TD 11 : Terminaison et unification

{lionel.rieg,paolo.tranquilli}@ens-lyon.fr

Exercice 1. *Terminaison de système de réécriture*

Soit Σ une signature et $\mathcal{T}(\Sigma, X)$ l'algèbre libre des termes sur Σ à variables dans X.
Une relation $>$ est un *ordre de réécriture* pour $\mathcal{T}(\Sigma, X)$ si :
– c'est un ordre (transitif, anti-symétrique),
– elle est *compatible* : si $u > v$ alors

$$f(t_1, \ldots, t_{i-1}, u, t_{i+1}, \ldots, t_n) > f(t_1, \ldots, t_{i-1}, v, t_{i+1}, \ldots, t_n)$$

– elle est *close par substitution* : si $u > v$ alors pour toute substitution σ, $u\sigma > v\sigma$.
Un *ordre de réduction* est un ordre de réécriture nœthérien.

1. Montrez qu'un système de réécriture R termine si et seulement si il existe un ordre de réduction $>$ tel que pour toute règle $l \to r$ de R, on a $l > r$.

Une Σ-algèbre [1] $\mathcal{A}$ est dite *ordonnée* si elle est munie d'un ordre $>$. L'ordre éventuel de l'algèbre induit un ordre $>_{\mathcal{A}}$ sur $\mathcal{T}(\Sigma, X)$ défini par : $u >_{\mathcal{A}} v$ si pour tout homomorphisme d'algèbres $\pi : \mathcal{T}(\Sigma, X) \to \mathcal{A}$, on a $\pi(u) > \pi(v)$.
Une fonction $f : \mathcal{A}^n \to \mathcal{A}$ est *monotone* si $b > b'$ implique $f(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_n) > f(a_1, \ldots, a_{i-1}, b', a_{i+1}, \ldots, a_n)$.

2. Montrez que si $>$ est nœthérien, et tous les $f^{\mathcal{A}}$ sont monotones, alors l'ordre $>_{\mathcal{A}}$ induit sur $\mathcal{T}(\Sigma, X)$ est un ordre de réduction.

3. Justifier ou infirmer la terminaison des systèmes de réécriture suivants :

(a) $f(f(x, x), y) \to f(y, y)$

(b) $f(0, 1, x) \to f(x, x, x)$

(c) $\begin{cases} p(s(i), j) \to p(i, j) \\ p(i, s(j)) \to p(i, j) \end{cases}$

(d) $\begin{cases} a(0, x) \to s(x) \\ a(s(x), 0) \to a(x, s(0)) \\ a(s(x), s(y)) \to a(x, a(s(x), y)) \end{cases}$

(e) $\begin{cases} p(s(i), j) \to p(i, i) \\ p(i, s(j)) \to p(i, j) \end{cases}$

(f) $\begin{cases} x * (y * z) \to (x * y) * z \\ f(x * y) \to f(y) * f(x) \end{cases}$

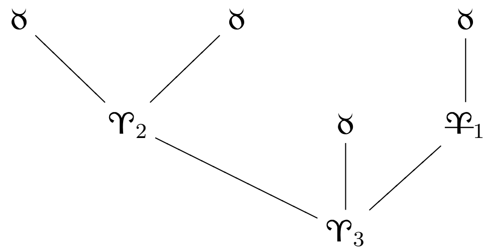
(g) $\begin{cases} a(a(x)) \to b(c(x)) \\ b(b(x)) \to a(c(x)) \\ c(c(x)) \to a(b(x)) \end{cases}$

Exercice 2. *Le deuxième travail d'Héraklès*

Sur l'ordre des dieux, le héros Héraklès du se soumettre à douze tâches surhumaines qui lui furent données par le roi Eurysthée. Le deuxième de ces douze travaux consista à vaincre l'Hydre de Lerne, redoutable monstre dont les têtes repoussaient toujours plus nombreuses chaque fois que

1. On rappelle qu'une Σ-*algèbre* est un ensemble $\mathcal{A}$, muni d'une fonction $f^{\mathcal{A}} : \mathcal{A}^n \to \mathcal{A}$ pour tout symbole de fonction f d'arité n dans Σ. En particulier, $\mathcal{T}(\Sigma, X)$ en est une.

l'on en tranchait une, et qui hantait le marais de Lerne, tuant les voyageurs imprudents qui se risquaient à le traverser. La bataille fut exrêmement longue et âpre, et Héraklès faillit de nombreuses fois y laisser sa vie, mais il finit par l'emporter.
On considère ici un état de l'Hydre comme un arbre sur la signature infinie suivante : les symboles nullaires $\Taurus$ et $\Pisces$ représent respectivement une tête et une tête coupée ; le symbole k-aire $\Aries_k$ représente un cou se ramifiant en k branches ($k > 0$) et le symbole k-aire $\cancel{\Aries}_k$ représente un cou blessé auquel il reste k branches ($k \geqslant 0$).
La racine de l'arbre est appelée le *cœur* de l'Hydre. La *profondeur* d'une position $p = i_1 \dots i_k$ est égale à la longueur de cette position. Un état de l'Hydre est dit *indemne* s'il ne comprte aucun symbole $\Pisces$ ou $\cancel{\Aries}_k$.
Voici un état de l'Hydre, encodé par le mot $\Aries_3(\Aries_2(\Taurus, \Taurus), \Taurus, \cancel{\Aries}_1(\Taurus))$:



Le combat d'Héraklès et de l'Hydre peut être représenté comme l'alternance des deux étapes suivantes :

1. Héraklès donne un coup à l'Hydre indemne, lui coupant un tête.
2. Le cou d'où était issu la tête se duplique un nombre fini arbitraire de fois. Ce faisant, si jamais il ne lui restait plus de tête, il devient un tête.

Héraklès gagne s'il parvient à trancher le cœur de l'Hydre, c.-à-d. s'il atteint le terme $\Taurus$, qu'il ne lui reste plus qu'à trancher sans repousse possible (ce qui donnera le terme $\Pisces$).
On peut formaliser ceci par un système de réécriture. La première étape se traduit par :

$$\Taurus \xrightarrow{1} \Pisces$$

et la seconde se divise en deux sous-étapes, tout d'abord :

$$\Aries_k(c_1, \dots, c_{i-1}, \Pisces, c_{i+1}, \dots, c_k) \xrightarrow{2} \cancel{\Aries}_{k-1}(c_1, \dots, c_{i-1}, c_{i+1}, \dots, c_k)$$

puis (avec dans toutes les règles $j > 0$ et $n \geqslant 0$) :

$$\begin{array}{rcl}
\Aries_k(\overrightarrow{C}, \cancel{\Aries}_j(\overrightarrow{X}), \overrightarrow{C'}) & \xrightarrow{3} & \Aries_{k+n}(\overrightarrow{C}, \Big[\, \Aries_j(\overrightarrow{X}), \Big]^{n+1}, \overrightarrow{C'}) \\
\Aries_k(\overrightarrow{C}, \cancel{\Aries}_0, \overrightarrow{C'}) & \xrightarrow{3} & \Aries_{k+n}(\overrightarrow{C}, [\,\Taurus, \,]^{n+1}, \overrightarrow{C'}) \\
\cancel{\Aries}_j(c_1, \dots, c_j) & \xrightarrow{3} & \Aries_j(c_1, \dots, c_j) \\
\cancel{\Aries}_0 & \xrightarrow{3} & \Taurus
\end{array}$$

On considère donc le système de réécriture $\mathcal{H}$ sur les termes représentant les états indemnes de l'Hydre, dont la relation de réduction est la relation $\xrightarrow{1}\xrightarrow{2}\xrightarrow{3}$ (qui représente une phase entière de combat).

1. Expliquer en trois lignes pourquoi $\mathcal{H}$ traduit bien le combat tel qu'il est décrit.

2. indiquer les formes normales pour le système $\mathcal{H}$.

3. Exprimer en tant que propriétés abstraites de systèmes de réécriture ces deux propositions :

(i) Quoi que fasse l'Hydre, Héraklès peut gagner.

(ii) Quoi que fassent l'Hydre et Héraklès, il est sûr de gagner.

Sont-elles vérifiées ici ? Justifier la réponse.

4. Le combat d'Héraklès et de l'Hydre a-t-il la propriété de Church-Rosser ?

Exercice 3. *Unification modulo commutativité*

Étant donnée une algebre de termes $T(\Sigma, V)$, on appelle un *axiome* une paire $u \doteq v$ avec $u, v \in T(\Sigma, V)$ et $\mathrm{Var}(u) = \mathrm{Var}(v)$. Étant donné un ensemble d'axiomes $E = \{ u_1 \doteq v_1, \dots u_k \doteq v_k \}$ on denote par $=_E$ (*égalité modulo* E) la plus petite relation d'équivalence sur $T(\Sigma, V)$ telle qui est stable par substitution et compatible.

1. Donner la définition des notion ci-dessus en termes de ce que vous avez déjà vu en cours.

2. Étant donné un problème équationnel P, formaliser la notion d'unificateur modulo un ensemble d'axiomes E.

On va s'intéresser en particulier au cas de la commutativité. Étant donné $\Pi \subseteq \Sigma \setminus (\Sigma_0 \cup \Sigma_1)$, soit C_Π l'ensemble

$$C_\Pi = \{ f(x_1, \dots, x_i, x_{i+1}, \dots, x_k) \doteq f(x_1, \dots, x_{i+1}, x_i, \dots, x_k) \mid f \in \Pi, 1 \leq i < k \}.$$

Par exemple si $\Sigma = \{ 0 : 0, S : 1, + : 2 \}$, alors $C_{\{+\}} = \{ x_1 + x_2 \doteq x_2 + x_1 \}$.
On se propose d'étudier en général le problème de l'unification modulo C_Π.

3. L'equation $S(x) + (y + z) \stackrel{?}{\doteq} (x + S(x)) + y$ est-elle unifiable sans commutativité ? Et modulo $C_{\{+\}}$?

4. Est-ce que si P est unifiable modulo C_Π il en existe un unificateur le plus général ?

5. Élaborez une méthode pour trouver tous les unificateurs d'un problème équationnel P modulo C_Π, en en prouvant correction et complétude.