Formalising the Undeciability of Higher-Order Unification

Simon Spies

Advisor – Yannick Forster

Supervisor – Gert Smolka

Saarland University

Programming Systems Lab.

2nd October 2018

Timeline

Timeline

G. Huet (1973)

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

Timeline

G. Huet (1973)

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

W. Goldfarb (1981)

$$\mathbf{DE} \leq \mathbf{U}_2$$

SIMPLY TYPED λ-CALCULUS

$$s, t ::= \lambda x.\ s \mid s\ t \mid x \mid c \qquad x \in \mathcal{V}, c \in \{\mathsf{a}, \mathsf{b}, \mathsf{g}\}$$

$$A, B ::= \alpha \mid A \to B \mid \mathcal{T} \qquad \alpha \in \mathcal{TV}$$

SIMPLY TYPED λ-CALCULUS

$$s, t ::= \lambda x.\, s \mid s\ t \mid x \mid c \qquad x \in \mathcal{V}, c \in \{\mathsf{a}, \mathsf{b}, \mathsf{g}\}$$

$$A, B ::= \alpha \mid A \to B \mid \mathcal{T} \qquad \alpha \in \mathcal{TV}$$

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

$$\frac{}{\Gamma \vdash \mathsf{a} : \mathcal{T}} \qquad \frac{}{\Gamma \vdash \mathsf{b} : \mathcal{T}}$$

$$\frac{}{\Gamma \vdash \mathsf{g} : \mathcal{T} \to \mathcal{T} \to \mathcal{T}}$$

SIMPLY TYPED λ-CALCULUS

$$s, t ::= \lambda x.\ s \mid s\ t \mid x \mid c \qquad x \in \mathcal{V}, c \in \{\mathsf{a}, \mathsf{b}, \mathsf{g}\}$$

$$A, B ::= \alpha \mid A \to B \mid \mathcal{T} \qquad \alpha \in \mathcal{TV}$$

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

$$\frac{}{\Gamma \vdash \mathsf{a} : \mathcal{T}} \qquad \frac{}{\Gamma \vdash \mathsf{b} : \mathcal{T}}$$

$$\frac{}{\Gamma \vdash \mathsf{g} : \mathcal{T} \to \mathcal{T} \to \mathcal{T}}$$

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

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

SIMPLY TYPED λ-CALCULUS

$$s, t ::= \lambda x.\, s \mid s\; t \mid x \mid c \qquad x \in \mathcal{V}, c \in \{\mathsf{a}, \mathsf{b}, \mathsf{g}\}$$

$$A, B ::= \alpha \mid A \to B \mid \mathcal{T} \qquad \alpha \in \mathcal{TV}$$

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

$$\frac{}{\Gamma \vdash \mathsf{a} : \mathcal{T}} \qquad \frac{}{\Gamma \vdash \mathsf{b} : \mathcal{T}}$$

$$\frac{}{\Gamma \vdash \mathsf{g} : \mathcal{T} \to \mathcal{T} \to \mathcal{T}}$$

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

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

$$\boxed{s \succ t}$$

$$\frac{s \succ s'}{\lambda x.\, s \succ \lambda x.\, s'}$$

Unification

$$\mathbf{U}\left(\Gamma \vdash s \stackrel{?}{=} t : A\right) :=$$

$$\boxed{\Gamma \vdash s \stackrel{?}{=} t : A}$$

$$\frac{\Gamma \vdash s : A \quad \Gamma \vdash t : A}{\Gamma \vdash s \stackrel{?}{=} t : A}$$

Unification

$$\mathbf{U}\left(\Gamma \vdash s \overset{?}{=} t : A\right) :=$$

$$\exists \sigma \qquad s[\sigma] \equiv t[\sigma]$$

$$\boxed{\Gamma \vdash s \overset{?}{=} t : A} \qquad \boxed{s \equiv t}$$

$$\frac{\Gamma \vdash s : A \quad \Gamma \vdash t : A}{\Gamma \vdash s \overset{?}{=} t : A} \qquad \frac{s \rhd v \quad t \rhd v}{s \equiv t}$$

Unification

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

$$\boxed{\Gamma \vdash s \stackrel{?}{=} t : A}$$

$$\frac{\Gamma \vdash s : A \quad \Gamma \vdash t : A}{\Gamma \vdash s \stackrel{?}{=} t : A}$$

$$\boxed{s \equiv t}$$

$$\frac{s \rhd v \quad t \rhd v}{s \equiv t}$$

Example

$$\mathbf{U}(\Gamma \vdash \lambda xy.\ f\ x \stackrel{?}{=} \lambda xy.\ f\ y : \alpha \to \alpha \to \alpha)$$

$$\Gamma := f : \alpha \to \alpha$$

Example

$$\mathbf{U}(\Gamma \vdash \lambda xy.\, f\ x \stackrel{?}{=} \lambda xy.\, f\ y : \alpha \to \alpha \to \alpha)$$

$$\Gamma := f : \alpha \to \alpha$$

Solution:

$$\sigma := \{f \mapsto \lambda\_.\, z\}$$

$$\Delta := z : \alpha$$

Example

$$\mathbf{U}(\Gamma \vdash \lambda xy.\ f\ x \stackrel{?}{=} \lambda xy.\ f\ y : \alpha \to \alpha \to \alpha)$$

$$\Gamma := f : \alpha \to \alpha$$

Solution:

$$\sigma := \{f \mapsto \lambda\_.\ z\} \qquad (\lambda xy.\ f\ x)[\sigma] \equiv \lambda xy.\ z$$

$$\Delta := z : \alpha \qquad \equiv \lambda xy.\ (\sigma f)\ y$$

nth-ORDER UNIFICATION ($\mathbf{U}_n$)

nth-ORDER UNIFICATION $(\mathbf{U}_n)$

$$\boxed{\mathsf{ord}\ A}$$

$$\mathsf{ord}\ \alpha = 1 \qquad \mathsf{ord}\ \mathcal{T} = 1$$

$$\mathsf{ord}\ (A \to B) =$$

$$\max\{\mathsf{ord}\ A + 1,\ \mathsf{ord}\ B\}$$

nth-ORDER UNIFICATION ($\mathbf{U}_n$)

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

$\text{ord } \alpha = 1 \qquad \text{ord } \mathcal{T} = 1$

$\text{ord } (A \to B) =$

$\max \{\text{ord } A + 1, \text{ ord } B\}$

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

$$\frac{(x : A) \in \Gamma \quad \text{ord } A \leq n}{\Gamma \vdash_n x : A}$$

$$\frac{\Gamma, x : A \vdash_n s : B \quad \text{ord } A < n}{\Gamma \vdash_n \lambda x.\, s : A \to B}$$

Timeline

G. Huet (1973)

$$\textbf{PCP} \leq \textbf{U}_3$$

W. Goldfarb (1981)

$$\textbf{DE} \leq \textbf{U}_2$$

PCP *with* $u, v \in \mathcal{V}$

Given

$$\boxed{\frac{x_1}{y_1}} \quad \boxed{\frac{x_2}{y_2}} \quad \dots \quad \boxed{\frac{x_n}{y_n}}$$

PCP *with* $u, v \in \mathcal{V}$

Given

$\boxed{\frac{x_1}{y_1}}$ $\boxed{\frac{x_2}{y_2}}$ $\dots$ $\boxed{\frac{x_n}{y_n}}$

Find

$[i_1, \dots, i_k]$

PCP *with* $u, v \in \mathcal{V}$

Given

$$\boxed{\frac{x_1}{y_1}} \quad \boxed{\frac{x_2}{y_2}} \quad \cdots \quad \boxed{\frac{x_n}{y_n}}$$

Find

$$[i_1, \ldots, i_k]$$

Such that

$$x_{i_1} \cdots x_{i_k} = y_{i_1} \cdots y_{i_k}$$

PCP *with* $u, v \in \mathcal{V}$

Given

$$\boxed{\frac{x_1}{y_1}} \quad \boxed{\frac{x_2}{y_2}} \quad \cdots \quad \boxed{\frac{x_n}{y_n}}$$

Find

$$[i_1, \ldots, i_k]$$

Such that

$$x_{i_1} \cdots x_{i_k} = y_{i_1} \cdots y_{i_k}$$

Example

$$\boxed{\frac{u}{uu}} \quad \boxed{\frac{v}{vv}} \quad \boxed{\frac{uuv}{u}}$$

PCP *with* $u, v \in \mathcal{V}$

Given

$$\boxed{\frac{x_1}{y_1}} \quad \boxed{\frac{x_2}{y_2}} \quad \dots \quad \boxed{\frac{x_n}{y_n}}$$

Find

$$[i_1, \dots, i_k]$$

Such that

$$x_{i_1} \cdots x_{i_k} = y_{i_1} \cdots y_{i_k}$$

Example

$$\boxed{\frac{u}{uu}} \quad \boxed{\frac{v}{vv}} \quad \boxed{\frac{uuv}{u}} \quad [1, 3, 2]$$

PCP *with* $u, v \in \mathcal{V}$

Given

$$\frac{x_1}{y_1} \quad \frac{x_2}{y_2} \quad \cdots \quad \frac{x_n}{y_n}$$

Find

$$[i_1, \ldots, i_k]$$

Such that

$$x_{i_1} \cdots x_{i_k} = y_{i_1} \cdots y_{i_k}$$

Example

$$\frac{u}{uu} \quad \frac{v}{vv} \quad \frac{uuv}{u} \quad \overset{[1,\ 3,\ 2]}{\rightsquigarrow} \quad \frac{u}{uu}\frac{uuv}{u}\frac{v}{vv} = \frac{uuuvv}{uuuvv}$$

PCP $\leq$ $\mathbf{U}_3$ – IDEA

$$\vdash_3 s : \underbrace{(\alpha \to \alpha) \to \cdots \to (\alpha \to \alpha)}_{n \text{ times}} \to \alpha \to \alpha$$

PCP $\leq$ $\mathbf{U}_3$ – IDEA

$$\vdash_3 s : \underbrace{(\alpha \to \alpha) \to \cdots \to (\alpha \to \alpha)}_{n \text{ times}} \to \alpha \to \alpha$$

$$s\ f_1\ \cdots\ f_n\ t \equiv f_{i_1}(\cdots(f_{i_k}\ t)\cdots)$$

PCP $\leq$ U$_3$ – IDEA

$$\vdash_3 s : \underbrace{(\alpha \to \alpha) \to \cdots \to (\alpha \to \alpha)}_{n \text{ times}} \to \alpha \to \alpha$$

$$s\ f_1\ \cdots\ f_n\ t \equiv f_{i_1} (\cdots (f_{i_k}\ t) \cdots)$$

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

$$\boxed{\mathbf{PCP}(S) \leftrightarrow \mathbf{U}_3(f(S))}$$

PCP $\leq$ U$_3$ – ENCODING

Encoding

$$\overline{c_1 c_2 \cdots c_n} = \lambda x.\, c_1(c_2(\cdots(c_n\ x))) \qquad c_i \in \{u, v\} \subseteq \mathcal{V}$$

PCP $\leq$ U$_3$ – ENCODING

Encoding

$$\overline{c_1 c_2 \cdots c_n} = \lambda x.\, c_1(c_2(\cdots(c_n\ x))) \qquad c_i \in \{u, v\} \subseteq \mathcal{V}$$

Properties

- $\overline{A}\left(\overline{B}\ s\right) \equiv \overline{A +\!\!+ B}\ s$
- $\dfrac{\Gamma \vdash u : \alpha \to \alpha \quad \Gamma \vdash v : \alpha \to \alpha}{\Gamma \vdash \overline{A} : \alpha \to \alpha}$

$\mathbf{PCP} \leq \mathbf{U}_3$ – REDUCTION

$$\mathbf{PCP}(S) \leftrightarrow \mathbf{U}_3(f(S))$$

$\mathbf{PCP} \leq \mathbf{U}_3$ – REDUCTION

$\mathbf{PCP}(S) \leftrightarrow \mathbf{U}_3(f(S))$

$f : [x_1/y_1, \ldots, x_n/y_n] \mapsto$

PCP $\leq$ $\mathbf{U}_3$ – REDUCTION

$$\mathbf{PCP}(S) \leftrightarrow \mathbf{U}_3(f(S))$$

$f : [x_1/y_1, \ldots, x_n/y_n] \mapsto$

$$x_f \; \overline{x_1} \cdots \overline{x_n} \; z \stackrel{?}{=} x_f \; \overline{y_1} \cdots \overline{y_n} \; z$$

$$\Gamma := \begin{cases} u : \alpha \to \alpha, \; v : \alpha \to \alpha, \; z : \alpha \\ x_f : \underbrace{(\alpha \to \alpha) \to \cdots \to (\alpha \to \alpha)}_{n \text{ times}} \to \alpha \to \alpha \end{cases}$$

$\mathbf{PCP} \leq \mathbf{U}_3$ – REDUCTION

$$\mathbf{PCP}(S) \leftrightarrow \mathbf{U}_3(f(S))$$

$f : [x_1/y_1, \ldots, x_n/y_n] \mapsto$

$$\lambda uvz.\, x_f\, \overline{x_1} \cdots \overline{x_n}\, z \stackrel{?}{=} \lambda uvz.\, x_f\, \overline{y_1} \cdots \overline{y_n}\, z$$

$$\Gamma := x_f : \underbrace{(\alpha \to \alpha) \to \cdots \to (\alpha \to \alpha)}_{n \text{ times}} \to \alpha \to \alpha$$

PCP $\leq$ $\mathbf{U}_3$ – REDUCTION

$\mathbf{PCP}(S) \leftrightarrow \mathbf{U}_3(f(S))$

$f : [x_1/y_1, \ldots, x_n/y_n] \mapsto$

$$\lambda uvz.\, x_f\ \overline{x_1} \cdots \overline{x_n}\ z \stackrel{?}{=} \lambda uvz.\, x_f\ \overline{y_1} \cdots \overline{y_n}\ z$$

and $$\lambda uz.\, x_f\ u \cdots u\ z \stackrel{?}{=} \lambda uz.\, u\ (d\ u\ z)$$

$$\Gamma := \begin{cases} d : (\alpha \to \alpha) \to \alpha \to \alpha \\ x_f : \underbrace{(\alpha \to \alpha) \to \cdots \to (\alpha \to \alpha)}_{n \text{ times}} \to \alpha \to \alpha \end{cases}$$

PCP $\leq$ $\mathbf{U}_3$ – REDUCTION

$\mathbf{PCP}(S) \leftrightarrow \mathbf{U}_3(f(S))$

$f : [x_1/y_1, \ldots, x_n/y_n] \mapsto$

$$\lambda uvz.\, x_f\, \overline{x_1} \cdots \overline{x_n}\, z \stackrel{?}{=} \lambda uvz.\, x_f\, \overline{y_1} \cdots \overline{y_n}\, z$$

and $$\lambda uz.\, x_f\, u \cdots u\, z \stackrel{?}{=} \lambda uz.\, u\, (d\, u\, z)$$

$$\Gamma := \begin{cases} d : (\alpha \to \alpha) \to \alpha \to \alpha \\ x_f : \underbrace{(\alpha \to \alpha) \to \cdots \to (\alpha \to \alpha)}_{n \text{ times}} \to \alpha \to \alpha \end{cases}$$

PCP $\leq$ $\mathbf{U}_3$ – REDUCTION

$\mathbf{PCP}(S) \leftrightarrow \mathbf{U}_3(f(S))$

$f : [x_1/y_1, \ldots, x_n/y_n] \mapsto$

$$\lambda uv.\, x_f\ \overline{x_1} \cdots \overline{x_n} \stackrel{?}{=} \lambda uv.\, x_f\ \overline{y_1} \cdots \overline{y_n}$$

and $$\lambda u.\, x_f\ u \cdots u \stackrel{?}{=} \lambda u.\, u\ (d\ u)$$

$$\Gamma := \begin{cases} d : (\alpha \to \alpha) \to \alpha \\ x_f : \underbrace{(\alpha \to \alpha) \to \cdots \to (\alpha \to \alpha)}_{n \text{ times}} \to \alpha \end{cases}$$

$\mathbf{PCP} \leq \mathbf{U}_3$ – REDUCTION

$$\mathbf{PCP}(S) \leftrightarrow \mathbf{U}_3(f(S))$$

$f : [x_1/y_1, \ldots, x_n/y_n] \mapsto$

$$\lambda uvh.\, h\ (x_f\ \overline{x_1} \cdots \overline{x_n})\ (x_f\ u \cdots u)$$
$$\stackrel{?}{=} \lambda uvh.\, h\ (x_f\ \overline{y_1} \cdots \overline{y_n})\ (u\ (d\ u))$$

$$\Gamma := \begin{cases} d : (\alpha \to \alpha) \to \alpha \\ x_f : \underbrace{(\alpha \to \alpha) \to \cdots \to (\alpha \to \alpha)}_{n \text{ times}} \to \alpha \end{cases}$$

$\mathbf{PCP} \leq \mathbf{U}_3$ – REDUCTION

$\mathbf{PCP}(S) \leftrightarrow \mathbf{U}_3(f(S))$

$f : [x_1/y_1, \ldots, x_n/y_n] \mapsto$

$$\lambda uvh.\, h\, (x_f\, \overline{x_1} \cdots \overline{x_n})\, (x_f\, u \cdots u)$$
$$\stackrel{?}{=} \lambda uvh.\, h\, (x_f\, \overline{y_1} \cdots \overline{y_n})\, (u\, (d\, u))$$

$$\Gamma := \begin{cases} d : (\alpha \to \alpha) \to \alpha \\ x_f : \underbrace{(\alpha \to \alpha) \to \cdots \to (\alpha \to \alpha)}_{n \text{ times}} \to \alpha \end{cases}$$

$$A := (\alpha \to \alpha) \to (\alpha \to \alpha) \to (\alpha \to \alpha \to \alpha) \to \alpha$$

Timeline

G. Huet (1973)

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

W. Goldfarb (1981)

$$\mathbf{DE} \leq \mathbf{U}_2$$

TIMELINE

Coq

G. Huet (1973)

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

W. Goldfarb (1981)

$\mathbf{DE} \leq \mathbf{U}_2$

Example

Lemma

$$h\ s_1\ s_2 \equiv h\ t_1\ t_2 \quad \textit{iff} \quad \forall i.\ s_i \equiv t_i$$

Example

Lemma

$$h\ s_1\ s_2 \equiv h\ t_1\ t_2 \quad \textit{iff} \quad \forall i.\ s_i \equiv t_i$$

- *If* $s \succ s'$ *and* isLam(head s') *then* isLam(head s)
- *If* $s\ t \succ^* v$ *then* $s \succ^* s', t \succ^* t'$ *and* $v = s'\ t'$ *for some* s', t' *or* $s \succ^* \lambda x.\ s'$, isLambda (head s) *for some* s'
- *If* $s_1\ s_2 \equiv t_1\ t_2$, isVar (head s_1) *and* isVar (head t_1) *then* $\forall i.\ s_i \equiv t_i$

Timeline

G. Huet (1973)

PCP $\leq$ **U**$_3$

W. Goldfarb (1981)

DE $\leq$ **U**$_2$

Diophantine Equations

$$e ::= x + y = z \mid x \cdot y = z \mid x = c \qquad (x, y, z \in \mathcal{V}, c \in \mathbb{N})$$

Diophantine Equations

$$e ::= x + y = z \mid x \cdot y = z \mid x = c \qquad (x, y, z \in \mathcal{V}, c \in \mathbb{N})$$

$$\boxed{\sigma \;\vDash\; e}$$

$$\frac{\sigma\ x = c}{\sigma \;\vDash\; x = c} \qquad \frac{\sigma\ x + \sigma\ y = \sigma\ z}{\sigma \;\vDash\; x + y = z} \qquad \frac{\sigma\ x \cdot \sigma\ y = \sigma\ z}{\sigma \;\vDash\; x \cdot y = z}$$

DIOPHANTINE EQUATIONS

$$e ::= x + y = z \mid x \cdot y = z \mid x = c \qquad (x, y, z \in \mathcal{V}, c \in \mathbb{N})$$

$$\boxed{\sigma \vDash e}$$

$$\frac{\sigma\ x = c}{\sigma \vDash x = c} \qquad \frac{\sigma\ x + \sigma\ y = \sigma\ z}{\sigma \vDash x + y = z} \qquad \frac{\sigma\ x \cdot \sigma\ y = \sigma\ z}{\sigma \vDash x \cdot y = z}$$

$$\frac{\forall e \in E.\ \sigma \vDash e}{\mathbf{DE}(E)}$$

$\mathbf{DE} \leq \mathbf{U}_2$ – IDEA

$\mathbf{DE} \leq \mathbf{U}_2$ – IDEA

$$\Gamma := \{x : \mathcal{T} \to \mathcal{T} \mid x \in \mathcal{V}\}$$

$\mathbf{DE} \leq \mathbf{U}_2$ – IDEA

$$\Gamma \coloneqq \{x : \mathcal{T} \to \mathcal{T} \mid x \in \mathcal{V}\}$$

Translation

$$x\ s \equiv +_n\ s$$

$\mathbf{DE} \leq \mathbf{U}_2$ – IDEA

$$\Gamma := \{x : \mathcal{T} \to \mathcal{T} \mid x \in \mathcal{V}\}$$

Addition

$$\boxed{+_n\ s}$$

$$+_0\ s = s \qquad +_{\mathsf{S}n}\ s = \mathsf{g}\ \mathsf{a}\ (+_n\ s)$$

Translation

$$x\ s \equiv +_n\ s$$

$\mathbf{DE} \leq \mathbf{U}_2$ – IDEA

$$\Gamma := \{x : \mathcal{T} \to \mathcal{T} \mid x \in \mathcal{V}\}$$

Addition

$$\boxed{+_n\ s}$$

$$+_0\ s = s \qquad\qquad +_{\mathsf{S}n}\ s = \mathsf{g}\ \mathsf{a}\ (+_n\ s)$$

Translation

$$x\ s \equiv +_n\ s \quad \rightsquigarrow \quad x\ (+_1\ \mathsf{a}) \stackrel{?}{=} +_1\ (x\ \mathsf{a})$$

$\mathbf{DE} \leq \mathbf{U}_2$ – IDEA

$$\Gamma \coloneqq \{x : \mathcal{T} \to \mathcal{T} \mid x \in \mathcal{V}\}$$

Addition

$$\boxed{+_n\ s}$$

$$+_0\ s = s \qquad\qquad +_{\mathsf{S}n}\ s = \mathsf{g}\ \mathsf{a}\ (+_n\ s)$$

Translation

$$x\ s \equiv +_n\ s \quad \rightsquigarrow \quad x\ (+_1\ \mathsf{a}) \stackrel{?}{=} +_1\ (x\ \mathsf{a})$$

$$x = c \quad \rightsquigarrow \quad x\ \mathsf{a} \stackrel{?}{=} +_c\ \mathsf{a}$$

$\mathbf{DE} \leq \mathbf{U}_2$ – IDEA

$$\Gamma := \{x : \mathcal{T} \to \mathcal{T} \mid x \in \mathcal{V}\}$$

Addition

$$\boxed{+_n\ s}$$

$$+_0\ s = s \qquad\qquad +_{\mathsf{S}n}\ s = \mathsf{g}\ \mathsf{a}\ (+_n\ s)$$

Translation

$$x\ s \equiv +_n\ s \quad \leadsto \quad x\ (+_1\ \mathsf{a}) \stackrel{?}{=} +_1\ (x\ \mathsf{a})$$

$$x = c \quad \leadsto \quad x\ \mathsf{a} \stackrel{?}{=} +_c\ \mathsf{a}$$

$$x + y = z \quad \leadsto \quad x\ (y\ \mathsf{a}) \stackrel{?}{=} z\ \mathsf{a}$$

CONCLUSION

CONCLUSION

G. Huet (1973)

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

Conclusion

G. Huet (1973)

$$\textbf{PCP} \leq \textbf{U}_3$$

W. Goldfarb (1981)

$$\textbf{DE} \leq \textbf{U}_2$$

Conclusion

G. Huet (1973)

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

W. Goldfarb (1981)

$$\mathbf{DE} \leq \mathbf{U}_2$$

Future Work

- Semi-unification
- System F typeability
- System F inhabitation

RELATED WORK I

G. Huet.
The undecidability of unification in third order logic.
Information and control, 1973.

W. Goldfarb.
The undecidability of the second-order unification problem.
Theoretical Computer Science, 1981.

Y. Forster, E. Heiter, G. Smolka.
Verification of PCP-Related Computational Reductions in Coq.
International Conference on Theorem Proving, 2018.

W. Farmer.
Simple second-order languages for which unification is undecidable.
Theoretical Computer Science, 1991.

Related Work II

A. Schubert.
Second-order unification and type inference for Church-style polymorphism.
Proceedings of the 25th ACM SIGPLAN-SIGACT symposium on Principles of programming languages, 1998.

J. Levy and M. Veanes.
On the undecidability of second-order unification.
Information and Computation, 2000.

Multiplication

$x \cdot y = z \rightsquigarrow$

$$G\ \mathsf{a}\ \mathsf{b}\ (\mathsf{g}\ (\mathsf{g}\ (z\ \mathsf{a})(y\ \mathsf{b}))\ \mathsf{a}) \stackrel{?}{=} \mathsf{g}\ (\mathsf{g}\ \mathsf{a}\ \mathsf{b})(G\ (x\ \mathsf{a})\ (+_1\ \mathsf{b})\ \mathsf{a})$$
$$G\ \mathsf{b}\ \mathsf{a}\ (\mathsf{g}\ (\mathsf{g}\ (z\ \mathsf{b})(y\ \mathsf{a}))\ \mathsf{a}) \stackrel{?}{=} \mathsf{g}\ (\mathsf{g}\ \mathsf{b}\ \mathsf{a})(G\ (x\ \mathsf{b})\ (+_1\ \mathsf{a})\ \mathsf{a})$$

SET UNIFICATION

$$\mathbf{SU}_n^A \{\Gamma \vdash_n s_i \stackrel{?}{=} t_i : A \mid 1 \leq i \leq k\} :=$$
$$\exists \sigma \Delta.\ \Delta \vdash \sigma : \Gamma \quad \mathit{and} \quad \forall i.\ s_i[\sigma] \equiv t_i[\sigma]$$

$\mathbf{SU}_2^{\mathcal{T}} \leq \mathbf{U}_2$

$$\{\Gamma \vdash_2 s_i \stackrel{?}{=} t_i : \mathcal{T} \mid 1 \leq i \leq k\} \mapsto$$

$$\Gamma \vdash_2 \mathsf{g}\ s_1\ (\cdots\ (\mathsf{g}\ s_k\ \mathsf{a})) \stackrel{?}{=} \mathsf{g}\ t_1\ (\cdots\ (\mathsf{g}\ t_k\ \mathsf{a})) : \mathcal{T}$$

Lemma

$$\mathsf{g}\ s_1\ s_2 \equiv \mathsf{g}\ t_1\ t_2 \quad \textit{iff} \quad \forall i.\ s_i \equiv t_i$$

FORMALISATION

$\boxed{A\ s}$	$\boxed{s\ A}$	$\boxed{\Lambda_n\ s}$
$\mathsf{nil}\ s = s$	$s\ \mathsf{nil} = s$	$\Lambda_0\ s = s$
$(t :: A)\ s = t\ (A\ s)$	$s\ (t :: A) = (A\ s)\ t$	$\Lambda_{\mathsf{S}n} s = \lambda x.\ \Lambda_n\ s$

PCP

Definition in[1]

$$\tau_j\ \mathsf{nil} = \mathsf{nil}$$
$$\tau_j\ (a :: A) = x_j +\!\!+\ \tau_j\ A \qquad a = x_1/x_2$$
$$\mathbf{PCP}(S) \coloneqq \exists A \subseteq S, A \neq \mathsf{nil}.\ \tau_1\ A = \tau_2\ A$$

Our Definition

$$\tau_j\ \mathsf{nil} = \mathsf{nil}$$
$$\tau_j\ (i :: A) = x_j +\!\!+\ \tau_j\ A \qquad S[i] = x_1/x_2$$
$$\mathbf{PCP}(S) \coloneqq \exists A \colon \mathcal{L}\ \mathbb{F}_{|S|}, A \neq \mathsf{nil}.\ \tau_1\ A = \tau_2\ A$$

[1] Forster, Heiter, and Smolka 2017.

$\mathbf{PCP}(S) \to \mathbf{U}_3(f(S))$

Given

$$[i_1, \ldots, i_k]$$

Pick

$$\Delta \coloneqq z : \alpha$$

$$\sigma \coloneqq \left\{ \begin{array}{l} x_f \mapsto \lambda x_1 \ldots x_n .\, x_{i_1}(\cdots(x_{i_k}\ z)) \\ d \mapsto \lambda u.\, \underbrace{u(\cdots(u}_{k-1}\ z)) \end{array} \right\}$$

$$\begin{aligned} (\sigma x_f)\ \overline{x_1} \cdots \overline{x_n} &\equiv \overline{x_{i_1} \cdots x_{i_k}}\ z \\ &= \overline{y_{i_1} \cdots y_{i_k}}\ z \\ &\equiv (\sigma x_f)\ \overline{y_1} \cdots \overline{y_n} \end{aligned}$$

$$\begin{aligned} (\sigma x_f)\ u \cdots u &\equiv u(\cdots(u\ z)) \\ &\equiv u((\sigma d)\ u) \end{aligned}$$

$\mathbf{U}_3(f(S)) \to \mathbf{PCP}(S)$

$$(\lambda uvh.\ h\ (x_f\ \overline{x_1} \cdots \overline{x_n})\ (x_f\ u \cdots u))[\sigma] \equiv (\lambda uvh.\ h\ (x_f\ \overline{y_1} \cdots \overline{y_n})\ (u\ (d\ u)))[\sigma]$$

We get

$$\sigma x_f\ \overline{x_1} \cdots \overline{x_n} \equiv \sigma x_f\ \overline{y_1} \cdots \overline{y_n} \tag{1}$$

$$\sigma x_f\ u \cdots u \equiv u\ (\sigma d\ u) \tag{2}$$

By normalisation $\sigma x_f \equiv \lambda x_1 \cdots x_l.\ s$ for some l, s where s is normal. By (2) and typing we know that $1 < l \leq n$ and $s \equiv x_i\ s'$.

Continued

Case analysis.

- Let $l < n$. Then $\sigma x_f\ \overline{x_1} \cdots \overline{x_n} \equiv (\overline{x_i}\ s'[\overline{x_1}/x_1, \ldots, \overline{x_l}/x_l])\ \overline{x_{l+1}} \cdots \overline{x_n}$ and $\sigma x_f\ \overline{y_1} \cdots \overline{y_n} \equiv (\overline{y_i}\ s'[\overline{y_1}/x_1, \ldots, \overline{y_l}/x_l])\ \overline{y_{l+1}} \cdots \overline{y_n}$. Thus $\overline{x_{l+1}} \equiv \overline{y_{l+1}}$ by (1) and $x_{l+1} = y_{l+1}$.
- Let $l = n$. Let $x_{i_1}, \ldots, x_{i_k}$ be the longest sequence s.t. $s = x_{i_1}(\cdots (x_{i_k}\ s''))$. Then $\sigma x_f\ \overline{x_1} \cdots \overline{x_n} \equiv \overline{x_{i_1}}(\cdots (\overline{x_{i_k}}\ s''[\overline{x_1}/x_1, \ldots, \overline{x_n}/x_n]))$ and $\sigma x_f\ \overline{y_1} \cdots \overline{y_n} \equiv \overline{y_{i_1}}(\cdots (\overline{y_{i_k}}\ s''[\overline{y_1}/x_1, \ldots, \overline{y_n}/x_n]))$. Since u, v cannot appear free in s'' we get $x_{i_1} \cdots x_{i_k} = y_{i_1} \cdots y_{i_k}$.