920

NOM : PINAULT Prénom : Lauveline Jury :

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi : 920. Réécriture et formes normales. Exemples.

Autre sujet :

I) Contexte et motivation

1) De la réécriture partout.

Exple 1 (Calcul formel). Différentiation symbolique :

$$\begin{cases} Dx(X) \to 1 \\ Dx(Y) \to 0 \\ Dx(u+v) \to Dx(u) + Dx(v) \\ Dx(u*v) \to (Dx(u)*v) + (u*Dx(v)) \end{cases}$$

Exple 2 (Théories équationnelles). Théorie des groupes.

$$\begin{cases} (x*y)*z = x*(y*z) \\ e*x = x \\ x^{-1}*x = e \end{cases}$$

Exple 3 (Programmation fonctionnelle). Factorielle.

```
fun fact(0) = 1
  | fact(n+1) = (n+1)* fact(n)
```

Exple 4 (Grammaire). Fractions rationnelles.

$F, G := P \mid P/Q \mid F+G \mid F*G$. P, Q polynomes

2) Formalisation de la notion de réécriture

a) Définition et exemples

Def 5 (SR) Un système de réécriture est une paire $(A, \to)$ où A est un ensemble et $\to$ une relation binaire sur A. On écrit $a \to b$ pour $(a,b) \in \to$. Et on note :

- $\xrightarrow{n}$: $\to \circ \cdots \circ \to$, la composition de $\to$ n fois pour $n \in \mathbb{N}$
- $\xrightarrow{=}$: la clôture réflexive de $\to$
- $\xrightarrow{+}$: la clôture transitive de $\to$
- $\xrightarrow{*}$: la clôture réflexive et transitive de $\to$
- $\leftarrow$: $(\to)^{-1}$, l'inverse de $\to$
- $\leftrightarrow$: la clôture symétrique de $\to$
- $\xleftrightarrow{+}$: la clôture symétrique et transitive de $\to$
- $\xleftrightarrow{*}$: la clôture réflexive, symétrique et transitive de $\to$.

Exple 6 (SRM). Un système de réécriture de mots est la donnée d'un alphabet Σ et d'un ensemble de règles $\begin{cases} \Sigma^* \to \Sigma^* \\ r_i \mapsto l_i \end{cases}$. Alors $A = \Sigma^*$ et $\to = \{(u r_i v, u l_i v),\ u, v \in \Sigma^*,\ r_i \to l_i\}$.

Exple 7 (SRT) Un système de réécriture de termes est la donnée d'un langage $\mathcal{L}$ de constantes et de fonctions et d'un ensemble de règles $\begin{cases} \mathcal{T}(\mathcal{L}) \to \mathcal{T}(\mathcal{L}) \\ r_i \mapsto l_i \end{cases}$ où $\mathcal{T}(\mathcal{L})$ est l'ensemble des termes formés à partir de $\mathcal{L}$. Alors $A = \mathcal{T}(\mathcal{L})$ et $\to = \{(s,t);\ s,t \in \mathcal{T}(\mathcal{L}),\ \exists p, \sigma\ s|_p = l_i\sigma,\ t = s[r_i\sigma]_p,\ r_i \to l_i\}$. (voir fig 1, annexe).

b) Propriétés possibles d'un SR

Def 8 Soit $(A, \to)$ un SR. On dit que :

- x est réductible si $\exists y,\ x \to y$. Sinon on dit que x est irréductible ou en forme normale. Si $\exists y,\ x \xrightarrow{*} y$ et que y est irréductible on dit que y est une forme normale de x. Si elle est unique, on la note $x\downarrow$
- x et y sont joignables si $\exists z,\ x \xrightarrow{*} z$ et $y \xrightarrow{*} z$. On note alors $x \downarrow y$

Def 9 Soit $(A, \to)$ un SR. On dit qu'il est :

- normalisant si tout élément a un forme normale

- terminant si il n'existe pas de réécriture infinie
- Church-Rosser si $\forall x,y \quad x \overset{*}{\leftrightarrow} y \Rightarrow x \downarrow y$
- Confluent si $\forall x, y_1, y_2 \quad y_1 \overset{*}{\leftarrow} x \overset{*}{\rightarrow} y_2 \Rightarrow y_1 \downarrow y_2$
- Convergent si il est terminant et confluent (cf annexe, fig 2).

Exple 10. $A = \mathbb{N} \setminus \{0,1\}$, $\rightarrow = \{(m,n),\ m > n \wedge n \mid m\}$
Ce système termine mais n'est pas convergent.

Exple 11. $A = \{a,b\}^*$, $\rightarrow = \{(ubav, uabv), u,v \in A\}$
Ce système est convergent.

Exple 12.



Ce système est confluent et normalisant mais pas terminant.

Prop 13. Church-Rosser $\Leftrightarrow$ confluent.

3. Les questions que l'on se pose

Exple 14. (Théories équationnelles). Est-ce que $a = b$? (par exemple est-ce que $xx^{-1} = e$?)
Ce problème appelé problème du mot en général se reformule comme le problème de savoir, étant donné un SR $(A, \rightarrow)$ et $a, b \in A$, si $a \overset{*}{\leftrightarrow} b$.
Une manière de le résoudre est de comparer, si elles existent, $a\downarrow$ et $b\downarrow$.
Se pose alors la question de l'existence et l'unicité d'une forme normale.

Exple 15. (Calculs et programmation fonctionnelle) Est-ce que le calcul va aboutir ? (est-ce que le programme va s'arrêter ?) Et est-il déterministe ?
On se demande si les éléments ont une forme normale et si elle est unique.

Exple 16. (Grammaires). Est-ce qu'on peut réécrire l'ensemble généré sous une forme normale plus facile à manipuler ? (par exemple existence et unicité de la décomposition en éléments simples pour les fractions rationnelles).
Là est surtout important l'existence d'une telle forme normale, et aussi devoir un algorithme permettant de l'obtenir.

II Existence et unicité d'une forme normale (FN)

1 Existence ~~et lien avec la terminaison~~

Prop 17. (Importante pour travailler avec des systèmes terminants). Induction Bien Fondée (IBF)
Un SR est terminant ssi il vérifie l'induction bien fondée : $[\forall x \in A\ (\forall y \in A\ x \overset{+}{\rightarrow} y \Rightarrow P(y)) \Rightarrow P(x)] \Rightarrow \forall x \in A\ P(x)$

a) Lien entre l'existence d'une FN et la terminaison.

Prop 18. Terminant $\Rightarrow$ normalisant.

Prop 19. Si un système est terminant alors on dispose d'un algorithme permettant de trouver une FN.

b) Prouver la terminaison.

Prop 20. Le problème de déterminer si un SR est terminant est en général indécidable. DVT 1

Prop 21. Soit R un SRT tel que pour chaque règle $l_i \rightarrow r_i$, $Var(r_i) = \emptyset$. Alors le problème de savoir si R termine est décidable.

Prop 22. Si un système $(A, \rightarrow)$ est à branchement fini (un élément a un nombre fini de successeurs) alors il termine ssi il existe un plongement monotone de $(A, \rightarrow)$ dans $(\mathbb{N}, >)$.

Exple 23. Un SRS dont les règles font diminuer la longueur des mots est terminant.

Exple 24. $\begin{cases} (i+1, j) \rightarrow (i, 2) \\ (i, j+1) \rightarrow (i, j) \end{cases}$ est terminant mais il n'existe pas de plongement monotone dans $(\mathbb{N}, >)$.

Prop 25. Le produit lexical de deux relation terminantes est terminant.

Prop 26. Un ordre multiset basé sur un ordre strict est strict.

c) Stratégies de réécriture

Idée 27. Dans le cas où un système est normalisant mais pas terminant on peut essayer de mettre en place des stratégies de réduction pour arriver à une forme normale.

Exple 28. Pour le λ-calcul, la stratégie de réécriture à gauche donne toujours une forme normale s'il en existe une.

2 Unicité ~~et lien avec la confluence~~

a) Lien entre l'unicité d'une FN et la confluence

Prop29. Si un système est confluent alors tout élément a au plus une forme normale.

Prop30. Si un système est normalisant et confluent, chaque élément a une forme normale et alors $\forall x, y \quad x \overset{*}{\leftrightarrow} y \Leftrightarrow x\downarrow = y\downarrow$ (résolution du problème du mot).

Rq31. Même si on a l'unicité et l'existence, on ne dispose pas forcément d'un moyen effectif de trouver la forme normale.

b) Prouver la confluence.

Prop32. Le problème de déterminer si un SR est confluent est indécidable.

Def33. Un SR est dit :
- localement confluent si $\forall x, y_1, y_2, \; y_1 \leftarrow x \rightarrow y_2 \Rightarrow y_1 \downarrow y_2$
- fortement confluent si $\forall x, y_1, y_2, \; y_1 \leftarrow x \rightarrow y_2 \Rightarrow \exists z \; y_1 \overset{=}{\rightarrow} z \overset{=}{\leftarrow} y_2$
- avoir la propriété du diamant si $\forall x, y_1, y_2, \; y_1 \leftarrow x \rightarrow y_2 \Rightarrow \exists z, \; y_1 \rightarrow z \leftarrow y_2$.

(voir annexe, figure 2)

Prop34. Confluent $\Leftarrow$ fortement confluent $\Leftarrow$ diamant.

Prop35. Si un système est terminant alors il est confluent ssi il est localement confluent (Lemme de Newman).

Prop36. Si $\rightarrow_1$ et $\rightarrow_2$ sont confluents et commutent alors $\rightarrow_1 \cup \rightarrow_2$ est confluent.

Prop37. Un SRT est localement confluent ssi toutes ses paires critiques sont jointables ($\Rightarrow$ décidable).

c) Complétion

Algo38. (Knuth-Bendix). On peut essayer de compléter un SR en un SR confluent grâce à l'algorithme de Knuth-Bendix.

d) Stratégies de réécriture

Idée39. Même si le SR n'est pas confluent, on peut avoir un calcul déterministe en choisissant une stratégie de réécriture.

III Exemples de SR et de formes normales.

1 λ-calcul et programmation fonctionnelle

Prop40. Le λ-calcul vérifie la propriété de Church-Rosser et est donc confluent.

Prop41. Le λ-calcul n'est pas terminant. Mais la stratégie de réécriture à gauche donne une forme normale si elle existe.

2 Formes normales du calcul des prédicats

Prop42. Une formule propositionnelle peut être mise sous forme normale conjonctive (CNF) avec le SR suivant :

$$\begin{aligned}
&\varphi \Leftrightarrow \psi \rightarrow (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)\\
&\varphi \Rightarrow \psi \rightarrow \neg\varphi \vee \psi\\
&\neg\neg\varphi \rightarrow \varphi\\
&\neg(\varphi \wedge \psi) \rightarrow \neg\varphi \vee \neg\psi\\
&\neg(\varphi \vee \psi) \rightarrow \neg\varphi \wedge \neg\psi\\
&\varphi \vee (\psi \wedge \chi) \rightarrow (\varphi \vee \psi) \wedge (\varphi \vee \chi)\\
&(\varphi \wedge \psi) \vee \chi \rightarrow (\varphi \vee \chi) \wedge (\psi \vee \chi)
\end{aligned}$$

Prop43. De même, elle peut être mise sous forme normale disjonctive (DNF).

Idée44. Ces formes normales permettent des facilités par exemple pour tester des satisfiabilités ou pour designer un circuit. Cependant elles peuvent avoir des tailles exponentielles en la taille originale de la formule.

3 Mise sous forme prénexe

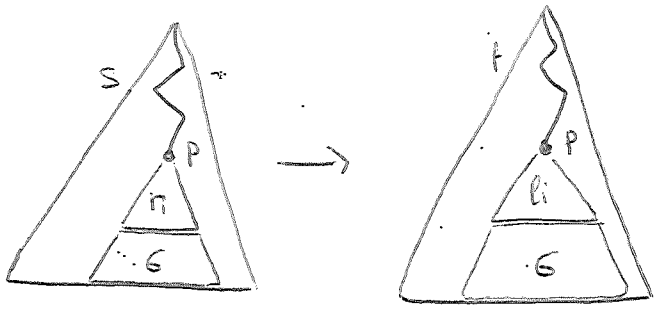
Prop45. Une formule du premier ordre peut être mise sous forme prénexe $Q_{x_1} \ldots Q_{x_n} G$ où $Q_i \in \{\forall, \exists\}$ et G est sans quantificateur par le SR suivant :

$$\begin{aligned}
&\neg Q x \, A \rightarrow Q^d x (\neg A)\\
&(Q x A) \oplus B \rightarrow Q x (A \oplus B)\\
&A \oplus (Q x B) \rightarrow Q x (A \oplus B)\\
&(Q x A) \Rightarrow B \rightarrow Q^d x (A \Rightarrow B)\\
&A \Rightarrow (Q x B) \rightarrow Q x (A \Rightarrow B)
\end{aligned}$$

Application46. L'arithmétique de Presburger est décidable.

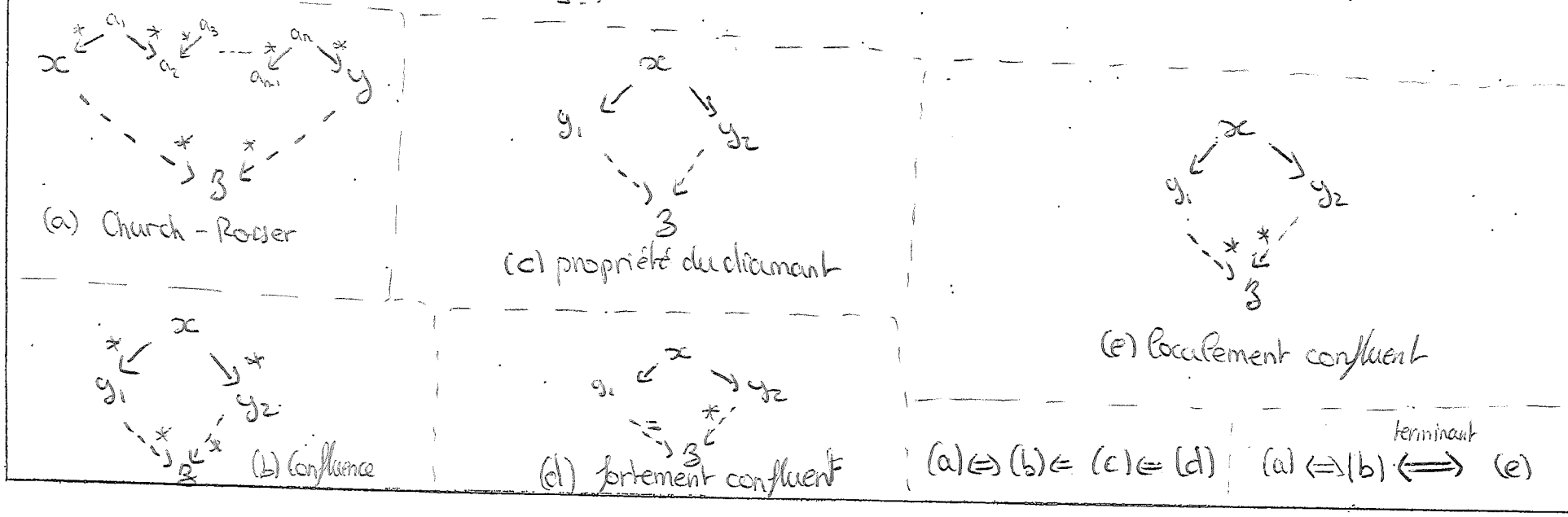
DVT 2

FIG 1 : Schéma de l'application de la règle $r_i \to l_i$ d'un SRT dans un terme s à la position p avec la substitution σ :



Références : Baader & Nipkow, Term Rewriting and all that
Lalement, Logique Réduction Résolution
Robinson & Voronkov, Handbook of automated Reasoning

FIG 2 : Les différentes formes de confluence
($\longrightarrow = \forall$ $\dashrightarrow = \exists$)


(a) Church - Rosser
(b) Confluence
(c) propriété du diamant
(d) fortement confluent
(e) localement confluent

$(a) \Leftrightarrow (b) \Leftarrow (c) \Leftarrow (d)$

$(a) \Leftrightarrow (b) \overset{\text{terminant}}{\Longleftrightarrow} (e)$