An arithmetic for non-size-increasing polynomial-time computation

Klaus Aehlig

A term system for Ptime

- based on Hofmann 1999
- for non-size-increasing functions only
- size is measured by a special type $\diamond$
  - technically measures the number of free variables
  - constructor symbols for lists are of the types

$$\begin{array}{ll} \mathbf{nil}_\tau & \mathbf{L}(\tau) \\ \mathbf{cons}_\tau & \diamond \multimap \tau \multimap \mathbf{L}(\tau) \multimap \mathbf{L}(\tau) \end{array}$$

  - linear typing to avoid

$$\mathbf{cons}_\tau d^\diamond a_1(\ldots(\mathbf{cons}_\tau d^\diamond a_n \mathbf{nil}_\tau))$$

A term system for Ptime (cont'd)

- Iteration over lists:

$$\frac{\Gamma \vdash t^{\mathbf{L}(\tau)} \qquad \emptyset \vdash s^{\diamond \multimap \tau \multimap \rho \multimap \rho}}{\Gamma \vdash (t\,\{s\})^{\rho \multimap \rho}}$$

- Terms can be normalized in polynomial many steps
  - Length is measured by the number of free variable
  - Degree of the Polynomial is the nesting of $\{\cdot\}$'s
  - Every closed term denotes a Ptime function

Formulae and computational content (naive approach):

$$A, B ::= \; P(\vec{t}) \mid A \wedge B \mid A \to B \mid \exists x A \mid \forall x A$$

$$[\![P(\vec{t})]\!] \quad = \quad \star$$

$$[\![\forall x^\tau A]\!] \quad = \quad \begin{cases} \star & [\![A]\!] = \star \\ \tau \multimap [\![A]\!] & \text{otherwise} \end{cases}$$

$$[\![\exists x^\tau A]\!] \quad = \quad \begin{cases} \tau & [\![A]\!] = \star \\ \tau \otimes [\![A]\!] & \text{otherwise} \end{cases}$$

$$[\![A \to B]\!] \quad = \quad \begin{cases} [\![B]\!] & [\![A]\!] = \star \\ \star & [\![B]\!] = \star \\ [\![A]\!] \multimap [\![B]\!] & \text{otherwise} \end{cases}$$

Induction versus Iteration

If we took induction like this

$$\frac{\forall x^{\mathbf{L}(\tau)} \forall y^{\diamond} \forall z^{\tau}. A \to A[\mathbf{cons}_\tau yzx/x] \qquad t^{\mathbf{L}(\tau)}}{A[\mathbf{nil}_\tau/x] \to A[t/x]}$$

we would get a step term of type

$$\mathbf{L}(\tau) \multimap \diamond \multimap \tau \multimap [\![A]\!] \multimap [\![A]\!]$$

So we need a proof *uniform in* $x^{\mathbf{L}(\tau)}$!

The “strong” for-all quantifier

- New quantifier $\forall^*$ that quantifies “computationally irrelevant”
- Mark the computational relevant variables and assumptions as being the computational (“essential” context)

$$\frac{\Psi, x^\tau \; ; \; \Phi, x^\tau \; \vdash N \; : \; A \qquad \texttt{Vars!}}{\Psi \; ; \; \Phi \; \vdash \lambda x^\tau . N \; : \; \forall x^\tau A}$$

$$\frac{\Psi, x^\tau \; ; \; \Phi \; \vdash N \; : \; A \qquad x \notin \Phi \qquad \texttt{Vars!}}{\Psi \; ; \; \Phi \; \vdash \lambda^* x^\tau . N \; : \; \forall^* x^\tau A}$$

$$\frac{\Psi \; ; \; \Phi \; \vdash N \; : \; \forall x^\tau \qquad \Gamma \vdash t^\tau \qquad \Gamma \subset \Psi}{\Psi \; ; \; \Phi, \Gamma \; \vdash N t \; : \; A[t/x]}$$

$$\frac{\Psi \; ; \; \Phi \; \vdash N \; : \; \forall^* x^\tau \qquad \Gamma \vdash t^\tau \qquad \Gamma \subset \Psi}{\Psi \; ; \; \Phi \; \vdash N t \; : \; A[t/x]}$$

Computational context

- Pruning

$$\frac{\Psi\,;\,\Phi \vdash N : A \qquad [\![A]\!] = \star}{\Psi\,;\,\emptyset \vdash N : A}$$

- Weakening

$$\frac{\begin{array}{c}\Psi\,;\,\Phi \vdash N : A \\ \Psi \subset \Psi' \qquad \Phi \subset \Phi'\end{array}}{\Psi'\,;\,\Phi' \vdash N : A}$$

Proof rules

$$\frac{\Psi\ ;\ \emptyset \vdash N : \forall^* x^{\mathbf{L}(\tau)} \forall y^{\diamond} \forall z^{\tau}. A \to A[\mathbf{cons}_\tau yzx/x] \qquad \Gamma \vdash t^{\mathbf{L}(\tau)} \qquad \Gamma \subset \Psi}{\Psi\ ;\ \Gamma \vdash t\,\{N\} : A[\mathbf{nil}_\tau/x] \to A[t/x]}$$

$$\frac{\Psi\ ;\ \Phi_1 \vdash N : A \to B \qquad \Psi\ ;\ \Phi_2 \vdash M : A}{\Psi\ ;\ \Phi_1, \Phi_2 \vdash NM : B}$$

Proof rules (cont'd)

$$\boxtimes_{x,A} \quad : \quad \forall x. A \to \exists x A$$

$$\frac{\begin{array}{l}\Psi \; ; \; \Phi_1 \; \vdash N \; : \; \exists x^\tau A \\ \Psi, x^\tau, u^A \; ; \; \Phi_2, x^\tau, u^A \; \vdash M \; : \; B \\ \texttt{Vars!}\end{array}}{\Psi \; ; \; \Phi_1, \Phi_2 \; \vdash N(\lambda x^\tau, u^A \, M) \; : \; B}$$

Extracted terms

$$
\begin{aligned}
[\![u^A]\!] &= x_{u^A} \\[1em]
[\![\lambda u^A\, N^B]\!] &= \begin{cases} \varepsilon & [\![B]\!] = \star \\ [\![N]\!] & [\![A]\!] = \star \neq [\![B]\!] \\ \lambda x_u\ [\![N]\!] & \text{otherwise} \end{cases} \\[1em]
[\![N^{A\to B} M]\!] &= \begin{cases} \varepsilon & [\![B]\!] = \star \\ [\![N]\!] & [\![A]\!] = \star \neq [\![B]\!] \\ [\![N]\!]\ [\![M]\!] & \text{otherwise} \end{cases}
\end{aligned}
$$

more extracted terms (only main cases shown):

$$
\begin{array}{lcl}
[\![\lambda x^{\tau}\, N^{A}]\!] & = & \lambda x\ [\![N]\!] \\
[\![N^{\forall x.A} t]\!] & = & [\![N]\!]\ t \\
[\![\lambda^{*} x^{\tau} N]\!] & = & [\![N]\!] \\
[\![N^{\forall^{*} x.A} t]\!] & = & [\![N]\!] \\
\boxtimes_{x^{\tau},A} & = & \otimes_{\tau,[\![A]\!]} \\
[\![N^{\exists x A}(\lambda x, u\, M^{B})]\!] & = & [\![N]\!]\ (\lambda x, x_{u}\ [\![M]\!]) \\
[\![t^{\mathbf{L}(\tau)}\ \{N^{B}\}]\!] & = & t\,\{[\![N]\!]\}
\end{array}
$$

Realizability

$$\varepsilon \,\underline{\mathbf{mr}}\, P(\vec{t}) \quad = \quad P(\vec{t})$$

$$r \,\underline{\mathbf{mr}}\, \exists x A \quad = \quad \begin{cases} \varepsilon \,\underline{\mathbf{mr}}\, A[r/x] & [\![A]\!] = \star \\ r\pi_1 \,\underline{\mathbf{mr}}\, A[r\pi_0/x] & \text{otherwise} \end{cases}$$

$$r \,\underline{\mathbf{mr}}\, (A \to B) \quad = \quad \begin{cases} \varepsilon \,\underline{\mathbf{mr}}\, A \to r \,\underline{\mathbf{mr}}\, B & [\![A]\!] = \star \\ \forall x.x \,\underline{\mathbf{mr}}\, A \to \varepsilon \,\underline{\mathbf{mr}}\, B & [\![A]\!] \neq \star = [\![B]\!] \\ \forall x.x \,\underline{\mathbf{mr}}\, A \to rx \,\underline{\mathbf{mr}}\, B & \text{otherwise} \end{cases}$$

Realizability (cont'd)

$$r \, \underline{\mathbf{mr}} \, \forall x A \quad = \quad \begin{cases} \forall x . \varepsilon \, \underline{\mathbf{mr}} \, A & [\![A]\!] = \star \\ \forall x . r x \, \underline{\mathbf{mr}} \, A & \text{otherwise} \end{cases}$$

$$r \, \underline{\mathbf{mr}} \, \forall^* x A \quad = \quad \forall x . r \, \underline{\mathbf{mr}} \, A$$

Soundness

- Soundness of typing:

$$\vec{u}, \vec{x} \,;\, \vec{v}, \vec{y} \vdash N : A \Longrightarrow [\![\vec{v}]\!] , \vec{y} \vdash [\![N]\!]^{[\![A]\!]}$$

- Soundness of realizibility:

Assume $\Psi \,;\, \Phi \vdash N : A$ with $\Phi \subset \Psi$. Then there is a proof term $\mu(N)$ with $\overline{\Psi} \,;\, \emptyset \vdash \mu(N) : [\![N]\!]\ \underline{\mathbf{mr}}\, A$.

Example (Append)

- Axioms:

$$\mathtt{APP}(\mathbf{nil}_\tau, l^{\mathbf{L}(\tau)}, l^{\mathbf{L}(\tau)})$$

$$\mathtt{APP}(l^{\mathbf{L}(\tau)}, l'^{\mathbf{L}(\tau)}, l''^{\mathbf{L}(\tau)}) \to \mathtt{APP}(\mathbf{cons}_\tau x^\diamond y^\tau l, l', \mathbf{cons}_\tau x y l'')$$

- We show $\forall l'^{\mathbf{L}(\tau)}, l^{\mathbf{L}(\tau)} \exists l''^{\mathbf{L}(\tau)} \mathtt{APP}(l, l', l'')$.

- Induction on l. Step case

  Prove $\exists l''^{\mathbf{L}(\tau)} \mathtt{APP}(\mathbf{cons}_\tau x^\diamond y^\tau l, l', l'')$ from l', l, $\underline{x^\diamond}$, $\underline{y^\tau}$ and $\underline{\exists l''^{\mathbf{L}(\tau)} \mathtt{APP}(l, l', l'')}$.

- Extracted program

$$\begin{aligned} \lambda l', l \quad & l\{\lambda x^\diamond, z^\tau, x_u^{\mathbf{L}(\tau)} \quad (\lambda l'' \\ & (\lambda y^{\mathbf{L}(\tau)}\, y)(\mathbf{cons}_\tau x z l''))x_u\} \\ & ((\lambda y^{\mathbf{L}(\tau)}\, y) l') \end{aligned}$$

Other approaches

Berger, Hofmann, Schwichtenberg 1999 (unpublished draft)

- E–predicates and computational irrelevant quantifiers
  - computational relevance by quantifiers relativised to E
  - extra axioms ensuring the "existence" of certain terms
- handle $\diamond$ as a proposition
- restriction to ground types
  - higher types via *logical* implication
  - realizability statement in the meta level
- take the computational context only
- axioms instead of rules