Alexandre DIKOVSKY
Université de Nantes

Lambda-calcul et Systèmes de Réécriture

Cours 5. Systèmes de réécriture (SRT)

Les SRT sont les systèmes finis des égalités orientées, c'est-à-dire, des règles $s \to t$, où s, t sont des termes. L'idée des SRT est de calculer $u =_E v$ en utilisant $\twoheadrightarrow_E$ au lieu de $\overset{*}{\leftrightarrow}_E$.

Définition 1. *Un système de règles $R = \{s_i \to t_i \mid i \in I \ fini\}$ est un SRT, si*
(*i*) $Var(t_i) \subseteq Var(s_i)$ *et*
(*ii*) $s_i \notin Var(R)$ *pour tout* $i \in I$.
$\to_R$ *est la relation correspondante fermée par congruences et contextes dite* **relation de réécriture**.

Un terme t est **en forme R-normale** *(FN_R), si $t \to_R u$ pour aucun terme u. R est* **convergent**, *si $\to_R$ est terminale et CR.*

Remarque : Si (i) ou (ii) est faux, alors il n'y a pas de FN_R.

Comme il a été remarqué, les TE terminales et confluentes sont décidables.

Proposition 1. *Si R est convergent, alors le problème "$s \overset{*}{\leftrightarrow}_R t$" est décidable.*

Il reste de trouver des conditions suffisantes de convergence des SRT utilisables dans la pratique.

1 Sémantique opérationnelle des SRT

Etant donné un SRT R, il induit uniquemment la relation de réécriture $\to_R$ sur $T_\Sigma[X]$. Le quasi-ordre [1] $\twoheadrightarrow_R$ est la relation suivante de R-**réducibilité** (ou de R-**dérivabilité**). Une règle $\rho = (l \to r) \in R$ réduit s à t (noté : $s \overset{\rho}{\to}_R t$) veut dire : il existe une occurrence $p \in O(s)$ telle que

$$s/p = \sigma(l), \quad t = s[p \to \sigma(r)]$$

pour une substitution σ. S/p est un R-**rédex**

$$(t_1 \overset{\rho_1}{\to}_R t_2 \overset{\rho_2}{\to}_R \ldots \overset{\rho_n}{\to}_R t_n) \ \ ou \ \ (t_1 \to_R t_2 \to_R \ldots \to_R t_n)$$

est une R-**réduction** (ou une R-**dérivation**) de t_1 à t_n : $t_1 \twoheadrightarrow_R t_n$.

Exemple 1. *Soit le SRT suivant PA (alternateur des piles) :*

$$PA \quad \begin{cases} top(push(x,y)) \to x \\ pop(push(x,y)) \to y \\ alternate(\epsilon, z) \to z \\ alternate(push(x,y), z) \to push(x, alternate(z,y)) \end{cases}$$

[1] Une relation binaire réflexive et transitive.

"push/2" : constructeur de piles : $\epsilon, push(s_1,\epsilon), push(s_1, push(s_2,\epsilon))$, etc...

$alternate(push(s_1, push(s_2,\epsilon)), push(u_1,\epsilon)) \xrightarrow{4}_{PA}$
$push(s_1, alternate(push(u_1,\epsilon), push(s_2,\epsilon))) \xrightarrow{4}_{PA}$
$push(s_1, push(u_1, alternate(push(s_2,\epsilon),\epsilon))) \xrightarrow{4}_{PA}$
$push(s_1, push(u_1, push(s_2, alternate(\epsilon,\epsilon)))) \xrightarrow{3}_{PA}$
$push(s_1, push(u_1, push(s_2,\epsilon)))$: PA-irréductible

Définition 2. *Un SRT R est* **(faiblement) confluent** *si $\rightarrow_R$ l'est. R est* **terminal** *si $\rightarrow_R$ l'est. R est* **convergent** *s'il est confluent et terminal. R est* **fermé** *si toutes ses règles le sont. Une égalité $s \approx t$ est* **prouvable** *dans R (noté : $s \approx_R t$) s'il existent les dérivations $s \twoheadrightarrow_R v \twoheadleftarrow_R t$ pour un terme v (pas forcement irréductible).*

Exemple 2. *Montrons que*

$$alternate(push(top(push(0,z)),z),\epsilon) \approx_{PA} alternate(push(0, pop(push(y,z))),\epsilon)$$

est vrai dans le SRT PA :

$alternate(push(top(push(0,z)),z),\epsilon) \xrightarrow{1}_{PA}$
$alternate(push(0,z),\epsilon) \xrightarrow{4}_{PA}$
$push(0, alternate(\epsilon,z)) \equiv v_0$
$alternate(push(0, pop(push(y,z))),\epsilon) \xrightarrow{4}_{PA}$
$push(0, alternate(\epsilon, pop(push(y,z)))) \xrightarrow{2}_{PA}$
$push(0, alternate(\epsilon,z)) = v_0$.

Questions : v_0 : est-il PA-irréductible ?
$alternate(top(\epsilon),\epsilon)$: est-il PA-irréductible ?

2 Problèmes de décision

Soit un SRT R sur Σ, X.

Notation : $s \overset{!}{\twoheadrightarrow}_R t =_{df} (s \twoheadrightarrow_R t \wedge t \textit{ irréductible})$. R peut formaliser une théorie équationnelle E dans le sens suivant :

Définition 3. *R est* **correct** *par rapport à E si $\rightarrow_R \subseteq \overset{*}{\leftrightarrow}_E$*
R est **adéquat** *pour E si $\overset{*}{\leftrightarrow}_E \subseteq \overset{*}{\leftrightarrow}_R$ (on dit aussi* **complet***).*

Exemple 3. *Le SRT PA est correct et adéquat par rapport à la théorie*

$$EPA \quad \begin{cases} top(push(x,y)) \approx x \\ pop(push(x,y)) \approx y \\ alternate(\epsilon,z) \approx z \\ alternate(push(x,y),z) \approx push(x, alternate(z,y)) \end{cases}$$

Définition 4. *R décide E veut dire que*

$$s \approx_E t \quad ssi \quad s \approx_R t \qquad (\Delta)$$

et le problème $s \twoheadrightarrow_R t$ est décidable.

Un exemple important où R décide E :

Proposition 2. *Si R est :*

(1) fini,

(2) convergent,

(3) correct et adéquat par rapport à E,

alors R décide E.

Preuve. Effectivement :

(i) En présence de p.(2), (3) $\equiv$ (Δ).

(ii) la confluence (CR) implique

$$\overset{*}{\leftrightarrow}_R = \twoheadrightarrow_R \circ \twoheadleftarrow_R,$$

et la terminaison implique :

$$\twoheadrightarrow_R \circ \twoheadleftarrow_R = \overset{!}{\twoheadrightarrow}_R \circ \overset{!}{\twoheadleftarrow}_R .$$

En plus,

(iii) la finitude implique la décidabilité de $\overset{!}{\twoheadrightarrow}_R$.

Ainsi tout SRT R fini, convergent, correct et adéquat par rapport à une TE E décide cette théorie.

Pour cette raison, les problèmes de terminaison et de confluence sont deux problèmes centraux de la théorie des SRT.

Théorème 1. *(i) Les problèmes de terminaison et de confluence sont non-décidable dans le cas général.*

(ii) Il existent des théories équationnelles décidables qui ne sont pas décidées par un SRT.

Exemple 4. *Aucune TE-décidable avec l'axiome de commutativité $xy = yx$ (comme dans les groupes abéliens) n'est décidé par SRI. La raison est que $xy \rightarrow yx$ contredit à la terminaison, parce que aucun terme n'est FN_R.*

Exercice. Montrez que le SRT

$$FG \ : \ \begin{cases} f(a,b,x) \rightarrow f(x,b,x) \\ g(x,y) \rightarrow x \\ g(x,y) \rightarrow y \end{cases}$$

n'est pas terminal.

3 Conditions suffisantes de terminaison

Soit $\overset{+}{\rightarrow}_R$ la fermeture transitive de $\rightarrow_R$. Si on trouve un ordre $\prec$ sur $T_\Sigma[X]$ qui est **bien fondé** (c'est-à-dire n'a pas de chaîne infinie décroissante) et qui contient $\overset{+}{\rightarrow}_R$, alors R est terminal.

Définition 5. *Une relation de réécriture $\rightarrow_R$ est un* **ordre de réécriture***, si elle est transitive et irreflexive.*

Ainsi, $\overset{+}{\rightarrow}_R$ est un ordre de réécriture pour tout SRT R. Un ordre de réécriture est un **ordre de réduction**, s'il est bien fondé.

3.1 Images homomorphes

Manna et Ness ont proposé une méthode de preuve de terminaison de SRT en trouvant un homomorphisme $\Theta : T_\Sigma \to \mathcal{A}_\prec$ dans une structure $\mathcal{A}$ ordonnée par un ordre bien fondé $\prec$ tel que :

(1) $\to_R \subseteq \prec_\Theta$, où $\prec_\Theta$ est l'ordre suivant sur T_Σ : $s \prec_\Theta t =_{df} \Theta(s) \prec \Theta(t)$

(2) $\prec_\Theta$ est fermé par substitutions et par contextes :
$s \prec_\Theta t$ implique $\sigma(s) \prec_\Theta \sigma(t)$ pour toute substitution fermée
$s \prec_\Theta t$ implique $C[s] \prec_\Theta C[t]$ pour tout contexte $C[\,]$.

Proposition 3. *Si un tel homomorphisme Θ et une telle structure $\mathcal{A}_\prec$ existent, alors R est terminal.*

Exemple 5. *Soit le SRT*

$$Bool \ : \ \begin{cases} not(not(x)) \to x \\ not(or(x,y)) \to and(not(x), not(y)) \\ not(and(x,y)) \to or(not(x), not(y)) \\ and(x, or(y,z) \to or(and(x,y), and(x,z)) \\ and(or(y,z), x) \to or(and(y,x), and(z,x)) \end{cases}$$

Définissons $\Theta : T_{Bool} \to \mathcal{A}_< = \{2, 3, ...; <\}$ comme ça (l'ordre $<$ sur les nombres naturels est bien fondé) :

$or_\Theta(a,b) = a + b + 1$	$and_\Theta(a,b) = a * b$
$not_\Theta(a) = 2^a$	$\Theta(c) = 2$

pour tous $a, b \in \{2, 3, ...\}$ et toute constante $c \in \Sigma_{Bool}$. Alors Θ vérifie les conditions (1)-(2). Par exemple,

$$\Theta(not(or(x,y))) = 2^{x+y+1} > \Theta(and(not(x), not(y))) = 2^x * 2^y = 2^{x+y}.$$

3.2 Ordres de simplification

L'idée sous-jacente l'utilisation des ordres pour prouver la terminaison des SRT sur une signature Σ finie est que si un ordre de réécriture $\to_R$ contenant la relation $s \trianglerighteq t$ ($\equiv t$ est un sous-terme de s) est bien fondé, alors R est terminal.
Ce genre de raisonement est basé sur un théorème de Kruskal concernant les bons ordres.

Définition 6. *Un quasi-ordre (donc réflexif) $\preceq$ est* bon *si pour toute chaîne $t_1, t_2, ..., t_i, ...$ infinie, il existe une paire de positions $i < j$ telle que*

$$t_i \preceq t_j.$$

Exercice : Prouvez que tout bon ordre est bien fondé. En fait, on peut prouver :

Proposition 4. *Un ordre bien fondé $\prec$ sur T est bon ssi tout sous-ensemble $T_0 \subseteq T$ des éléments deux-à-deux $\prec$ non-comparable est fini.*

Proposition 5. *Une restriction $\prec_1$ d'un bon ordre $\prec$ est bien fondée si $\prec_1$ elle-même est un quasi-ordre.*

Kruskal a introduit le schéma suivant de définition des ordres bien fondés des termes à partir des ordres sur la signature Σ :

Soit un bon ordre $\preceq$ sur Σ (remarquez que si Σ est finie, alors chaque quasi-ordre sur Σ est bon). On considère le SRT eventuellement infini suivant :

$$R_{\prec} \ : \ \begin{cases} f(s_1, ..., s_n) \rightarrow s_i & (1 \leq i \leq n) \\ f(s_1, ..., s_n) \rightarrow g(s_{i_1}, ..., s_{i_k}), & \end{cases}$$

pour $f \succeq g$ dans Σ, pour tous termes fermés sur Σ et $1 \leq i_1 < ... < i_k \leq n$, $k \leq n$.
Si on ferme $\rightarrow_{R_\prec}$ par Σ-contextes et par substitutions, alors on obtient un ordre de réécriture $\succeq_{emb}$ sur $T_\Sigma[X]$.

Théorème 2. $[Kruskal]$ *Si $\succeq$ est un bon ordre sur Σ, alors $\succeq_{emb}$ est un bon ordre sur $T_\Sigma[X]$.*

Corollaire 1. *Si $\succeq$ est un bon ordre sur Σ, $\succeq_{emb}$ est un ordre de réduction.*

Remarque : Dans le cas particulier où $\preceq$ sur Σ est vide, $R_{\preceq}$ consiste des règles

$$f(s_1, ..., s_n) \rightarrow s_i \qquad (1 \leq i \leq n).$$

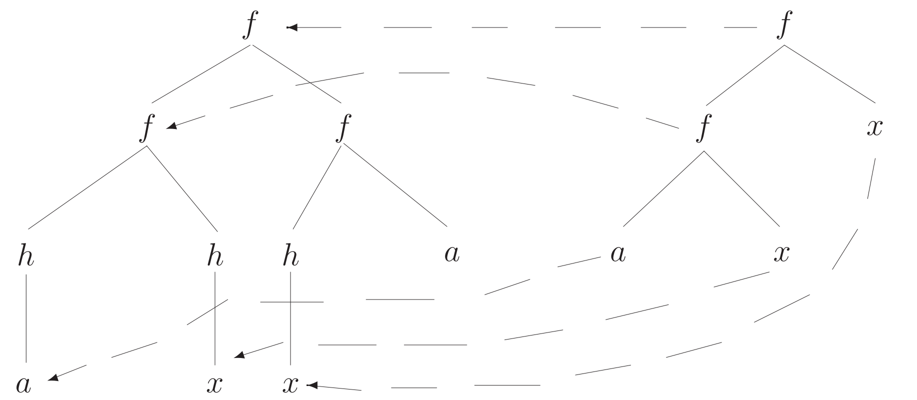
En les fermant par Σ -contextes et substitutions on obtient l'ordre de réécriture $\succeq_{emb}$ minimal, contenant les règles

$$f(x_1, ..., x_n) \rightarrow x_i \qquad (1 \leq i \leq n).$$

où x_i sont variables. Cet ordre minimal s'appelle **plongement homomorphique**.

Exemple 6. $s \equiv f(f(h(a), h(x)),\ f(h(x), a)) \trianglerighteq f(f(a, x), x) \equiv t$

$s \equiv$



$\equiv t$

Selon le théorème de Kruskal, cet ordre est bon.

Définition 7. *Soit l'ordre $t \triangleright s =_{df} \exists(p \in O(t))\ (s = t/p)$. Alors un ordre de réécriture $\succ$ est un* **ordre de simplification** *si $\triangleright \subseteq \succ$: $s = t/p$ implique $t \succ s$.*

Corollaire 2 (Kruskal). *Chaque ordre de simplification est un ordre de réduction.*

Ce corollaire est la source de nombre des conditions suffisantes de terminaison.

Définition 8. Ordres lexicographiques. *Soit un bon ordre $<$ sur Σ finie. Alors l'ordre suivant $<_{lex}$ sur $T_\Sigma[X]$ est* **lexicographique :**

$$(LEX)\ \begin{cases} (l1) & s >_{lex} x, \quad x \in Var, \ x \not\equiv s \ (donc\ s \notin Var) \\ (l2) & f(s_1, ..., s_m) >_{lex} g(t_1, ..., t_n), \quad si \\ & \quad (l2a) \ \ s_i \geq_{lex} g(t_1, ..., t_n) \quad \textbf{pour un } i, \ \ 1 \leq i \leq m, \\ & \quad \textbf{ou} \\ & \quad (l2b) \ \ f > g \ \ dans \ \ \Sigma \ \ et \ \ f(s_1, ..., s_m) >_{lex} t_j \quad \textbf{pour tous } j, \ \ 1 \leq j \leq n, \\ & \quad \textbf{ou} \\ & \quad (l2c) \ \ f \equiv g \ \ et \ \ f(s_1, ..., s_m) >_{lex} t_j \quad \textbf{pour tous } j, \quad 1 \leq j \leq n, \quad \textbf{et} \\ & \qquad\qquad s_1 \equiv t_1, ..., s_{k-1} \equiv t_{k-1} \ \ \textbf{et} \ \ s_k >_{lex} t_k \ \textbf{pour un } k, \ k \geq 1. \end{cases}$$

Théorème 3. *Tout ordre lexicographique de réécriture $>_{lex}$ défini à partir d'un bon ordre $<$ sur Σ finie est un ordre de simplification.*

Corollaire 3. *Soit un SRT R. Si on trouve un bon ordre $<$ sur Σ tel que $l >_{lex} r$ pour toute règle $l \to r \in R$, alors R est terminal.*

Exemple 7. *Le SRT $i(f(x, y)) \to f(i(y), i(x))$ est terminal. Soit $i > f$. Alors :*

$$\dfrac{i(f(x,y)) >_{lex} f(i(y), i(x)) \qquad (l2b)}{i > f \quad et \quad \dfrac{i(f(x,y)) >_{lex} i(y) \qquad (l2c)}{i \equiv i, \quad f(x,y) >_{lex} y \qquad (l1)} \qquad et \quad \dfrac{i(f(x,y)) > i(x) \qquad (l2c)}{i \equiv i, \quad f(x,y) >_{lex} x \qquad (l1)}}$$

Excercice : Prouvez que le SRT $f(f(x, y), z) \to f(x, f(y, z))$ est terminal.
Excercice : Prouvez que le SRT

$$Ackerman \ : \ \begin{cases} a(0, y) \to s(y) \\ a(s(x), 0) \to a(x, s(0)) \\ a(s(x), s(y)) \to a(x, a(s(x), y)) \end{cases}$$

est terminal.

Proposition 6. *Un bon ordre $<$ sur Σ étant donné, le problème $t >_{lex} s$ est décidable en temps polynomial.*

Définition 9. *Un* **multi-ensemble** *E est une fonction $f_E \ : \ E \to \mathcal{Z}^+$ ($f_E(e)$ étant le nombre des occurrences de e dans E). $e \in E$ veut dire $f_E(e) > 0$. $E_1 \cup E_2$ est défini par $f_{E_1 \cup E_2}(e) = f_{E_1}(e) + f_{E_2}(e)$, $E_1 - E_2$ par $f_{E_1 - E_2}(e) = f_{E_1}(e) \dot{-} f_{E_2}(e)$ (soustraction bornée), $f_{E_1 \cap E_2} = (E_1 \cup E_2) - ((E_1 - E_2) \cup (E_2 - E_1))$, $E_1 \subseteq E_2 =_{df} \forall e (f_{E_1}(e) \leq f_{E_2}(e))$.*

Exemple 8. $\emptyset \subseteq \{\{a\}\} \subseteq \{\{a, a\}\} \subseteq \{\{a, a, b\}\}$. $\{\{a, b, b, b\}\} - \{\{a, a, b, c\}\} = \{\{b, b\}\}$.

Soit $\mathcal{M}$ un ensemble d'objets avec un ordre $>$. Soient deux multi-ensembles $\mathcal{M}_1, \mathcal{M}_2$ avec les éléments dans $\mathcal{M}$ (multi-ensembles sur $\mathcal{M}$). $\mathcal{M}_2 \prec^1 \mathcal{M}_1$, si $\mathcal{M}_2 = (\mathcal{M}_1 - \{\{e\}\}) \cup \mathcal{Z}$ pour un $e \in \mathcal{M}_1$ et un $\mathcal{Z}$ tel que

$$\forall v \in \mathcal{Z}(e > v).$$

Un multi-ordre $\ll$ sur les multi-ensembles sur $\mathcal{M}$ est la fermeture transitive de $\prec_1$.

Exemple 9. $\{\{5, 3, 1, 1\}\} \gg \{\{4, 3, 3, 1\}\}$.

Proposition 7. *Si l'ordre de base $>$ sur $\mathcal{M}$ est bien fondé, alors $\gg$ l'est aussi.*

Définition 10. Ordres multi-ensemblistes. *Soit un bon ordre $>$ sur Σ finie. Alors l'ordre* **multi-ensembliste** *est défini à partir de $>$ par le schéma LEX avec le point (l2c) remplacé par*

$$(m2c) \quad \left\{ \begin{array}{l} f \equiv g, \quad f(s_1, ..., s_m) >_{lex} t_j \quad (\forall j \; 1 \leq j \leq n) \textbf{ et} \\ \{\{s_1, ..., s_m\}\} \gg \{\{t_1, ..., t_n\}\}. \end{array} \right.$$

Notation : $t \succ_{mult} s$.

Exemple 10. $f(g(c, h(a)), c) >_{mult} g(g(k, l, a, a), h(a)) \quad si \quad f > g, c > k, c > l.$ *(Vérifiez le !)*

Théorème 4. *Tout ordre multi-ensembliste de réécriture $>_{mult}$ défini à partir d'un bon ordre $>$ sur Σ finie est un ordre de simplification.*

Corollaire 4. *Soit un SRT R. Si on trouve un bon ordre $>$ sur Σ (finie) tel que $l >_{mult} r$ pour toute règle $l \to r \in R$, alors R est terminal.*

Définition 11. Ordres mixtes. *Supposons que chaque foncteur $f/k \in \Sigma$ ait son statut :*
  (l) lexicographique *ou*
  (m) multi-ensembliste
et qu'on applique le point (l2c) du schéma LEX pour le statut (l) et le point (m2c) pour le statut (m). Alors on obtient un ordre dit mixte.

Théorème 5. *Tout ordre mixte de réécriture $>_{mix}$ défini à partir d'un bon ordre $>$ sur Σ finie est un ordre de réduction.*

Corollaire 5. *Soit un SRT R. Si on trouve un bon ordre $>$ sur Σ (finie) et des statuts (l) ou (m) pour tous ses foncteur afin que $l >_{mix} r$ soit vrai pour toute règle $l \to r \in R$, alors R est terminal.*

Exemple 11. *Soit*

$$R \;=\; \left\{ \begin{array}{lcl} (x + y) + z & \to & x + (y + z) \\ x * s(y) & \to & x + (y * x) \end{array} \right.$$

Vérifiez que R est terminal en posant :

$$statut(t) = l, \quad statut(*) = m \quad et \quad * > +.$$

Remarque : Tout ordre de réduction n'est pas un ordre de simplification :

Exemple 12. $R \;=\; \{f(f(x)) \to f(g(f(x)))\}$
  (i) prouvez que $\twoheadrightarrow_R$ est terminal (c'est-à-dire, un ordre de réduction)
  (ii) prouvez que $\twoheadrightarrow_R$ n'est pas un ordre de simplification.

4 Confluence

Selon le théorème de Newman, un SRT terminal faiblement confluent est confluent (et donc convergent). D'où l'intérêt de trouver les SRT faiblement confluents.
Non-confluence / non-confluence faible sont causées par la multiplicité des rédex. Mais il existent les cas qui ne causent pas la non-confluence, et il y en a ceux qui la causent.

Classification des cas :

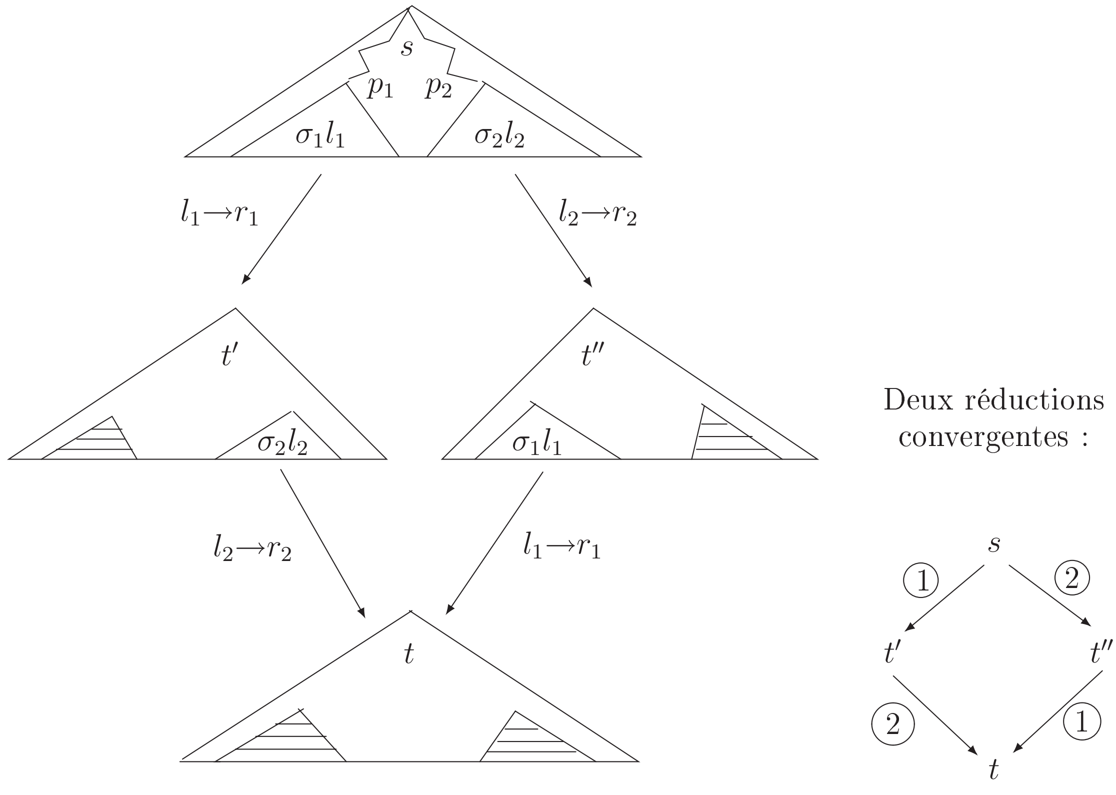


FIG. 1 – Cas 1

Cas 1 : $l_1 \rightarrow r_1$, $l_2 \rightarrow r_2$, $s/p_1 = \sigma_1(l_1)$, $s/p_2 = \sigma_1(l_2)$, **mais** $p_1 \parallel p_2$ (indépendantes) : voir Fig. 1.

Si les rédex dans s sont **indépendants**, alors les réductions correspondantes convergent.

Cas 2 : Un rédex est imbriqué dans un autre.

Cas 2.1 : Le rédex imbriqué se trouve dans l'image $\sigma_1(x)$, où $x \in Var(l_1)$: voir Fig. 2.

Cette variable peut avoir plusieurs occurrences dans les parties gauches et droites des règles.

Le rédex imbriqué se trouve dans l'image $\sigma_1(x)$, où $x \in Var(l_1)$:

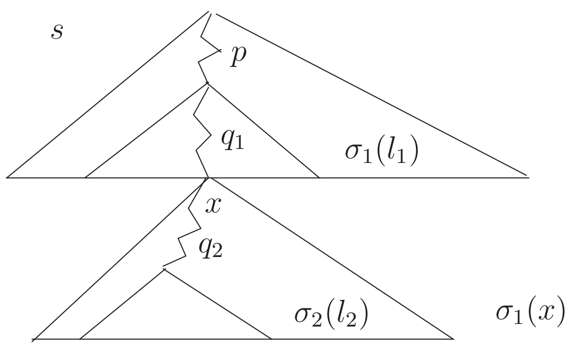


FIG. 2 – Cas 2.1

Dans la Fig. 3 on peut voir un schéma avec 3 occurrences dans la partie gauche et 2 occurrences dans la partie droite des règles :

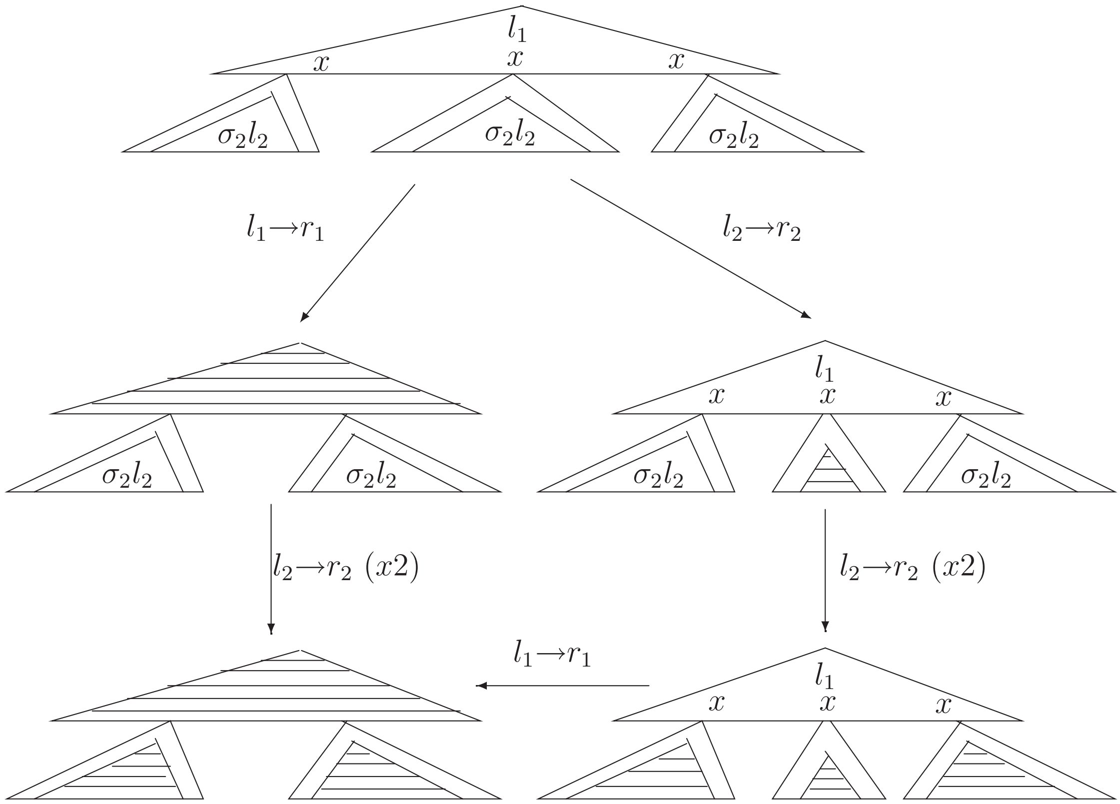


Fig. 3. - Cas 2.1. Réductions convergentes

Si les rédex imbriqués se trouvent dans les images $\sigma(x)$ des variables dans le rédex englobant, alors les réductions correspondantes convergent.

Cas 2.2 : Les rédex se chevauchent. C'est le cas qui peut poser problème : voir Fig. 4.

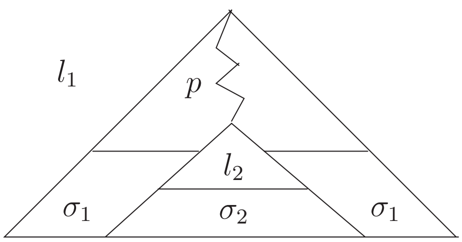


Fig. 4. - Cas 2.2.

Définition 12. *Soient* $\pi_1 = (l_1 \to r_1)$, $\pi_2 = (l_2 \to r_2) \in R$ *deux règles dont les variables sont renommées afin que* $Var(\pi_1) \cap Var(\pi_2) = \emptyset$. *Soit* $p \in O(l_1)$ *une occurrence telle que :*

(i) $l_1/p \notin Var$

(ii) $l_1/p =_\Theta l_2$ *—unifiables par l'unificateur le plus général* Θ.

Alors la paire

$$< \Theta(r_1), \quad \Theta(l_1)[p \leftarrow \Theta(r_2)] >$$

est **critique** *et* π_2 *est* **superposable** *sur* π_1 *dans l'occurrence* p*. (NB : on peut superposer sur la racine.)*

Exemple 13. *(i)* $f(f(x,y),z) \to f(x,f(y,z))$
(ii) $f(i(u),u) \to e$
Alors, pour l'unificateur $\Theta = \{x \mapsto i(u),\ y \mapsto u\}$ *on obtient la paire critique*

$$< f(i(u),f(u,z)),\ f(e,z) > :$$

$$\begin{array}{ccc} & f(f(i(u),u),z) & \\ \swarrow^{(i)} & & \searrow^{(ii)} \\ f(i(u),f(u,z)) & & f(e,z) \end{array}$$

Lemme 1. *Si* $s \to_R t_1$ *et* $s \to_R t_2$*, alors soit* t_1 *et* t_2 *convergent :* $t_1 \downarrow_R t_2$*, soit* $t_1 = s[p \leftarrow u_1]$*,* $t_2 = s[p \leftarrow u_2]$*,* (u_1,u_2) *étant un cas particulier d'une paire critique (par* σ*).*

Preuve : Voir l'analyse des cas 1, 2.1, 2.2.

Théorème 6 (Knuth-Bendix, Huet). *Un SRT* R *est faiblement confluent ssi toute sa paire critique est convergente.*

Preuve : ($\Longrightarrow$) Soit (u_1,u_2) une paire critique. Par définition :

$$u_1 = \Theta(r_1) \leftarrow_R \Theta(l_1) \to_R \Theta(l_1)[p \leftarrow \Theta(r_2)] = u_2$$

R étant faiblement confluent, $u_1 \downarrow_R u_2$.
($\Longleftarrow$) Supposons que $t_1 \leftarrow_R s \to_R t_2$. Selon le lemme 1, soit $t_1 \downarrow_R t_2$, soit $t_1 = s[p \leftarrow u_1]$, $t_2 = s[p \leftarrow u_2]$, où $u_1 = \sigma(v_1)$, $u_2 = \sigma(v_2)$ et (v_1,v_2) et une paire critique. Par l'hypothèse, $v_1 \downarrow_R v_2$, d'où $u_1 \downarrow_R u_2$ et $t_1 \downarrow_R t_2$.

Corollaire 6. *Un SRT* R *terminal est confluent ssi chaque sa paire critique est convergente.*

Corollaire 7. *Pour un SRT* R *terminal, le problème de confluence est décidable.*

Preuve : Le nombre des paires critiques différentes de R est borné par un polynôme $p(\mid R \mid)$.

Exemple 14. *Soit* $R_0 = \{f(f(x)) \to g(x)\}$*. Alors* $f(f(x)) \to g(x)$ *est superposable sur elle-même dans l'occurrence* 1 *par la substitution* $\sigma = \{y \mapsto f(x)\}$ *(on l'applique à la copie* $f(f(y)) \to g(y)$*). Ainsi on obtient la paire critique :*

$$\begin{array}{ccc} & f(f(f(x))) & \\ \swarrow & & \searrow \\ g(f(x)) & & f(g(x)) \end{array}$$

Ces termes sont FN_R*, donc non-confluents. Cela veut dire que* R *n'est pas confluent.*

5 Complétion

Rappelons-nous que pour tous SRT R, $\to_R$ est correct par rapport à $\approx_R$ ($\to_R \subseteq \approx_R$). Alors, si pour une paire critique (u_1, u_2) de R on rajoute $u_1 \to u_2$ ou $u_2 \to u_1$ à R, on obtient un nouveau SRT R^+ toujours correct par rapport à R : $\to_{R^+} \subseteq \approx_R$ (toute paire critique est une conséquence de R).

Cela nous amène à l'idée de complétion d'une SRT :
On calcule les paires critiques et les rajoute à R afin d'obtenir un nouveau système R^c correct par rapport à R et éventuellement **complet, terminal et confluent**.

Exemple 15. *Rajoutons $f(g(x)) \to g(f(x))$ à R_0. En utilisant l'ordre $f > g$, on prouve par le schéma lexicographique, que le SRT résultant R_0^c est terminal. Il suffit de prouver sa confluence faible. Mais une nouvelle paire critique apparaît :*

$$g(g(x)) \leftarrow_{R_0^c} f(f(g(x))) \to_{R_0^c} f(g(f(x))) \qquad (\sigma \ : \ y \mapsto g(x))$$

qui est convergente :

$$f(g(f(x))) \to_{R_0^c} g(f(f(x))) \to_{R_0^c} g(g(x)).$$

Alors R_0^c s'avère convergent.

Voici une procédure de complétion proposée par Knuth et Bendix. Elle s'applique à un SRT E, et à un ordre $>$ sur la signature Σ finie.

Procédure-de-complétion $KB(E, >)$:
Entrée : un SRT E (fini), l'ordre de réduction induit par $>$.
Sortie : un SRT R fini équivalent à E, si la procédure se termine par un succes, sinon "F" ou une boucle.
Initialisation :
si $s \approx t \in E$, $s \not\equiv t$, $s \not< t$, et $t \not< s$,
alors échec ("F").
sinon $i := 0$; $R_0 := \{l \to r \mid (l \approx r) \in E \cup E^{-1} \ \wedge \ l > r\}$

répéter $R_{i+1} := R_0$;
  pour tout $< s, t > \in PaireCrit(R_i)$:
    réduire $s \twoheadrightarrow_{R_i} \hat{s}$ (FN_{R_i}), $t \twoheadrightarrow_{R_i} \hat{t}$ (FN_{R_i}) ;
    si $(\hat{s} \not\equiv \hat{t} \ \wedge \ \hat{s} \not< \hat{t} \ \wedge \ \hat{t} \not< \hat{s})$
    alors $\acute{e}chec(\text{"}F\text{"})$
    fin − si ;
    si $(\hat{s} > \hat{t})$
    alors $R_{i+1} := R_{i+1} \cup \{\hat{s} \to \hat{t}\}$ − *une nouvelle règle*
    fin − si ;
    si $(\hat{t} > \hat{s})$
    alors $R_{i+1} := R_{i+1} \cup \{\hat{t} \to \hat{s}\}$
    fin − si ;
    fin − boucle ;
  $i := i + 1$
jusqu'à ce que $R_i = R_{i-1}$; − *stabilisation*
rendre R_i ;

Il y a trois possibilités :

A. La procédure se termine avec un success et rend R,

B. La procédure se termine avec un échec et rend "F",

C. La procédure boucle (produit un ensemble infini de règles).

Exercice. Appliquez KB aux théories :

$E_1 = \{(x * y) * (y * z) \approx y\}$ (stabilise au R_1),

$E_2 = \{x * (y + z) \approx (x * y) + (x * z),\ (u + v) * w \approx (u * w) + (v * w)\}$ et $* > +$ (un échec),

$E_3 = \{x + 0 \approx x,\ s(x + y) \approx x + s(y),\ x + s(0) \approx s(x)\}$ et $s > +$ (une boucle).

Théorème 7. *Soit une théorie équationnelle E et un ordre de réduction $>$.*

(1) Si $KB(E, >) = R_n$ pour un n, alors R_n est complet (adéquat) pour E, fini et convergent.

(2) Si $KB(E, >)$ boucle, alors $R_\infty =_{df} \bigcup_{i=0}^{\infty} R_i$ est un SRT infini complet pour E et convergent.

Corollaire 8. *Si $KB(E, >) = R_n$ pour un n, alors le SRT R_n décide le problème $E \models s \approx t$. Si $KB(E, >)$ boucle, alors R_∞ énumère ce problème.*