Cours 2-5
Démonstration automatique

Évelyne Contejean

28 septembre 2012

Récriture

(suite)

Rappels

$$s \longrightarrow_R t \quad \text{si} \quad s = s[l\sigma]_p \quad t = s[r\sigma]_p \quad \text{où} \quad l \to r \in R$$

Théorème

Si $\leftarrow_R$ est bien fondée et $\rightarrow_R$ est localement confluente, alors

$$\forall s, t, \quad s \overset{*}{\underset{R}{\longleftrightarrow}} t \iff s \overset{*}{\underset{R}{\longrightarrow}} \overset{*}{\underset{R}{\longleftarrow}} t$$

Rappel : convergent = bien fondé + (localement) confluent

Algèbres de formes normales I

Théorème

Si R est un système de récriture convergent, alors

$$\forall s, t, \quad s \overset{*}{\underset{R}{\longleftrightarrow}} t \iff s{\downarrow_R} = t{\downarrow_R}$$

quand R est un ensemble fini, on peut effectivement calculer les formes normales

Algèbres de formes normales II

Théorème

R un système de récriture convergent sur $\mathcal{T}(\mathcal{F}, \mathcal{X})$. *La* $\mathcal{F}$*-algèbre* $\mathcal{A}$ *définie par :*

- *le support* $\mathcal{A}_s$ *est égal à l'ensemble des formes normales closes pour* $\rightarrow_R$ *de sorte s,*
- *si* $f : s_1 \times \ldots \times s_n \rightarrow s$ *est un symbole de fonction de* $\mathcal{F}$*, alors :*

$$f_{\mathcal{A}}(u_1{\downarrow_R}, \ldots, u_n{\downarrow_R}) = (f(u_1, \ldots, u_n)){\downarrow_R}$$

est isomorphe à $\mathcal{T}(\mathcal{F})/E_R$.

Systèmes de récriture canoniques

Définition

R un système de récriture sur $\mathcal{T}(\mathcal{F}, \mathcal{X})$ est dit interréduit si pour toute règle $l \to r$ de R

- $l = l\downarrow_{R\setminus\{l\to r\}}$,
- $r = r\downarrow_R$.

Un système de récriture est canonique si il est convergent et interréduit.

Théorème

R et R' deux systèmes de récriture sur $\mathcal{T}(\mathcal{F}, \mathcal{X})$ tels que

- $\forall s, t,\ \ s =_{E_R} t \iff s =_{E_{R'}} t$,
- *R et R' sont canoniques,*
- $\leftarrow_{R\cup R'}$ *est bien fondée.*

Alors $R = R'$ (à renommage près).

Problèmes

- Comment savoir si $\leftarrow_R$ est bien fondée ?
  $\mapsto$ cours XU
- Que faire si $\leftarrow_R$ n'est pas bien fondée ?
  $\mapsto$ suite de ce cours (récriture modulo)
- Comment savoir si $\rightarrow_R$ est localement confluente ?
  $\mapsto$ suite de ce cours (lemme des paires critiques)
- Que faire si $\rightarrow_R$ n'est pas localement confluente ?
  $\mapsto$ prochain cours (complétion)

Que faire si $\leftarrow_R$ n'est pas bien fondée ?

Groupe commutatif

$$\left\{\begin{array}{rcl} x \cdot e & = & x \\ x \cdot I(x) & = & e \\ x \cdot (y \cdot z) & = & (x \cdot y) \cdot z \\ x \cdot y & = & y \cdot x \end{array}\right\}$$

$$x \cdot y \rightarrow y \cdot x \quad \text{ou} \quad y \cdot x \rightarrow x \cdot y \ ?$$

dans les deux cas

$$a \cdot b \rightarrow b \cdot a \rightarrow a \cdot b \rightarrow \ldots$$

Récriture modulo, v1

R sytème de récriture + S ensemble d'équations

récriture dans les classes modulo $=_S$ (Ballantine & Lankford, 1977)

$$s \longrightarrow_{R/S} t \quad \text{si} \quad \exists s', \exists t', s =_S s' \ \wedge \ t =_S t' \ \wedge \ s' \rightarrow_R t'$$

problème : trouver s' et t', donc énumérer les classes

Récriture modulo, v2

R sytème de récriture + S ensemble d'équations

récriture étendue modulo $=_S$ (Peterson & Stickel, 1981)

$$s \longrightarrow_{S\backslash R} t \quad \text{si} \quad \exists l \to r \in R \;\; \exists p \in \mathrm{Pos}(s) \;\; \exists \sigma \;\; s|_p =_S l\sigma \;\; \wedge \;\; t \equiv s[r\sigma]_p$$

problème : trouver σ, donc filtrer modulo S

Adapter la notion de confluence

Définition (Church-Rosser, confluence, confluence locale))

$\mathscr{A}$ un ensemble, $\to_R$ et $\to_S$ deux relations sur $\mathscr{A}$, et $\to_R \subseteq \to_{R^S} \subseteq \to_{R/S}$

- *$\to_R$ est $\to_{R^S}$-Church-Rosser modulo $\to_S$ ssi*

$$\forall x, y \in \mathscr{A},\ x \overset{*}{\underset{R\cup S}{\longleftrightarrow}} y \Rightarrow (\exists z, z' \in \mathscr{A},\ x \overset{*}{\underset{R^S}{\to}} z \overset{*}{\underset{S}{\longleftrightarrow}} z' \overset{*}{\underset{R^S}{\leftarrow}} y)$$

- *$\to_{R^S}$ est confluente modulo $\to_S$ ssi*

$$\forall x, y, z \in \mathscr{A},\ y \overset{*}{\underset{R^S}{\leftarrow}} x \overset{*}{\underset{R^S}{\to}} z \Rightarrow (\exists v, v' \in \mathscr{A},\ y \overset{*}{\underset{R^S}{\to}} v \overset{*}{\underset{S}{\longleftrightarrow}} v' \overset{*}{\underset{R^S}{\leftarrow}} z)$$

- *$\to_{R^S}$ est localement confluente avec $\to_R$ modulo $\to_S$ ssi*

$$\forall x, y, z \in \mathscr{A},\ y \underset{R^S}{\leftarrow} x \underset{R}{\to} z \Rightarrow (\exists v, v' \in \mathscr{A},\ y \overset{*}{\underset{R^S}{\to}} v \overset{*}{\underset{S}{\longleftrightarrow}} v' \overset{*}{\underset{R^S}{\leftarrow}} z)$$

Ça ne suffit pas : cohérence

Définition (cohérence, cohérence locale)

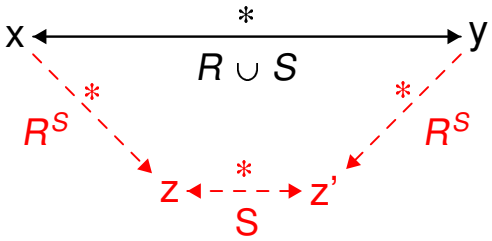
- $\rightarrow_{R^S}$ *est* *cohérente modulo* $\rightarrow_S$ *ssi*

$$\forall x, y, z \in \mathscr{A},\ y \underset{R^S}{\overset{*}{\leftarrow}} x \overset{*}{\underset{S}{\longleftrightarrow}} z \Rightarrow (\exists v, v' \in \mathscr{A},\ y \overset{*}{\underset{R^S}{\rightarrow}} v \overset{*}{\underset{S}{\longleftrightarrow}} v' \overset{*}{\underset{R^S}{\leftarrow}} z)$$

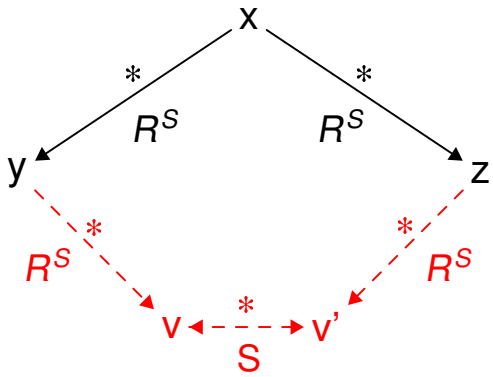
- $\rightarrow_{R^S}$ *est* *localement cohérente modulo* $\rightarrow_S$ *ssi*

$$\forall x, y, z \in \mathscr{A},\ y \underset{R^S}{\leftarrow} x \underset{S}{\longleftrightarrow} z \Rightarrow (\exists v, v' \in \mathscr{A},\ y \overset{*}{\underset{R^S}{\rightarrow}} v \overset{*}{\underset{S}{\longleftrightarrow}} v' \overset{*}{\underset{R^S}{\leftarrow}} z)$$

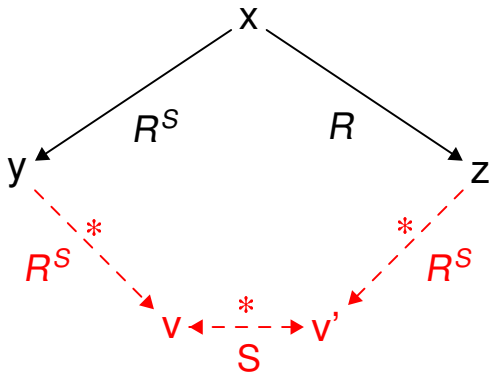
Définitions graphiques



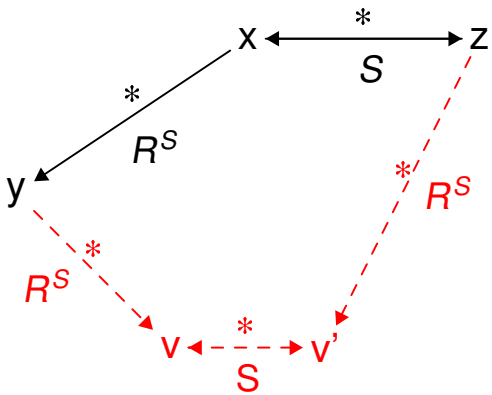
Church-Rosser



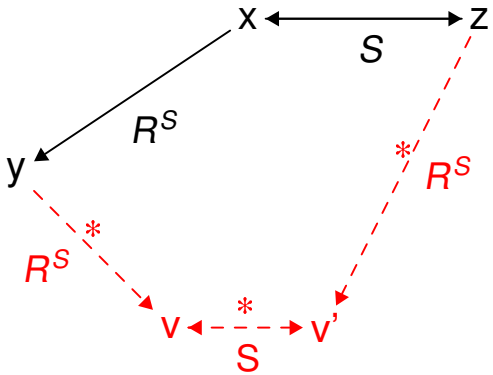
Confluence



Confluence locale



Cohérence



Cohérence locale

Convergence de la récriture modulo

Théorème (Jouannaud & Kirchner, 1984)

$\mathscr{A}$ un ensemble, $\to_R$, $\to_S$ et $\to_{R^S}$ trois relations sur $\mathscr{A}$, avec $\to_R \subseteq \to_{R^S} \subseteq \leftarrow_{R/S}$ et $\leftarrow_{R/S}$ bien fondée Les propriétés suivantes sont équivalentes :

1. *$\to_R$ est $\to_{R^S}$-Church-Rosser modulo $\to_S$,*
2. *$\to_{R^S}$ est confluente et cohérente modulo $\to_S$,*
3. *$\to_{R^S}$ est localement confluente et localement cohérente avec $\to_R$ modulo $\to_S$,*
4. *pour tous éléments x et y de $\mathscr{A}$, $x \overset{*}{\longleftrightarrow}_{R \cup S} y$ si et seulement si pour toutes les formes normales x' de x et toutes les formes normales y' de y pour $\to_{R^S}$, $x' \overset{*}{\longleftrightarrow}_S y'$.*

Un cas pratique important : la récriture AC-étendue

infixe		préfixe
$x + y = y + x$	(C)	$f(x, y) = f(y, x)$
$(x + y) + z = x + (y + z)$	(A)	$f(f(x, y), z) = f(x, f(y, z))$

(C) ne s'oriente pas ($a + b \to b + a \to a + b \to \ldots$)

en présence de (C), (A) ne s'oriente pas non plus

si $(x + y) + z \to x + (y + z)$ alors

$(a + b) + c \to_A a + (b + c) =_C (c + b) + a \to_A c + (b + a) =_C (a + b) + c \to_A$

si $x + (y + z) \to (x + y) + z$ alors

$a + (b + c) \to_A (a + b) + c =_C c + (b + a) \to_A (c + b) + a =_C a + (b + c) \to_A$

Cohérence locale de la récriture AC-étendue

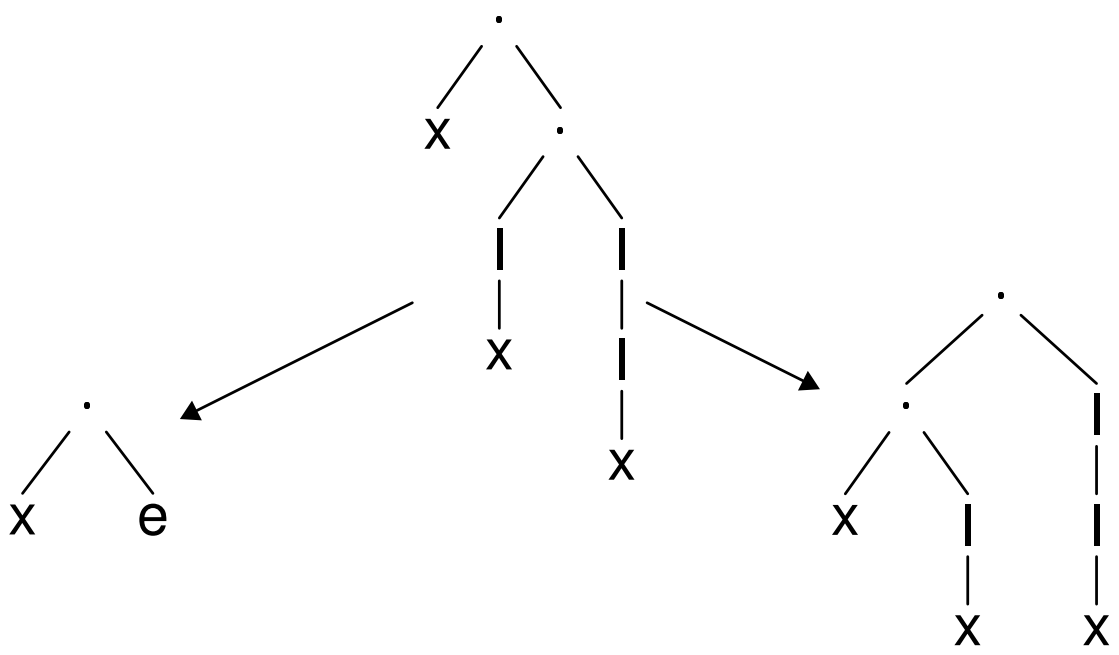
Proposition

- *La cohérence locale de* $\rightarrow_{AC\setminus R}$ *avec (C) est toujours acquise.*
- *Si pour toute règle de R de la forme* $l_1 + l_2 \rightarrow r$,
  R contient $l_1 + l_2 + x \rightarrow r + x$, $x \notin Var(l_1 + l_2) \cup Var(r)$, $\rightarrow_{AC\setminus R}$ *est localement cohérente avec (A).*

$l_1 + l_2 + x \rightarrow r + x$: extension (AC) de $l_1 + l_2 \rightarrow r$

Confluence locale de la récriture

$$R = \left\{ \begin{array}{rcl} x \cdot e & \rightarrow & x \\ x \cdot I(x) & \rightarrow & e \\ x \cdot (y \cdot z) & \rightarrow & (x \cdot y) \cdot z \end{array} \right\}$$



D'où vient le problème ?

$$x \cdot (l(x) \cdot l(l(x)))|_\Lambda = x \cdot (y \cdot z)\{y \mapsto l(x); z \mapsto l(l(x))\}$$

$$x \cdot (l(x) \cdot l(l(x)))|_2 = x \cdot l(x)\{x \mapsto l(x)\}$$

2 réductions possibles à des positions « incompatibles »

test possible directement sur les règles : le problème d'unification

$$x' \cdot (y' \cdot z')|_2 = x \cdot l(x)$$

a des solutions

Unification

Unification syntaxique : Définition

Définition (Problème)

$\mathcal{T}(\mathcal{F}, \mathcal{X})$ *une algèbre de termes. Un problème d'unification est*

- $\top$
- $\bot$
- $s_1 = t_1 \wedge \ldots \wedge s_n = t_n$

Définition (Solutions)

- *Toute substitution est solution de* $\top$,
- *aucune substitution n'est solution de* $\bot$,
- σ *est solution de* $s_1 = t_1 \wedge \ldots \wedge s_n = t_n$ *si pour tout* $i = 1, \ldots, n$, $s_i\sigma = t_i\sigma$.

$\mathcal{U}(P)$ ensemble des solutions de P

Unification syntaxique : unitaire

Théorème

Soit $\mathcal{T}(\mathcal{F}, \mathcal{X})$ une algèbre de termes et soit P un problème d'unification dans cette algèbre. Alors $\mathcal{U}(P)$ vérifie l'une des propriétés suivantes :

- *$\mathcal{U}(P)$ est vide,*
- *$\mathcal{U}(P)$ est non vide, et admet une substitution principale, unique à renommage près μ :*

$$\mathcal{U}(P) = \{\mu\sigma \mid \sigma \text{ substitution}\}$$

$\mathrm{mgu}(P)$ pour *most general unifier*

Problèmes équivalents

Définition

P_1 et P_2 deux problèmes sont équivalents si

$$\mathscr{U}(P_1) = \mathscr{U}(P_2)$$

Exemple : $x = f(y, g(y)) \wedge y = a$ et $f(x, z) = f(f(y, g(a)), z) \wedge y = a$

$$\{x \mapsto f(a, g(a)),\ y \mapsto a\}$$

Formes résolues

problèmes en forme résolue : solutions immédiates

Définition

P est en forme résolue si P est égal à

- $\top$
- $\bot$
- $x_1 = t_1 \wedge \ldots \wedge x_n = t_n$,
  - *x_i sont des variables deux à deux distinctes,*
  - *les t_j ne contiennent pas les variables x_i.*

Solutions des problèmes en forme résolue

Proposition

$P \equiv x_1 = t_1 \wedge \ldots \wedge x_n = t_n$ en forme résolue, θ la substitution

$$\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$$

alors

$$\mathscr{U}(P) = \{\theta\sigma \mid \sigma \text{ substitution}\}$$

Transformation en forme résolue : règles d'inférence I

Trivial $$\frac{s = s}{\top}$$

Decompose $$\frac{f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n)}{s_1 = t_1 \wedge \ldots \wedge s_n = t_n}$$

Clash $$\frac{f(s_1, \ldots, s_n) = g(t_1, \ldots, t_m)}{\bot} \quad \text{si } f \neq g$$

Transformation en forme résolue : règles d'inférence II

Union Var. $$\frac{x = y \wedge P}{x = y \wedge P\{x \mapsto y\}} \quad \text{si } x, y \in \mathrm{Var}(P)$$

Var. Rep. $$\frac{x = s \wedge P}{x = s \wedge P\{x \mapsto s\}} \quad \text{si } x \in \mathrm{Var}(P) \backslash \mathrm{Var}(s) \text{ et } s \notin \mathscr{X}$$

Merge $$\frac{x = s \wedge x = t}{x = s \wedge s = t} \quad \text{si } x \in \mathscr{X}, s, t \notin \mathscr{X} \text{ et } \mathrm{size}(s) \leqslant \mathrm{size}(t)$$

Occur Check $$\frac{x_1 = t_1[x_2]_{p_1} \wedge \ldots x_n = t_n[x_1]_{p_n}}{\bot} \quad \text{si } p_1 \cdot \ldots \cdot p_n \neq \Lambda$$

Correction I

Théorème

Pour toute règle d'inférence de l'unification syntaxique,

$\frac{P}{P'}$ *si C, si P satisfait C et* $\sigma \in \mathscr{U}(P')$, *alors* $\sigma \in \mathscr{U}(P)$.

Pas de nouvelles solutions introduites

Correction II

Théorème

Pour toute règle d'inférence de l'unification syntaxique,

$\frac{P}{P'}$ *si* C, *si* P *satisfait* C *et* $\sigma \in \mathscr{U}(P)$, *alors* $\sigma \in \mathscr{U}(P')$.

Pas de solutions perdues

Terminaison

Théorème

P, problème d'unification, pas de séquence infinie

$$P \equiv P_0 \rightarrow_U P_1 \rightarrow_U \ldots \rightarrow_U P_n \rightarrow_U P_{n+1} \ldots$$

telle que P_{n+1} est obtenu à partir de P_n en appliquant une des règles d'unification.

Pas de calcul infini

Mesure $\Phi(P)$

Définition

- *Une variable x est résolue dans P si x apparaît exactement une fois dans* $P \equiv x = s \wedge Q$ *(*$x \notin Var(s) \cup Var(Q)$*).*
- *La taille de* $s = t$ *est égale à* $(\max(size(s), size(t)))$.

$\Phi(P) = (\Phi_1(P), \Phi_2(P), \Phi_3(P))$

- $\Phi_1(P)$: nombre de variables non résolues dans P.
- $\Phi_2(P)$: multi-ensemble des tailles de ses équations.
- $\Phi_3(P)$: nombre d'équations dont l'un des membres (au moins) est une variable.

$$P > Q \text{ si } \Phi(P) > \Phi(Q)$$

Décroissance de la mesure

	Φ_1	Φ_2	Φ_3
Trivial	$\geqslant$	$>$	
Décomposition	$\geqslant$	$>$	
Incompatibilité	$\geqslant$	$>$	
Union de deux variables	$>$		
Remplacement de variable	$>$		
Fusion	$\geqslant$	$\geqslant$	$>$
Test d'occurrence	$\geqslant$	$>$	

Complétude

Théorème

Soit P un problème d'unification sur lequel aucune des règles d'unification ne peut s'appliquer. Alors P est en forme résolue.

Formes normales = formes résolues

Unification syntaxique : unitaire

Corollaire

P un problème d'unification. Alors $\mathscr{U}(P)$ vérifie l'une des propriétés suivantes :

- $\mathscr{U}(P)$ *est vide,*
- $\mathscr{U}(P)$ *est non vide, il existe μ unique à renommage près :*

$$\mathscr{U}(P) = \{\mu\sigma \mid \sigma \text{ substitution}\}$$

Démonstration.

P' une forme résolue/normale de P :

- obtenue en temps fini
- $\mathscr{U}(P') = \mathscr{U}(P)$
-
  - $P' = \bot, \mathscr{U}(P') = \varnothing$
  - $P' = \top, \mathrm{mgu}(P') = \{\}$
  - $P' = x_1 = t_1 \wedge \ldots, \mathrm{mgu}(P') = \{x_1 \mapsto t_1, \ldots\}$ + unicité

Exemple I

$$\text{Décomposition}\ \frac{f(a,b) = f(a,a)}{a = a \wedge b = a}$$

$$\text{Trivial}\ \frac{a = a \wedge b = a}{b = a}$$

$$\text{Incompatibilité}\ \frac{b = a}{\bot}$$

$$\mathscr{U}\left(f(a,b) = f(a,a)\right) = \varnothing$$

Exemple II

$$\text{Décomposition}\ \frac{f(x,y) = f(z,z)}{x = z \wedge y = z}$$

$$\mathscr{U}\left(f(x,y) = f(z,z)\right) = \{x \mapsto z, y \mapsto z\}$$

Exemple III

$$\text{Décomposition}\ \frac{f(g(x), f(y,z)) = f(x,a)}{g(x) = x \wedge a = f(y,z)}$$

$$\text{Test d'occurrence}\ \frac{g(x) = x \wedge a = f(y,z)}{\bot}$$

$$\mathscr{U}\left(f(g(x), f(y,z)) = f(x,a)\right) = \varnothing$$

Exercices

$$f(x, f(a, b)) = f(f(y, z), y)$$

$$f(x, f(a, y)) = f(f(b, z), x)$$

$$f(g(a), f(y, z) = f(x, x)$$

$$f(x, f(x, v)) = f(f(y, z), y)$$

$$f(x, f(x, v)) = f(f(y, z), y)$$

Un véritable algorithme

CAML

Récriture

(suite de la suite)

Paires critiques : définition

essence de la (non-)confluence locale

Definition

R un système de récriture ; $l \to r, g \to d \in R$ se superposent
s'il existe ρ renommage de l et $p \in \mathrm{Pos}(l)$ avec

- $l(p) \notin \mathscr{X}$
- $l\rho|_p$ et g unifiables, $\mu = \mathrm{mgu}(l\rho|_p = g)$

La paire critique de $g \to d$ sur $l \to r$ (à la position p) est

$$r\rho\mu = (l\rho[d]_p)\mu$$

Une règle peut se superposer sur elle-même

Exemple

$(\mathscr{S}, \mathscr{F}, \tau)$ signature monosortée

$$\begin{aligned} \mathscr{S} &= \{s\} \\ \mathscr{F} &= \{e, I, \cdot\} \\ \tau(e) &= s \\ \tau(I) &= s \to s \\ \tau(\cdot) &= s \times s \to s \end{aligned}$$

$(x \cdot y) \cdot z \to x \cdot (y \cdot z)$ se superpose sur elle-même en 1 :

$$\mathrm{mgu}((x' \cdot y') \cdot z'|_1 = \mu = (x \cdot y) \cdot z) = \{x' \mapsto x \cdot y; y' \mapsto z\}$$

paire critique $r'\mu = l'[r]_1\mu$:

$$x' \cdot (y' \cdot z')\{x' \mapsto x \cdot y; y' \mapsto z\} = (x' \cdot y') \cdot z'[x \cdot (y \cdot z)]_1\mu$$
$$(x \cdot y) \cdot (z \cdot z') = (x \cdot (y \cdot z)) \cdot z'$$

paire joignable

Exercice

Paires critiques de $x \cdot e \to x$ et $(x \cdot y) \cdot z \to x \cdot (y \cdot z)$?

Théorème (Huet, 1980)

Un système de récriture est localement confluent si et seulement si toutes ses paires critiques sont localement confluentes.

Schéma de démonstration : 3 cas

$$u \to^{p}_{l \to r, \sigma} s \quad \text{et} \quad u \to^{q}_{g \to d, \tau} t$$

$l \to r$ déjà renommée

- cas disjoint, $p || q$, $p = p' \cdot i \cdot p''$, $q = p' \cdot j \cdot q''$, $i \neq j$
- superposition dans les variables, $q = p \cdot q' \cdot q''$ avec $l(q') = x \in \mathscr{X}$
- superposition dans les feuilles, $q = p \cdot q'$ avec $q' \in \mathrm{Pos}(l)$ et $l(q') \notin \mathscr{X}$

Schéma de démonstration : cas disjoint

$p||q, p = p' \cdot i \cdot p'', q = p' \cdot j \cdot q'', i \neq j$

Schéma de démonstration : superposition dans les variables

$q = p \cdot q' \cdot q''$ avec $l(q') = x \in \mathscr{X}$

Schéma de démonstration : superposition dans les termes

$q = p \cdot q'$ avec $q' \in \mathrm{Pos}(l)$ et $l(q') \notin \mathscr{X}$