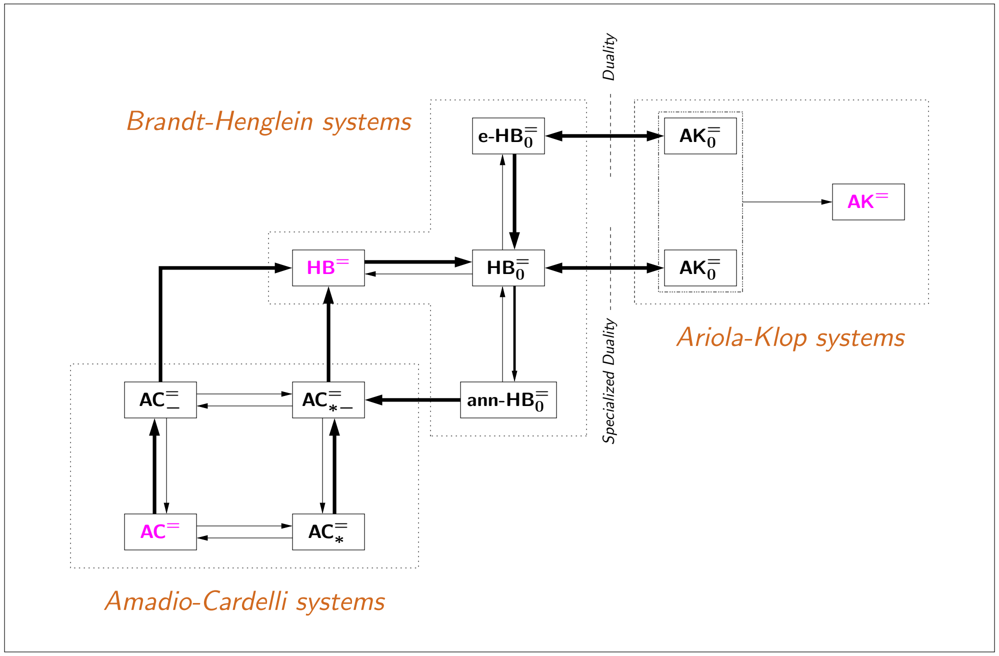
Relating Proof Systems for Recursive Types

Clemens Grabmayer



22^{nd} of March 2005

Types and Recursive Types

Types: "Collections of values sharing a common structure or shape."
[Amadio, Cardelli].

– *Basic types*: e.g. Int (integers), Real (reals), Bool (booleans).

– *Composite types*: e.g. $\mathsf{Int} \times \mathsf{Int}$ (pairs), $\mathsf{Real} \longrightarrow \mathsf{Int}$ (functions), $\mathsf{Bool} + \mathsf{Int}$ (elements of constituent types).

Types and Recursive Types

Types: "Collections of values sharing a common structure or shape."
[Amadio, Cardelli].

- *Basic types*: e.g. Int (integers), Real (reals), Bool (booleans).
- *Composite types*: e.g. Int $\times$ Int (pairs), Real $\longrightarrow$ Int (functions), Bool $+$ Int (elements of constituent types).

Recursive Types: types that satisfy recursive equations like e.g.:

$$\text{List} = \text{Unit} + (\text{Int} \times \text{List}) \qquad \text{(type of \textit{integer lists})} \tag{1}$$

(where Unit $= \{\underline{eol}\}$), because $() \triangleq \underline{eol}$, and e.g.

$$(5, 8, 13) \triangleq \langle 5, (8, 13) \rangle \in \text{Int} \times \text{List}$$

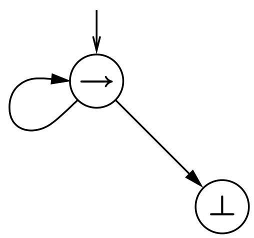
Notation for a solution of (1): $\text{List} = \mu\alpha.\,(\text{Unit} + (\text{Int} + \alpha))$.

Recursive Type Equality

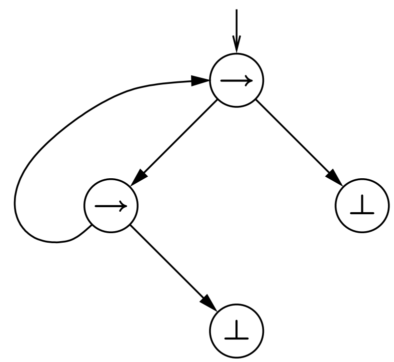
Example. The recursive types

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

can be visualized as the different cyclic term graphs

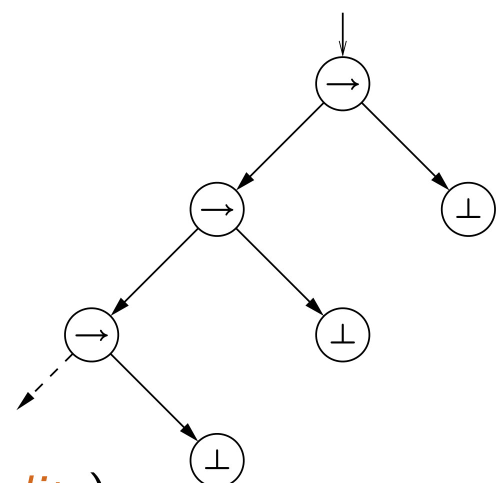


and



but possess the same *tree unfolding*

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



Such pairs of recursive types satisfy the same recursive equations and are called *strongly equivalent*. For τ and σ this is expressed as: $\tau =_\mu \sigma$ ($=_\mu$ is called *recursive type equality*).

Proof Systems for Recursive Type Equality

- Sound and complete axiomatisations of $=_\mu$:
  - $\mathbf{AC}^=$ by Amadio and Cardelli (1993) is *of "traditional form"* (similar systems in formal language theory, process algebra, . . .).
  - $\mathbf{HB}^=$ by Henglein and Brandt (1998) is *coinductively motivated*.

$$\begin{aligned} \tau =_\mu \sigma \quad &\Longleftrightarrow \quad \vdash_{\mathbf{AC}^=} \tau = \sigma \\ &\Longleftrightarrow \quad \vdash_{\mathbf{HB}^=} \tau = \sigma \; . \end{aligned}$$

- 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).

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

Specific Rules in AC$^=$, HB$^=$, and AK$^=$

- in **AC**$^=$: $$\frac{\sigma_1 = \tau[\sigma_1/\alpha] \qquad \sigma_2 = \tau[\sigma_2/\alpha]}{\sigma_1 = \sigma_2}\,\text{UFP} \quad (\text{if } \alpha \downarrow \tau)$$

- in **HB**$^=$: $$\frac{\begin{array}{c}[\tau_1 \to \tau_2 = \sigma_1 \to \sigma_2]^{u} \\ \mathcal{D}_1 \\ \tau_1 = \sigma_1\end{array} \qquad \begin{array}{c}[\tau_1 \to \tau_2 = \sigma_1 \to \sigma_2]^{u} \\ \mathcal{D}_2 \\ \tau_2 = \sigma_2\end{array}}{\tau_1 \to \tau_2 = \sigma_1 \to \sigma_2}\,\text{ARROW/FIX}, u$$

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

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

Questions investigated

- *Main Question*: What kind of proof-theoretic relationships do exist between the systems $\mathbf{AC}^{=}$, $\mathbf{HB}^{=}$, and $\mathbf{AK}^{=}$?
  - Can an observation of J.W. Klop about a seemingly close connection between $\mathbf{HB}^{=}$ and $\mathbf{AK}^{=}$ be made *precise*?
  - Can the "traditional" proofs in $\mathbf{AC}^{=}$ be transformed into the "coinductive" proofs in $\mathbf{HB}^{=}$?
  - And *vice versa*: Does there exist a transformation of proofs in $\mathbf{HB}^{=}$ into proofs in $\mathbf{AC}^{=}$?

- *Side-Issue*: What is the relevance of "derivability" and "admissibility" of inference rules for finding proof-transformations?

Answers offered

- Introduction of "analytic" variant systems $\mathbf{HB}_{\mathbf{0}}^{=}$ and $\mathbf{AK}_{\mathbf{0}}^{=}$ of the systems $\mathbf{HB}^{=}$ and $\mathbf{AK}^{=}$.
- A *network* of proof-transformations:
  - A *duality* via a reflection-effect between derivations in $\mathbf{HB}_{\mathbf{0}}^{=}$ and "consistency-unfoldings" in $\mathbf{AK}_{\mathbf{0}}^{=}$.

Answers offered

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

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

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

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:
  - A *duality* via a reflection-effect between derivations in $\mathbf{HB}_0^=$ and "consistency-unfoldings" in $\mathbf{AK}_0^=$.
  - A proof-transformation from $\mathbf{AC}^=$ to $\mathbf{HB}^=$.
  - A proof-transformation from $\mathbf{HB}^=$ via $\mathbf{HB}_0^=$ to $\mathbf{AC}^=$.
- A study of rule derivability and rule admissibility in abstract versions of pure Hilbert systems and of natural-deduction systems.
  – Results that help to clarify the relationship of these notions to the possibility of "rule elimination".

The found network of proof-transformations