Techniques de réécriture

Frédéric Blanqui

2020-2021

Table des matières

Évaluation

Il y a des exercices à faire d'une semaine sur l'autre, et on est interrogés dessus. Le but c'est pas forcément de savoir faire tout l'exo.

Il y aura un devoir maison, prévu avant les vacances de la Toussaint.

Enfin il y a un examen à la fin du cours.

La note finale est la moyenne de ces trois notes.

1 La réécriture

1.1 Termes

On a des relations binaires, et on va s'intéresser à ce qui se passe quand on itère cette relation. Il y a quelques propriétés qui nous intéressent :
— la *terminaison*, savoir si itérer la relation termine,
— la *confluence*, savoir si prendre des chemins différents permet de relier au même endroit.

Définition 1.1 Mot/séquence

Un mot ou une séquence sur un ensemble A est une séquence finie d'éléments de A : $a_1, ..., a_n$.

Notation 1.1 Ensemble des mots

L'ensemble des mots sur l'ensemble A est noté A^*.

Notation 1.2 Longueur

On note $|a|$ la longueur du mot a : $|a_1, ..., a_n| = n$.

Notation 1.3 Concaténation

On note la concaténation avec l'opérateur $\cdot$.

Notation 1.4 Mot vide

On note ε le mot vide.

Définition 1.2 Signature

Pour chaque arité $n \in \mathbb{N}$ on suppose donné un ensemble $\mathcal{F}_n$ de symboles de fonctions.
On pose $\mathcal{F} = \bigcup_{n\in\mathbb{N}} \mathcal{F}_n$.

Exemple 1.1 Termes de l'arithmétique

— Zéro est un symbole d'arité 0.
— Le successeur est un symbole d'arité 1.
— Le + et le - sont des symboles d'arité 2.

Définition 1.3 Termes

L'ensemble des termes $\mathcal{C}(\mathcal{F}, \mathcal{V})$ sur $\mathcal{F}$, où $\mathcal{V}$ est un ensemble de variables disjoint de $\mathcal{F}$, est le plus petit ensemble tel que :
— toute variable est un terme
— si $f \in \mathcal{F}_n$ et $t_1, ..., t_n$ sont des termes alors $f\, t_1\, t_2 \ldots t_n$ est un terme.

Notation 1.5 Variables d'un terme

On note $\mathcal{V}(t)$ l'ensemble des variables du terme t.

Définition 1.4 Terme linéaire

Un terme est linéaire s'il ne contient aucune variable plus d'une fois.

Exemple 1.2

$+\,x\,x$ n'est pas linéaire.

Définition 1.5 Terme clos

Un terme est clos s'il en contient pas de variable.

Exemple 1.3

$+\,0\,0$ est clos.

Remarque 1.1

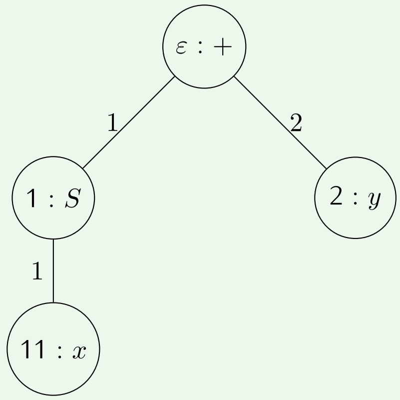
Tout terme clos est linéaire.

Définition 1.6 **Position**

Une position est un mot sur $\mathbb{N}$. ε désigne le sommet.
On définit l'ensemble des positions d'un terme par :
— $\mathrm{Pos}(x) = \{\varepsilon\}$ et
— $\mathrm{Pos}(f\, t_1 \dots t_n) = \{\varepsilon\} \cup \bigcup_{i=1}^{n} i\mathrm{Pos}(t_i)$.

Exemple 1.4

$+\,(S\,x)\,y$:



Définition 1.7 **Sous-terme**

Le sous-terme d'un terme t à la position $p \in \mathrm{Pos}(t)$ est défini par :
— $t|_{\varepsilon} = t$
— $f\, t_1 \dots t_n|_{ip} = (t_i)|_p$.

Notation 1.6 **Remplacer**

On peut remplacer t_p par u et on note $t[u]_p$.

Définition 1.8 **$\mathcal{F}$-algèbre**

Une $\mathcal{F}$-algèbre I est définie par :
— un ensemble non vide A
— pour tout $f \in \mathcal{F}_n$, une fonction $f_I : A^n \to A$.

Définition 1.9 **Interpolation**

Une interpolation des termes dans A est une valuation $\zeta : \mathcal{V} \to A$ telle que :
— $x\,\zeta = \zeta(x)$
— $(f\, t_1 \dots t_n)\,\zeta = f_I(t_1\,\zeta, \dots, t_n\,\zeta)$.

Exemple 1.5

L'ensemble des termes est une $\mathcal{F}$-algèbre :
— $A = \mathcal{C}(\mathcal{F}, \mathcal{V})$
— $f_I(t_1, \dots, t_n) = f\, t_1 \dots t_n$.

Définition 1.10 **Substitution**

Une substitution de termes est une valuation $\sigma : \mathcal{V} \to \mathcal{C}(\mathcal{F}, \mathcal{V})$.

Lemme 1.1

$(t\,\sigma)\,\zeta = t\,(\sigma\,\zeta)$

Preuve du lemme 1.1.

$\sigma\,\zeta$ est la valuation. Par induction sur t :
— $(x\,\sigma)\,\zeta = x\,(\sigma\,\zeta)$
— $((f\,t_1\,...\,t_n)\,\sigma)\,\zeta) = f_I\,((t_1\,\sigma)\,\zeta\,...\,(t_n\,\sigma)\,\zeta) = f_I\,(t_1\,(\sigma\,\zeta),...,t_n\,(\sigma\,\zeta))$.

Voilà !

1.2 Règles de réécriture

Définition 1.11 **Règle de réécriture**

Une règle de réécriture est un couple de termes (l, r) noté $l \to r$ tel que :
— l n'est pas une variable
— toutes les variables de r sont dans l.

Définition 1.12 **Système de réécriture**

Un système de réécriture est un ensemble de règles $\mathcal{R}$.

Définition 1.13 **Relation de réécriture engendrée**

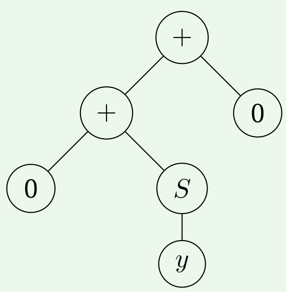
La relation de réécriture engendrée par $\mathcal{R}$, notée $\to_{\mathcal{R}}$ est telle que :

$$t \to_{\mathcal{R}} u \text{ ssi } \exists p \in \mathsf{Pos}(t), \exists \sigma, \exists l \to r \in \mathcal{R}, t|_p = l\sigma \wedge u = t[r\sigma]_p.$$

Exemple 1.6

On considère le système de réécriture $\mathcal{R} = \{+\,x\,0 \to x, +\,0\,x \to x, +\,x\,(S\,y) \to S\,(+\,x\,y)\}$.

On note plus simplement $\left|\begin{array}{l} x + 0 \to x \\ 0 + x \to x \\ x + (S\,y) \to s\,(x + y). \end{array}\right.$



On a toujours deux choix possibles quand on doit appliquer une réécriture : la position et la règle.

Définition 1.14 **Filtrage**

Un terme est t filtre (ou matche) un terme l (appelé motif ou pattern) s'il existe σ tel que $t = l\,\sigma$.
Le problème de filtrage est décidable sur les termes du premier ordre de complexité linéaire.

Exemple 1.7

En considérant le terme $x - x \to 0$, on a que $t - u$ matche $x - x$ si $t = u$.

Remarque 1.2

La réécriture est Turing-complète. La terminaison et la confluence sont indécidables.

Définition 1.15 **Contexte**

Un contexte C est un terme avec une occurence unique d'une variable $\square$ particulière. C'est en gros un terme avec un trou.
Le remplacement du trou par u est noté $C[u]$ ou $C[u]_p$.

Définition 1.16 **Relation stable, monotone, de réécriture**

Une relation $\mathcal{R}$ sur les termes est :
- stable (par substitution) ssi $\forall t, u, \sigma, t\mathcal{R}u \Rightarrow t_\sigma \mathcal{R} u_\sigma$
- monotone (stable par un contexte) ssi $\forall t, u, C, t\mathcal{R}u \Rightarrow C[t]\mathcal{R}C[u]$
- de réécriture ssi $\mathcal{R}$ est stable et monotone.

Exemple 1.8

$\to_\mathcal{R}$ est une relation de réécriture (à vérifier comme un grand).

Définition 1.17 **Relation qui termine, de réduction**

Une relation $\mathcal{R}$:
- termine s'il n'y a pas de séquence infinie $t_0 \,\mathcal{R}\, t_1 \,\mathcal{R}\, t_2 \,\mathcal{R} \ldots$
- est une relation de réduction ssi $\mathcal{R}$ est une relation de réécriture qui termine.

2 Preuves de terminaison

2.1 Terminaison d'une relation de la forme $\to_\mathcal{R}$

Lemme 2.1

$\to_\mathcal{R}$ termine ssi il existe un ordre de réduction $>$ contenant $\mathcal{R}$, c'est à dire $>$ termine et est un ordre stable et monotone.

Preuve du lemme 2.1.

Montrons que s'il existe un ordre de réduction $>$ contenant $\mathcal{R}$ alors $\to_\mathcal{R}$ termine.
Si $t = C[l_\sigma] \to_\mathcal{R} u = C[r_\sigma]$. Or $l > r$ et $>$ est stable, donc $l_\sigma > r_\sigma$, et par monotonie, $C[l_\sigma] > C[r_\sigma]$. D'où $\to_\mathcal{R} \subseteq >$, donc $\to_\mathcal{R}$ termine.
Pour l'autre implication il suffit de prendre la fermeture transitive pour avoir un ordre.

Voilà !

Lemme 2.2

$\mathcal{R}$ termine ssi sa clôture transitive $\mathcal{R}^+$ termine.

Preuve du lemme 2.2.

À faire comme un grand.

C'est ce que je voulais !

2.2 Technique de terminaison n°1

On va apprendre à construire des ordres de réduction.

2.2.1 Algèbre monotone bien fondée

Définition 2.1 **$\mathcal{F}$-algèbre relationnelle**

C'est une $\mathcal{F}$-algèbre I munie d'une relation $\mathcal{R}$ sur le domaine A de I.
On pose alors $t \,\mathcal{R}_I\, u$ ssi $\forall \zeta : \mathcal{V} \to A, t\,\zeta \,\mathcal{R}\, u\,\zeta$.

Définition 2.2 **$\mathcal{F}$-algèbre relationnelle bien fondée**

On dit que (I, A) est bien fondée si $\mathcal{R}$ est bien fondée.

Définition 2.3 $\mathcal{F}$-algèbre relationnelle monotone

On dit que (I, R) est monotone si $\forall n, \forall f \in \mathcal{F}_n, f_I$ est monotone par rapport à $\mathcal{R}$ en chaque argument. $\forall i, x_i \, \mathcal{R} \, x'_i \Rightarrow f_I(..., x_i, ...) \, \mathcal{R} \, f_I(..., x'_i, ...)$

Proposition 2.3 Propriétés de R_I

1. R_I est stable.
2. R_I est monotone si (I, R) est monotone.
3. R_I est un ordre de réduction si (I, R) est une algèbre monotone bien fondée.

Preuve du proposition 2.3.

1. $t\,\sigma \, \mathcal{R}_I \, u\,\sigma \Leftrightarrow \forall \zeta, (t\,\sigma)\,\zeta \, \mathcal{R} \, (u\,\sigma)\,\zeta \Leftrightarrow \forall \zeta, t\,(\sigma\,\zeta) \, \mathcal{R} \, u\,(\sigma\,\zeta)$.
2. À faire comme un grand.
3. À faire comme un grand en prenant $A = (\mathbb{N}, >)$, et des fonctions f_I sous formes de polynômes de très faible degré (au plus 2) avec des coefficients petits (au plus 3).

Et là c'est le plus beau jour de ma vie.

Exemple 2.1

On peut prendre $A = (\mathbb{R}, >_\delta)$ avec un delta pour avoir un ordre bien fondé, ou l'ordre normal avec des fonctions f_I expansibles ($f_I(x) > x$), ou encore $A = (\mathbb{N}^d, >)$.

Notation 2.1

Étant donnée une relation $\mathcal{R}$, on note :
— $\mathcal{R}(t) = \{u \,|\, r\mathcal{R}u\}$ (les successeurs de t)
— $\mathcal{R}^+$ la cloture transitive de $\mathcal{R}$
— $\mathcal{R}^*$ la cloture réflexive et transitive de $\mathcal{R}$
— $\mathcal{R}^=$ la cloture réflexive de $\mathcal{R}$
— $\mathcal{R}^{-1}$ la relation inverse de $\mathcal{R}$.

Définition 2.4 Forme normale/irréductible

Un élément a est sous forme normale ou irréductible si $\mathcal{R}(a) = \emptyset$.

Définition 2.5 Pré-ordre

Un pré-ordre est une relation réflexive et transitive. C'est un ordre non anti-symétrique.

Remarque 2.1

À partir d'un pré-ordre on peut définir une relation d'équivalence $\sim$ entre x et y si $x \leqslant y$ et $y \leqslant x$.

Définition 2.6 Partie stricte d'un pré-ordre

On définit la partie stricte $<$ d'un pré-ordre $\leqslant$ par $x < y$ ssi $x \leqslant y$ et $x \not\geqslant y$.

2.2.2 Induction bien fondée

Théorème 2.4

Si :
— $\mathcal{R}$ est une relation qui termine sur un ensemble A
— $P \subseteq A$ est une propriété sur A
— $\forall t \in A, t \in P$ si $\mathcal{R}(t) \subseteq P$.
Alors $P = A$.

Exemple 2.2 Récurrence sur les entiers

On a $A = \mathbb{N}$ et $\mathcal{R} = \{(n+1, n) \mid n \in \mathbb{N}\}$.
Alors pour $n \in \mathbb{N}$, $n \in P$ si $\mathcal{R}(n) \subseteq P$.
On a bien l'initialisation avec $\mathcal{R}(0) = \emptyset$ et qu'il faut dont montrer seulement $0 \in P$.

Preuve du théorème 2.4.

Si d'aventure $A \setminus P \neq \emptyset$, on a un élément $t \in A \setminus P$, donc $\mathcal{R}(t) \not\subseteq P$, donc on a encore un élément qui n'est pas dans P. On construit de cette manière, avec l'axiome du choix dépendant, une suite non terminante, ce qui termine l'aventure.

Voilà !

Définition 2.7 Axiome du choix dépendant

Si $A \neq \emptyset$ et $\mathcal{R}$ est une relation sur A tq $\forall x \exists y, x\mathcal{R}y$, alors il existe $f : \mathbb{N} \to A, \forall n, f(n)\mathcal{R}f(n+1)$.

2.3 Techniques de confluence

2.3.1 Définitions de confluences

Définition 2.8 Confluence locale (LCR)

$$\begin{tikzcd} & {} \arrow[dl, "\mathcal{R}"'] \arrow[dr, "\mathcal{R}"] & \\ {} \arrow[dr, dashed, "\mathcal{R}^*"'] & & {} \arrow[dl, dashed, "\mathcal{R}^*"] \\ & {} & \end{tikzcd}$$

Définition 2.9 Confluence (CR)

$$\begin{tikzcd} & {} \arrow[dl, "\mathcal{R}^*"'] \arrow[dr, "\mathcal{R}^*"] & \\ {} \arrow[dr, dashed, "\mathcal{R}^*"'] & & {} \arrow[dl, dashed, "\mathcal{R}^*"] \\ & {} & \end{tikzcd}$$

Lemme 2.5 Lemme de Newman

S'il y a confluence locale et terminaison, alors il y a confluence.

Preuve du lemme 2.5.

On montre par induction bien fondée sur $\mathcal{R}$ la propriété $P(t)$ de confluence :

$$\forall u, v, t\mathcal{R}^*u \wedge t\mathcal{R}^*v \Rightarrow \exists w, u\mathcal{R}^*w \wedge v\mathcal{R}^*w.$$

$$\begin{tikzcd}
t \arrow[r, "\mathcal{R}"] \arrow[d, "\mathcal{R}"'] & t_1 \arrow[r, "\mathcal{R}^*"] \arrow[d, dashed, "\mathcal{R}^*"'] & u \arrow[d, dashed, "\mathcal{R}^*"'] \\
t_2 \arrow[r, dashed, "\mathcal{R}^*"] \arrow[dd, "\mathcal{R}^*"'] & t_3 \arrow[r, dashed, "\mathcal{R}^*"] & t_4 \arrow[dd, dashed, "\mathcal{R}^*"'] \\
& & \\
v \arrow[rr, dashed, "\mathcal{R}^*"'] & & t_5
\end{tikzcd}$$

cskifo

2.3.2 Relation sur les paires

Définition 2.10 Produit parallèle, produit séquentiel, produit lexicographique

Soit $\mathcal{R}$ une relation sur A et $\mathcal{S}$ une relation sur B.
On définit :
— Le produit parallèle : $(a,b)\,\mathcal{R}\times_{\mathsf{par}}\mathcal{S}\,(a',b')$ ssi $a\,\mathcal{R}\,a' \wedge b\,\mathcal{S}\,b'$
— Le produit séquentiel : $(a,b)\,\mathcal{R}\times_{\mathsf{seq}}\mathcal{S}\,(a',b')$ ssi $a\,\mathcal{R}\,a' \wedge b = b'$ ou $a = a' \wedge b\,\mathcal{S}\,b'$
— Le produit lexicographique : $(a,b)\,\mathcal{R}\times_{\mathsf{lex}}\mathcal{S}\,(a',b')$ ssi $a\,\mathcal{R}\,a'$ ou $a = a' \wedge b\,\mathcal{S}\,b'$.

Lemme 2.6

Si $\mathcal{R}$ et $\mathcal{S}$ terminent, alors $\mathcal{R}\times_{\mathsf{par}}\mathcal{S}$, $\mathcal{R}\times_{\mathsf{seq}}\mathcal{S}$ et $\mathcal{R}\times_{\mathsf{lex}}\mathcal{S}$ terminent.

Preuve du lemme 2.6.

Par l'absurde.

Et là c'est le plus beau jour de ma vie.

2.3.3 Relation sur les mots

Définition 2.11 Ordre lexicographique

Soit $\mathcal{R}$ une relation sur A.
On définit $\mathcal{R}_{\mathsf{lex}}$ sur A^* par $a_1 ... a_p\,\mathcal{R}_{\mathsf{flex}}\,b_1 ... b_q$ ssi $\exists i, a_i = b_i \wedge \forall j < i, a_j = b_j$.

Exemple 2.3 $\mathcal{R}_{\mathsf{lex}}$ ne préserve pas la terminaison

Si $\mathcal{R} = \{(a,b)\}$, alors $a\,\mathcal{R}_{\mathsf{lex}}\,ba\,\mathcal{R}_{\mathsf{lex}}\,bba\,\mathcal{R}_{\mathsf{lex}}\,...$

2.3.4 Relations sur les multi-ensembles

Définition 2.12 Multi-ensemble, multiplicité, cardinal

Un multi-ensemble sur un ensemble A est une fonction $M : A \to \mathbb{N}$ à support fini ($\{a \mid M(a) > 0\}$ est fini).
$M(a)$ est appelé multiplicité de A.
On appelle cardinal de M, et on note $|M| = \sum_{a\in A} M(a)$.

Notation 2.2

On notera par exemple $M = [a,a,b]$ le multi-ensemble tel que $M(a) = 2$, $M(b) = 1$ et sinon $M(x) = 0$.

Notation 2.3 Ensemble des multi-ensembles sur un ensemble

On note $\mathcal{M}(A)$ l'ensemble des multi-ensembles sur A.

Définition 2.13 Ordre sur les multi-ensembles

Soit $>$ une relation sur A.
On définit $>_{\text{mul}}$ sur $\mathcal{M}(A)$ par $M >_{\text{mul}} N$ ssi $\exists X, Y, Z$:
— $M = Z + X$
— $N = Z + Y$
— $X \neq \emptyset$
— $\forall y \in Y, \exists x \in X, x > y$.

Remarque 2.2

$>_{\text{mul}} = >_{\text{m}}^{+}$ où $>_{\text{m}}$ impose d'avoir X un singleton.

Théorème 2.7

Si $>$ est un ordre strict qui termine alors $>_{\text{mul}}$ est un ordre strict qui termine.

Preuve du théorème 2.7.

On veut montrer que tout M termine pour $>_{\text{m}}$.
On fait une induction sur $|M|$:
— si $M = \emptyset$ alors ça termine
— si $M = N + [x]$ et que N termine par hypothèse alors on fait une induction bien fondée sur (x, N) avec l'ordre $> \times_{\text{lex}} >_{\text{m}}$: $\forall x, \forall N$ qui termine, $N + [x]$ termine.
De manière générale, t termine si tous ses successeurs terminent.
Les successeurs de $N + [x]$ peuvent être :
1. $N = N' + [x']$, alors $N + [x] > N' + [x] + Y$, avec $Y < x'$.
2. $N + [x] > N + Y$, avec $Y < x$. Et pour savoir si $N + Y$ termine on fait une induction sur $|Y|$:
— Si $|Y| = 0$ c'est bon
— Si $Y = Y' + [y]$, on a $N + Y'$ qui termine, et $N + Y' + [y]$ qui termine.

Voilà !

2.3.5 Relations sur les termes

Définition 2.14 Recursive Path Ordering (RPO)

On étend un préordre $\geqslant_{\text{F}}$ sur les symboles de fonction en un pré-ordre sur les termes : $t >_{\text{rpo}} u$ ssi $t = f\, t_1 \dots t_n$ et soit :
1. cas sous-terme : $\exists i, t_i >_{\text{rpo}}^{=} u$
2. cas précédence : $u = g\, u_1 \dots u_p$, $f >_{\text{F}} g$, $\forall i, t >_{\text{rpo}} u_i$
3. cas équivalence : $u = g\, u_i \dots u_p$, $f \sim_{\text{F}} g$, $\forall i, t >_{\text{rpo}} u_i$, $[t_1 \dots t_p](>_{\text{rpo}})_{\text{mul}}[u_1 \dots u_p]$.

Théorème 2.8

Si $>_{\text{F}}$ termine, alors $>_{\text{rpo}}$ termine.
$>_{\text{rpo}}$ est stable et monotone.

Preuve du théorème 2.8.

On a besoin de montrer que $\forall f, \forall t_1, \dots t_n$ qui terminent, $f\, t_1\ \dots\ t_n$ termine, c'est à dire que tous les successeurs terminent.
Trouver la bonne induction pour organiser cette preuve comme un grand.

cskifo

Remarque 2.3

Il y a des variantes de RPO selon comment un compare les arguments dans le cas équivalence. Par exemple on pourrait prendre l'ordre lexicographique.

2.4 Preuve de terminsaison incrémentale

Définition 2.15 — Paire de réduction

Une paire de réduction (E, T) est un couple tel que :
— E est un pré-ordre de réécriture
— T est un ordre qui est stable et termine (donc strict)
— $E\,T \subseteq T$ ou $T\,E \subseteq T$ (composition des relations).
Une paire est monotone si T est monotone.

Exemple 2.4 — Exemples de paires de réduction

— $(\geqslant_I, >_I)$ où $(I, >)$ est une interprétation monotone bien fondée
— $(>_{\mathsf{rpo}}^{=}, >_{\mathsf{rpo}})$
sont des paires de réduction monotone.

Remarque 2.4

$>_I$ est strictement inclus dans la partie stricte de $\geqslant_I$.
— $t \geqslant_I u$ ssi $\forall \xi, t\,\xi \geqslant u\xi$
— $t >_I u$ ssi $\forall \xi, t\,\xi > u\xi$
La partie stricte de $\geqslant_I$est $\geqslant_I \setminus \leqslant_I$.
Par exemple avec $f_I(x) = 2x$ et $z_I = 0$ dans une interprétation dans $\mathbb{N}$, on a $f(x) \geqslant_I x$ mais $x \not\geqslant_I f(x)$ car en substituant x par 1 on n'a pas la relation. Donc $(f(x), x)$ est dans la partie stricte de la relation, et $f(z), z)$ est dans l'équivalence.

Remarque 2.5

La partie stricte n'est pas forcément stable.

Lemme 2.9

Soit $\mathcal{R}$ un ensemble de règles de réécriture.
$\rightarrow_{\mathcal{R}}$ termine ssi il existe une paire de réduction *monotone* (E, T) telle que $\mathcal{R} \subseteq E$ et $\rightarrow_{\mathcal{R}\setminus T}$ termine.

Preuve du lemme 2.9.

$\Longrightarrow$: On prend $(\rightarrow_{\mathcal{R}}^{*}, \rightarrow_{\mathcal{R}}^{+})$.
$\Longleftarrow$: Si d'aventure on a une séquence infinie de $\mathcal{R}$ $t_0 \rightarrow_{\mathcal{R}} t_1 \rightarrow_{\mathcal{R}} \cdots$, comme $\mathcal{R} \setminus T$ termine, toutes les séquences de $\mathcal{R} \setminus T$ sont finies. Donc la séquence est une répétition de séquences de la forme $\rightarrow_{\mathcal{R}\setminus T}^{*}\rightarrow_{\mathcal{R}\cap T}$, qui est incluse dans $E^{*}\,T$ qui est inclus dans T par définition. Donc la séquence est finie. Que nenni ! Fichtre ! Vertudieu ! L'aventure est finie.

Voilà !

3 Paires de dépendance

L'idée va être de revenir au point de départ et d'essayer de comprendre quand on n'a pas de terminaison, ce qui permet d'avoir une séquence infinie de réécriture.

Supposons qu'on a une séquence infinie $t_0 \rightarrow_{\mathcal{R}} t_1 \rightarrow_{\mathcal{R}} \cdots$. On décale la séquence pour avoir t_0 de taille minimale (en taille). t_0 est de la forme $f\,\bar{u}$ et tous ses sous-termes terminent. La séquence est alors de la forme :

$$t_0 = f\,\bar{u} \xrightarrow{>\varepsilon}{}_{\mathcal{R}}^{*} f\,\bar{v} = f\,\bar{l}\sigma \xrightarrow{\varepsilon} r\,\sigma \rightarrow \cdots$$

où on a $f\,\bar{l} \rightarrow r \in \mathcal{R}$.

Donc il existe $p \in \mathsf{Pos}(r)$ tel que $r|_p\,\sigma$ ne termine pas, donc $r|_p$ n'est pas une variable et est de la forme $g\,\bar{m}$ et il existe une règle de la forme $g\,\bar{w} \rightarrow s$.

Définition 3.1 — Symbole défini

Un symbole f est défini s'il existe une règle de la forme $f\,\bar{l} \rightarrow r$.

Définition 3.2 — Paire de dépendance

Une paire de dépendance est une paire de termes $(f\,\bar{l}, g\,\bar{m})$ telle qu'il existe une règle $f\,\bar{l} \rightarrow r$ et $g\,\bar{m}$ est un sous-terme de r.

Exemple 3.1

Pour définir la multiplication :
- $x \times (s\,y) \to (x \times y) + x$
- $x \times 0 \to 0$
- $x + 0 \to x$
- $x + (s\,y) \to s\,(x+y)$

Les symboles définis sont $+$ et $\times$ et les symboles non définis sont 0 et s.
Les paires de dépendance sont :
- $(x \times (s\,y), x \times y)$
- $(x \times (s\,y), (x \times y) + x)$
- $(x + (s\,y), x + y)$.

On a donc que pour tout terme non-terminant minimal t_0, il existe un autre terme non terminant minimal $g\,\bar{m}\,\sigma$ tel que $t_0 \xrightarrow{>\varepsilon}{}^*_{\mathcal{R}} \xrightarrow{\varepsilon}_P g\,\bar{m}\,\sigma$, où P est l'ensemble des paires de dépendance.

Théorème 3.1 — Théorème des paires de dépendances

$\to_{\mathcal{R}}$ termine ssi $\left(\xrightarrow{>\varepsilon}_{\mathcal{R}}\right)^* \xrightarrow{\varepsilon}_P$ termine, où P est l'ensemble des paires de dépendance.

Preuve du théorème 3.1.

$\Longleftarrow$: c'est ce qu'on a montré, si $\to_{\mathcal{R}}$ ne termine pas alors l'autre ne termine pas.
$\Longrightarrow$: Avec $\rhd$ la relation sous-terme stricte, on a $\xrightarrow{\varepsilon}_P \subseteq \xrightarrow{\varepsilon}_{\mathcal{R}} \unrhd$, donc $\left(\xrightarrow{>\varepsilon}_{\mathcal{R}}\right)^* \xrightarrow{\varepsilon}_P \subseteq \xrightarrow{\varepsilon}{}^+_{\mathcal{R}} \unrhd$.
Or si $\xrightarrow{\varepsilon}_{\mathcal{R}}$, $\xrightarrow{\varepsilon}_{\mathcal{R}} \rhd$ termine car $\rhd \xrightarrow{\varepsilon}_{\mathcal{R}} \subseteq \xrightarrow{\varepsilon}_{\mathcal{R}} \rhd$.

Voilà !

Lemme 3.2 — Terminaison avec des symboles marqués par les paires de dépendances

À chaque symbole défini f d'arité n on ajoute un symbole $f^\#$ d'arité n. On crée des symboles marqués pour les paires de dépendances. On crée une nouvelle algèbre.
Alors $\left(\xrightarrow{>\varepsilon}_{\mathcal{R}}\right)^* \xrightarrow{\varepsilon}_P$ termine sur $T(\mathcal{F}, \mathcal{V})$ ssi $\to^*_{\mathcal{R}} \xrightarrow{\varepsilon}_{P\#}$ termine sur $T(\mathcal{F} \cup \mathcal{F}^\#, \mathcal{V})$.

Définition 3.3 — DP-problème

Un DP-problème est une paire $(\mathcal{R}, \mathcal{P})$ où $\mathcal{R}$ et $\mathcal{P}$ sont des ensembles de règles de réécriture tels que les symboles de $\mathcal{P}$ n'apparraissent ni dans $\mathcal{R}$ ni dans les sous-termes stricts de $\mathcal{P}$.

Définition 3.4 — Terminaison d'un DP-problème

Un DP-problème $(\mathcal{R}, \mathcal{P})$ termine si $\to^*_{\mathcal{R}} \xrightarrow{\varepsilon}_{\mathcal{P}}$ termine.

Lemme 3.3

$(\mathcal{R}, \mathcal{P})$ termine ssi il existe un epaire de réduction (E, T) telle que :
- $\mathcal{R} \cup \mathcal{P} \subseteq E$
- $(\mathcal{R}, \mathcal{P} \setminus T)$ termine.

Preuve du lemme 3.3.

On part à l'aventure en supposant qu'on a une séquence infinie de $\longrightarrow^*_{\mathcal{R}} \xrightarrow{\varepsilon}_{\mathcal{P}}$.

Voilà !

L'avantage est qu'on n'a pas la contrainte de monotonie sur T.
$(\geqslant_I, >_I)$ est monotone si les fonctions d'interprétation f_I sont monotones par rapport à $\geqslant_I$ et $>_I$.

3.1 Graphe de dépendances

Définition 3.5 — Graphe de dépendances (DG)

Le graphe de dépendance est défini par :
- noeuds : les paires de dépendance P

— arêtes : il y a une arête de (l_1, r_1) à (l_2, r_2) s'il existe σ_1 et σ_2 telles que $r_1\sigma_1 \to^*_{\mathcal{R}} l_2\sigma_2$.

À toute séquence de réduction correspond un chemin dans le graphe (mais pas l'inverse).

Exemple 3.2

En reprenant l'exemple de la multiplication :
— A : $(x \times (s\, y), x \times y)$
— B : $(x \times (s\, y), (x \times y) + x)$
— C : $(x + (s\, y), x + y)$.
On a le graphe suivant :

$$\begin{tikzcd} \mathsf{A} \arrow[r] \arrow[loop below] & \mathsf{B} \arrow[r] & \mathsf{C} \arrow[loop below] \end{tikzcd}$$

Théorème 3.4

Étant donné un système de réécriture $\mathcal{R}$ *fini*, $\to_{\mathcal{R}}$ termine ssi pour tout cycle C du graphe de dépendances $(\mathcal{R}, C)$ termine.

En pratique on se content de vérifier pour les cycles maximaux, i.e. les composantes fortement connexes, car il y a un nombre exponentiel de cycles et un nombre linéaire de composantes fortement connexe.

Théorème 3.5

Étant donné un système de réécriture $\mathcal{R}$ *fini*, $\to_{\mathcal{R}}$ termine ssi pour tout cycle C du graphe de dépendances, il existe une paire de réduction (E, T) telle que
— $\mathcal{R} \subseteq E$
— $C \subseteq E \cup T$
— $C \cap T \neq \emptyset$.
C'est à dire qu'il suffit d'une étape stricte dans chaque cycle.

DG n'est pas décidable, mais il existe des sur-approximations qui le sont.

3.2 Graphe EDG

Définition 3.6 RC

On a $\mathsf{RC}(t) = u$ où tout sous-terme égal à une variable ou de la forme $f\, u_1 \dots u_n$ avec f définie est remplacé par une variable *fraîche*.
Ce n'est pas un nom standard.

Exemple 3.3

Si a et c ne sont pas définis et que f l'est :
— $\mathsf{RC}(c\, x\, x) = c\, x_1\, x_2$
— $\mathsf{RC}(c\, (f\, x)\, a) = c\, y\, a$

Remarque 3.1

$\mathsf{RC}(t)$ est linéaire et ne contient aucun symbole défini.

Remarque 3.2

Pour tout terme t, il existe une substitution θ_t elle que $t = \mathsf{RC}(t)\, \theta_t$.

Définition 3.7 EDG

Le graphe EDG est défini par :
— noeuds : les paires de dépendances
— arêtes : $(l_1^\#, r_1^\#) \to (l_2^\#, r_2^\#)$ ssi $\mathsf{RC}(r_1^\#)$ et $l_2^\#$ sont unifiables, et $\mathsf{RC}(r_1^\#) = l_2^\#$ admet une solution.

Remarque 3.3

Le graphe de dépendances DG est inclus dans un graphe EDG (mêmes sommets mais moins d'arêtes).

$r_1\,\sigma_1 = \mathsf{RC}(r_1)\,\theta_{r_1}\,\sigma_1 \to_{\mathcal{R}}^* l_2\,\sigma_2$ et par définition de $\mathsf{RC}(r_1)$, on a $l_2\,\sigma_2 = \mathsf{RC}(r_1)\theta'$ avec $\theta_{r_1}\,\sigma_1 \to_{\mathcal{R}}^* \theta'$.

4 Retour sur la confluence

4.1 Pré-ordre d'instanciation

Définition 4.1 Pré-ordre d'instanciation sur les termes

$\leqslant$ est un pré-ordre d'instanciation sur les termes si $t \leqslant u$ ssi $\exists \theta, t\,\theta = u$.

L'idée est que t est plus général que u. C'est le *filtrage*.

Remarque 4.1

Cette relation définit bien un pré-ordre (réflexif et transitif).
De plus, on a $t \simeq u$ ssi t et u sont égaux à permutation des variables près.

Définition 4.2 Pré-ordre sur les substitutions

$\sigma \leqslant \sigma'$ ssi $\exists \theta, \sigma\,\theta = \sigma'$ et $x\,(\sigma\,\theta) = (x\,\sigma)\,\theta$

Remarque 4.2

On a $\sigma \simeq \sigma'$ ssi $\exists \rho$ permutation des variables$, \sigma\,\rho = \sigma'$.

Définition 4.3 Unification

Résoudre des systèmes d'équations sur les termes.

Exemple 4.1

$f\,x\,x = f\,a\,b$

Un problème d'unification et l'ensemble de ses solutions :
— $\perp$, tel que $\mathsf{Sol}(\perp) = \emptyset$
— un ensemble P d'équations entre termes, $\mathsf{Sol}(P) = \{\sigma \mid \forall t = u \in P, t\,\sigma = u\,\sigma\}$

Exemple 4.2

— On considère l'équation $f\,(s\,x)\,y = f\,y\,(s\,a)$.
  Alors on a $s\,x = y$ et $y = s\,a$, donc $\mathsf{Sol} = \{\sigma\}$ avec $\sigma = \{x \mapsto a, y \mapsto s\,a\}$.
— On considère les équations $x = f\,y$ et $y = f\,x$.
  Alors il faudrait avoir $x = f\,(f\,x)$ donc $\mathsf{Sol} = \emptyset$.
— On considère l'équation $f\,x = y$.
  Alors $\mathsf{Sol} = \{\{x \mapsto t, y \mapsto f\,t\} \mid t \text{ terme}\}$.

Proposition 4.1

Si un système d'équations P a une solution alors P a une plus petite solution (appelée mgu[a]) pour l'ordre d'instanciation.
$\mathsf{Sol}(P) = \leqslant(\mathsf{mgu}(P)) = \{\mathsf{mgu}(P)\,\theta \mid \theta\}$

a. most general unifier

Remarque 4.3

Un problème d'unification est décidable, de complexité linéaire.

4.2 Utiliser la réécriture pour résoudre un problème d'unification

On va transformer les équations pas à pas jusqu'à ce que la solution soit lisible directement. On peut faire le parallèle avec la méthode du pivot de Gauss.

On considère alors le système de réécriture suivant :

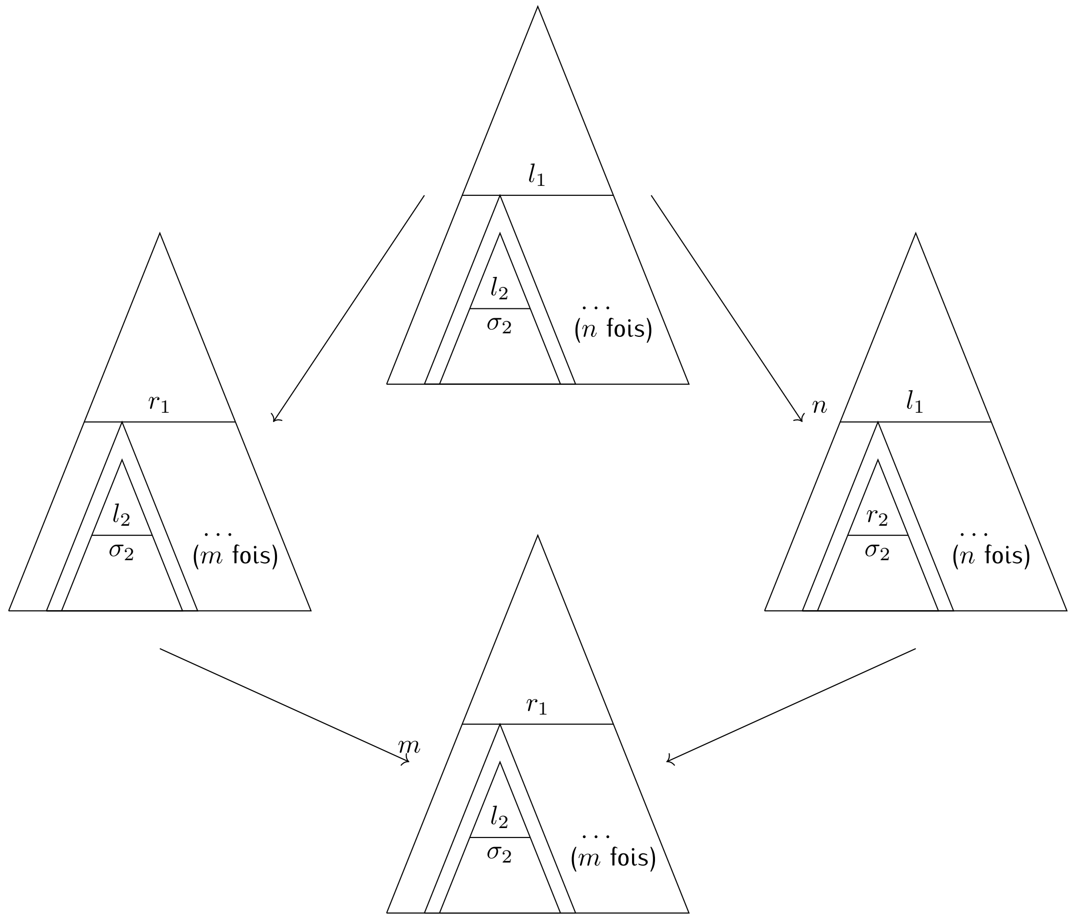
— $P \uplus \{f\, t_1 \dots t_n = f\, u_1 \dots u_n\} \to P \cup \{t_1 = u_1\} \cup \dots \cup \{t_n = u_n\}$
— $P \uplus \{f\, t_1 \dots t_n = g\, u_1 \dots u_p\} \to \bot$ si $f \neq g$
— $P \uplus \{t = t\} \to P$
— $P \uplus \{x = t\} \to P\{x \mapsto t\} \cup \{x = t\}$, où $x \in \mathsf{Var}(P)$ et $x \notin \mathsf{Var}(t)$
— $P \uplus \{t = x\} \to P \cup \{x = t\}$

Pour résoudre P, on applique les règles autant que possible (ça termine), jusqu'à obtenir une forme normale P' de la forme $\{x_1 = t_1, \dots, x_n = t_n\}$ avec $x_i \notin \mathsf{Var}(t_1 \dots t_n)$, ou $\bot$. On dit que P' est une forme résolue et définit une substitution idempotente. C'est le mgu.

Propriété 4.2 Propriétés de ce procédé

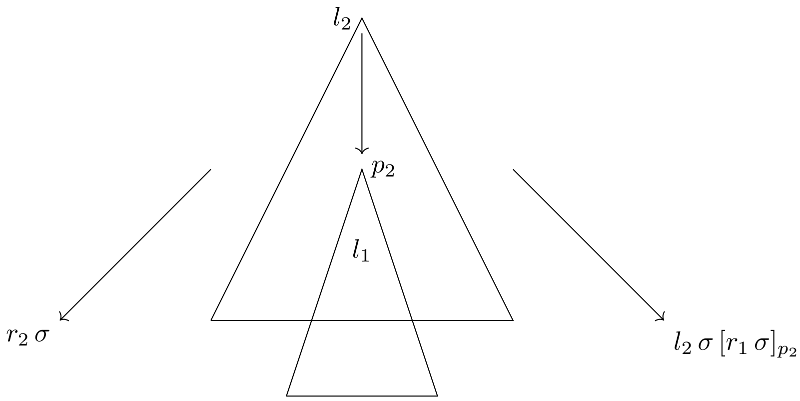
— Correction : si $P \to Q$ alors $\mathsf{Sol}(Q) \subseteq \mathsf{Sol}(P)$.
— Complétude : si $P \to Q$ alors $\mathsf{Sol}(P) \subseteq \mathsf{Sol}(Q)$.
— Terminaison : $\to$ termine.
— Minimalité : si P est une forme normale pour $\to$ alors P est en forme résolue.

4.3 Confluence locale sur les termes



Définition 4.4 Paire critique

L'ensemble des paires critiques entre $l_1 \to r_1$ et $l_2 \to r_2$, noté $\mathsf{CP}(l_1 \to r_1, l_2 \to r_2)$, est l'ensemble des paires $(r_2\, \sigma, l_2\, \sigma[r_1\, \sigma]_{p_2})$ où $\sigma = \mathsf{mgu}(l_2|_{p_2}, l_1)$.



Théorème 4.3 **Théorème des points critiques**

$\xleftarrow[\mathcal{R}]{}\xrightarrow[\mathcal{R}]{} \subseteq \xrightarrow[\mathcal{R}]{*}\xleftarrow[\mathcal{R}]{*} \cup \xleftrightarrow[\mathrm{CP}(\mathcal{R})]{}$

$\longrightarrow_{\mathcal{R}}$ est LCR ssi toutes les paires critiques sont joignables et $\mathrm{CP}(\mathcal{R}) \subseteq \xrightarrow[\mathcal{R}]{*}\xleftarrow[\mathcal{R}]{*}$.

Exemple 4.3

On considère le système de réécriture $\{x+0 \underset{1}{\rightarrow} x, x+s\,y \underset{2}{\rightarrow} s\,(x+y), x+(y+z) \underset{3}{\rightarrow} (x+y)+z\}$.

$$\begin{tikzcd}
 & x+(y+(t+u)) \arrow[dl, "\text{pos } \varepsilon\ 3"'] \arrow[dr, "3\ \text{pos } 2"] & \\
(x+y)+(t+u) \arrow[ddr] & & x+((y+t)+u) \arrow[d] \\
 & & (x+(y+t))+u \arrow[dl] \\
 & ((x+y)+t)+u &
\end{tikzcd}$$

Le système n'est pas joignable sans la règle $0+x \rightarrow x$ car

$$\begin{tikzcd}
 & (x+0)+z \arrow[dl, "3"'] \arrow[dr, "1"] & \\
x+(0+z) & & x+z
\end{tikzcd}$$

Cependant $CP = \emptyset$ n'implique pas confluence.

Exemple 4.4 **Système de réécriture sans paire critique ni confluence**

On considère le système suivant :

$$\begin{aligned} f\,x\,x &\rightarrow a \\ f\,x\,(g\,x) &\rightarrow b \\ c &\rightarrow g\,c \end{aligned}$$

4.4 Complétion de Knuth-Bendix

Un système d'équations $\mathcal{E}$ est un ensemble d'équations, c'est à dire de paires de termes.

La théorie équationnelle engendrée par $\mathcal{E}$ (resp. un système de réécriture $\mathcal{R}$) est la plus petite relation d'équivalence monotone et stable contenant $\mathcal{E}$ (resp. $\mathcal{R}$).

Question. Comment décider une théorie équationnelle $\mathcal{E}$? (problème de mot)

A-t-on $t =_{\varepsilon} u$?

Exemple 4.5 **La théorie des groupes**

On a comme signature :

— $*$ d'arité 2
— e d'arité 0

— $^{-1}$ d'arité 1.
On a les équations suivantes :
— $(x * y) * z = x * (y * z)$
— $x * e = x$
— $e * x = x$
— $x * x^{-1} = e$
— $x^{-1} * x = e$.

Pour décider si $t =_\varepsilon u$, on peut trouver un système $\mathcal{R}$ el que
— $=_\mathcal{R} = =_\varepsilon$
— $\mathcal{R}$ SN $\Rightarrow$ tout terme adet au moins une forme normale
— $\mathcal{R}$ CR $\Rightarrow$ tout terme adet au plus une forme normale
On peut alors décider si $t =_\varepsilon u$ en vérifiant $\mathrm{nf}(t) = \mathrm{nf}(u)$.

Problème. Comment obtenir un $\mathcal{R}$ à partir d'un E ?

Knuth-Bendix. Prenons un ordre de réduction $>$ et orientons les équations avec.
Si on a $t = u$ et $t > u$ on prend la règle $t \to u$.

La procédure peut être décrite par un ensemble de règles :

$$\begin{array}{llcll}
\text{(deduce)} & \mathcal{E}, \mathcal{R} & \longrightarrow & \mathcal{E} \cup \{l = r\}, \mathcal{R} & \text{si } l = r \in \mathrm{CP}(\mathcal{R}) \\
\text{(orient)} & \mathcal{E} \uplus \{l = r\}, \mathcal{R} & \longrightarrow & \mathcal{E}, \mathcal{R} \cup \{l \to r\} & \text{si } l > r \\
\text{(delete)} & \mathcal{E} \uplus \{t = t\}, \mathcal{R} & \longrightarrow & \mathcal{E}, \mathcal{R} & \\
\text{(simplify)} & \mathcal{E} \uplus \{t = u\}, \mathcal{R} & \longrightarrow & \mathcal{E} \cup \{t' = u'\}, \mathcal{R} & \text{si } t \to_\mathcal{R} t' \text{ et } u \to_\mathcal{R} u' \\
\text{(compose)} & \mathcal{E}, \mathcal{R} \uplus \{l \to r\} & \longrightarrow & \mathcal{E}, \mathcal{R} \cup \{l \to r'\} & \text{si } r \to_\mathcal{R} r' \\
\text{(collapse)} & \mathcal{E}, \mathcal{R} \uplus \{l \to r\} & \longrightarrow & \mathcal{E} \cup \{l' = r\}, \mathcal{R} & \text{si } l \to_\mathcal{R} l'.
\end{array}$$

Proposition 4.4

— Si $(\mathcal{R}, \mathcal{E}) \longrightarrow (\mathcal{R}', \mathcal{E}')$ alors $=_{\mathcal{R} \cup \mathcal{E}} = =_{\mathcal{R}' \cup \mathcal{E}'}$.
— Si $(\mathcal{E}, \emptyset) \longrightarrow (\emptyset, \mathcal{R})$ en forme normale pour $\to$ alors $\mathcal{R}$ termine car $\mathcal{R} \subseteq >$ et est confluent car $\mathcal{R}$ SN et LCR ($\mathcal{R}$ LCR car $\mathrm{CP}(\mathcal{R}) = \emptyset$).

4.5 Système orthogonal

Définition 4.5 Système orthogonal

Un système est orthogonal s'il est linéaire gauche et n'a pas de paires critiques.

Théorème 4.5

Tout système orthogonal est confluent.

Preuve du théorème 4.5.

On définit une relation S telle que :
— S est confluente
— $\to_\mathcal{R} \subseteq S \subseteq \to_\mathcal{R}^*$

$$\begin{tikzcd}
 & \cdot \arrow[dl, "\mathcal{R}^* \subseteq S^*"'] \arrow[dr, "\mathcal{R}^* \subseteq S^*"] & \\
\cdot \arrow[dr, dashed, "\mathcal{R}^* \subseteq S"'] & & \cdot \arrow[dl, dashed, "\mathcal{R}^* \subseteq S"] \\
 & \cdot &
\end{tikzcd}$$

S est la plus petite relation linéaire réflexive $\Rrightarrow_\mathcal{R}$ stable contenant $\mathcal{R}$ et telle que :
(mon) $t_1 \Rrightarrow_\mathcal{R} u_1$, ..., $t_n \Rrightarrow_\mathcal{R} u_n$ implique $f\, t_1 \dots t_n \Rrightarrow_\mathcal{R} f\, u_1 \dots u_n$
(refl) $t \Rrightarrow_\mathcal{R} t$
($\mathcal{R}$) $l\,\sigma \Rrightarrow_\mathcal{R} r\,\sigma$ si $l \to r \in \mathcal{R}$

On montre par induction que l'on a confluence forte, la propriété du diamant : $\mathrel{\leftarrow\!\!\!\!\!\parallel}\mathrel{\parallel\!\!\!\!\!\rightarrow}\subseteq\mathrel{\parallel\!\!\!\!\!\rightarrow}\mathrel{\leftarrow\!\!\!\!\!\parallel}$.
Cas (mon),(mon) :

$$\begin{tikzcd}
 & f\,t_1\dots t_n \arrow[dl, "\parallel"'] \arrow[dr, "\parallel"] & \\
f\,u_1\dots u_n \arrow[dr, dashed, "\parallel"'] & & f\,v_1\dots v_n \arrow[dl, dashed, "\parallel"] \\
 & f\,w_1\dots w_n &
\end{tikzcd}$$

Et par hypothèse d'induction, $u_i \mathrel{\parallel\!\!\!\!\!\rightarrow} w_i \mathrel{\leftarrow\!\!\!\!\!\parallel} v_i$.
Cas ($\mathcal{R}$),($\mathcal{R}$) :

$$\begin{tikzcd}
 & l_2\,\sigma_2 = l_1\,\sigma_1 \arrow[dl, "\parallel"'] \arrow[dr, "\parallel"] & \\
r_2\,\sigma_2 & & r_1\,\sigma_1
\end{tikzcd}$$

Et comme on n'a pas de paires critiques, $l_1 = l_2$.
Cas (mon),($\mathcal{R}$) :

$$\begin{tikzcd}
 & f\,t_1\dots t_n = l\,\sigma \arrow[dl, "\parallel"'] \arrow[dr, "\parallel"] & \\
f\,u_1\dots u_n = l\,\theta \arrow[dr, dashed, "\parallel"'] & & r\,\sigma \arrow[dl, dashed, "\parallel"] \\
 & r\,\theta &
\end{tikzcd}$$

Avec $\sigma \mathrel{\parallel\!\!\!\!\!\rightarrow} \theta$.
Et $u_i = l_i\,\theta$ car on n'a pas de paires critiques et on est linéaire gauche.

cskifo

4.6 Confluence par diagramme décroissant

On suppose que $\mathcal{R} = \bigcup_{i \in I} \mathcal{R}_i$.
À une réduction $\mathcal{R}^*$ correspond un mot dans I^* :

$$\begin{array}{cccc}
\xrightarrow{\mathcal{R}_{i_1}} & \xrightarrow{\mathcal{R}_{i_2}} & \dots & \xrightarrow{\mathcal{R}_{i_n}} \\
i_1 & i_2 & \dots & i_n
\end{array}$$

On suppose un ordre bien fondé sur les pics

$$\begin{tikzcd}
\cdot \arrow[r, "b"] \arrow[d, "a"'] & {} \\
{} &
\end{tikzcd}$$

où $a, b \in I^*$.
On doit vérifier :

$$\begin{tikzcd} \cdot \arrow[r, "b"] \arrow[d, "a"'] & \cdot \\ \cdot & \end{tikzcd} \quad < \quad \begin{tikzcd} \cdot \arrow[r, "ib"] \arrow[d, "ia"'] & \cdot \\ \cdot & \end{tikzcd}$$

Définition 4.6 **Ordre lexicographique maximal**

Soit $<$ un ordre strict sur I. On définit l'ordre lexicographique maximal par :

$$a <_{\mathsf{lm}} b \text{ ssi } |a| <_{\mathsf{mul}} |b|$$

où $|\varepsilon| = \emptyset$ et $|ia| = [i] + (|a| \setminus < (i))$ (on élimine de a toutes les occurences $< i$).

Exemple 4.6

— $|1\,3\,2\,3\,4\,3| = [1, 3, 3, 4]$
— $|2\,1\,1| = [2]$

Propriété 4.6

— Si $>$ termine alors $>_{\mathsf{ln}}$ termine.
— $ab = a + b \setminus a$

Définition 4.7 **Diagramme décroissant (DD)**

Un diagramme

$$\begin{tikzcd} \cdot \arrow[r, "b"] \arrow[d, "a"'] & \cdot \arrow[d, "a'"] \\ \cdot \arrow[r, "b'"'] & \cdot \end{tikzcd}$$

est décroissant si $b' \setminus a \leqslant b$ et $a' \setminus b \leqslant a$.

Propriété 4.7

Si on a un des diagrammes suivant

$$\begin{tikzcd} \cdot \arrow[r, "b"] \arrow[d, "a"'] \arrow[dr, phantom, "\text{DD}"] & \cdot \arrow[d, "a'"] \arrow[r, "c"] & \cdot \\ \cdot \arrow[r, "b'"'] & \cdot & \end{tikzcd} \qquad \begin{tikzcd} \cdot \arrow[r, "b"] \arrow[d, "a"'] \arrow[dr, phantom, "\text{DD}"] & \cdot \arrow[d, "a'"] \\ \cdot \arrow[r, "b'"'] \arrow[d, "c"'] & \cdot \\ \cdot & \end{tikzcd}$$

alors on a $a' + c < a + bc$ ou $b' + c < ac + b$.

Preuve du propriété 4.7.

$$\begin{aligned} a' + c &= (a' + c) \cap > (b) + (a' + c)/b \\ &< b + a'/b + c/b \\ &\leqslant b + a + c/b \\ &= a + bc \end{aligned}$$

Propriété 4.8

Si on a le diagramme suivant

$$\begin{tikzcd} \cdot \arrow[r, "b"] \arrow[d, "a"'] \arrow[dr, phantom, "\text{DD}"] & \overset{\text{DD}}{\cdot} \arrow[r, "c"] \arrow[d, "a'"] \arrow[dr, phantom, "\text{DD}"] & \cdot \arrow[d, "a''"] \\ \cdot \arrow[r, "b'"'] & \cdot \arrow[r, "c'"'] & \cdot \end{tikzcd}$$

Alors :
1. $(a''/c)/b \leqslant a'/b \leqslant a$
2. $b'c'/a \leqslant bc$.

Théorème 4.9

Soient $(\to_i)_{i\in I}$ et $(\to_j)_{j\in J}$ deux familles de relation sur un ensemble Δ et un ordre bien fondé sur $I \cup J$.

Alors $I = \bigcup_{i\in I} \to_i$ et $J = \bigcup_{j\in J} \to_j$ commutent si $\forall i, \forall j$, il y a un DD $\begin{tikzcd} \cdot \arrow[r, "j"] \arrow[d, "i"'] & \cdot \arrow[d] \\ \cdot \arrow[r] & \cdot \end{tikzcd}$ pour $>_{\mathrm{lm}}$.

$$\begin{tikzcd} \cdot \arrow[r, "I^*"] \arrow[d, "J^*"'] & \cdot \arrow[d, "J^*"] \\ \cdot \arrow[r, "I^*"'] & \cdot \end{tikzcd} \qquad \begin{tikzcd} \cdot \arrow[r, "j"] \arrow[d, "i"'] & \cdot \arrow[d, "a"] \\ \cdot \arrow[r, "b"'] & \cdot \end{tikzcd} \quad \begin{array}{l} a/j \leqslant i \\ \\ b/i \leqslant j \end{array}$$

$$\begin{tikzcd} \cdot \arrow[rrr, "j"] \arrow[dddd, "i"'] \arrow[ddddrrr, phantom, "\text{DD}"] & & & \cdot \arrow[d, "*"', ">(j)"] \\ & & & \cdot \arrow[d] \\ & & & \cdot \arrow[d] \\ & & & \cdot \arrow[d] \\ \cdot \arrow[r, "J^*"] & \cdot \arrow[r] & \cdot \arrow[r] & \cdot \end{tikzcd}$$

Définition 4.8 — Relation localement diagramme décroissante (LDD)

Une relation $\to$ est LDD s'il existe une famille $(\to_i)_{i\in I}$ avec $I, >)$ un domaine bien fondé telle que $\to = \bigcup_{i\in I} \to_i$ et $\forall i, \forall j, \exists$ $\begin{tikzcd} \cdot \arrow[r, "j"] \arrow[d, "i"'] \arrow[dr, phantom, "\text{DD}"] & \cdot \arrow[d] \\ \cdot \arrow[r] & \cdot \end{tikzcd}$.

On a montré que LDD implique confluence, mais on a aussi confluence et normalisation faible implique LDD, où la normalisation faible est l'existence d'une forme normale.

Définition 4.9 — Séquence cofinale

Une séquence de réécriture (finie ou infinie) $t_0 \to t_1 \to \ldots$ est dite cofinale si $\forall u \leftarrow^* t_0, \exists k, u \to^* t_k$.
Une relation $\to$ est cofinale (CF) s'il existe une séquence cofinale.

Lemme 4.10

Une relation cofinale est confluente.

Preuve du lemme 4.10.

$$\begin{tikzcd}
 & t = t_0 \arrow[r] \arrow[dl, "*"'] \arrow[dr, "*"] & t_1 \arrow[r, dashed] & t_i \arrow[r, dashed] & t_j \\
u \arrow[urrrr, bend right, "*"'] & & v \arrow[ur, bend right, "*"'] & &
\end{tikzcd}$$

CF

Et là c'est le plus beau jour de ma vie.

Lemme 4.11

Toute relation confluente et faiblement normalisée est cofinale.

Lemme 4.12

Toute relation confluente et dénombrable est cofinale.

Preuve du lemme 4.12.

Soit t un élément du domaine. On peut éliminer les réduits de t : $a_0, a_1, \ldots$. On construit une séquince cofinale partant de t par récurrence sur k :
— $s_0 = t = a_0$
— s_{k+1} est :

$$\begin{tikzcd}
t \arrow[r, "*"] \arrow[rr, bend left, "*"] & s_k \arrow[dr, "*"'] & a_{k+1} \arrow[d, "*"] \\
 & & s_{k+1}
\end{tikzcd}$$

C'est ce que je voulais !

Théorème 4.13

Toute relation cofinale est localement diagramme décroissante.

Preuve du théorème 4.13.

Par modularité on peut se restreindre aux classes d'équivalences modulo $\overset{*}{\leftrightarrow}$.
Soit t un élément. Par hypothèse on a une séquence cofinale partant de t dans $\overset{*}{\leftrightarrow}(t)$: $t = t_0 \to t_1 \to \ldots$.

cskifo

Lemme 4.14

Si $(\to_k)_{k \in K}$ est une famille disjointe de relations LDD alors $\bigcup_{k \in K} \to_k$ est LDD.

Preuve du lemme 4.14.

On prend $I = \mathbb{N}$ et $>=>_{\mathbb{N}}$.
On annote $a \to b$ par :
— 0 si $\exists k, a = t_k$ et $b = t_{k+1}$
— $i + 1$ où i est le plus petit nombre d'étapes de réécriture pour aller de b à un élément t_k de la séquence cofinale.
Sans perte de généralité on peut supposer les t_k distincts deux à deux.
Avec $k = l$,

$$\begin{tikzcd}
a = t_k = t_l \arrow[r, "0"] \arrow[d, "0"'] \arrow[dr, phantom, "\mathrm{DD}"] & b = t_{k+1} \\
c = t_{l+1} &
\end{tikzcd}$$

Avec $k \geqslant l$,

$$\begin{tikzcd}
a \arrow[rrrr, "0"] \arrow[dddd, "0"'] & & & & b \arrow[d, "i-1"] \\
& & & & {} \arrow[d, "i-2"] \\
& & \mathrm{DD} & & {} \\
& & & & {} \arrow[d, "1"] \\
c \arrow[r, "j-1"'] & {} \arrow[r, "j-2"'] & {} & {} \arrow[r, "1"'] & t_l \arrow[r, "0"'] & t_k
\end{tikzcd}$$

cskifo

5 Modularité de la confluence

Définition 5.1 **Modularité**

Une propriété P sur les systèmes de réécriture ou les relations est modulaire si

$$P(\mathcal{R}) \wedge P(\mathcal{S}) \implies P(\mathcal{R} \cup \mathcal{S}).$$

Remarque 5.1

La terminaison n'est pas modulaire.

Exemple 5.1 **Contre-exemple de Toyama**

Soient $\mathcal{R} = \{f\,a\,b\,x \to f\,x\,x\,x\}$ et $\mathcal{S} = \{g\,x\,y \to x, g\ y \to y\}$.
Ils terminent tous les deux, mais $f\,a\,b\,(g\,a\,b) \to^2 f\,a\,b\,(g\,a\,b)$.

Théorème 5.1 **Théorème de Toyama (1988)**

La confluence est modulaire quand les signatures sont disjointes.

Preuve du théorème 5.1.

On considère deux symboles de fonction $\mathcal{F}_1$ et $\mathcal{F}_2$, $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2$, et $\mathcal{T}_a = \mathcal{T}(\mathcal{F}_a, V)$. On peut voir 1 et 2 comme des couleurs.
On considère 2 ensembles de règles de réécriture $\mathcal{R}_a \subseteq \mathcal{T}_a^2$. On a :
— $\to_{\mathcal{R}_a}$ la relation engendrée par $\mathcal{T}_a$
— $\to_a$ la relation engendrée par $\mathcal{T}$
— $\to = \to_1 \cup \to_2$.
On a des multi-contextes $C \in \mathcal{T}(\mathcal{F} \cup \{\square\}, V$ qui ont plusieurs "trous" que l'on veut combler par des termes. Si C est un multi-contexte avec des occurences de $\square$ aux positions $p_1, \ldots, p_n$, alors $C[t_1, \ldots, t_n]$ est le terme obtenu en remplaçant $C|_{t_i}$ par t_i.

Définition 5.2 **Cap et alien**

Soit un terme t de la forme $f\,\bar{t}$ avec f de couleur a.
Le cap de f est le plus grand multi-contexte monochrome (de couleur a).
Les aliens d'une liste de termes $t_1 ... t_n$ de la forme $g\,\bar{u}$ avec g de couleur $\bar{a}$ tels que $t = C[t_1, ..., t_n]$.

On définit alors la cap reduction par $t \to^c u$ si $t \xrightarrow{p} u$ avec $p \in \mathsf{Pos}(\mathsf{cap}(t))$ et l'alien reduction par $t \to^a u$ si $t \xrightarrow{p} u$ avec $p \notin \mathsf{Pos}(\mathsf{cap}(t))$.

Si $t \to^c u$ alors il y a deux cas :
1. $u \in \mathsf{aliens}(t)$
2. $\mathsf{cap}(t) \to_i \mathsf{cap}(u)$ et $\mathsf{aliens}(u) \subseteq \mathsf{aliens}(t)$

Si $t \to^a u$ et $\mathsf{aliens}(t) = [t_1, ..., t_n$ alors $u = \mathsf{cap}(t)[t_1, ..., t'_k, ... t_n]$ avec $t_k \to t'_k$. ($\mathsf{cap}(u) \neq \mathsf{cap}(t)$ en général)

Définition 5.3 **Rang**

Le rang d'un terme t, note $\mathsf{rg}(t)$, vaut $1 + \max\{\mathsf{rg}(u) \mid u \in \mathsf{aliens}(t)\}$, avec $\max \emptyset = 0$.

Lemme 5.2

Si $t \to u$ alors $\mathsf{rg}(t) \geqslant \mathsf{rg}(u)$.

Définition 5.4 **Sous-termes spéciaux**

L'ensemble des sous-termes spéciaux est $S(t) = \{t\} \cup \bigcup \{S(u) \mid u \in \mathsf{aliens}(t)\}$.

Définition 5.5 **Relation effondrante**

$t \Rrightarrow u$ ssi $\exists c, s \in S(t), s', t = C[s], s \to^* s', u = C[s']$, soit $s' \in V$, soit $\mathsf{root}(s')$ et $\mathsf{root}(s)$ sont de couleur différente.

Lemme 5.3

$\Rrightarrow$ termine.

Preuve du lemme 5.3.

On va utiliser l'ordre multi-ensemble pour montrer qu'on remplace quelque chose de gros par une multitude de choses de plus petites.
On prend comme mesure de t : $\|t\| = [\mathsf{rg}(s) \mid s \in S(t)]$.

Voilà !

On a alors que pour tout terme t, il existe un terme t' tel que $t \to^* t' \not\Rrightarrow$.

Définition 5.6 **Terme stable**

Un terme en forme normale pour $\Rrightarrow$ est stable.

Tout terme admet un réduit stable.

On revient à la preuve de la confluence en elle-même.

$$\begin{tikzcd}
 & t \arrow[dl, "*"'] \arrow[dr, "*"] & \\
u \arrow[dr, dashed, "*"'] & & v \arrow[dl, dashed, "*"] \\
 & ? &
\end{tikzcd}$$

On montre que tout terme t est confluent par induction sur $\mathsf{rg}(t)$ (t est confluent si toute réduction à partir de

t est confluente).

Définition 5.7 — Terme alien-stable

Un terme est alien-stable si ses aliens sont stables.

Définition 5.8 — Témoin

Un témoin d'un terme t, avec aliens$(t) = [t_1, ..., t_n]$, est un terme de la forme cap$(t)[u_1, ..., u_n]$ avec $t_i \to^* u_i$ stable et $u_i = u_j$ si $t_i = t_j$.

On a que tout terme t admet un témoin qu'on note $\dot{t}$.

$$\begin{tikzcd}
& t \arrow[dl, "*"'] \arrow[d, "*"] \arrow[dr, "*"] & \\
u \arrow[d, "*"'] & \dot{t} & v \arrow[d, "*"] \\
\dot{u} & & \dot{v}
\end{tikzcd}$$

Lemme 5.4

Si $t \to u$ et les aliens de t sont confluents alors $\dot{t} \downarrow \dot{u}$ (t et u ont un réduit commun)

Preuve du lemme 5.4.

$t =$ cap$(t)[t_1, ..., t_n$, $\dot{t} =$ cap$(t)[u_1, ..., u_n]$ et $t_i \to^* u_i$
Si $t \to^c u$ on a deux cas possibles.
1. Cas $u = t_i$. Alors

$$\begin{tikzcd}
\dot{t} \arrow[r] & u_i \arrow[dr, "*"'] & t_i \arrow[l, "*"'] \arrow[r] & \dot{t}_i \arrow[dl, "*"] \\
& & {} &
\end{tikzcd}$$

2. Cas $u =$ cap$(u)[t_{k_1}, ..., t_{k_p}]$. Alors $\dot{u} =$ cap$(u)[v_{k_1}, ..., v_{k_p}]$,$\dot{t} =$ cap$(u)[u_{k_1}, ..., u_{k_p}]$. Donc

$$\begin{tikzcd}
& t_{k_i} \arrow[dl, "*"'] \arrow[dr, "*"] & \\
u_{k_i} \arrow[dr, "*"'] & & v_{k_i} \arrow[dl, "*"] \\
& {} &
\end{tikzcd}$$

3. Cas $t \to^a u$.

Youpi !

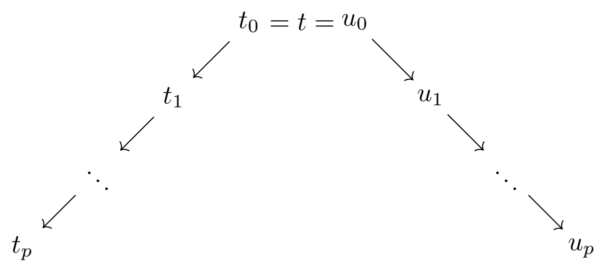
$$\begin{tikzcd}
& & t \arrow[dl, "*"'] \arrow[dd, "*"] \\
& u \arrow[dl, "*"'] \arrow[dd, "*"] & \\
v \arrow[dd, "*"] & & \dot{t} \arrow[d, "*"] \\
& \dot{u} \arrow[r, "*"'] \arrow[d, "*"] & {} \arrow[d, "*"] \\
\dot{v} \arrow[r, "*"'] & {} \arrow[r, "*"'] & {}
\end{tikzcd}$$

Lemme 5.5

$\to$ est confluente sur les termes alien-stables.

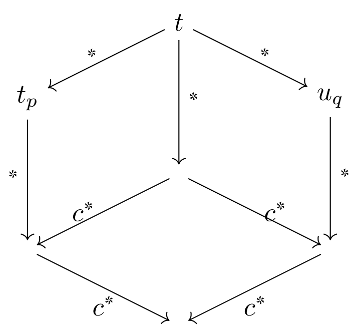
Preuve du lemme 5.5.

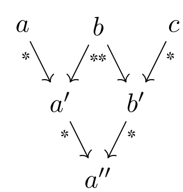
On va montrer par induction sur le rang de t que les aliens sont confluents.



Youpi !

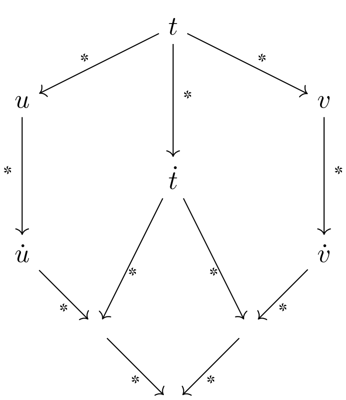
Soit M l'ensemble des sous-termes maximaux de $\{t_i, u_i\}$ dont le symbole de tête est de couleur 2.
Tous les éléments de M sont confluents.





Le relation $\downarrow$ est une relation d'équivalence sur M.
M est fini. À chaque classe d'équivalence on peut associer un réduit commun. On suppose une fonction de choix $\wedge : M \to T$ telle que $a \downarrow b \Rightarrow \hat{a} = \hat{b}$.

Soit $\tilde{t}$ le terme obtenu en remplaçant dans t tout élément s de M par $\hat{s}$.
Alors si $a \to b$ est une étape $t_i \to t_{i+1}$ ou $u_i \to u_{i+1}$, alors $\tilde{a} \to_1^c \tilde{b}$ ou $\tilde{a} = \tilde{b}$....
Ce qui termine la preuve.



cskifo

Index des définitions

Index des résultats