A modular technique for termination proofs in abstract rewriting systems

David Chemouil

ONERA/DTIM Toulouse

2009-06-30, Séminaire Vérification de Toulouse

Motivation

Follow-up to Ralph Matthes' presentation of May 19, 2009.
Some aspects of Ralph's presentation:

- Extension of simply-typed λ-calculus with new reduction rules;
- Proof of termination (a.k.a strong normalisation) using a simulation technique;
- Introduction of "garbage" to fit the hypotheses of the technique.

Motivation

Follow-up to Ralph Matthes' presentation of May 19, 2009.
Some aspects of Ralph's presentation:

- Extension of simply-typed λ-calculus with new reduction rules;
- Proof of termination (a.k.a strong normalisation) using a simulation technique;
- Introduction of "garbage" to fit the hypotheses of the technique.

This presentation:

- My position: garbage is dirty :-)
- Introduction of a new abstract technique for termination proofs;
- Application to two λ-calculi.

Work during my PhD [Chemouil, 2004] and recently published in [Chemouil, 2008]. However, these results were never presented (in this shape) in a conference until now.

What is it all about?

- Rewriting systems
- Abstract termination proofs

A new modular technique

- Infinite reduction sequences
- The insertion lemma
- Insertability
- Prosimulation as a reduction
- An application to adjournment

Applications

- A simply-typed λ-calculus with inductive types
- Copies of inductive types
- Group symmetries

Conclusion

What is it all about?

Deciding equivalence

A general, common, setting:

- "Objects": terms, graphs, λ-terms...
- Identities $t = u$ between objects.

Identities induce an equivalence relation $\approx$ on objects.

However, given two arbitrary objects:
can we *decide* whether they are equivalent w.r.t the relation?

Rewriting

An approach:
convert the n identities into $m \geqslant n$ *reduction rules* $t \to u$, such that the equivalence closure of $\to$ yields precisely $\approx$.

Now, $\to$ converges if:

termination : every reduction sequence terminates;

confluence : any "fork" can be closed.

Proposition

$\to$ converges $\Rightarrow$ $\approx$ is decidable.

Abstract reduction systems

Definition

An abstract reduction system (ARS) is given by a set A of *objects* and a set $\{\rightarrow_R \mid R \in I\}$ of *binary relations* on A.

$\rightarrow_R$ is sometimes written R. Now some other notation:

$$
\begin{aligned}
\leftarrow_R &:= {\rightarrow_R}^{-1} \\
\rightarrow_R \rhd \rightarrow_S &:= \{(x,z) \mid \exists y \in A \cdot x \rightarrow_R y \wedge y \rightarrow_S z\} \\
\overset{0}{\rightarrow}_R &:= \{(x,x) \in A^2\} \\
\overset{n+1}{\rightarrow}_R &:= \overset{n}{\rightarrow}_R \rhd \rightarrow_R \\
\overset{*}{\rightarrow}_R &:= \bigcup_{n \geqslant 0} \overset{n}{\rightarrow}_R \\
\overset{+}{\rightarrow}_R &:= \bigcup_{n \geqslant 1} \overset{n}{\rightarrow}_R \\
\rightarrow_{RS} &:= \rightarrow_R \cup \rightarrow_S
\end{aligned}
$$

Relational and diagrammatic notations

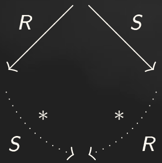
Proving properties of ARS will often lead to formulas of the shape:

$$\forall r \cdot r \to_R r' \wedge r \to_S r'' \Rightarrow \exists r''' \cdot r' \stackrel{*}{\to}_S r''' \wedge r'' \stackrel{*}{\to}_R r'''$$

Their relational representation is often more readable:

$$\leftarrow_R \rhd \to_S \subseteq \stackrel{*}{\to}_S \rhd \stackrel{*}{\leftarrow}_R$$

...as is the diagrammatic representation:



Termination

Definition
Given a binary relation $\to_R$ on A, the set SN of terminating objects is the smallest one such that $\forall r\ (\forall s \cdot r \to_R s \Rightarrow s \in \mathsf{SN}) \Rightarrow r \in \mathsf{SN}$.

This is *classically* equivalent to saying that, for any object in SN, there is no infinite reduction sequence starting from this object.

Definition
Let R be a reduction relation on a set A. Then R terminates, written $R \models \Downarrow$, if all objects in A are terminating under R.

Proving termination

Now, how to show termination of a rewriting system?

Proving termination

Now, how to show termination of a rewriting system?

- Be clever: semantic approaches (*e.g.* Tait-Girard);

Proving termination

Now, how to show termination of a rewriting system?

- Be clever: semantic approaches (*e.g.* Tait-Girard);
- Be masochistic: show that the reduction relation is a well-founded ordering by exhibiting a nice measure $A \to \mathbb{N}$;

Proving termination

Now, how to show termination of a rewriting system?

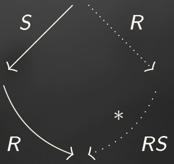
- Be clever: semantic approaches (*e.g.* Tait-Girard);
- Be masochistic: show that the reduction relation is a well-founded ordering by exhibiting a nice measure $A \to \mathbb{N}$;
- Be lazy: compose easily-proven results about subsystems using lemmas on ARS.

Adjournment

Lemma (Adjournment)
Let R and S be ARS s.t.:

- $R \models \Downarrow$
- $S \models \Downarrow$
- $S \rhd R \subseteq R \rhd (RS)^*$ (adjournment).

Then $RS \models \Downarrow$.



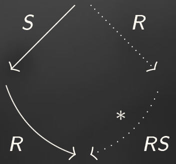
Proof.
Suppose $R \models \Downarrow$, $S \models \Downarrow$ and $S \rhd R \subseteq R \rhd (RS)^*$. Suppose RS doesn't terminate: then there is an infinite sequence of RS-reductions, alternating finite fragments of R- and S-reductions, as $R \models \Downarrow$ and $S \models \Downarrow$. Running along the sequence from the beginning, "lift" an R-reduction every time $S \rhd R$ is met, building a new infinite RS-sequence. Iterating this process, an infinite R-reduction subsequence is built. Contradiction. $\therefore$

Adjournment

Lemma (Adjournment)
Let R and S be ARS s.t.:

- $R \models \Downarrow$
- $S \models \Downarrow$
- $S \triangleright R \subseteq R \triangleright (RS)^*$ (adjournment).

Then $RS \models \Downarrow$.



Proof.
Suppose $R \models \Downarrow$, $S \models \Downarrow$ and $S \triangleright R \subseteq R \triangleright (RS)^*$. Suppose RS doesn't terminate: then there is an infinite sequence of RS-reductions, alternating finite fragments of R- and S-reductions, as $R \models \Downarrow$ and $S \models \Downarrow$. Running along the sequence from the beginning, "lift" an R-reduction every time $S \triangleright R$ is met, building a new infinite RS-sequence. Iterating this process, an infinite R-reduction subsequence is built. Contradiction. $\therefore$

Simulation

Definition

Let T and U be two ARS. An application $|-|$ from the carrier of T to that of U is:

- a weak simulation if $r \to_T s \Rightarrow |r| \xrightarrow{*}_U |s|$;
- a simulation if $r \to_T s \Rightarrow |r| \xrightarrow{+}_U |s|$.

Lemma

Let T and U be two ARS. If there is a simulation from T to U, then $U \models \Downarrow \quad \Rightarrow \quad T \models \Downarrow$.

Proof.

Suppose T doesn't terminate: then there is an infinite sequence of T-reductions. Simulating it yields an infinite sequence of U-reductions (as the simulation produces *at least one* U-reduction for any T-reduction). Contradiction. $\therefore$

Simulation

Definition

Let T and U be two ARS. An application $|{-}|$ from the carrier of T to that of U is:

- a weak simulation if $r \to_T s \Rightarrow |r| \xrightarrow{*}_U |s|$;
- a simulation if $r \to_T s \Rightarrow |r| \xrightarrow{+}_U |s|$.

Lemma

Let T and U be two ARS. If there is a simulation from T to U, then $U \models \Downarrow \quad \Rightarrow \quad T \models \Downarrow$.

Proof.

Suppose T doesn't terminate: then there is an infinite sequence of T-reductions. Simulating it yields an infinite sequence of U-reductions (as the simulation produces *at least one* U-reduction for any T-reduction). Contradiction.

∴

A new modular technique

Reductio ad absurdum

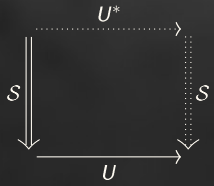
Quite a number of termination proofs on ARS rely on *reductio ad absurdum*. The general argument to show the termination of T, given the termination of U, is the following:

- Suppose T doesn't terminate, *i.e* there is an infinite sequence of T-reductions;
- Provide a constructive way to build an infinite sequence of U-reductions out of any sequence of T-reductions;
- Derive a contradiction.

Prosimulation

Definition

Let U be an ARS and $\mathcal{S}$ be a binary relation on the domain of U. Then $\mathcal{S}$ prosimulates U if $\mathcal{S} \rhd\!\!\to_U \subseteq \overset{*}{\to}_U\!\rhd \mathcal{S}$.



Insertion

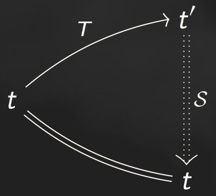
Definition

Let U, T be ARS, $\mathcal{S}$ a relation, u a finite sequence of U-reductions beginning with an object t and (t, t') a T-reduction, s.t.:

- $\mathcal{S}$ prosimulates U;
- and $(t', t) \in \mathcal{S}$.

Define an insertion operator $\Theta_{\mathcal{S}}^{t,t'}$ by recursion on u:

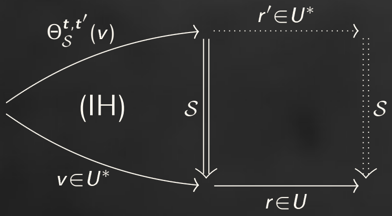
- If u is empty, insert the T-reduction: $\Theta_{\mathcal{S}}^{t,t'}(u) := (t, t') \in T$.
  As $(t', t) \in \mathcal{S}$, we have:



Insertion (cont.)

Definition (cont.)

- Otherwise, $u = v \triangleright r$ with $v \in U^*$ and $r \in U$. Then, we have $\Theta^{t,t'}_{\mathcal{S}}(u) := \Theta^{t,t'}_{\mathcal{S}}(v) \triangleright r'$ with:

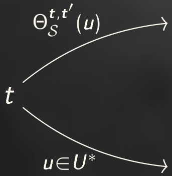


Remark: we only consider deterministic or finite and bounded cases, hence the case when there exist arbitrarily many r' such that $\Theta^{t,t'}_{\mathcal{S}}(u) := \Theta^{t,t'}_{\mathcal{S}}(v) \triangleright r'$ will not occur.

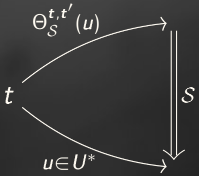
Remarks on this definition

The sequence $\Theta_{\mathcal{S}}^{t,t'}(u)$ begins with the T-reduction (t, t'), and ensures that:

(I1) the fork



can be closed by $\mathcal{S}$:



(I2) and $\Theta_{\mathcal{S}}^{t,t'}(u \triangleright r) = \Theta_{\mathcal{S}}^{t,t'}(u) \triangleright r'$ where $r' \in U^*$.

(I2) enables us to extend the operator to infinite reduction sequences: appending a new reduction step to an initial finite sequence keeps unchanged the reduction sequence corresponding to the initial fragment.

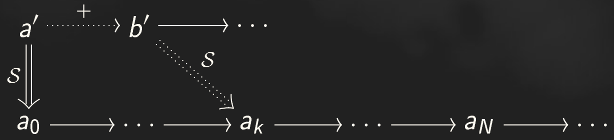
Echoing

Definition

Let $\to$ be an ARS and $\mathcal{S}$ a relation on objects. Then $\mathcal{S}$ echoes $\to$ if

$$\forall a_0 \cdot \forall a' \,\mathcal{S}\, a_0 \cdot \exists N \in \mathbb{N}^* \cdot \forall a_0 \to \cdots \to a_N \cdot$$
$$\exists k \in \{1, \ldots, N\} \cdot \exists b' \,\mathcal{S}\, a_k \cdot a' \xrightarrow{+} b'$$

That is, there is a bound $N > 0$ s.t. for every finite fragment of length N of any (possibly infinite) sequence of reductions beginning by a_0, there is an object a_k in this fragment (with $k \geqslant 1$) with an object b' s.t. $b' \,\mathcal{S}\, a_k$ which, itself, derives from a' in at least one step.



The insertion lemma

Lemma

Let U, T be ARS and $\mathcal{S}$ a relation s.t. $\mathcal{S}$ prosimulates and echoes U. Then, for any infinite sequence u of U-reductions, beginning by t, and every T-reduction (t, t') s.t. $(t', t) \in \mathcal{S}$, the sequence $\Theta_{\mathcal{S}}^{t,t'}(u)$ is also infinite.

Proof.

Let u be an infinite sequence of U-reductions beginning by an object t_0. As $\mathcal{S}$ prosimulates U, we can build $\Theta_{\mathcal{S}}^{t_0,t'}(u)$. This sequence cannot end as, because $\mathcal{S}$ echoes U, there necessarily exists a bound to the length of initial fragments of u for which there is at least a reduction step in $\Theta_{\mathcal{S}}^{t_0,t'}(u)$. This process of stepping along u and finding corresponding steps in $\Theta_{\mathcal{S}}^{t_0,t'}(u)$ can be iterated infinitely as u is not terminating. $\therefore$

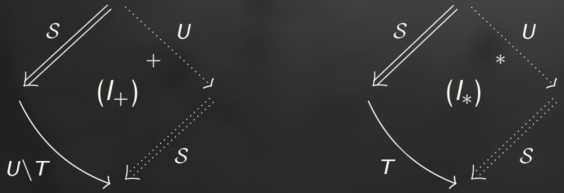
Introduction to insertability

Suppose we have $T \subsetneq U$. As we want the sequence $\Theta_{S}^{t,t'}(u)$ to be infinite provided the sequence u is, two cases are possible:

- In the case where a reduction in u comes from $U \setminus T$, it should be echoed by at least one U-reduction.
- On the other hand, if it is a T-reduction, there could even be no corresponding U-reduction because inserting a T-reduction at the very beginning of $\Theta_{S}^{t,t'}(u)$ implies that, perhaps, the T-reduction which stood in u is not needed anymore at the same time in $\Theta_{S}^{t,t'}(u)$.

Insertability

Then we should be able to "come back" to u through $\mathcal{S}$. It is thus necessary to ensure that the following diagrams can be closed:



Definition

Let U, T be ARS and $\mathcal{S}$ a binary relation on the domain of U. Then T can be inserted in U w.r.t. $\mathcal{S}$ if:

- $T \subsetneq U$;
- (I_+) $\quad \mathcal{S} \rhd \rightarrow_{U \backslash \rightarrow_T} \subseteq \stackrel{+}{\rightarrow}_U \rhd \mathcal{S}$;
- (I_*) $\quad \mathcal{S} \rhd \rightarrow_T \subseteq \stackrel{*}{\rightarrow}_U \rhd \mathcal{S}$.

Insertability and echoing

Lemma (Insertability)

Let U, T be ARS and $\mathcal{S}$ a binary relation on the domain of U s.t.:

- T is finitely branching ;
- T can be inserted in U w.r.t. $\mathcal{S}$;
- $T \models \Downarrow$.

Then $\mathcal{S}$ prosimulates and echoes U.

Proof.

First, T can be inserted in U w.r.t. $\mathcal{S}$, therefore $\mathcal{S}$ obviously prosimulates U. Furthermore, by König's Lemma, the fact that T is finitely branching and terminating implies it is always possible to find, for every initial term, the bound necessary to echoing. $\therefore$

What if the prosimulation is a reduction?

Now, $\mathcal{S}$ may itself be a reduction sequence from terms in $\Theta_{\mathcal{S}}^{t,t'}(u)$ to those in u.

As we insert a T-reduction at the beginning of the sequence, we must be able to come back to the initial sequence by "anti-reducing" the descendants of the subterm which was T-reduced initially.

As these descendants may enjoy several occurrences, we consider a relation T' such that $T^{-1} \subseteq T'$ and we take T'^{*} for $\mathcal{S}$.

Prosimulation as a reduction

Lemma

Let U, T and T' be ARS s.t.:

- $T \subsetneq U$;
- $T \models \Downarrow$;
- $T^{-1} \subseteq T'$;
- $T' \rhd (U \setminus T) \subseteq U^* \rhd (U \setminus T) \rhd U^* \rhd T'^*$;
- $T' \rhd T \subseteq U^* \rhd T'$.

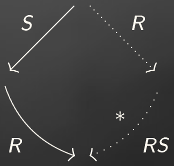
Then, for any infinite sequence u of U-reductions, beginning by t, and every T-reduction (t, t'), the sequence $\Theta^{t,t'}_{T'^*}(u)$ is also infinite.

Proof.

Long: see [Chemouil, 2008]. ∴

Conditional adjournment

Recall the adjournment diagram. A recurring problem is that the object a the root may not be in a completely satisfactory shape, while not being too far from it.



Definition (Conditional Adjournment)

Let R and S be ARS and P a predicate on objects. Then S is adjournable w.r.t. R under condition P if

$$\forall a \forall b \forall c \cdot P(a) \wedge a \rightarrow_S b \wedge b \rightarrow_R c \Rightarrow \exists d \cdot a \rightarrow_R d \xrightarrow{*}_{RS} c \quad .$$

Now, how to *realise* P?

Realisation

Definition (Realisation)

Let T be an ARS, P a predicate on objects and a and object.
Then T realises P for a if $\exists b \cdot a \xrightarrow{*}_T b \wedge P(b)$.
And T realises P if T realises P for any object a.

Pre-adjusted adjournment

Lemma (Pre-Adjusted Adjournment)

Let R, S, and T be ARS, $\mathcal{S}$ a relation and P a predicate s.t.:

- S is adjournable w.r.t. R under condition P;
- $T \subseteq R$;
- $R \models \Downarrow$;
- $S \models \Downarrow$;
- T realises P
- $\mathcal{S}$ prosimulates RS;
- $\mathcal{S}$ echoes RS.

Then $RS \models \Downarrow$.

Applications

Terms

$$\frac{(x,\rho) \in \Gamma}{\Gamma \vdash x : \rho}\ (V) \qquad \frac{}{\Gamma \vdash \star : 1}\ (1\text{-I})$$

$$\frac{\Gamma \vdash r : \rho \qquad \Gamma \vdash s : \sigma}{\Gamma \vdash \langle r, s\rangle^{\rho\times\sigma} : \rho \times \sigma}\ (\times\text{-I}) \qquad \frac{\Gamma \vdash r : \rho \times \sigma}{\Gamma \vdash (\mathsf{p_1}^{\rho\times\sigma} r) : \rho}\ (\times\text{-E}_1)$$

$$\frac{\Gamma \vdash r : \rho \times \sigma}{\Gamma \vdash (\mathsf{p_2}^{\rho\times\sigma} r) : \sigma}\ (\times\text{-E}_2)$$

$$\frac{\Gamma, x : \rho \vdash r : \sigma}{\Gamma \vdash (\lambda x^{\rho} r) : \rho \to \sigma}\ (\to\text{-I}) \qquad \frac{\Gamma \vdash r : \rho \to \sigma \qquad \Gamma \vdash s : \rho}{\Gamma \vdash (rs) : \sigma}\ (\to\text{-E})$$

$$\frac{(c, \overrightarrow{\rho} \to \alpha) \in \hat{\mu} \qquad \Gamma \vdash \overrightarrow{r} : \overrightarrow{\rho}[\alpha := \hat{\mu}]}{\Gamma \vdash (c\,\overrightarrow{r}) : \hat{\mu}}\ (\mu\text{-I}) \qquad \frac{\Gamma \vdash \overrightarrow{t} : \overrightarrow{\delta_c^{\hat{\mu},\sigma}}}{\Gamma \vdash (\!|\overrightarrow{t}|\!)^{\hat{\mu},\sigma} : \hat{\mu} \to \sigma}\ (\mu\text{-E})$$

β-reduction

Definition (β-reduction)

$$
\begin{array}{lll}
(\lambda x r)s & \to_{\beta_\to} & r[x := s] \\
\mathrm{p}_1\langle r, s\rangle & \to_{\beta_{\times_1}} & r \\
\mathrm{p}_2\langle r, s\rangle & \to_{\beta_{\times_2}} & s \\
(\!| \vec{t} |\!)\ (c_i\ \vec{r}) & \to_{\beta_\mu} & t_i\ \vec{r}\ \overrightarrow{\Delta_r} \qquad \text{where:}
\end{array}
$$

$$
\Delta_r := \begin{cases} (\!| \vec{t} |\!)\ r & \text{if the operator corresponding to } r \text{ is 0-recursive,} \\ (\!| \vec{t} |\!) \circ r & \text{if the operator corresponding to } r \text{ is 1-recursive,} \\ \varnothing & \text{otherwise.} \end{cases}
$$

Brouwer's ordinals

The strictly-positive approach for inductive types enables to define infinitely branching trees with finite depth.

A typical example is given by the representation $\mathbf{O}$ of Brouwer's ordinals (where $\mathbf{N}$ is the inductive type of natural numbers):

$$\mathbf{O} := \mu\alpha\,(0 : \alpha, S : \alpha \to \alpha, L : (\mathbf{N} \to \alpha) \to \alpha)$$

Here, α is an empty schema, $\alpha \to \alpha$ is 0-recursive and $(\mathbf{N} \to \alpha) \to \alpha$ is 1-recursive.

The rules for β_μ-reduction on Brouwer's ordinals are then:

$$\begin{array}{lll} (\!|t_0, t_S, t_L|\!)\ 0 & \to_{\beta_\mu} & t_0 \\ (\!|t_0, t_S, t_L|\!)\ (S\ \ p) & \to_{\beta_\mu} & t_S\ \ p\ ((\!|t_0, t_S, t_L|\!)\ \ p) \\ (\!|t_0, t_S, t_L|\!)\ (L\ \ k) & \to_{\beta_\mu} & t_L\ \ k\ ((\!|t_0, t_S, t_L|\!) \circ k) \end{array}$$

η-reduction

Definition (η-reduction)

$$r \quad \to_{\eta_\to} \quad \lambda x^\rho \cdot r x \qquad \text{if } \begin{cases} r : \rho \to \sigma, \\ x \notin \mathsf{FV}(r), \\ r \text{ is not an abstraction} \\ \qquad \text{nor in applicative position} \end{cases}$$

$$r \quad \to_{\eta_\times} \quad \langle \mathsf{p}_1\, r, \mathsf{p}_2\, r \rangle \quad \text{if } \begin{cases} r \text{ is of product type,} \\ r \text{ is not a pair nor projected.} \end{cases}$$

$$r \quad \to_{\eta_1} \quad \star \qquad \text{if } \begin{cases} r : 1, \\ r \neq \star. \end{cases}$$

Properties of $\beta\eta$

Theorem

$\beta\eta \models \Downarrow \wedge \beta\eta \models \diamond$.

Not so easy to prove because η is context-sensitive. This could be solved by orienting the reduction backwards but then new problems arise that don't "scale" well.

Type isomorphisms

Suppose we have an equivalence relation $\sim$ on terms,
an associative composition operator $\circ_{\rho,\sigma,\tau} : (\sigma \to \tau) \to (\rho \to \sigma)$
and a term $\mathrm{id}_\rho : \rho \to \rho$ which is a unit for $\circ$ (for all types ρ, σ, τ).

($\circ$ and id_ρ can be defined the obvious way, but not necessarily.)

Definition
Two types ρ and σ are isomorphic, written $\rho \cong \sigma$, if there exist two terms $f : \rho \to \sigma$ and $g : \sigma \to \rho$ s.t. $f \circ g \sim \mathrm{id}_\sigma$ and $g \circ f \sim \mathrm{id}_\rho$.

Notice that an isomorphism between types might be provable but not computable. This is the reason why it is necessary to devise a rewriting relation implementing $\sim$ and prove its convergence.

Note also that isomorphisms are of extensional nature, hence we can't do without η.

Faithful copies of inductive types

Definition

Let there be two types π and π' and two inductive types φ and φ' s.t. if π appears in φ, it is only as a parameter or as the full domain of the functional argument of a 1-recursive operator.

Let there also be a *computable* isomorphism $f : \pi \overset{\sim}{=} \pi' : f'$.

Then, φ' is a faithful copy of φ induced by f and f' if the first type only differs from the second one by constructor names and by the fact that zero or several occurrences of π in φ are replaced by π' in φ'.

Obviously, faithful copies form *provable* isomorphisms. We shall make them *computably* isomorphic by adding an adequate reduction (χ).

Realising faithful copies

Define $\mathsf{fc} : \mu\alpha\,(\overrightarrow{c} : \overrightarrow{\kappa}) \to \mu\alpha\,(\overrightarrow{c'} : \overrightarrow{\kappa'})$, $\mathsf{fc}' : \mu\alpha\,(\overrightarrow{c'} : \overrightarrow{\kappa'}) \to \mu\alpha\,(\overrightarrow{c} : \overrightarrow{\kappa})$ for terms obtained from two faithful copies and terms $f : \pi \stackrel{\sim}{=} \pi' : f$.

Example

Suppose we have $f : \mathbf{N} \stackrel{\sim}{=} \mathbf{P} : f'$ and:

$$\varphi := \mu\alpha\,(c_1{:}\alpha, c_2{:}((\mathbf{N}\to\mathbf{N})\to\alpha)\to\alpha, c_3{:}\mathbf{N}\to\alpha\to\alpha, c_4{:}(\mathbf{N}\to\alpha)\to\alpha)$$

$$\varphi' := \mu\alpha\,(c_1'{:}\alpha, c_2'{:}((\mathbf{N}\to\mathbf{N})\to\alpha)\to\alpha, c_3'{:}\mathbf{P}\to\alpha\to\alpha, c_4'{:}(\mathbf{P}\to\alpha)\to\alpha)$$

Then the general definition of fc gives:

$$\begin{aligned}
\mathsf{fc}\ c_1 &:= c_1' \\
\mathsf{fc}\ (c_2\ k) &:= c_2'\ k \\
\mathsf{fc}\ (c_3\ h\ t) &:= c_3'\ (f\ h)\ (\mathsf{fc}\ t) \\
\mathsf{fc}\ (c_4\ k) &:= c_4'\ (\mathsf{fc} \circ k \circ f')
\end{aligned}$$

Adding reduction rules

Definition (χ-reduction)

$$(\chi_1) \quad \mathsf{fc}' \; (\mathsf{fc} \; r) \to_\chi r$$
$$(\chi_2) \quad \mathsf{fc} \; (\mathsf{fc}' \; r) \to_\chi r$$

How to prove convergence of χ? Unfortunately, it does not seem possible to use a simulation or Akama-Di Cosmo's Lemma.

Given a term r, we call maximal abstracted form of r the term written $\lceil r \rceil$ s.t. $\lceil r \rceil$ begins by as many λ-abstractions as the arity of r.

Note $r \xrightarrow{*}_{\eta_\to} \lceil r \rceil$ but $\lceil r \rceil$ may differ from the $\eta_\to$-normal form of r because the strict subterms of $\lceil r \rceil$ may still contain $\eta_\to$-redices.

Problems with adjournment

Adjournment seems adequate to show the termination. Suppose we have a term $(\!|\overrightarrow{t}|\!)\ (\mathrm{fc}'\ (\mathrm{fc}\ (c_i\ \overrightarrow{r^p}\ \overrightarrow{r^0}\ \overrightarrow{r^1})))$ and following reductions:

$$\begin{aligned}(\!|\overrightarrow{t}|\!)\ (\mathrm{fc}'\ (\mathrm{fc}\ (c_i\ \overrightarrow{r^p}\ \overrightarrow{r^0}\ \overrightarrow{r^1}))) &\to_\chi (\!|\overrightarrow{t}|\!)\ (c_i\ \overrightarrow{r^p}\ \overrightarrow{r^0}\ \overrightarrow{r^1})\\ &\to_{\beta_\mu} t_i\ \overrightarrow{r^p}\ \overrightarrow{r^0}\ \overrightarrow{r^1}\ \overrightarrow{((\!|\overrightarrow{t}|\!)r^0)}\ \overrightarrow{((\!|\overrightarrow{t}|\!)\circ r^1)}\end{aligned}$$

Adjourning χ w.r.t. $\beta\eta$ means looking for a term s s.t.

$$(\!|\overrightarrow{t}|\!)\ (\mathrm{fc}'\ (\mathrm{fc}\ (c_i\ \overrightarrow{r^p}\ \overrightarrow{r^0}\ \overrightarrow{r^1}))) \to_{\beta\eta} s \overset{*}{\to}_{\beta\eta\chi} t_i\ \overrightarrow{r^p}\ \overrightarrow{r^0}\ \overrightarrow{r^1}\ \overrightarrow{((\!|\overrightarrow{t}|\!)r^0)}\ \overrightarrow{((\!|\overrightarrow{t}|\!)\circ r^1)}$$

Alas the sequence we end up with is rather of the following form:

$$\begin{aligned}(\!|\overrightarrow{t}|\!)\ (\mathrm{fc}'\ (\mathrm{fc}\ (c_i\ \overrightarrow{r^p}\ \overrightarrow{r^0}\ \overrightarrow{r^1}))) &\to_{\beta_\mu}\overset{*}{\to}_{\beta\eta} (\!|\overrightarrow{t}|\!)\ (c_i\ \overrightarrow{r^p}\ \overrightarrow{r^0}\ \overrightarrow{\lceil r^1\rceil})\\ &\overset{*}{\to}_{\beta\eta} t_i\ \overrightarrow{r^p}\ \overrightarrow{r^0}\ \overrightarrow{\lceil r^1\rceil}\ \overrightarrow{((\!|\overrightarrow{t}|\!)\ r^0)}\ \overrightarrow{((\!|\overrightarrow{t}|\!)\circ\lceil r^1\rceil)}\\ &\overset{*}{\to}_{\beta_\to} t_i\ \overrightarrow{r^p}\ \overrightarrow{r^0}\ \overrightarrow{\lceil r^1\rceil}\ \overrightarrow{((\!|\overrightarrow{t}|\!)\ r^0)}\ \overrightarrow{((\!|\overrightarrow{t}|\!)\circ r^1)}\end{aligned}$$

Towards a solution

Let us use the insertion operator in the case where the relation $\mathcal{S}$ is a reduction relation containing the inverse of $\eta_{\to}$:

Definition ($\overline{\eta}_{\to}$-reduction, η-contraction)

$$\lambda x^{\rho} \cdot rx \to_{\overline{\eta}_{\to}} r \quad \text{if } x \notin \mathsf{FV}(r),$$

Lemma

$\eta_{\to}$ can be inserted $\beta\eta\chi$ w.r.t. $\overline{\eta}_{\to}$.

Proof.

We obviously have $\eta_{\to} \subsetneq \beta\eta\chi$. We must show $\to_{\overline{\eta}_{\to}} \rhd \to_{\eta_{\to}} \subseteq \overset{*}{\to}_{\beta\eta\chi} \rhd \overset{*}{\to}_{\overline{\eta}_{\to}}$ and $\to_{\overline{\eta}_{\to}} \rhd \to_{\beta\eta_{\times,\mathbf{1}}\chi} \subseteq \overset{*}{\to}_{\beta\eta\chi} \rhd \to_{\beta\eta_{\times,\mathbf{1}}\chi} \rhd \overset{*}{\to}_{\beta\eta\chi} \rhd \overset{*}{\to}_{\overline{\eta}_{\to}}$.
Tedious diagrams chasings. $\therefore$

Termination of $\beta\eta\chi$

Lemma
$\beta\eta\chi \models \Downarrow$.

Proof.
Define a condition P on terms s.t. 1-recursive arguments be in maximal abstracted form. We have:

- $\eta_\rightarrow \subsetneq \beta\eta$, $\beta\eta \models \Downarrow$ and $\chi \models \Downarrow$;
- $\eta_\rightarrow$ realises P as 1-recursive arguments are not in applicative position;
- $\eta_\rightarrow$ can be inserted in $\beta\eta\chi$ w.r.t. $\overline{\eta}_\rightarrow$ and $\eta_\rightarrow \models \Downarrow$.
  Hence, $\overline{\eta}_\rightarrow$ prosimulates and echoes $\beta\eta\chi$.

As $\eta_\rightarrow^{-1} \subseteq \overline{\eta}_\rightarrow$, for any pair $(t, t') \in \eta_\rightarrow$, we have $(t', t) \in \overline{\eta}_\rightarrow$.
By pre-adjusted adjournment, we must prove χ can be adjourned w.r.t. $\beta\eta$ under condition P. Tedious diagram chasings. $\therefore$

Back to college

A permutation is a bijection from a finite set to itself. The carrier of a permutation on a set is made of those elements which aren't invariant.

The set of permutations on $[n]$, with composition as the product, is a group, called the symmetric group of order n and denoted σ_n.

A cycle on a set E is a permutation s s.t. there is $\{a_1, \ldots, a_n\} \subseteq E$ s.t.

$$\begin{array}{rcll} s(a_i) & = & a_{i+1} & \text{for } i < n; \\ s(a_n) & = & a_1 & \\ s(b) & = & b & \text{for } b \notin \{a_1, \ldots, a_n\}. \end{array}$$

σ-reduction

Every permutation $s \neq \mathrm{id}$ can be decomposed uniquely (up to the ordering of factors) in a product of disjoint cycles. The composition is commutative but it's possible to set up an ordering $<$, lexicographical for instance, on cycles in order to obtain a canonical decomposition.

Hence, every map $f : [n] \to [n]$ ($n \geqslant 2$) is equal to a product of m mutually disjoint cycles ($m \geqslant 2$) $f_1, \ldots, f_m$:

$$f = f_1 \circ \cdots \circ f_m \quad \text{(with } f_1 < \ldots < f_m\text{)}.$$

Definition (σ-reduction)

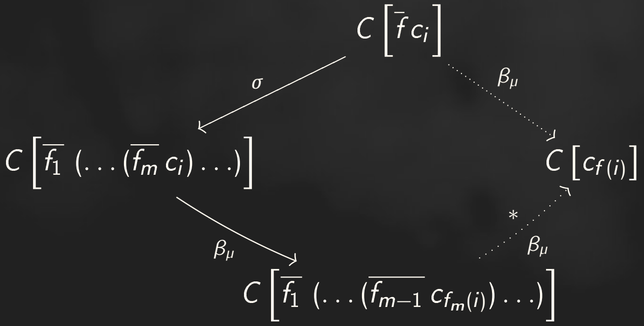
$$\overline{f}\, r \to_\sigma \overline{f_1}\ (\ldots(\overline{f_m}\, r)\ldots)$$

for every permutation $f \in \sigma_n$, for all $n \geqslant 2$, where f is decomposed into $m \geqslant 2$ mutually disjoint cycles $\{f_1, \ldots, f_m\} \subseteq \sigma_n$.

Proving termination: getting the idea

Let us call $\beta_{\overline{n}}$-reduction the fragment of β_μ applying to terms $\overline{f} : \overline{n} \to \overline{n}$; we then have: $\overline{f}\, c_i^{\overline{n}} \to_{\beta_{\overline{n}}} c_{f(i)}^{\overline{n}}$ for all $\overline{f} : \overline{n} \to \overline{n}$.

Then, to show termination of $\beta\eta\sigma$-reduction, there is a difficulty: if we try to adjourn σ w.r.t. $\beta\eta$, we get the following diagram for β_μ-reduction:



Proving termination: getting the idea (cont.)

This suggests to use pre-adjusted adjournment using as a condition the fact that terms must be in $\beta_{\overline{n}}$-normal form, *i.e* the lemma must be used in full generality (*i.e* not w.r.t. a reduction).

Notice that it would be hard to consider a deterministic reduction relation $\beta'_{\overline{n}}$ containing the inverse of $\beta_{\overline{n}}$. Indeed, the inverse image of a constructor c_i by the relation $\beta_{\overline{n}}$ is generally of cardinality strictly greater than 1. Intuitively, $\beta_{\overline{n}}$ is not injective.

Nevertheless, after a first observation of the situation, we can see that the inverse image by $\beta_{\overline{n}}$ is finite and that $\beta_{\overline{n}}$-redices are closed terms: therefore, it remains possible to build systematically $\mathcal{S}$ by choosing a term $\overline{g}$ s.t. $\overline{g}\, c_i \rightarrow_{\beta_{\overline{n}}} c_{f(i)}$.

This term shall only collapse, be duplicated or be reduced (even after the decomposition of $\overline{g}$ itself) to $c_{f(i)}$.

Defining the prosimulation

Definition

Let f be a permutation in σ_n. Define a binary relation $\mathcal{S}_f$ on terms this way: given two terms a and a', tag (with different numbers) every subterm of a' of the form $c_{f(i)}$, for all i, and denote by $L_{a'}$ the list of these labelled constructors.

Then $a' \mathcal{S}_f a$ if there exists a substitution ζ, mapping a labelled constructor to a term, s.t.:

- $a'\zeta = a$;
- and $\forall c^{\ell}_{f(i)} \in L_{a'}$, one has $c^{\ell}_{f(i)}\zeta \xrightarrow{*}_{\beta_{\overline{n}}} c_{f(i)}$ (where ℓ is a label).

Notice that it is not enough to show that $\beta_{\overline{n}}$-reduction can be inserted in $\beta\eta\sigma$ w.r.t. $\mathcal{S}_f$! Indeed, a $\beta_{\overline{n}}$-redex happens to be also a σ-redex. Write $\sigma \sqcap \beta_{\overline{n}}$ for the set of σ-reductions whose left-hand sides are $\beta_{\overline{n}}$-redices, that is of the form $\bar{f}\ c_i$ (obviously $\sigma \sqcap \beta_{\overline{n}} \subseteq \sigma$).

Echoing

Lemma
$\mathcal{S}_f$ echoes $\beta\eta\sigma$.

Proof.
We must show that

$$\forall a_0 \cdot \forall a' \;\mathcal{S}_f\; a_0 \cdot \exists N \in \mathbb{N}^* \cdot \forall a_0 \to_{\beta\eta\sigma} \cdots \to_{\beta\eta\sigma} a_N \cdot$$
$$\exists k \in \{1, \dots, N\} \cdot \exists b' \;\mathcal{S}_f\; a_k \cdot a' \xrightarrow{+}_{\beta\eta\sigma} b'$$

Let a_0 and a' be s.t. $a' \;\mathcal{S}_f\; a_0$, *i.e* there is a substitution ζ s.t. $a'\zeta = a_0$ and, for all $c^\ell_{f(i)} \in L_{a'}$, we have $c^\ell_{f(i)}\zeta \xrightarrow{*}_{\beta_{\overline{n}}} c_{f(i)}$.

Now, consider all possible reduction sequences beginning by a_0 and taken from $\beta_{\overline{n}} \cup (\sigma \sqcap \beta_{\overline{n}})$. As this latter relation terminates (easily shown), there exists a bound — write it N_0 — to the length of these sequences. Define $N := N_0 + 1$.

Echoing (cont.)

Proof (cont.).

Take an arbitrary sequence $a_0 \to_{\beta\eta\sigma} \cdots \to_{\beta\eta\sigma} a_N$ of length N. We must find a $k \in \{1, \ldots, N\}$ s.t. there is a b' s.t. $b' \mathcal{S}_f a_1$ and $a' \xrightarrow{+}_{\beta\eta\sigma} b'$.

- Either $a_0 \to_{\beta\eta\sigma \setminus \beta_{\boldsymbol{n}}} a_1$: then it is enough to put $k = 1$ and to apply the same reduction on a' thus obtaining b' s.t. $b' \mathcal{S}_f a_1$. Notice that the value of N is not important when such a reduction is applied to a_0. This comes from the fact that subterms of a_0 in the image of ζ are $\beta_{\overline{n}}$-redices and therefore, here, can only collapse or be duplicated (in the general case, they may also enjoy a $\beta_{\overline{n}}$-reduction). The echoing is therefore obviously determined.
- Or $a_0 \to_{\beta_{\boldsymbol{n}} \cup (\sigma \sqcap \beta_{\boldsymbol{n}})} a_1$. In that case, we can glance through the sequence $a_0 \to_{\beta_{\overline{n}} \cup (\sigma \sqcap \beta_{\overline{n}})} \cdots \to_{\beta\eta\sigma} a_N$ until reaching the first occurrence of a reduction different from $\beta_{\overline{n}}$ and $\sigma \sqcap \beta_{\overline{n}}$. It necessarily exists as $N > N_0$: its ordering number is the sought k and it is enough to echo it the same way than in the previous case.

$\therefore$

Termination

Lemma
$\beta\eta\sigma \models \Downarrow$.

Proof.
Define a condition P on terms s.t. these are in $\beta_{\overline{n}}$-normal form. We have:

- $\beta_{\overline{n}}\sigma \subsetneq \beta\eta$;
- $\beta\eta \models \Downarrow$;
- $\sigma \models \Downarrow$ (easy);
- $\beta_{\overline{n}}\sigma$ obviously realises P (in fact, $\beta_{\overline{n}}$ is enough) ;
- $\mathcal{S}_f$ prosimulates (easy) and echoes $\beta\eta\sigma$.

By the pre-adjusted adjournment, we just need to show that σ is adjournable w.r.t. $\beta\eta$ under condition P. Tedious diagram chasings. $\therefore$

Conclusion

So?

You may not believe me, but the proposed technique is:

- not so hard to understand;
- general enough to be applied in a number of complex cases;
- quite abstract.

Still, there's room for improvement:

- a more general and synthetic presentation [Lengrand, 2006];
- extending lemmas other than the adjournment one.

Finally, could it be of some use for Ralph's work?

References

- Chemouil, D. (2004).
  Types inductifs, isomorphismes et récriture extensionnelle.
  Thèse de doctorat, Université Paul Sabatier, Toulouse, France.
- Chemouil, D. (2008).
  An insertion operator preserving infinite reduction sequences.
  Mathematical Structures in Computer Science, 18(Special Issue 04):693–728.
- Lengrand, S. (2006).
  Normalisation & Equivalence en Théorie de la Démonstration & Théorie des Types.
  PhD thesis, Université Denis Diderot - Paris VII; University of St Andrews.