DERSHOWITZERIES

JJL 23 octobre 1981.

Rappel: (Kruskaleries) Si $\gg$ est un prébel ordre et $\geqslant$ un préordre vérifiants:

Ax1: $f(\ldots t \ldots) \geqslant t$,

Ax2: ($t_{i_1} \geqslant u_1, t_{i_2} \geqslant u_2, \ldots, t_{i_n} \geqslant u_n$ pour $i_1 < i_2 < \ldots < i_n$) et $f\vec{t} \gg g\vec{u}$ impliquent $f\vec{t} \geqslant g\vec{u}$,

Alors $>$ est bien fondé.

<u>Définition</u> : (Plaisted 78 - revue Dershowitz 73). Soit $\gtrsim$ un préordre donné sur les termes. Le "recursive path ordering" associé (en court rpo ($\gtrsim$)) est défini par : $t = f\vec{t} > g\vec{u} = u$ ssi

(1) $t \mathrel{\dot{>}} u$ et $t > u_i$ pour tout i,

(2) $t \doteq u$ et $\{t_1, t_2, \dots t_n\} >_m \{u_1, u_2, \dots u_p\}$,

(3) $t_i \gtrsim u$ pour un i,

où $>_m$ est l'ordre sur les multi-ensembles associé à $\gtrsim$ et $t \gtrsim u$ ssi $t > u$ ou $t \simeq u$, avec $\simeq$ défini par :

$t \simeq u$ ssi $t \doteq u$, $t = f\vec{t}$, $u = g\vec{u}$ et $\{t_1, t_2, \dots t_n\} \simeq_m \{u_1, u_2, \dots u_p\}$.

Nous allons montrer les théorèmes suivants :

<u>Théorème 1</u> : Si $\mathrel{\dot{>}}$ est bien-fondé, alors rpo ($\gtrsim$) est aussi bien-fondé.

<u>Théorème 2</u> : Si $\gtrsim$ vérifie :

(μ) $t \to u$ implique $f(\dots t \dots) \gtrsim f(\dots u \dots)$

et si un système $\mathcal{E} = \{\alpha_i \to \beta_i\}$ vérifie $\sigma(\alpha_i) > \sigma(\beta_i)$ pour toute substitution close σ (où $>$ est le rpo ($\gtrsim$)), alors $\to$ est noetherien.

Lemmes :

(a) $\simeq$ est une relation d'équivalence,

(b) $t > u \simeq v \Rightarrow t > v$,

(c) $t \simeq u > v \Rightarrow t > v$,

(d) $t > u > v \Rightarrow t > v$,

(e) $>$ est irréflexif,

Démonstrations :

(a) immédiat puis $\doteq$ est une équivalence

(b) Par récurrence sur $\|t\|+\|u\|+\|v\|$. Trois cas selon la définition de $t > u$.

Cas 1 : $t \gtrdot u$ et $t > u_i$ pour tout i. Or $u \doteq v$, puisque $u \simeq v$. Donc $t \gtrdot v$. Or, par définition de $\simeq_m$, pour tout v_i, il existe un u_j tel que $u_j \simeq v_i$. Or $t > u_j$. Donc $t > v_i$ par récurrence. Donc $t > v$ par la règle 1.

Cas 2 : $t \doteq u$ et $\{t_1, \cdots t_n\} >_m \{u_1, \cdots u_p\}$. Comme $u \simeq v$, on a $u \doteq v$ et $\{u_1, \cdots u_p\} \simeq_m \{v_1, \cdots v_q\}$. Donc $t \doteq v$ et par récurrence $\{t_1, \cdots t_n\} >_m \{v_1, \cdots v_q\}$. D'où $t > v$ par la règle 2.

Cas 3 : $t_i \gtrsim u$ pour un i. Comme $u \simeq v$, on a $t_i \gtrsim v$ par récurrence. Donc $t > v$ par la règle 3.

(c) Par récurrence sur $\|t\| + \|u\| + \|v\|$. Trois cas selon la définition de $u > v$.

Cas 1 : $t \doteq u \gtrdot v$. Donc $t \gtrdot v$. De plus $u > v_i$ pour tout i. Donc $t > v_i$ par récurrence, Donc $t > v$ par la règle 1.

Cas 2 : $t \doteq u \doteq v$. Et $\{t_1 \cdots t_n\} \simeq_m \{u_1, \cdots u_p\} >_m \{v_1 \cdots v_q\}$. Donc $\{t_1, \cdots t_n\} >_m \{v_1, \cdots v_q\}$ par récurrence. D'où $t > v$ par la règle 2.

Cas 3 : $u_i \gtrsim v$ pour un i. Or $\{t_1, \cdots t_n\} \simeq_m \{u_1, \cdots u_p\}$. Donc, il existe j tel que $t_j \simeq u_i$. D'où $t_j \gtrsim v$ par récurrence. Et $t > v$ par la règle 3.

(d) Même récurrence.

(e) $t > t$ est impossible, par récurrence sur $\|t\|$. Par la règle 1, c'est impossible puisque $t \gtrdot t$ est impossible. Par la règle 2, impossible puisque $>_m$ est irréflexif, puisque par (d) et récurrence on sait que $>$ est un ordre strict pour les termes de taille plus petite que $\|t\|$. Par la règle 3, on aurait $t_i \gtrsim t$ pour un i.

Or $t > t_i$ par la règle 3 également. Donc $t_i > t_i$ par (c) et (d). Impossible par récurrence. □

Démonstration du théorème 1: $\gg$ est bien-fondé. Or on peut compléter $\gg$ en $\gg'$ bon ordre admettant $\doteq$ aussi pour équivalence compatible. (voir Birkoff). Notons $t \ggeq' u$ pour $t \gg' u$ ou $t \doteq u$. Les lemmes a, b, ... e restent vrai pour le rpo associé à $\gg'$. Notons $>'$ ce rpo. Et $t \gtrsim' u$ pour $t >' u$ et $t \simeq u$. Les bons ordres étant des cas particuliers des prébelordres, il reste à montrer que $\gtrsim'$ vérifie Ax1 et Ax2 (par rapport à $\ggeq'$) pour affirmer que $>'$ est bien fondé. Or, puisque $\gg'$ est une extension de $\gg$, on a trivialement $>'$ extension de $>$, et donc $>$ est bien-fondé. Montrons donc Ax1 et Ax2. D'abord Ax1 est vrai par la règle 3 puisque $t \simeq t$. Pour Ax2, on a deux cas. Si $t = f\vec{t} \gg' g\vec{u} = u$, alors $t >' u$ par la règle 1, puisque $t >' t_{i_k} \gtrsim' u_k$ pour tout k. Si $t = f\vec{t} \doteq g\vec{u} = u$, alors on a soit $\{t_1, \dots t_p\} >'_m \{u_1, \dots u_n\}$, soit $\{t_1, \dots t_p\} \simeq_m \{u_1, \dots u_n\}$, i.e. soit $t >' u$ par règle 2, soit $t \simeq u$. Donc $t \gtrsim' u$. □

Démonstration du théorème 2: On va montrer que $> \cap \to$ est compatible avec la structure. Donc, supposons $t \to u$ et $t > u$, montrons que $f(\dots t \dots) > f(\dots u \dots)$. D'après l'axiome ($\mu$), on a $f(\dots t \dots) \gg f(\dots u \dots)$. Et on applique soit les règles 1 ou 2. □

Exemples :

1) Posons $t = f\vec{t} \succ g\vec{u} = u$ ssi $f \succ g$ dans un ordre supposé bien fondé sur les symboles de fonctions, et $t = f\vec{t} \doteq g\vec{u} = u$ ssi $f = g$. Remarquons que $\doteq$ est compatible avec $\succ$, et que (μ) est trivialement vrai. On retrouve les vraies définitions de Plaisted ou Dershowitz.

$$\begin{cases} \neg\neg p \to p \\ \neg(p \vee q) \to \neg p \wedge \neg q \\ \neg(p \wedge q) \to \neg p \vee \neg q \\ p \wedge (q \vee r) \to (p \wedge q) \vee (p \wedge r) \\ (p \vee q) \wedge r \to (p \wedge r) \vee (q \wedge r) \end{cases}$$

Prenons $\neg \succ \wedge \succ \vee$ comme ordre sur les symboles.

2) Factorielle :

$$\begin{cases} f(sx) \to sx * f(p(sx)) \\ f(0) \to s0 \\ p(sx) \to x \end{cases}$$

Dénotons par $[\![t]\!]$ l'interprétation naturelle sur $\mathbb{N}$. Posons $f(t) \succ f(u)$ ssi $[\![t]\!] >_{\mathbb{N}} [\![u]\!]$, $f(t) \succ u * v$, $f(t) \succ p(u)$, $f(t) \succ su$ pour tout t, u et v. Alors (μ) est trivialement vérifié. Et les réécritures vérifient le rpo.

Dans cet exemple, remarquons que l'on a :

$p(sx) > sx$, mais $f(sx) > f(p(sx))$.

Quelques remarques supplémentaires sur $>$:

1) termes ouverts : Le rpo $>$ a été défini dans le cas des termes clos. Pour les termes avec variables, il suffit de considérer les variables comme des symboles de fonctions non reliés par $>$ aux autres symboles ou variables. Alors, on montre que $>$ est fermé par substitution, et coïncide sur les termes fermés.

2) ambiguïté de la définition : Les cas 1 et 2 de la définition du rpo sont exclusifs. Pas le cas 3 ! Ce qui peut être coûteux pour calculer si deux termes sont reliés. Montrons que la définition est équivalente si on change la règle 3 en :

$$(3') \quad t \not\geqslant u \text{ et } t_i \gtrsim u \text{ pour un } i.$$

Appelons $>'$ l'ordre défini avec (3'). Clairement, on a $>'$ inclus dans $>$. Montrons le contraire, c'est à dire que $t > u$ implique $t >' u$ par récurrence sur $\|t\| + \|u\|$.

Cas 1 et 2 : immédiats.

Cas 3 : On a $t_i \gtrsim u$ pour un i. On a trois sous-cas, selon que $t > u$, $t \doteq u$ ou $t \not\geqslant u$.

Cas 3.1 : $t > u$. Comme $t_i \gtrsim u$ et $u > u_j$ pour tout j. On a $t_i > u_j$. Comme $t > t_i$, on a $t > u_j$ pour tout j. Donc $t >' u_j$ pour tout j par récurrence, et $t >' u$ par règle 1.

Cas 3.2 : $t \doteq u$. De même $t_i > u_j$ pour tout j. Donc $t_i >' u_j$ pour tout j par récurrence. D'où $t >' u$ par règle 2.

Cas 3.3 : $t \not\geqslant u$. Alors $t_i \gtrsim' u$ par récurrence. Donc $t >' u$ par règle 3. $\square$

En conclusion, le rpo se calcule vite, si on sait calculer vite $\geq_m$ ou $\simeq_m$. C'est un problème relatif aux multiensembles avec des ordres partiels. (On peut vérifier que dans le cas d'un ordre total $\gtrsim$ un simple tri suffit).

<u>Rpo avec ordres lexicographiques</u> :

<u>Définition : (Kamin + JJL 80)</u>. Soit $\gtrsim$ un préordre donné sur les termes. Le "lexicographic recursive path ordering" (lrpo) associé est défini par : $t = f\vec{t} > g\vec{u} = u$ ssi

(1) $t \gtrdot u$ et $t > u_i$ pour tout i,

(2) $t \doteq u$ et $\vec{t} >_{lex} \vec{u}$ et $t > u_i$ pour tout i,

(3) $t_i \gtrsim u$ pour un i,

où $>_{lex}$ est l'ordre lexicographique associé à $\gtrsim$, et $t \gtrsim u$ ssi $t > u$ et $t \simeq u$, où ;

$t \simeq u$ ssi $t \doteq u$, $t = f\vec{t}$, $u = g\vec{u}$ et $t_i \simeq u_i$ pour tout i.

On démontre aussi les théorèmes 1 et 2. La remarque sur les termes ouverts reste vraie. L'ordre marche mieux pour les exemples suivants :

<u>Exemple 1</u> :

$$\begin{cases} \neg\neg p \to p \\ \neg(p \vee q) \to \neg p \wedge \neg q \\ \neg(p \wedge q) \to \neg p \vee \neg q \\ p \wedge (q \vee r) \to (p \wedge q) \vee (p \wedge r) \\ (p \vee q) \wedge r \to (p \wedge r) \vee (q \wedge r). \\ (p \wedge q) \wedge r \to p \wedge (q \wedge r). \\ (p \vee q) \vee r \to p \vee (q \vee r). \end{cases}$$

Exemple 2: les groupes (voir Knuth-Bendix)

Quelques remarques supplémentaires:

1) ambiguïté de la définition: On peut remplacer (2) et (3) de la définition du lrpo par: (en notant $\alpha(t)$ le nombre n de fils de $t = f(t_1, t_2, \dots t_n)$):

(2') $t \doteq u$ et $[\alpha(t) > \alpha(u)$ ou $[\alpha(t) = \alpha(u)$ et $t_1 \simeq u_1, t_2 \simeq u_2, \dots t_{i-1} \simeq u_{i-1}, t_i > u_i, t > u_{i+1}, t > u_{i+2}, \dots t > u_n]]$

(3') $[[t \not> u$ ou $[t \doteq u$ et $\alpha(t) < \alpha(u)]]$ et $t_i \gtrsim u$ pour un $i]$ ou $[t \doteq u$ et $\alpha(t) = \alpha(u)$ et $t_1 \simeq u_1, t_2 \simeq u_2, \dots t_{i-1} \simeq u_{i-1}, t_i \not> u_i$ et $t_{i+k} \gtrsim u$ pour un i.$]$

Cette définition compliquée peut être montrée équivalente à celle donnée par 1, 2, 3. (La démonstration est identique à celle effectuée pour les multiensembles). L'intérêt est que les cas 1, 2', 3' sont exclusifs et la complexité de calculer $t > u$ a l'air d'être $O(\|t\| \times \|u\|)$.

2) complexité de la définition avec les multiensembles:

Cette définition me semble curieusement avoir la même complexité. En effet, pour calculer $t > u$, le cas douloureux semble le cas 2. Or, pour calculer $\{t_1, t_2, \dots t_n\} \gg_m \{u_1, \dots u_p\}$, on peut éliminer les paires $t_i \simeq u_j$ en comparant toutes les paires successivement, puis vérifier que tous les u_i restants sont dominés par un t_i restant, en recomparant à nouveau les ensembles qui restent. Donc :

$$\begin{aligned} C(t,u) &\leq k + \sum_j C(t,u_j) && \text{(règle 1)} \\ &\leq k + \sum_{i,j} C(t_i,u_j) + k'K^2 && \text{(règle 2)} \\ &\leq k + 2\times\sum_i C(t_i,u) && \text{(règle 3')} \end{aligned}$$

en partant du principe que $t > u$ et $t \simeq u$ ont même complexité $C(t,u)$. Par récurrence, on en conclut que $C(t,u) = O(\|t\| \times \|u\| + K^2)$. Par ailleurs, pour calculer $\{t_1, \dots t_m\} >_m \{u_1, \dots u_n\}$, on a besoin de $m \times n$ comparaisons dans le cas pire où tous les éléments ne sont pas reliés. Donc $\|t\| \times \|u\|$ ne semble pas si mauvais comme complexité.
(Remarque : K est l'arité maximale d'un symbole de fonction).