Relating Proof Systems for Recursive Types

Clemens Grabmayer
Department of Computer Science
Vrije Universiteit Amsterdam

3^{rd} December 2004

Recursive Types (with only type-constructor $\rightarrow$)

Definition 1. The set μTp of *recursive types* is generated by

$$\tau ::= \alpha \mid \bot \mid \top \mid (\tau \rightarrow \tau) \mid (\mu\alpha.\,\tau) \qquad (\alpha \in TVar).$$

where $TVar$ is a set of *type variables*; the *leading symbol* $\mathcal{L}(\tau)$ of a recursive type τ appears coloured.

Examples: $\mu\beta.\,(\beta \rightarrow \bot)$, $\mu\alpha.\,((\alpha \rightarrow \alpha) \rightarrow \alpha)$, $\mathcal{L}(\mu\gamma.\,\gamma) =_{\text{def}} \bot$.

Important operations on recursive types are *unfolding* and *folding*:

$$\mu\alpha.\,\tau \rightarrow_{\text{unfold}} \tau[\mu\alpha.\,\tau/\alpha] \quad \text{and} \quad \tau[\mu\alpha.\,\tau/\alpha] \rightarrow_{\text{fold}} \mu\alpha.\,\tau\ .$$

Definition 2. *Recursive type equality* $=_\mu$ is a binary relation on μTp:

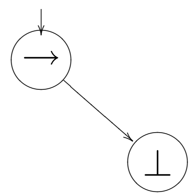
$$\tau =_\mu \sigma \iff_{\text{def}} \textbf{Tree}(\tau) = \textbf{Tree}(\sigma)\ .$$

Tree Unfolding, Recursive Type Equality

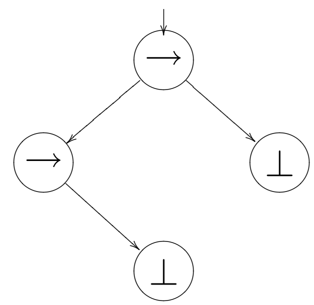
Example 3. The recursive types

$$\tau \equiv \mu\alpha.\,(\alpha \to \bot) \qquad \text{and} \qquad \sigma \equiv \mu\beta.\,((\beta \to \bot) \to \bot)$$

correspond respectively to the different cyclic term graphs

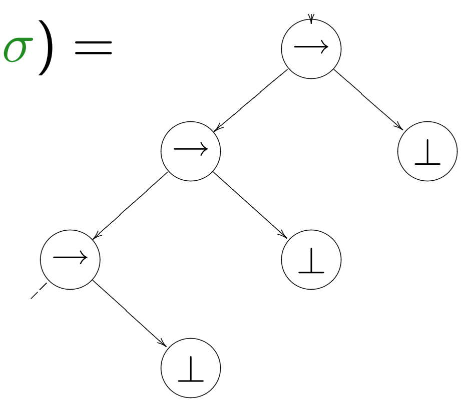


and



but possess the same tree unfolding

$$\mathbf{Tree}(\tau) = \mathbf{Tree}(\sigma) =$$



Hence $\tau =_\mu \sigma$ holds.

Proof Systems for Recursive Type Equality

- Sound and complete axiom systems w.r.t. $=_\mu$:
  - $\mathbf{AC}^=$ by Amadio and Cardelli (1993) is *of "traditional form"*.
  - $\mathbf{HB}^=$ by Henglein and Brandt (1998) is *coinductively motivated*.

$$\tau =_\mu \sigma \iff \vdash_{\mathbf{AC}^=} \tau = \sigma \quad \left(\iff \vdash_{\mathbf{HB}^=} \tau = \sigma \right) .$$

- A system on which "consistency-checking" w.r.t. $=_\mu$ can be based:
  - $\mathbf{AK}^=$, a "syntactic-matching" system à la Ariola and Klop (1995).

$\tau =_\mu \sigma \iff$ no "contradiction" is derivable in $\mathbf{AK}^=$ from assumption $\tau = \sigma$.

$\chi_1 = \chi_2$ is a *contradiction* iff $\mathcal{L}(\chi_1) \neq \mathcal{L}(\chi_2)$; such as: $\bot = \top$, $\tau_1 \to \tau_2 = \alpha$, $\gamma = \bot$, $\mu\alpha.\,\alpha = \top$, and $\alpha = \beta$ (for $\alpha \neq \beta$).

Specific Rules in $\mathbf{AC}^{=}$, $\mathbf{HB}^{=}$, and $\mathbf{AK}^{=}$

- in $\mathbf{AC}^{=}$:

$$\frac{\sigma_1 = \tau[\sigma_1/\alpha] \qquad \sigma_2 = \tau[\sigma_2/\alpha]}{\sigma_1 = \sigma_2}\,\text{UFP}$$

(if α "guarded" in τ by "$\rightarrow$")

- in $\mathbf{HB}^{=}$:

$$\frac{\begin{array}{cc} [\tau_1 \to \tau_2 = \sigma_1 \to \sigma_2]^{u} & [\tau_1 \to \tau_2 = \sigma_1 \to \sigma_2]^{u} \\ \mathcal{D}_1 & \mathcal{D}_2 \\ \tau_1 = \sigma_1 & \tau_2 = \sigma_2 \end{array}}{\tau_1 \to \tau_2 = \sigma_1 \to \sigma_2}\,\text{ARROW/FIX}, u$$

- in $\mathbf{AK}^{=}$:

$$\frac{\tau_1 \to \tau_2 = \sigma_1 \to \sigma_2}{\tau_i = \sigma_i}\,\text{DECOMP (for } i \in \{1,2\})$$

Present in all systems: REFL, SYMM, TRANS, (FOLD/UNFOLD).

Derivations in $\mathbf{HB}^{=}$ and $\mathbf{AK}^{=}$

Example 4. Derivations in (slight variants) of $\mathbf{HB}^{=}$ and $\mathbf{AK}^{=}$:

$$
\dfrac{\dfrac{\dfrac{\mathsf{FOLD}_{l/r}\,\dfrac{(\tau\to\bot=(\sigma\to\bot)\to\bot)^{u}}{\tau=\sigma} \qquad \dfrac{\mathsf{(REFL)}}{\bot=\bot}}{\tau\to\bot=\sigma\to\bot}\,\mathsf{ARROW/FIX}}{\tau=\sigma\to\bot}\,\mathsf{FOLD}_{l} \qquad \dfrac{\mathsf{(REFL)}}{\bot=\bot}}{\dfrac{\tau\to\bot=(\sigma\to\bot)\to\bot}{\underbrace{\mu\alpha.\,(\alpha\to\bot)}_{\equiv\tau}=\underbrace{\mu\beta.\,((\beta\to\bot)\to\bot)}_{\equiv\sigma}}\,\mathsf{FOLD}_{l/r}}\,\mathsf{ARROW/FIX},\ u
$$

Derivations in HB$^=$ and AK$^=$

Example 4. Derivations in (slight variants) of **HB**$^=$ and **AK**$^=$:

$$
\dfrac{\dfrac{\dfrac{\dfrac{\text{FOLD}_{l/r}\,\dfrac{(\tau\to\bot=(\sigma\to\bot)\to\bot)^{u}}{\tau=\sigma} \qquad \dfrac{\text{(REFL)}}{\bot=\bot}}{\tau\to\bot=\sigma\to\bot}\,\text{ARROW/FIX}}{\tau=\sigma\to\bot}\,\text{FOLD}_l \qquad \dfrac{\text{(REFL)}}{\bot=\bot}}{\tau\to\bot=(\sigma\to\bot)\to\bot}\,\text{ARROW/FIX},\ u}{\underbrace{\mu\alpha.\,(\alpha\to\bot)}_{\equiv\tau}=\underbrace{\mu\beta.\,((\beta\to\bot)\to\bot)}_{\equiv\sigma}}\,\text{FOLD}_{l/r}
$$

$$
\text{UNFOLD}_{l/r}\,\dfrac{\text{DECOMP}\,\dfrac{\text{UNFOLD}_l\,\dfrac{\text{DECOMP}\,\dfrac{\text{UNFOLD}_{l/r}\,\dfrac{\mu\alpha.\,(\alpha\to\bot)=\mu\beta.\,((\beta\to\bot)\to\bot)}{\tau\to\bot=(\sigma\to\bot)\to\bot}}{\tau=\sigma\to\bot}}{\tau\to\bot=\sigma\to\bot}}{\tau=\sigma}}{\tau\to\bot=(\sigma\to\bot)\to\bot}
$$

Questions investigated in my thesis

- What kind of proof-theoretic relationships do exist between $\mathbf{AC}^{=}$, $\mathbf{HB}^{=}$, and $\mathbf{AK}^{=}$?
  - How can a connection between $\mathbf{HB}^{=}$ and $\mathbf{AK}^{=}$ (as suggested by Example 4) be made *precise*?
  - Can "coinductive" proofs in $\mathbf{HB}^{=}$ be effectively transformed into "traditional" proofs in $\mathbf{AC}^{=}$? And . . . , *vice versa*?

- More generally concerning proof-transformations and *interpretational proof-theory*:
  - What is the relevance of the notions "derivability" and "admissibility" of rules for finding proof-transformations?
  - How to define rule "derivability" and "admissibility" in natural-deduction systems *properly*?

A duality between $\mathbf{HB}_{\mathbf{0}}^{=}$ and $\mathbf{AK}_{\mathbf{0}}^{=}$

Example 5. A duality between a derivation in $\mathbf{HB}_{\mathbf{0}}^{=}$ and a *consistency-unfolding* in $\mathbf{AK}_{\mathbf{0}}^{=}$:

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(\tau \to \perp = (\sigma \to \perp) \to \perp)^{\boldsymbol{u}}}{\tau = \sigma}\,\text{FOLD}_{l/r} \qquad \dfrac{}{\perp = \perp}\,\text{(REFL)}}{\tau \to \perp = \sigma \to \perp}\,\text{ARROW}}{\tau = \sigma \to \perp}\,\text{FOLD}_{l} \qquad \dfrac{}{\perp = \perp}\,\text{(REFL)}}{\tau \to \perp = (\sigma \to \perp) \to \perp}\,\text{ARROW/FIX}, \boldsymbol{u}}{\underbrace{\mu\alpha.\,(\alpha \to \perp)}_{\equiv \tau} = \underbrace{\mu\beta.\,((\beta \to \perp) \to \perp)}_{\equiv \sigma}}\,\text{FOLD}_{l/r}
$$

$$
\begin{array}{c}
\mu\alpha.\,(\alpha \to \perp) = \mu\beta.\,((\beta \to \perp) \to \perp) \\
\hline\hline
(\tau \to \perp = (\sigma \to \perp) \to \perp)^{\boldsymbol{u}}
\end{array}\;\text{UNFOLD}_{l/r}
$$

$$
\dfrac{(\tau \to \perp = (\sigma \to \perp) \to \perp)^{\boldsymbol{u}}}{\tau = \sigma \to \perp \qquad \perp = \perp}\;\text{DECOMP}
$$

$$
\dfrac{\tau = \sigma \to \perp}{\tau \to \perp = \sigma \to \perp}\;\text{UNFOLD}_{l}
$$

$$
\dfrac{\tau \to \perp = \sigma \to \perp}{\tau = \sigma \qquad \perp = \perp}\;\text{DECOMP}
$$

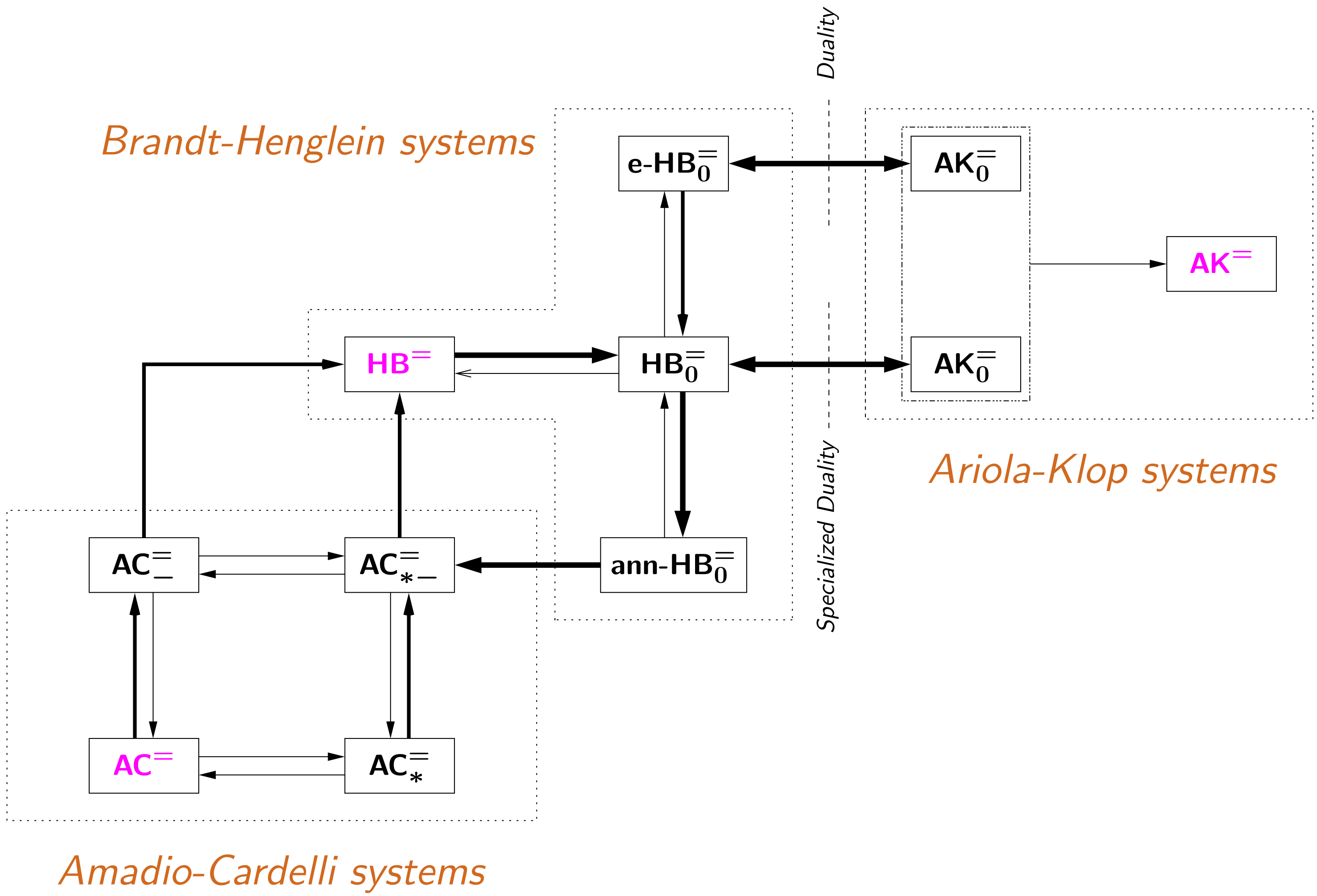
$$
\begin{array}{c}
\tau = \sigma \\
\hline\hline
(\tau \to \perp = (\sigma \to \perp) \to \perp)^{\boldsymbol{u}}
\end{array}\;\text{UNFOLD}_{l/r}
$$

Answers offered

- Introduction of "analytic" variant systems $\mathbf{HB}_0^=$ and $\mathbf{AK}_0^=$ of the systems $\mathbf{HB}^=$ and $\mathbf{AK}^=$.
- A "network" of proof-transformations is given:
  - A *duality* between derivations in $\mathbf{HB}_0^=$ and "consistency-unfoldings" in $\mathbf{AK}_0^=$ (is formally proved to exist).
  - A proof-transformation from $\mathbf{AC}^=$ to $\mathbf{HB}^=$.
  - A proof-transformation from $\mathbf{HB}^=$ via $\mathbf{HB}_0^=$ to $\mathbf{AC}^=$.

  (In the first step: *effective SYMM- and TRANS-elimination*.)
- A study of rule derivability and rule admissibility in (abstract versions of) pure Hilbert systems and of natural-deduction systems. Results that help clarify the relationship of these notions to the possibility of "rule elimination".

Found network of proof-transformations



Defense of my thesis

22nd of March 2005, 13:45

Aula of the Vrije Universiteit

De Boelelaan 1105, Amsterdam

Everybody is kindly welcome!

References

[AmCa93] Amadio, R.M., Cardelli, L.: "Subtyping Recursive Types", *ACM Transactions on Programming Languages and Systems* **15***:4* (1993) 575–631.

[ArKl95] Ariola, Z.H., Klop, J.W.: "Equational Term Graph Rewriting", *Fundamenta Informaticae* **26***:(3,4)* (1996) 207–240.

[BrHe98] Brandt, M., Henglein, F.: "Coinductive Axiomatization of Recursive Type Equality and Subtyping", *Fundamenta Informaticae* **33** (1998) 1–30.

[CG] Grabmayer, C.: "Relating Proof Systems for Recursive Types", `http://www.cs.vu.nl/~clemens/proefschrift.ps` .

[CG02] Grabmayer, C.: "A Duality in Proof Systems for Recursive Type Equality and Bisimulation Equivalence on Cyclic Term Graphs", Proceedings of the Workshop TERMGRAPH 2002, Barcelona, October 2002; and *VU Amsterdam Report* (2002), http://www.cs.vu.nl/~clemens/duality_report.ps.gz .

[CG03] Grabmayer, C.: "Derivability and Admissibility of Inference Rules in Abstract Hilbert systems", *VU Amsterdam Report* (2003), http://www.cs.vu.nl/~clemens/dairahs.ps .

[Gra04] Grabmayer, C.: "Derivability and Admissibility of Inference Rules in Abstract Hilbert Systems", *Collegium Logicum*, Kurt Gödel Society, Vienna (2004), http://www.cs.vu.nl/~clemens/collegiumlogicum.ps .