Isomorphisms in the presence of sum and function types

Axioms and decidability

Danko ILIK

Parsifal, Inria

February 7, 2014
Deducteam Seminar, Paris

Types in the language $\{\top, \times, +, \to\}$

Language of *polynomials* **with exponentiation**

$$\mathcal{E} \ni f, g ::= 1 \mid x_i \mid f + g \mid fg \mid g^f,$$

$$\begin{aligned} [\![1]\!] &= \top \\ [\![x_i]\!] &= \mathbf{x_i} \\ [\![g^f]\!] &= [\![f]\!] \to [\![g]\!] \\ [\![fg]\!] &= [\![f]\!] \times [\![g]\!] \\ [\![f+g]\!] &= [\![f]\!] + [\![g]\!] \end{aligned}$$

Write "$\tau \in \mathcal{E}$" when $[\![f]\!] = \tau$ for some $f \in \mathcal{E}$

Isomorphisms of types (Constructive cardinality of sets)

Definition ($\tau \cong \sigma$)

Types τ and σ are isomorphic when there exist

$$\phi : \tau \to \sigma, \quad \psi : \sigma \to \tau$$

such that

$$\phi \circ \psi = \mathsf{id}_\sigma, \quad \psi \circ \phi = \mathsf{id}_\tau\ .$$

In typed lambda calculus, one would work with $\beta\eta$-equality,

$$\lambda x.\phi(\psi x) =_{\beta\eta} \lambda x.x, \quad \lambda y.\psi(\phi y) =_{\beta\eta} \lambda y.y.$$

Type isomorphisms for $\mathcal{E}$

Questions

1. Completeness: Can we always, given $[\![f]\!] \cong [\![g]\!]$, show that a finite number of rewrite equations suffice to derive it? — i.e. is there a set of **axioms** for $\cong$ over $\mathcal{E}$?
2. Decidability: Can we always, given f and g, effectively decide whether $[\![f]\!] \cong [\![g]\!]$ or not?

Type isomorphisms for $\mathcal{E} \setminus \{+\}$ and $\mathcal{E} \setminus \{\rightarrow\}$

Finitely axiomatizable and decidable (Soloviev 1981)

Take the corresponding fragment of *High School Identities* (**HSI**):

$$f \doteq f$$

$$f + g \doteq g + f$$

$$(f+g)+h \doteq f+(g+h)$$

$$fg \doteq gf$$

$$(fg)h \doteq f(gh)$$

$$f(g+h) \doteq fg + fh$$

$$1f \doteq f$$

$$f^1 \doteq f$$

$$1^f \doteq 1$$

$$f^{g+h} \doteq f^g f^h$$

$$(fg)^h \doteq f^h g^h$$

$$(f^g)^h \doteq f^{gh}$$

In simultaneous presence of $+$ and $\to$, we do have

$$\mathsf{HSI} \vdash f \doteq g \;\Rightarrow\; [\![f]\!] \cong [\![g]\!] \;\Rightarrow\; \mathbb{N}^{+} \models f \equiv g,$$

but

$$\mathbb{N}^{+} \models f \equiv g \;\not\Rightarrow\; \mathsf{HSI} \vdash f \doteq g$$

and

$$[\![f]\!] \cong [\![g]\!] \;\not\Rightarrow\; \mathsf{HSI} \vdash f \doteq g.$$

Type isomorphisms for $\mathcal{E}$

Martin-Wilkie-Gurevič negative solution of the HSI Problem

Take

$$(A^x + B^x)^y (C^y + D^y)^x \equiv (A^y + B^y)^x (C^x + D^x)^y,$$

where $A = 1 + x, B = 1 + x + x^2, C = 1 + x^3, D = 1 + x^2 + x^4$.

The equation holds both in $\mathbb{N}^+$ and as a type isomorphism, but it is **not derivable** from the HSI axioms.

In fact,

$$(A^{2^x} + B_n^{2^x})^x (C_n^x + D_n^x)^{2^x} \equiv (A^x + B_n^x)^{2^x} (C_n^{2^x} + D_n^{2^x})^x,$$

where $A = x + 1$, $B_n = 1 + x + x^2 + \cdots + x^{n-1}$, $C_n = 1 + x^n$, $D_n = 1 + x^2 + x^4 + \cdots + x^{2(n-1)}$, has the same fate, **for any odd** $n > 3$.

This means that type isomorphism over $\mathcal{E}$ is **not finitely axiomatizable**.

What about decidability?

Theorem (Richardson 1969, Macintyre 1981)

One can effectively decide $\mathbb{N}^+ \models f \equiv g$ *for any* $f, g \in \mathcal{E}$.

Unfortunately, although

$$\mathsf{HSI} \vdash f \doteq g \;\Rightarrow\; [\![f]\!] \cong [\![g]\!] \;\Rightarrow\; \mathbb{N}^+ \models f \equiv g,$$

a proof of

$$[\![f]\!] \cong [\![g]\!] \;\Leftarrow\; \mathbb{N}^+ \models f \equiv g$$

is not known, and HSI is not complete:

$$\mathsf{HSI} \vdash f \doteq g \;\not\Leftarrow\; \mathbb{N}^+ \models f \equiv g.$$

Type isomorphisms for the subclass $\mathcal{L} \subsetneq \mathcal{E}$

Levitz 1975, Henson-Rubel 1984

Recall

$$\mathcal{E} \ni f, g ::= 1 \mid x_i \mid f + g \mid fg \mid g^f.$$

Definition (The subclass $\mathcal{L}$)

$$\mathcal{L} \ni f, g ::= 1 \mid x_i \mid f + g \mid fg \mid l^f,$$

where $l \in \Lambda$ is defined by

$$\Lambda \ni f, g ::= 1 \mid x_i \mid f + g \mid fg \mid l_0^f,$$

and $l_0 \in \Lambda$ has no variables.

Type isomorphisms for the subclass $\mathcal{L} \subsetneq \mathcal{E}$

Theorem (Henson-Rubel 1984)

For all $f, g \in \mathcal{L}$,

$$\mathbb{N}^+ \vDash f \equiv g \;\Rightarrow\; HSI \vdash f \doteq g.$$

Corollary

Type isomorphisms for $\mathcal{L}$ is decidable and finitely axiomatizable.

Proof.

$$\mathrm{HSI} \vdash f \doteq g \;\Rightarrow\; [\![f]\!] \cong [\![g]\!] \;\Rightarrow\; \mathbb{N}^+ \vDash f \equiv g \;\Rightarrow\; \mathrm{HSI} \vdash f \doteq g$$

□

Example

Consider the identity

$$(A^x + B^x)^y (C^y + D^y)^x \equiv (A^y + B^y)^x (C^x + D^x)^y,$$

where $A = 1 + x, B = 1 + x + x^2, C = 1 + x^3, D = 1 + x^2 + x^4$.

We have $(A^x + B^x)^y, (C^x + D^x)^y \notin \mathcal{L}$, because bases of exponentiation are not allowed to contain bases of exponentiation that contain variables

Example

The typed versions of the induction axiom for a decidable predicate,

$$(y+z)^{x(y+z)(y+z)^{x(y+z)}} \in \mathcal{L},$$

but its curried form,

$$\left(((y+z)^x)^{((y+z)^{y+z})^x}\right)^{y+z} \notin \mathcal{L}$$

although the two terms are inter-derivable using the HSI axioms.

Example

The typed versions of the induction axiom for a decidable predicate,

$$(y+z)^{x(y+z)(y+z)^{x(y+z)}} \in \mathcal{L},$$

but its curried form,

$$\left(((y+z)^x)^{((y+z)^{y+z})^x}\right)^{y+z} \notin \mathcal{L}$$

although the two terms are inter-derivable using the HSI axioms.

This means that one could in principle further extend $\mathcal{L}$.

Wilkie's *positive* solution of the HSI Problem

For the whole of $\mathcal{E}$, the axioms of HSI are *almost* complete.

Wilkie's *positive* solution of the HSI Problem

For the whole of $\mathcal{E}$, the axioms of HSI are *almost* complete.
Define

$$\mathcal{E}^* \ni f, g ::= t_z \mid 1 \mid x_i \mid g^f \mid fg \mid f + g,$$

where z is a *positive polynomial with integer monomial coefficients* and t_z are new constant symbols indexed by such polynomials.

Wilkie's *positive* solution of the HSI Problem

For the whole of $\mathcal{E}$, the axioms of HSI are *almost* complete.
Define

$$\mathcal{E}^* \ni f, g ::= t_z \mid 1 \mid x_i \mid g^f \mid fg \mid f + g,$$

where z is a *positive polynomial with integer monomial coefficients* and t_z are new constant symbols indexed by such polynomials.
Define HSI* by extending HSI with

$$\begin{aligned} t_1 &\doteq 1 \\ t_{x_i} &\doteq x_i \\ t_{zu} &\doteq t_z t_u \\ t_{z+u} &\doteq t_z + t_u \\ t_z &\doteq t_u && \text{(when } \mathbb{N}^+ \models z \equiv u\text{)} \end{aligned}$$

Type isomorphism for $\mathcal{E}$ is recursively axiomatizable

Theorem (Wilkie 1981)

*For all $f, g \in \mathcal{E}$ (i.e. all f, g of $\mathcal{E}^*$ that do **not** contain t_z-symbols), we have that $\mathbb{N}^+ \models f \equiv g$ implies HSI* $\vdash f \doteq g$.*

Corollary

Type isomorphism for $\mathcal{E}$ is axiomatizable by the primitively recursive set HSI.*

Type isomorphism for $\mathcal{E}$ is decidable?

We have

$$\mathsf{HSI} \vdash f \doteq g \;\Rightarrow\; [\![f]\!] \cong [\![g]\!] \;\Rightarrow\; \mathbb{N}^+ \models f \equiv g \;\Rightarrow\; \mathsf{HSI}^* \vdash f \doteq g,$$

but to close the circle we need

$$\mathsf{HSI}^* \vdash f \doteq g \;\Rightarrow\; [\![f]\!] \cong [\![g]\!].$$

Question:

$$[\![t_z]\!] = ?$$

Soundness of HSI* as type isomorphisms

We do not need negative types. Use the fact that z — even if has negative coefficients — is point-wise positive:

$$\forall x_1, \ldots, x_n \in \mathbb{N}^+.\ z(x_1, \ldots, x_n) \in \mathbb{N}^+.$$

So, define the interpretation of types point-wise:

$$\begin{aligned}
[\![1]\!]_\rho &= \mathbf{1} \\
[\![x_i]\!]_\rho &= \rho(x_i) \\
[\![g^f]\!]_\rho &= [\![f]\!]_\rho \to [\![g]\!]_\rho \\
[\![fg]\!]_\rho &= [\![f]\!]_\rho \times [\![g]\!]_\rho \\
[\![f + g]\!]_\rho &= [\![f]\!]_\rho + [\![g]\!]_\rho \\
[\![t_z]\!]_\rho &= \underbrace{1 + 1 + \cdots + 1}_{k\text{-times}} = \mathbf{k} \qquad \text{where } k = \mathrm{eval}(t_z, \rho)
\end{aligned}$$

Soundness of HSI* as type isomorphisms

Theorem

Let $f, g \in \mathcal{E}^*$. If HSI $\vdash f \doteq g$ then $[\![f]\!]_\rho \cong [\![g]\!]_\rho$ for any ρ that interprets variables by types of form* **k***.*

Corollary

Given two types $f, g \in \mathcal{E}$, one can decide whether $[\![f]\!]_\rho \cong [\![g]\!]_\rho$ or not, and this holds at least when ρ interprets variable by types of form **k***.*

Beyond decidability for base types of form **k**

Consider base types given in Cantor normal form (CNF),

$$\omega^{\alpha_1} n_1 + \cdots + \omega^{\alpha_k} n_k,$$

where α_i are in CNF and $\alpha_1 > \cdots > \alpha_k$.

Beyond decidability for base types of form **k**

Consider base types given in Cantor normal form (CNF),

$$\omega^{\alpha_1} n_1 + \cdots + \omega^{\alpha_k} n_k,$$

where α_i are in CNF and $\alpha_1 > \cdots > \alpha_k$.

Since we could rewrite z as $p_1 - p_2$, where $p_1 > p_2$ and p_1, p_2 only have positive coefficients, the interpretation

$$[\![t_z]\!] = [\![t_{p_1 - p_2}]\!] = [\![t_{p_1}]\!] \dot{-} [\![t_{p_2}]\!]$$

is in CNF because subtraction ($\dot{-}$) between two CNFs is well defined when $[\![t_{p_1}]\!] > [\![t_{p_2}]\!]$.