Réécritures et formes normales. Exemples.

27/01 2015

920

conséquence logique.

Motivation : à partir d'un système d'égalités, pouvoir définir d'autres égalités, plus faciles à manier (ou plus générales).

Ex : Théorie des groupes. — Égalités

"composition" $\circ$ (binaire) — $(x\circ y)\circ z = x\circ(y\circ z)$

"inverse" i (unaire) — $e\circ x \simeq x$

"neutre" e (0-aire) — $i(x)\circ x \simeq e$.

↳ permet de déduire $e \simeq i(x)\circ x$.

I Formalisation de la théorie équationnelle

A) Généralités sur les langages.

BAA p 34 **Déf 1** : Une signature Σ est un ensemble de symboles de fonctions, chacune possédant une arité n (nombre d'arguments). On note $\Sigma^{(n)}$: fonctions d'arité n. $\Sigma^{(0)}$: symboles de constantes.

BAA p 35 **Déf 2** : Soit Σ une signature et X un ensemble de variables telles que $\Sigma \cap X = \emptyset$. On définit inductivement les termes T (ou $T(\Sigma, X)$) par : $X \subseteq T$ et $\forall n \geq 0, \forall f \in \Sigma^{(n)}, \forall t_1,\dots,t_n \in T, \; f(t_1,\dots,t_n) \in T$.

Exemple 3 : Théorie des groupes. $\Sigma = \{\circ, i, e\}$.

$\circ \in \Sigma^{(2)}$, $i \in \Sigma^{(1)}$, $e \in \Sigma^{(0)}$. Soit $x \in X$. Alors $\circ(x, i(\circ(x,e)))$ est un terme. On pourra noter $x\circ(i(x\circ e))$.

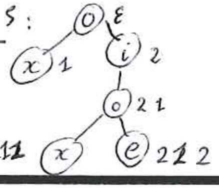
Déf 4 : On peut illustrer un terme par un arbre. On définit inductivement l'ensemble des positions d'un terme s : $Pos(s)$, ensemble de suites de nombres positifs :

- si $x \in X$, et $x = s$, $Pos(s) := \{\varepsilon\}$, soit la suite vide.
- si $s = f(s_1,\dots,s_n)$, $Pos(s) := \{\varepsilon\} \cup \bigcup_{i=1}^{n} \{ip \mid p \in Pos(s_i)\}$.

BAA p 36-37 La taille $|s|$ d'un terme s est le cardinal de $Pos(s)$. Le sous-terme de s à la position p se définit par induction) :

$s|_\varepsilon := s$ et $f(s_1,\dots,s_n)|_{iq} := s_i|_q$.

Exemple 5 :



pour $s = \circ(x, i(\circ(x,e)))$.

$Pos(s) = \{\varepsilon, 1, 2, 21, 211, 212\}$.

$|s| = 6$ $\quad s|_{21} = \circ(x,e)$.

Déf 6 : Une substitution sur $T(\Sigma, X)$ est une application $\sigma : V \to T$ telle que $\sigma(x) \neq x$ pour seulement un nombre fini de x. On l'étend par induction aux termes. Son domaine est $D(\sigma) = \{x \in V ; \sigma(x) \neq x\}$. Un terme t est une instance d'un terme s ssi il existe σ tq $\sigma(s) = t$. BAA p39

Exemple 7 : Sur la théorie des groupes, si $\sigma : x \mapsto (y\circ y)$, alors $\sigma(x\circ i(x\circ e)) = (y\circ y)\circ(i((y\circ y)\circ e))$.

B) Théorie équationnelle.

Déf 8 : Soit Σ une signature, V variables (infini dénombrables). Une identité est une paire $(s,t) \in T\times T$. On note $s \simeq t$. Si E est un ensemble d'identités, on définit la relation de réduction $\to_E \subseteq T\times T$ par : BAA p39

$s \to_E t$ ssi $\exists (l,r) \in E$, $p \in Pos(s)$, $\sigma \in Sub$, tq $s|_p = \sigma(l)$ et $t = s[\sigma(r)]_p$.

Exemple 9 : $G := \{x\circ e \simeq x ; \; x\circ i(x) \simeq e\}$.

$x\circ i(x\circ e) \to_G x\circ i(x) \to_G e$. (cf annexe 1).

Th 10 : Soit E un ensemble d'identités. La relation $\overset{*}{\leftrightarrow}_E$ (fermeture réflexive, transitive et symétrique de $\to_E$) est la plus petite relation d'équivalence sur T qui contient E et qui soit : BAA p41

- clos par substitution : $s \overset{*}{\leftrightarrow}_E t$ ssi $\forall \sigma$, $\sigma(s) \overset{*}{\leftrightarrow}_E \sigma(t)$
- clos par Σ-opérations : si $s_1 \equiv t_1, \dots, s_n \equiv t_n$, $\forall f \in \Sigma^{(n)}$, alors $f(s_1,\dots,s_n) \equiv f(t_1,\dots,t_n)$.

Exemple 11 : Avec les trois égalités de l'introduction sur la théorie des groupes (associativité, neutre à droite et inverse à gauche), $\overset{*}{\leftrightarrow}_E$ contiendra l'inverse et le neutre à gauche, l'unicité de l'inverse...

Déf 12 : Soit Σ une signature et E un ensemble de Σ-identités. Soit $\mathcal{M}$ constitué d'un domaine A et d'un morphisme qui à tout f de $\Sigma^{(n)}$, associe une fonction $f^{\mathcal{M}} : A^n \to A$. $\mathcal{M}$ est appelé modèle (noté $\mathcal{M} \models E$) si chaque identité de E tient dans $\mathcal{M}$. BAA p50

Déf 13 : La relation $s \simeq t$ est conséquence sémantique de E ($E \models s \simeq t$) si elle tient dans tout modèle de E. La relation $\simeq_E$ définie par $\simeq_E := \{(s,t) \in T\times T \mid E \models s \simeq t\}$ est appelée théorie équationnelle induite par E. BAA p50

Exemple 14 : Modèles de la théorie des groupes ; S_n, $M_n(\mathbb{Z})$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{F}_p$...

Prop 15 : La théorie équationnelle est close par morphisme ; pour tout morphisme ϕ sur T, $s \approx_E t$ implique $\phi(s) \approx_E \phi(t)$.

BAA p55 Th 16 (de Birkhoff) : Soit E un ensemble d'identités. Alors $\xleftrightarrow{*}_E$ coïncide avec $\approx_E$.

II Systèmes de réduction et de réécriture

BAA p7 Déf 17 : Un système de réduction abstrait est un couple $(A, \to)$, où la flèche $\to$, appelée réduction, est une relation binaire sur A.

Exemple 18 : La relation de réduction $\to_E$ est une réduction !

BAA p9 Déf 19. On considère $(A, \to)$, $x \in A$ est réductible si $\exists y \in A$ tq $x \to y$.
x est sous forme normale s'il n'est pas réductible.
y est une forme normale de x si $x \xrightarrow{*} y$ et y est une forme normale.
x et y sont joignables si $\exists z \in A$, $x \xrightarrow{*} z \xleftarrow{*} y$. On note $x \downarrow y$.

TER p60 Exemple 20 : On définit les entiers naturels par 0 (constante) et le successeur S (unaire), et la fonction Min (binaire). Les relations de réduction sont : $\{Min(Sx, Sy) \approx S(Min(x,y)),\ Min(x,0) \approx 0,\ Min(0,x) \approx 0\}$. $SSS(0)$ est une forme normale. C'est la forme normale de $Min(S^3(0), S^4(0))$. De plus, $Min(Min(S^3(0),0), S^2(0))$ et $Min(S(0),0)$ sont joignables.

BAA p9 Déf 21 : Une réduction $\to$ est dite :
- Church-Rosser si $x \xleftrightarrow{*} y \Rightarrow x \downarrow y$. (cf annexe 2)
- confluente si $y_1 \xleftarrow{*} x \xrightarrow{*} y_2 \Rightarrow y_1 \downarrow y_2$. (cf annexe 3)
- terminante si il n'y a pas de chaîne infinie $a_0 \to a_1 \to \dots$
- normalisante ssi chaque élément a une forme normale.
- convergente ssi elle est confluente et terminante.

BAA p11 Th 22 : Une réduction confluente est Church-Rosser, et réciproquement.

Coro 23 : Si $\to$ est confluente et $x \xleftrightarrow{*} y$ alors :
1) $x \xrightarrow{*} y$ si y est une forme normale.
2) si x et y sont en forme normale, alors $x = y$.

Coro 24 : Si $\to$ est confluent, chaque élément a au plus une forme normale. (cf exemple 15)

Coro 25 : Si $\to$ est normalisant et confluent, chaque élément a une unique forme normale.

Exemple 26 : Toujours sur les entiers, on définit l'addition $+$ (binaire) et les relations de réduction : $\{+(S(x),y) \approx S(x+y),\ +(0,x) \approx x\}$.
Normalisant + confluent $\Rightarrow \exists !$ forme normale.

BAA p61 Déf 27 : Une règle de réécriture est une identité $s \approx t$ telle que s ne soit pas une variable, et toutes les variables de t sont dans s. On peut écrire $s \to t$. Un système de réécriture (SR) est un ensemble de règles de réécriture.

Un système de réécriture est un cas particulier de système de réduction.

TER p65;67 Exemple 28 : La logique combinatoire, avec 3 fonctions unaires : S, K, I.
Règles de réduction : $\left\{ \begin{array}{ll} ((S\cdot x)\cdot y)\cdot z \approx (x\cdot z)\cdot(y \cdot z), & I \cdot x \approx x, \\ (K\cdot x)\cdot y \approx x & \end{array} \right\}$
Si on pose $B = S(KS)K$, avec la convention "les parenthèses sont les plus à gauche possible", on a : $B\,x\,y\,z \to x(yz)$.
On aimerait savoir si le système de réécriture est confluent !

BAA p14 Principe 29 d'induction bien fondée : Soit $(A, \to)$ un système de réduction terminant, et P une propriété sur les éléments de A :
$$\frac{\forall x \in A,\ (\forall y \in A,\ x \xrightarrow{+} y \Rightarrow P(y)) \Rightarrow P(x)}{\forall x \in A,\ P(x)}$$

BAA p18 Exemple 30 : L'ordre lexicographique sur deux systèmes de réduction terminants $(A, >_A)$ et $(B, >_B)$ défini par : $(A \times B, >_{A\times B})$ avec $(x,y) >_{A\times B} (x',y')$ ssi $(x >_A x') \vee (x = x' \wedge (y >_B y'))$.
$P(x) :=$ il n'y a pas de chaîne infinie commençant par x sur $A \times B$, montre que $A \times B$ est terminant.

BAA p28 Déf 31 : Une relation $\to$ est localement confluente si :
$y_1 \leftarrow x \to y_2 \Rightarrow y_1 \downarrow y_2$. (cf annexe 4).

Rem 32 : Ceci n'implique pas la confluence ! (cf annexe 5).

BAA p29 Lemme 33 (de Newmann) : Une relation terminante est confluente si et seulement si elle est localement confluente.

III Terminaison et confluence de systèmes de réécriture

A) Etude de la confluence

Dans un premier temps : étant donnés deux termes s et t on voudrait savoir s'il existe σ une substitution telle que $\sigma s \underset{E}{=} \sigma t$!

Déf 34 : La substitution σ est plus générale que la substitution σ' si il existe une substitution δ telle que $\sigma' = \delta\sigma$. On écrit $\sigma \lesssim \sigma'$.

Lemme 35 : $\lesssim$ est un pré-ordre sur les substitutions (réflexivité et transitivité)

BAA p 72 Déf 36 : Un problème d'unification est un ensemble fini d'équations $S = \{s_1 =^? t_1, \dots, s_n =^? t_n\}$. Un unificateur de S est une substitution telle que $\forall i,\ \sigma s_i = \sigma t_i$. σ est un unificateur le plus général si pour tout σ' unificateur, $\sigma \lesssim \sigma'$.

Ex 37 : $\Sigma = \{f : 2, g : 1, e : 0\}$, alors $s = f(f(e,y), g(x))$ et $t = f(z, y)$ sont unifiables ; l'unificateur le plus général est $\sigma = [\,{}^{z}/_{f(e,y)},\ {}^{y}/_{g(x)}\,]$.

BAA p 135 Th 38 : Le problème suivant est indécidable.

entrée : un SR, nommé R. sortie : oui si R est confluent.

Plusieurs cas peuvent se présenter si on a :

On a les règles $l_i \to r_i \in R$, des positions p_i et des substitutions σ_i telles que $s_{|p_i} = \sigma_i l_i$ et $t_i = s[\sigma_i r_i]_{p_i}$.

$$\begin{tikzcd} & s \arrow[dl, "l_1 \to r_1"'] \arrow[dr, "l_2 \to r_2"] & \\ t_1 & & t_2 \end{tikzcd}$$

1er cas : p_1 et p_2 sont dans des sous-arbres séparés (annexe 6). On a la confluence locale.

2ème cas : p_1 est un préfixe de p_2 (cf annexe 7).

Cas 2.1 : la règle de réécriture $l_1 \to r_1$ ne change pas le sous-arbre l_2 : on a la confluence locale (cf annexe 8).

BAA p 139 Cas 2.2 : les deux domaines de réécriture s'intersectent...

Déf 39 : En reprenant les notations précédentes : si $Var(l_1, r_1) \cap Var(l_2, r_2) = \emptyset$, soit p tel que $l_{1|p}$ ne soit pas une variable, et soit θ un unificateur le plus général de $l_{1|p} =^? l_2$. Cela détermine une paire critique $(\theta r_1, (\theta l_1)[\theta r_2]_{|p})$.

Th 40 (des paires critiques) : Un SR est localement confluent ssi toutes ses paires critiques sont joignables.

Coro 41 : La confluence d'un SR fini et terminant est décidable.

B) Étude de la terminaison.

Th 42 : Le problème TERM suivant : $\boxed{\text{DVT}}$ BAA p 93

entrée : un SR fini. sortie : oui s'il est terminant,

est indécidable.

Quelques éléments de théorie des ensembles :

Déf 43 : $\lesssim$ est un beau pré-ordre (ou pré-bel-ordre) sur un ensemble D si pour toute suite infinie $(s_i)_{i\in\mathbb{N}} \in D^{\mathbb{N}}$, il existe $i<j$ tel que $s_i \lesssim s_j$.

Prop 44 : Soit $\lesssim$ un pré-bel-ordre. On a équivalence entre :

- $\lesssim$ est un pré-bel-ordre.
- $\forall (s_i)_{i\in\mathbb{N}} \in D^{\mathbb{N}}$, $\exists \phi : \mathbb{N} \to \mathbb{N}$ strictement croissante, telle que $\forall i \in \mathbb{N}$, $s_{\phi(i)} \lesssim s_{\phi(i+1)}$.

Th 45 : de Higman : soit $\lesssim$ un pré-bel-ordre sur D. On définit $\trianglelefteq$ sur D^*.

- $\varepsilon \trianglelefteq \varepsilon$ - $s \trianglelefteq t$ et $b \in D$, alors $s \trianglelefteq bt$.
- si $a \lesssim b$ et $s \trianglelefteq t$ alors $as \trianglelefteq bt$.

C'est un pré-bel-ordre.

Déf 46 : Un ordre de réduction sur $T(\Sigma)$ est un ordre bien fondé, clos par substitution et Σ-opérations. Un ordre de simplification $<$ est un ordre sur les termes, clos par substitution, par Σ-opérations, et : $\forall f \in \Sigma^{(n)}$, $\forall i \leq n$, $x_i < f(x_1, \dots, x_n)$.

Th 47 : Un SR est terminant ssi il existe un ordre de réduction $>$ satisfaisant $l > r$ pour tout $l \to r \in R$. BAA p 103

Déf 48 : Σ signature, muni d'un pré-bel-ordre $<$. Ordre de plongement $\trianglelefteq$:

- si $s \trianglelefteq x_i$ alors $s \trianglelefteq t(x_1, \dots, x_i, \dots, x_n)$.
- si $s < t$, $a_1, \dots, a_m$, $b_1, \dots, b_n$ des termes avec $m \leq n$, et une suite croissante $j_1, \dots, j_m$ tq $a_i \trianglelefteq b_{j_i}$, alors $s(a_1, \dots, a_m) \trianglelefteq t(b_1, \dots, b_n)$.

Th 49 : Soit $<$ un ordre de simplification sur $T(\Sigma)$.

Si Σ est finie, alors $<$ est bien fondée. DVT

Annexe 1 :

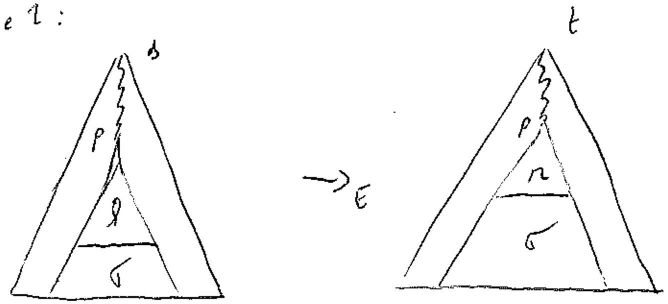
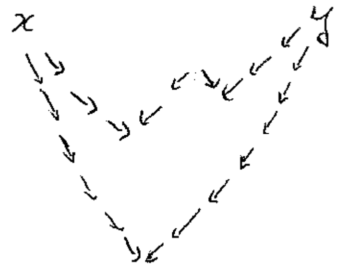
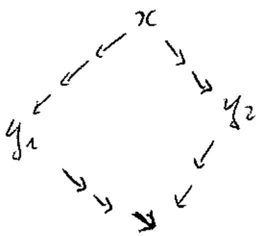


Illustration de $s \rightarrow_E t$.

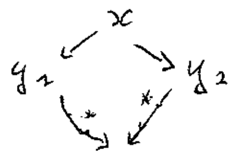
Annexe 2 :



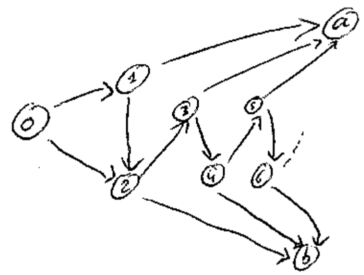
Annexe 3



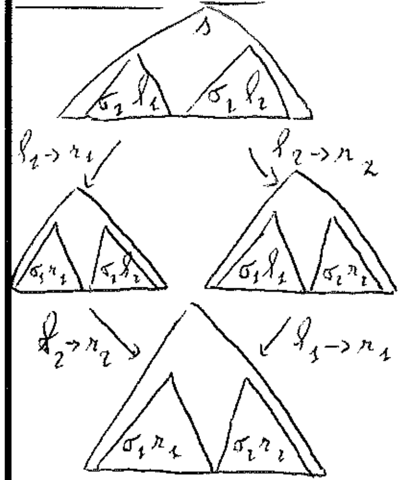
Annexe 4 :



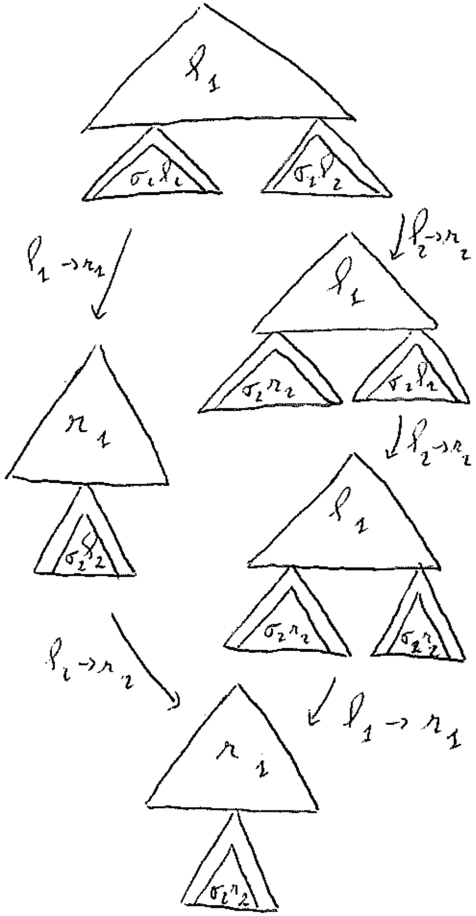
Annexe 5



Annexe 6 : cas 1 :



Annexe 8 : Cas 2.1.



Annexe 7 : cas 2 :