Algorithme d'unification.

Introduction à la logique. Théorie de la démonstration.
René David, Karim Nour, Christophe Raffalli

2011-2012

On cherche à unifier un ensemble d'équations.

On prend E un ensemble d'équations, et on construit deux suites E_n et σ_n par récurrence, avec $E_0 = E$ et $\sigma_0 = id$.

Puis :

1. Si $E_n = E' \sqcup \{f(u_1, \ldots, u_q) \sim g(v_1, \ldots, v_p\}$, alors
   – Si $f = g$, alors $E_{n+1} := E' \cup \{u_1 \sim v_1, \ldots, u_p \sim v_p\}$ et $\sigma_{n+1} := \sigma_n$.
   – Si $f \neq g$, alors renvoyer "Échec clash".
2. Si $E_n = E' \sqcup \{x \sim x\}$, on pose $E_{n+1} := E'$ et $\sigma_{n+1} := \sigma_n$.
3. Si $E_n = E' \sqcup \{x \sim u\}$ (ou $\{u \sim x\}$), avec $u \neq x$, alors
   – Si la variable x n'apparaît pas dans u, on pose $E_{n+1} := E'[x := u]$ et $\sigma_{n+1} := [x := u] \circ \sigma_n$.
   – Sinon, renvoyer "Échec occur-check".

Remarques :

– L'algorithme n'est pas déterministe ; cependant, l'ordre des opérations n'a pas d'importance.

– La complexité est exponentielle.

Proposition 1
L'algorithme ci-dessus termine toujours, soit par un échec, soit avec $E_n = \emptyset$.

Démonstration. On note respectivement a_n, b_n, c_n le nombre de variables, de symboles de fonction, d'équations dans E_n, et $f(n) = (a_n, b_n, c_n)$. On montre que si $E_n \neq \emptyset$ et pas d'échec à l'étape n, $f(n+1) < f(n)$ avec $<$ l'ordre lexicographique. On regarde suivant les cas de l'algorithme :

	a_n	b_n	c_n
Cas 1	$=$	$\searrow$	
Cas 2	$\searrow$ ou $=$	$=$	$\searrow$
Cas 3	$\searrow$		

$\square$

Théorème 2
Si l'algorithme termine avec $E_n = \emptyset$, alors σ_n est le mgu *de E. S'il échoue par clash ou occur-check, alors E n'a pas d'unificateur.*

Lemme 3
Soient x une variable, u un terme, et σ une substitution. Si $x[\sigma] = u[\sigma]$, alors $\sigma = \sigma \circ [x := u]$.

Démonstration. On pose $\sigma' = \sigma \circ [x := u]$. Alors

$$x[\sigma'] = x[x := u][\sigma] = u[\sigma] = x[\sigma],$$

et si $y \neq x$, alors

$$y[\sigma'] = y[x := u][\sigma] = y[\sigma].$$

□

Démonstration. On montre tout d'abord.

H_n = « À l'étape n de l'algorithme, σ unifie E *si, et seulement si* il existe σ' qui unifie E_n et telle que $\sigma = \sigma' \circ \sigma_n$. »

Si H_n est vraie pour tout n, alors, soit m la dernière étape de l'algorithme
- Si $E_m = \emptyset$, l'identité unifie E_m, et H_m nous dit alors que σ_m unifie E, et que c'est bien le *mgu*.
- Si l'algorithme échoue par clash : E_m contient une équation de la forme $f(x_1, \ldots, x_p) \sim g(y_1, \ldots, y_q)$ avec $f \neq g$, et donc E_m n'est pas unifiable. Par H_m, E n'est pas unifiable non plus.
- Si l'algorithme échoue par occur-check : il y a dans E_m une équation de la forme $x \sim u$, x variable de u, $x \neq u$. Alors pour toute substitution σ, la taille de $x[\sigma]$ est toujours strictement inférieure à $u[\sigma]$.
  E_m n'est donc pas unifiable, et par H_m, E non plus.
  Il ne nous reste plus qu'à montrer :

  Lemme 4
  Pour tout n tel que (E_n, σ_n) est défini, H_n.

  Démonstration. On a $\sigma_0 = id$ et $E_0 = E$, et donc H_0 est triviale.
  Soit donc n tel que (E_n, σ_n) et (E_{n+1}, σ_{n+1}) soient définis.
  Montrons alors

  $$\exists \sigma',\ \sigma = \sigma' \circ \sigma_n \text{ et } \sigma' \text{ unifie } E_n$$
  $$\Longleftrightarrow$$
  $$\exists \sigma'',\ \sigma = \sigma'' \circ \sigma_{n+1} \text{ et } \sigma'' \text{ unifie } E_{n+1}$$

  Regardons chaque cas de l'algorithme :
  1. $E_n = E' \sqcup \{f(u_1, \ldots, u_n) \sim f(v_1, \ldots, v_n)\}$, et donc $E_{n+1} = E' \sqcup \{u_1 \sim v_1, \ldots, u_n \sim v_n\}$ et $\sigma_n = \sigma_{n+1}$.
     Dans ce cas, on voie bien que l'équivalence est vérifiée.
  2. $E_n = E' \sqcup \{x \sim x\}$, et donc $E_{n+1} = E'$ et $\sigma_{n+1} = \sigma_n$.
     Ici encore, l'équivalence est vérifiée.
  3. $E_n = E' \sqcup \{x \sim u\}$ ou $\{u \sim x\}$ avec $x \neq u$ et x n'est pas une variable de u, et donc $E_{n+1} = E'[x := u]$ et $\sigma_{n+1} = \sigma_n$.
     Alors
     ($\Leftarrow$) On prend $\sigma' = \sigma'' \circ [x := u]$.
     ($\Rightarrow$) Si σ' unifie E_n, alors $x[\sigma'] = u[\sigma']$. Par le lemme 3, on a $\sigma' = \sigma' \circ [x := u]$, et donc on a le résultat en posant $\sigma'' = \sigma'$.

  ◊

□