq n + 1}{\Gamma \vdash_n c : \Omega c}$$

$$\frac{\Gamma \vdash_n s : A \to B \quad \Gamma \vdash_n t : A}{\Gamma \vdash_n s\ t : B} \qquad \frac{\Gamma, x : A \vdash_n s : B}{\Gamma \vdash_n \lambda x.s : A \to B}$$

Examples

$$\Gamma \vdash_1 \lambda x.x : \alpha \to \alpha \qquad \Gamma \vdash_2 \lambda x.x : \alpha \to \alpha$$

$$\Gamma \vdash_3 \lambda x.x : ((\alpha \to \alpha) \to \alpha) \to (\alpha \to \alpha) \to \alpha$$

Nth-Order Unification — $\mathbf{U}_n$

$$\mathbf{U}_n\ (\Gamma \vdash_n s \stackrel{?}{=} t : A) \coloneqq \exists \sigma \Delta.\ \Delta \vdash_n \sigma : \Gamma \quad \text{and} \quad s[\sigma] \equiv t[\sigma]$$

$$\boxed{\Delta \vdash_n \sigma : \Gamma}$$

$$\frac{\forall (x : A) \in \Gamma.\ \Delta \vdash_n \sigma x : A}{\Delta \vdash_n \sigma : \Gamma}$$

Conservativity

$$\mathbf{PCP} \preceq \mathbf{U}_3 \quad \text{and} \quad \mathbf{PCP} \preceq \mathbf{U} \qquad \leadsto \qquad \mathbf{PCP} \preceq \mathbf{U}_3 \preceq \mathbf{U}$$

Conservativity Let $n \leq m$.

$$\mathbf{U}_n \quad \subseteq \quad \mathbf{U}_m \quad \subseteq \quad \mathbf{U}$$

Overview

Higher-Order — U

following Dowek (2001)

Nth-Order — $\mathbf{U}_n$

$\mathbf{U}_n \subseteq \mathbf{U}$

Third-Order — $\mathbf{U}_3$

following Huet (1973)

Second-Order — $\mathbf{U}_2$

following Goldfarb (1981)

Third-Order Unification — $\mathbf{U}_3$

Huet (1973)

$$\mathbf{PCP} \preceq \mathbf{U}_3$$

↓

This Work

$$\mathbf{MPCP} \preceq \mathbf{U}_3$$

Modified Post Correspondence Problem — **MPCP**

Given

$$\boxed{\frac{l_0}{r_0}} \quad \text{and} \quad \boxed{\frac{l_1}{r_1}} \cdots \boxed{\frac{l_n}{r_n}}$$

(0) (1) (n)

Find Ordering

$$i_1, \ldots, i_k$$

Such that

$$l_0 l_{i_1} \cdots l_{i_k} = r_0 r_{i_1} \cdots r_{i_k}$$

Reduction

$$\lambda u_1 u_0.\overline{l_0}\ (x_f\ \overline{l_0}\ \cdots\ \overline{l_n}) \stackrel{?}{=} \lambda u_1 u_0.\overline{r_0}\ (x_f\ \overline{r_0}\ \cdots\ \overline{r_n})$$

where $x_f : (\alpha \to \alpha)^{n+1} \to \alpha$

Encoding Fix $u_1, u_0 : \alpha \to \alpha$.

$$\overline{110} := \lambda x.u_1\ (u_1\ (u_0\ x))$$

$\overline{l}\ (\overline{l'}\ s) \equiv \overline{ll'}\ s$ and $\overline{l_{i_1}}\ (\cdots(\overline{l_{i_k}}\ s)) \equiv \overline{l_{i_1}\cdots l_{i_k}}\ s$

Overview

Higher-Order — U

following Dowek (2001)

Nth-Order — $\mathbf{U}_n$

$\mathbf{U}_n \subseteq \mathbf{U}$

Third-Order — $\mathbf{U}_3$

following Huet (1973)

Second-Order — $\mathbf{U}_2$

following Goldfarb (1981)

Undecidability Second-Order

Goldfarb's Result

$$\mathbf{H10} \preceq \mathbf{U}_2^{\{g,a,b\}}$$

where $\mathbf{U}_2^{\{g,a,b\}}$ is second-order unification with constants $g : \alpha \to \alpha \to \alpha$ and $a, b : \alpha$.

Goldfarb Numerals

$$\boxed{\llbracket n \rrbracket}$$

$$\llbracket n \rrbracket := \lambda a.(\mathsf{g}\ \mathsf{a})^n\ a$$

Operations

$$\mathsf{add}\ s\ t := \lambda a.s\ (t\ a) \qquad \mathsf{mul}\ s\ t := ???$$

Characteristic Equation Let s be a normal.

$$\lambda a.s\ ((\mathsf{g}\ \mathsf{a})\ a)\ \equiv \lambda a.(\mathsf{g}\ \mathsf{a})\ (s\ a) \quad \text{iff} \quad \forall t.\ s\ t \equiv \llbracket n \rrbracket\ t \ \text{ for some } n : \mathbb{N}$$

Multiplication — $m \cdot n = p$

$$\begin{aligned}
&\mathsf{mult}(0,0) \text{ where} \\
&\mathsf{mult}(a,i) = a && \text{if } i = m \\
&\mathsf{mult}(a,i) = \mathsf{mult}(a+n, i+1) && \text{if } i \neq m
\end{aligned}$$

Multiplication Sequence

$$(0,0); (n,1); (2n,2); \cdots; (p,m)$$

Multiplication — $m \cdot n = p$

$$m \cdot n = p \quad \text{iff} \quad \exists X.\ (0,0); \mathsf{succ}\ X = X; (p,m)$$

where $\mathsf{succ}(a,i) := (a+n, i+1)$
$\mathsf{succ}\ X := \mathsf{map}\ \mathsf{succ}\ X$

t_0	t_1	t_2	$\cdots$	$(m \cdot n, m)$
t_0	t_1	$\cdots$	t_{m-1}	(p, m)

where $t_i := (i \cdot n, i)$ and $\mathsf{succ}(t_i) = t_{i+1}$.

Multiplication Equations

$$(\llbracket 0 \rrbracket\ \mathsf{a}, \llbracket 0 \rrbracket\ \mathsf{b}) :: X\ (y\mathsf{a})\ (\llbracket 1 \rrbracket\ \mathsf{b})\ []\ \stackrel{?}{=}\ X\ (\llbracket 0 \rrbracket\ \mathsf{a})\ (\llbracket 0 \rrbracket\ \mathsf{b})\ [(z\mathsf{a}, x\mathsf{b})]$$

$$(\llbracket 0 \rrbracket\ \mathsf{b}, \llbracket 0 \rrbracket\ \mathsf{a}) :: X\ (y\mathsf{b})\ (\llbracket 1 \rrbracket\ \mathsf{a})\ []\ \stackrel{?}{=}\ X\ (\llbracket 0 \rrbracket\ \mathsf{b})\ (\llbracket 0 \rrbracket\ \mathsf{a})\ [(z\mathsf{b}, x\mathsf{a})]$$

$$(s, t) := \mathsf{g}\ s\ t \qquad s :: t := \mathsf{g}\ s\ t \qquad [] := \mathsf{a}$$

Contributions

Higher-Order

$\mathbf{H10} \preceq \mathbf{SU} \preceq \mathbf{U}$

Nth-Order

$\mathbf{U}_n \subseteq \mathbf{U}$

Third-Order

$\mathbf{MPCP} \preceq \mathbf{U}_3$

Second-Order

$\mathbf{H10} \preceq \mathbf{U}_2^{\{g,a,b\}}$

Furthermore...

- Adding and Removing Constants

$$\mathbf{U}_2^{\{g,a,b\}} \preceq \mathbf{U}_2^{\{g\}} \preceq \mathbf{U}_3^{\{g\}} \preceq \mathbf{U}_3^{\emptyset} \preceq \mathbf{U}_3$$

- First-Order Unification

$$\mathbf{U}_1 \quad \text{is decidable}$$

- Enumerability

$$\mathbf{U}, \mathbf{SU}, \mathbf{U}_n, \text{and } \mathbf{SU}_n \quad \text{are enumerable}$$

Future Work

- Decidability Monadic Second-Order Unification
- Huet's Unification Procedure

References

Dowek, G.
2001. Higher-order unification and matching. *Handbook of automated reasoning*, 2:1009–1062.

Forster, Y., D. Kirst, and G. Smolka
2019. On synthetic undecidability in Coq, with an application to the Entscheidungsproblem. In *International Conference on Certified Programs and Proofs*.

Goldfarb, W. D.
1981. The undecidability of the second-order unification problem. *Theoretical Computer Science*, 13:225–230.

Huet, G. P.
1973. The undecidability of unification in third order logic. *Information and control*, 22(3):257–267.

Snyder, W. and J. H. Gallier
1989. Higher order unification revisited: Complete sets of transformations. *Technical Reports (CIS)*, P. 778.

Formalisation

Overview	Spec	Proofs
λ-calculus	790	1120
Unification	350	380
Third-Order	190	400
Second-Order	570	850
First-Order	290	510
Convervativity & Constants	480	890
Total	**2670**	**4150**

Remarks

- Autosubst 2 ♥
- Curry-style simpler than Church-style
- First-Order using Equations tool

Website

http://www.ps.uni-saarland.de/~spies/bachelor.php

SU $\preceq$ U

$$\textbf{SU}(E) \quad \text{iff} \quad \textbf{U}(f(E))$$

Proof.

Pick $f := \{\Gamma \vdash s_i \stackrel{?}{=} t_i : A_i \mid i = 1, \ldots, n\} \mapsto$

$$\Gamma \vdash \lambda h.h\ s_1\ \cdots\ s_n \stackrel{?}{=} \lambda h.h\ t_1\ \cdots\ t_n : A$$

where $A = (A_1 \to \cdots \to A_n \to \alpha) \to \alpha$. Follows with:

$$h\ u_1\ \cdots\ u_n \equiv h\ v_1\ \cdots\ v_n \quad \text{iff} \quad \forall i.\ u_i \equiv v_i$$

First-Order Unification

Traditionally

$$s, t ::= x \mid c \mid s\ t$$

This Work For normal forms:

$$\mathbf{U}_1(\Gamma \vdash_1 \lambda x_1 \cdots x_n.s \stackrel{?}{=} \lambda y_1 \cdots y_m.t : A)$$

$$\updownarrow$$

$\mathbf{U}(s \stackrel{?}{=} t)$, without affecting bound variables

and $n = m$

First-Order Unification Algorithm

Unification $\boxed{E \mapsto \sigma}$

$$\frac{\text{decomp } E = \text{nil}}{E \mapsto id} \qquad \frac{\text{decomp } E = x \stackrel{?}{=} s :: E' \quad E'[s/x] \mapsto \sigma \quad \forall y \in \text{vars } s.\ \text{free } y \quad \text{free } x \quad x \notin \text{vars } s}{E \mapsto \sigma[x := s[\sigma]]}$$

Example $\underbrace{\text{g a b} \stackrel{?}{=} \text{g a b} \qquad \text{g } x\ y \stackrel{?}{=} \text{g (g } y \text{ a) (g a a)}}$

$\downarrow$ decomp

$x \stackrel{?}{=} \text{g } y \text{ a} \qquad y \stackrel{?}{=} \text{g a a}$

Conservativity — $\mathbf{U}_n \subseteq \mathbf{U}$

Let $\Gamma \vdash_n s \stackrel{?}{=} t : A$.

$$s[\sigma] \equiv t[\sigma] \text{ for some } \Sigma \vdash_n \sigma : \Gamma$$
iff
$$s[\sigma] \equiv t[\sigma] \text{ for some } \Delta \vdash \sigma : \Gamma$$

Proof Sketch.
Replace free variables and constants not of order n with first-order terms. For example, $x : (\alpha \to \alpha) \to \alpha$ is replaced by $\lambda x_1.z$ where $z : \alpha$ and g : $\alpha \to \alpha \to \alpha$ is replaced by $\lambda x_1 x_2.z$. Normalise the result. □

Adding Constants

$$\mathbf{U}_n^{\mathcal{C}} \preceq \mathbf{U}_n^{\mathcal{D}} \quad \text{if } \mathcal{C} \subseteq \mathcal{D}$$

Proof Sketch.
Replace constants $d \in \mathcal{D} - \mathcal{C}$ with first-order terms, see conservativity. □

Removing Constans

$$\mathbf{U}_n^{\mathcal{D}} \preceq \mathbf{U}_n^{\mathcal{C}} \quad \text{if } \mathcal{C} \subseteq \mathcal{D} \text{ and } \forall d \notin C.\ \mathsf{ord}\ (\Omega d) < n$$

Proof Sketch.
Let $\mathcal{C} = \{\mathsf{g}\}$ and $\mathcal{D} = \{\mathsf{a}, \mathsf{g}\}$.

$$\begin{array}{lcl} \mathsf{g}\ x \stackrel{?}{=} \mathsf{g}\ \mathsf{a} & \rightsquigarrow & \lambda x_{\mathsf{a}}.\mathsf{g}\ (x\ x_{\mathsf{a}}) \stackrel{?}{=} \lambda x_{\mathsf{a}}.\mathsf{g}\ x_{\mathsf{a}} \\ \text{where}\ \ x : \alpha & & \text{where}\ \ x : \alpha \to \alpha \end{array}$$

□