NOM : PECATTE **Prénom :** Timothée **Jury :**

Algèbre ← Entourez l'épreuve → **Analyse**

Sujet choisi : 920. Réécriture et forme normale. Exemples.

Autre sujet :

I. Réécriture : définitions et propriétés

I.1. Motivations : 3 exemples

Exemple 1 : L'île aux caméléons

Exemple 2 : Haricots dans l'urne

Exemple 3 : Hercule contre l'hydre ⇝ Figure 1

I.2. Premières définitions et questions fondamentales :

Déf 4 : Un système de réduction est une paire $(A, \to)$ avec $\to \subseteq A \times A$.

Déf 5 : Un élément a de $(A,\to)$ est dit en forme normale si $\forall b \in A, (a,b) \notin \to$

Questions :

(i) Pour $a, b \in A$, est ce que $a \to^* b$? ⇝ ex 1

(ii) Pour $a \in A$, est ce qu'il existe un unique $b \in A$ en forme normale tel que $a \to^* b$? ⇝ ex 2

(iii) Est ce que pour tout $a \in A$, il existe b en forme normale tel que $a \to^* b$? ⇝ ex 3

Exemple 6 : $(\mathbb{N}, <)$

Exemple 7 : Graphe orienté

I.3. Formalisation et terminologie :

Déf 8 : (Opérations sur les relations binaires.)

Etant donné une relation binaire $\to$, on définie :

- $\to^0 = \{(x,x) \mid x \in A\}$
- $\to^{i+1} = \to^i \circ \to$ avec $R \circ S = \{(x,z) \mid \exists y \text{ tq } (x,y) \in R \text{ et } (y,z) \in S\}$
- $\to^+ = \bigcup_{i>0} \to^i$ la clôture transitive de $\to$
- $\to^* = \to^+ \cup \to^0$ la clôture réflexive, transitive de $\to$
- $\to^{-1} = \leftarrow = \{(y,x) \in A^2 \mid (x,y) \in \to\}$
- $\leftrightarrow = \to \cup \leftarrow$

Déf 9 : (Terminologie usuelle)

Etant donné un système de réduction $(A,\to)$ et $x \in A$, on dit que :

- x est réductible si $\exists y \in A$, $x \to y$
- x est en forme normale si $\forall y \in A$, $x \not\to y$
- $y \in A$ est une forme normale de x si $x \to^* y$ et y est en forme normale
- $y \in A$ est un successeur direct (ou fils) de x si $x \to y$
- $y \in A$ est un successeur de x si $x \to^+ y$
- x et y sont joignables si $\exists z$, $x \to^* z$ et $y \to^* z$, noté $x \downarrow z$

Exemple 10 : Soit le système de réduction suivant : $(\mathbb{N}, \to)$ avec $n \to m$ si $n > m$ et $m \mid n$

(i) $n \in \mathbb{N}$ est en forme normale si n est premier

(ii) p forme normale de n si p facteur premier de n

(iii) $\to^+ = \to$ car "divise" est transitif

(iv) $\leftrightarrow^* = \mathbb{N} \times \mathbb{N}$

I.4. Propriétés d'un système de réduction :

Déf 11 : (Normalisation) Etant donné un système de réduction $(A,\to)$, on dit que

- $(A,\to)$ est faiblement normalisant (WNF) si tout élément de A possède une forme normale
- $(A,\to)$ est fortement normalisant, ou termine, si toute réduction est finie (de manière équivalente, si $(A,\leftarrow)$ est bien fondé)
- $(A,\to)$ vérifie l'unicité des formes normales si $a \leftrightarrow^* b \Rightarrow a = b$ pour a,b formes normales
- $(A,\to)$ est convergent s'il est fortement normalisant et qu'il vérifie l'unicité

Exemple 11 : L'exemple 10 est fortement normalisant mais pas convergent.

Rem 12 : Fortement normalisant ⇒ faiblement normalisant

Equivalent pour l'unicité ?

Déf 13 : (Confluence) $(A,\to)$ est dit confluent si $y_1 \leftarrow^* x \to^* y_2 \Rightarrow y_1 \downarrow y_2$ ⇝ Figure 2

Rem 14 : Confluence ⇒ unicité des formes normales.

Proposition 15 : Un système de réduction confluent et terminant est convergent

I.5. De la réécriture "concrète" :

Déf 16 : (Signature) Une signature Σ est un ensemble de symbole de fonction où chaque $f \in \Sigma$ est associé à un entier positif n, appelé l'arité de f. Les éléments d'arité 0 sont appelés les constantes.

Exemple 17 :

- $\Sigma_{\mathbb{N}} = \{0_0, S_1\}$
- $\Sigma_{groupe} = \{e_0, i_1, *_2\}$
- $\Sigma_{arbre} = \{F_0, N_2\}$

Déf 18 : (Termes) Etant donné une signature Σ et X un ensemble de variable, avec $\Sigma \cap X = \emptyset$, on définit l'ensemble des termes $T(\Sigma, X)$ par induction :

- $X \subseteq T(\Sigma, X)$
- Pour tout symbole de fonction $f \in \Sigma$ d'arité n, pour tout termes $t_1, \dots, t_n \in T(\Sigma, X)$ on a $f(t_1, \dots, t_n) \in T(\Sigma, X)$

Exemple 19 :

- $T(\Sigma_{\mathbb{N}}, X) = \{ S(S(\dots S(x) \dots)) \mid x \in X \cup \{0\} \}$
- $*_2(i_1(e), *_2(x, i_1(y))) \in T(\Sigma_{groupe}, X)$
- $N_2(N_2(F_0, N_2(F_0, F_0)), F_0) \in T(\Sigma_{arbre}, \emptyset)$

Déf 20 : (Positions) L'ensemble des positions $Pos(s)$ d'un terme s est défini par induction sur le terme :

- Si $s = x \in X$, $Pos(s) := \{\varepsilon\}$ (mot vide)
- Si $s = f(s_1, \dots, s_n)$, $Pos(s) := \{\varepsilon\} \cup \bigcup_{i} \{ip \mid p \in Pos(s_i)\}$

La position ε est appelée la racine du terme.

Exemple 21: $\mathcal{P}os(*_1(u(e_0), *_2(x, u(y)))) = \{\varepsilon, 1, 11, 2, 21, 22, 221\}$

Déf 22: (Sous-terme) Le sous-terme de s, à la position p, est défini par induction sur p:
- $s|_\varepsilon = s$
- $f(s_1, \dots, s_n)|_{iq} = s_i|_q$

Déf 23: (Substitution) Pour t, s deux termes, p une position, le terme $s[t]_p$ est défini par induction sur p:
- $s[t]_\varepsilon = t$
- $f(s_1, \dots, s_n)[t]_{iq} = f(s_1, \dots, s_i[t]_q, \dots, s_n)$

Exemple 24: Notons t le terme de l'exemple 21. $t|_{22} = u(y)$. $t[e_0]_2 = *_2(u(e_0), e_0)$

Déf 25: (Système de réécriture de termes) Étant donné un ensemble d'égalité $E \subseteq T(\Sigma, X) \times T(\Sigma, X)$, on définit la relation de réduction $\to_E$ sur les termes par :

$s \to_E t$ ssi $\exists (\ell, r) \in E$, $p \in \mathcal{P}os(s)$, $\sigma : X \to T(\Sigma, X)$ tel que
- $s|_p = \sigma(\ell)$
- $t = s[\sigma(r)]_p$

II. La terminaison :

$\boxed{\text{Dév 1:}}$ La terminaison d'un système de réduction est indécidable.

II.1. Preuves élémentaires :

Lemme 26: Un système de réduction à branchement fini termine ssi il existe un plongement monotone dans $(\mathbb{N}, >)$

Exemple 27: $S(x) \to x$ sur $T(\Sigma_\mathbb{N}, X)$. On prend $\begin{cases} f(0) = 0 \\ f(S(t)) = f(t) + 1 \end{cases}$

Rem 28: Le plongement peut être dur à trouver, c'est pourquoi on dispose d'autres méthodes.

Déf 29: (Produit lexicographique). Étant donné $(A, <_A)$, $(B, <_B)$, on définit un ordre $<_{lex}$ sur $A \times B$:

$(x, y) <_{lex} (x', y')$ ssi $(x <_A x') \vee (x = x' \wedge y <_B y')$

Th 30: Le produit lexicographique de deux ordres terminant est encore terminant

Exemple 31: L'évaluation de la fonction d'Ackermann termine.

Déf 32: (Multi-ensemble) Un multi-ensemble M sur un ensemble A est une fonction $M : A \to \mathbb{N}$.

Déf 33: (Ordre multi-ensemble) Étant donné un ordre $<$ sur A, on définit l'ordre multi-ensemble $>_{mul}$ par :

$M >_{mul} N$ ssi $\exists X, Y$ tq $\bullet\ \emptyset \neq X \subseteq M$ $\bullet\ N = (M - X) \cup Y$ $\bullet\ \forall y \in Y, \exists x \in X, x > y$

Exemple 35: sur $\mathbb{N}^*$, $u(i+1)v \to uiiv$ termine.

Th 34: L'ordre multi-ensemble $>_{mul}$ termine ssi $>$ termine

II.2. Interprétation polynomiale :

Déf 35: Un ordre $>$ sur $T(\Sigma, X)$ est un ordre de réécriture ssi :

(i) Il est compatible avec Σ : $s_1 > s_2 \Rightarrow f(t_1, \dots, t_{i-1}, s_1, t_{i+1}, \dots, t_n) > f(t_1, \dots, s_2, \dots, t_n)$

(ii) Il est clos par substitution : $s_1 > s_2 \Rightarrow \sigma(s_1) > \sigma(s_2)$ $\forall \sigma \in Subst$

De plus, $>$ est un ordre de réduction s'il est bien fondé

Th 36: Un système de réécriture de termes termine $\Leftrightarrow$ $\exists$ un ordre de réduction $>$ tq $\ell > r$ pour $\ell \to r$

Déf 37: Une interprétation polynomiale d'une signature Σ est Σ-algèbre $\mathcal{A}$ vérifiant
- Les éléments de $\mathcal{A}$ sont les entiers naturels
- Chaque symbole f de fonction est associé avec un polynôme $P_f(X_1, \dots, X_n)$

Th 38: Étant donné une interprétation polynomiale, si l'interprétation $f^{\mathcal{A}}$ de chaque symbole de fonction est monotone, alors le système de réécriture associé termine

Exemple 39: $x \odot (y \oplus z) \to (x \odot y) \oplus (x \odot z)$ $\quad (x \odot y) \odot z \to x \odot (y \odot z)$

On prend $P_\odot := XY$ et $P_\oplus := 2X + Y + 1$

$\ell_1 \rightsquigarrow X(2Y + Z + 1) > r_1 \rightsquigarrow 2XY + XZ + 1$

$\ell_2 \to 4X + 2Y + Z + 3 > r_2 \rightsquigarrow 2X + 2Y + Z + 2$

II.3. Ordres de simplification :

Déf 40: Un ordre $>$ sur $T(\Sigma, X)$ est un ordre de simplification ssi c'est un ordre de réécriture qui vérifie la propriété du sous-terme : $\forall t \in T(\Sigma, X)$, $\forall p \in \mathcal{P}os(t) - \{\varepsilon\}$ on a $t > t|_p$

Exemple 41: Plongement homéomorphe : $s \trianglerighteq t$ si
(i) $s = x = t$ pour $x \in X$
(ii) $s = f(s_1, \dots, s_n)$ et $t = f(t_1, \dots, t_n)$ avec $s_1 \trianglerighteq t_1, \dots, s_n \trianglerighteq t_n$ $\rightsquigarrow$ Figure 3
(iii) $s = f(s_1, \dots, s_n)$ et $s_j \trianglerighteq t$ pour un certain $j \in [\![1, n]\!]$

Lemme 42: Pour tout ordre de simplification $<$ sur $T(\Sigma, X)$, on a $\trianglerighteq \subseteq >$.

$\boxed{\text{Dév 2:}}$ Tout ordre de simplification est un ordre de réduction.

Déf 43: Pour un ordre $<$ sur Σ, on définit l'ordre récursif multi-ensemble $>_{rmo}$ par :

$s = f(s_1, \dots, s_n) >_{rmo} t$ ssi (1) $s_i = t$ ou $s_i >_{rmo} t$ pour $i \in [\![1, n]\!]$
ou (2) $t = g(t_1, \dots, t_m)$ et
soit (2a) $f > g$ et $s >_{rmo} t_i$ pour tout $i \in [\![1, m]\!]$
soit (2b) $f = g$ et $\{s_1, \dots, s_n\} >^{mul}_{rmo} \{t_1, \dots, t_m\}$

Exemple 44: Hercule gagne contre l'hydre

III. La confluence :

$\boxed{\text{Dév 1 (suite):}}$ La confluence d'un système de réécriture est indécidable.

formes normales poly / formes normales preuves

III. 1. Propriétés équivalentes :

Déf 45 : (Church-Rosser) Une réduction $\to$ est CR ssi $x \overset{*}{\leftrightarrow} y \Rightarrow x \downarrow y$ $\rightsquigarrow$ Figure 2

Déf 46 : (Semi-confluence) Une réduction $\to$ est semi-confluente si $y_1 \leftarrow x \overset{*}{\to} y_2 \Rightarrow y_1 \downarrow y_2$

Th 47 : Les trois propriétés suivantes sont équivalentes : (i) $\to$ est confluente
(ii) $\to$ est semi-confluente
(iii) $\to$ est Church-Rosser

Déf 48 : (Confluence locale) Une relation $\to$ est confluente localement si $y_1 \leftarrow x \to y_2 \Rightarrow y_1 \downarrow y_2$

Exemple 49 : $a \leftarrow b \rightleftarrows c \to d$ est localement confluente mais pas confluente.

Déf 50 : $\to$ a la propriété du diamant si $y_1 \leftarrow x \to y_2 \Rightarrow \exists z$ tq $y_1 \to z \leftarrow y_2$

Exemple 51 : L'exemple 49 a la propriété du diamant

Rem 52 : Propriété du diamant $\Rightarrow$ confluence locale

Th 53 : Confluence locale + terminaison $\Rightarrow$ confluence

Lemme 54 : Si $\to_1 \subseteq \to_2 \subseteq \to_1^*$ et que $\to_1$ est confluent, alors $\to_2$ est confluent

Exemple 55 : Sert à montrer la confluence du λ-calcul

III. 2. Paires critiques :

Rem 56 : Lorsqu'on veut prouver confluence locale. $t_1 \xleftarrow{l_1 \to r_1} s \xrightarrow{l_2 \to r_2} t_2$

Avec p_i, σ_i tq $\begin{cases} s_{|p_i} = \sigma_i l_i \\ t_i = s[\sigma_i r_i]_{p_i} \end{cases}$

Rem 57 : Toutes les paires ne sont pas critiques : • $p_1 \| p_2 \Rightarrow t_1 \downarrow t_2$
• $p_2 = p_1 p$ et $p = q_1 q_2$ avec q_1 position d'une variable $\Rightarrow t_1 \downarrow t_2$

$\to$ Figure 4

Déf 58 : Pour $l_i \to r_i$, $i = 1, 2$, tq $Var(l_1 \cup r_1) \cap Var(l_2 \cup r_2) = \emptyset$. Si on a σ et $p \in Pos(l_1)$ tel que $\sigma l_{1|p} = \sigma l_2$, cela détermine une paire critique $\langle \sigma r_1, (\sigma l_1)[\sigma r_2]_p \rangle$

Exemple 59 : $f(f(x)) \to g(x)$ donne lieu à la paire critique $\langle g(f(x)), f(g(x)) \rangle$

Lemme 60 : Si $t_1 \leftarrow s \to t_2$, alors soit $t_1 \downarrow t_2$, soit $t_i = s[u_i]_p$ avec $\langle u_1, u_2 \rangle$ une paire critique.

Th 61 : Un système de réécriture de termes est localement confluent ssi toutes ses paires critiques sont joignables

Corollaire 62 : Un SRT terminant est confluent ssi toutes ses paires critiques sont joignables

Corollaire 63 : La confluence d'un SRT fini et terminant est décidable.

III. 3. Confluence et langages algébriques :

Déf 64 : Une grammaire G est ambiguë s'il existe un mot $w \in \mathcal{L}(G)$ qui possède deux dérivations différentes

Rem 65 : La notion d'ambiguïté est l'opposé de la notion de confluence

Dév 3 : Les contenus de pile des configurations accessibles d'un automate à pile forme un langage Rat.

IV. Des formes normales et du calcul :

Exemple 66 : Réécriture sur les formules booléennes : $\neg(x \wedge y) \to \neg x \vee \neg y$ $\quad \neg\neg x \to x$
$\neg(x \vee y) \to \neg x \wedge \neg y$
montre l'existence d'une CNF équivalente $\quad (a \wedge b) \vee c \to (a \vee c) \wedge (b \vee c)$

Exemple 67 : Réécriture sur les listes d'entiers (sans variable) : $qabr \to qbar$ si $b < a$
On a la confluence et la terminaison $\rightsquigarrow$ unique forme normale correspondant à la liste triée

Exemple 68 : Réécriture sur les polynômes : $D_x(X) \to 1$, $D_x(Y) \to 0$, $D_x(u \times v) \to (u \times D_x(v)) + (D_x(u) \times v)$
Forme normale $\rightsquigarrow$ différentiation symbolique. $D_x(u+v) \to D_x(u) + D_x(v)$,

Exemple 69 : λ-calcul

Exemple 70 : Herbrand-Gödel calculabilité : On travaille sur la signature $\Sigma_{\mathbb{N}}$, on note $\ulcorner n \urcorner = s^n(0)$.

On considère un système d'équation E : $r_1 = s_1, \dots, r_k = s_k$, avec $r_k \equiv P(t_1, \dots, t_n)$.
On dit que P est le symbole principal du système. Deux règles :
(R_1) De $t(x) = s(x)$ on peut dériver $t(\ulcorner n \urcorner) = s(\ulcorner n \urcorner)$
(R_2) Des équations $r = C[f(\ulcorner n_1 \urcorner, \dots, \ulcorner n_m \urcorner)]$ et $f(\ulcorner n_1 \urcorner, \dots, \ulcorner n_m \urcorner) = \ulcorner p \urcorner$, sans variables, on peut dériver $r = C[\ulcorner p \urcorner]$
On dit que $t = s$ peut être dérivé de E, noté $E \vdash_{HG} t = s$, s'il peut être obtenu à partir de $E + (R_1) + (R_2)$.
Une fonction $\phi : \mathbb{N}^k \to \mathbb{N}$ est HG-calculable si $\exists E$ avec P pour lettre principale tq $\phi(n_1, \dots, n_k) = p$ $\Leftrightarrow E \vdash_{HG} P(\ulcorner n_1 \urcorner, \dots, \ulcorner n_k \urcorner) = \ulcorner p \urcorner$

Th 71 : Les fonctions récursives (partielles) sont exactement les fonctions HG-calculables

Figure 1 : Hercule contre l'hydre

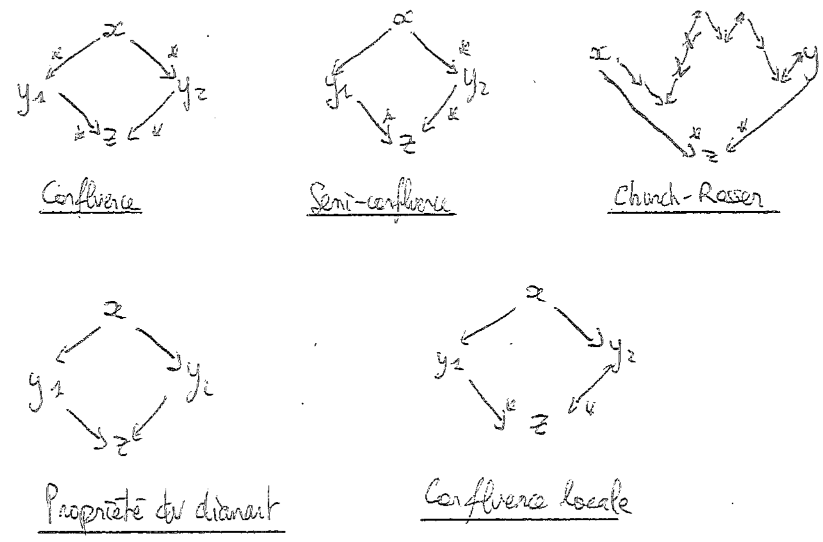

Figure 2 : Différentes notions de confluence

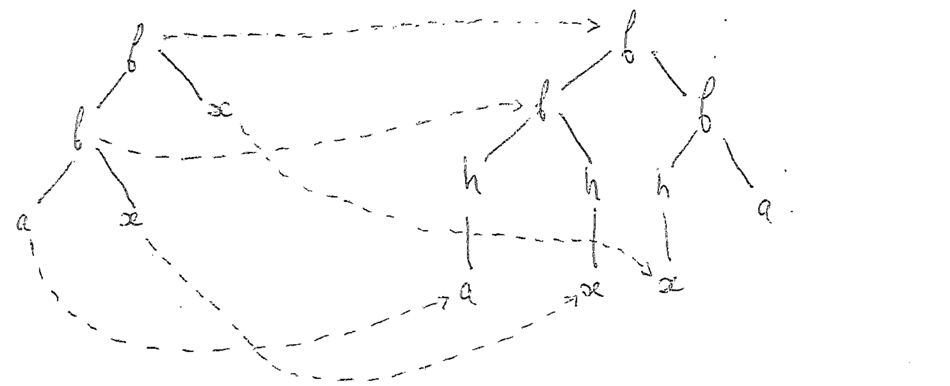

Figure 3 : Plongement homéomorphe de $f(f(a,x),x) \trianglelefteq f(f(h(a),h(x)),f(h(x),a))$

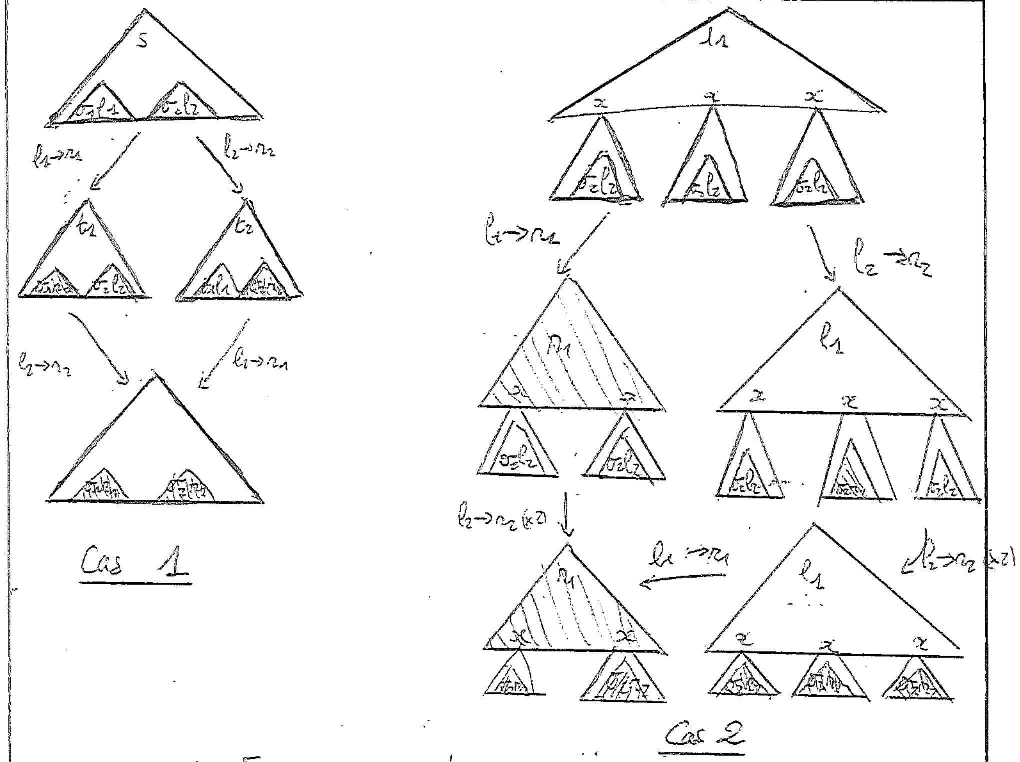

Figure 4 : Fausses paires critiques