Examen du 14 février 2006

Tous les documents sont autorisés.

Merci de rédiger les réponses aux trois parties sur des feuilles indépendantes.

Le barème est donné à titre indicatif.

Exercice 1 sur 10 points (questions 1,2,3 sur 3 points et questions 5,6,7 sur 7 points)
Exercice 2 sur 5 points
Exercice 3 sur 4 points
Exercice 4 sur 6 points

1 Étude de la commutativité ; théories syntaxiques

Exercice 1

1. Soit $=_C$ la théorie définie sur $\mathscr{T}(\{+\}, \mathscr{X})$ par l'unique axiome de commutativité pour $+$:
$$x + y = y + x \qquad (C)$$
Montrer que toute preuve équationnelle entre deux termes C-égaux de $\mathscr{T}(\{+\}, \mathscr{X})$ peut se faire avec 0 ou 1 étape en tête. Vous pouvez procéder par induction sur la longueur de la preuve équationnelle.

2. En déduire que $s_1 + t_1 =_C s_2 + t_2$ si et seulement si $(s_1 =_C s_2 \wedge t_1 =_C t_2) \vee (s_1 =_C t_2 \wedge s_2 =_C t_1)$.

3. Utiliser la remarque précédente pour obtenir un algorithme d'unification modulo C sur $\mathscr{T}(\{+\}, \mathscr{X})$ en modifiant l'algorithme donné en cours pour l'unification dans la théorie vide (unification standard). Vous justifierez brièvement la correction, la complétude et la terminaison de votre algorithme.

4. Il existe une classe de théories équationnelles pour lesquelles on peut espérer obtenir un algorithme d'unification en utilisant la méthode suggérée ci-dessus pour la commutativité ; les théories dites *syntaxiques.* Dans la suite, nous supposerons que $\mathscr{F}$ est une signature finie. On dit qu'une théorie équationnelle $=_E$ définie sur $\mathscr{T}(\mathscr{F}, \mathscr{X})$ est syntaxique s'il existe un ensemble *fini* d'égalités E' tel que que $=_E$ et $=_{E'}$ sont identiques et toute preuve équationnelle entre deux termes égaux modulo E (*i. e.* E') peut se faire avec E' en utilisant 0 ou 1 étape en tête. E' est appelée une *présentation résolvante* de $=_E$.
On appelle *équation générale* sur $\mathscr{T}(\mathscr{F}, \mathscr{X})$ toute équation de la forme
$$f(x_1, \ldots, x_n) = g(x_{n+1}, \ldots, x_{n+m})$$

si f et g sont deux symboles de $\mathscr{F}$, d'arités respectives n et m[1] et $\{x_1, \ldots, x_n, \ldots, x_{n+m}\}$ est un ensemble de variables deux à deux disjointes. On note cette équation $Ge(f, g, \{x_1, \ldots, x_{n+m}\})$. Si E est une théorie équationnelle sur $\mathscr{T}(\mathscr{F}, \mathscr{X})$, on note $Ue(f, g, \{x_1, \ldots, x_{n+m}\}, E)$ l'ensemble des substitutions :

Si $f \neq g$ $Ue(f, g, \{x_1, \ldots, x_{n+m}\}, E) =$

$$\{(x_i \mapsto t_i)_{i=1\ldots n+m} \mid f(t_1, \ldots, t_n) = g(t_{n+1}, \ldots, t_{n+m}) \in E\}.$$

Si $f = g$ $Ue(f, f, \{x_1, \ldots, x_{2n}\}, E) =$

$$\{(x_i \mapsto t_i)_{i=1\ldots 2n} \mid f(t_1, \ldots, t_n) = g(t_{n+1}, \ldots, t_{2n}) \in E\} \bigcup (x_{n+i} \mapsto x_i)_{i=1\ldots n}).$$

5. Soit E' une présentation résolvante de $=_E$. Montrer que $Ue(f, g, \{x_1, \ldots, x_{n+m}\}, E')$ est un ensemble complet[2] et fini d'unificateurs pour l'équation générale $Ge(f, g, \{x_1, \ldots, x_{n+m}\})$ modulo E *i. e.* E'.

6. Montrer que la règle de transformation suivante sur les problèmes d'unification modulo

$$E: \quad \text{Mutate} \quad \frac{f(s_1, \ldots, s_n) = g(s_{n+1}, \ldots s_{n+m}) \wedge P}{\bigvee_{\mu \in Ue(f,g,\{x_1,\ldots,x_{n+m}\},E')} ((\exists \vec{z}) \bigwedge_{i=1}^{n+m} x_i\mu = s_i \wedge P)}$$

où les variables de $\vec{z}$ sont les variables introduites par μ.

est correcte et complète si E' une présentation résolvante de $=_E$, et les renommages adéquats sont appliqués de façon à ce que les variables $x_1, \ldots, x_{n+m}$ n'apparaîssent pas dans le problème original, non plus que les variables introduites par les substitutions de $Ue(f, g, \{x_1, \ldots, x_{n+m}\}, E')$.

7. Montrer que si $=_E$ est une théorie sans effondrement[3] et si toute équation générale $Ge(f, g, \{x_1, \ldots, x_{n+m}\})$ admet un ensemble fini complet d'unificateurs modulo E noté $CSU(f, g, \{x_1, \ldots, x_{n+m}\}, E)$, alors $=_E$ est syntaxique. Vous pourrez pour celà montrer que $R(E) = E \cup \bigcup_{(f,g) \in \mathscr{F}^2} \bigcup_{\mu \in CSU(f,g,\{\vec{x}\},E)} f(x_1, \ldots, x_n)\mu = g(x_{n+1}, \ldots, x_{n+m})\mu$ est une présentation résolvante de $=_E$.

[1] On supposera que c'est le cas dans toute la suite du problème.

[2] c'est-à-dire que pour toute solution σ de $Ge(f, g, \{x_1, \ldots, x_{n+m}\})$, il existe $\mu \in Ue(f, g, \{x_1, \ldots, x_{n+m}\}, E')$ et θ, deux substitutions telles que $\forall x_i \in \{x_1, \ldots, x_{n+m}\}, \quad x_i\sigma =_{E'} x_i\mu\theta$

[3] c'est-à-dire qui ne contient pas d'équations de la forme $x = t$ où x est une variable et t un terme non variable.

Solutions des exercices

Exercice 1:

Question 1 : On va montrer par induction sur n la propriété suivante :

$$P(n) \equiv \forall s,t \quad s \underset{C}{\longleftrightarrow}^{n} t \quad \Rightarrow (s \overset{\neq\Lambda}{\underset{C}{\longleftrightarrow}}{}^{*} t) \vee (\exists s', t' \quad s \overset{\neq\Lambda}{\underset{C}{\longleftrightarrow}}{}^{*} s' \overset{\Lambda}{\underset{C}{\longleftrightarrow}} t' \overset{\neq\Lambda}{\underset{C}{\longleftrightarrow}}{}^{*} t)$$

1. Si $n = 0$, la propriété est trivialement vérifiée avec la partie gauche de la disjonction.
2. Supposons la propriété vraie pour n, montrons qu'elle est vraie pour $n+1$. Soient donc s et t deux termes C égaux par une preuve équationnelle de longueur $n+1$. Cette preuve peut se décomposer comme suit :

$$s \underset{C}{\longleftrightarrow} u \underset{C}{\longleftrightarrow}^{n} t$$

En appliquant l'hypothèse d'induction à la preuve entre u et t, on distingue deux cas :
- $u \overset{\neq\Lambda}{\underset{C}{\longleftrightarrow}}{}^{*} t$. Si la première étape entre s et u n'a pas lieu en tête, alors $s \overset{\neq\Lambda}{\underset{C}{\longleftrightarrow}}{}^{*} t$ (partie gauche de la disjonction), sinon, il suffit de prendre $s' := s$ et $t' := u$ dans la partie droite de la disjonction.
- $\exists s', t' \quad \wedge\, u \overset{\neq\Lambda}{\underset{C}{\longleftrightarrow}}{}^{*} s' \overset{\Lambda}{\underset{C}{\longleftrightarrow}} t' \overset{\neq\Lambda}{\underset{C}{\longleftrightarrow}}{}^{*} t$.
  Si la première étape entre s et u n'a pas lieu en tête, il suffit de prendre $s' := s'$ et $t' := t'$ dans la partie droite de la disjonction.
  Sinon s est égal à $s_1 + s_2$, u à $s_2 + s_1$, s' à $s'_1 + s'_2$ et $t' = s'_2 + s'_1$ avec

$$s_2 \overset{m}{\underset{C}{\longleftrightarrow}} s'_1 \qquad\qquad s_1 \overset{m'}{\underset{C}{\longleftrightarrow}} s'_2$$

donc

$$s \equiv s_1 + s_2 \overset{\neq\Lambda}{\underset{C}{\longleftrightarrow}} s'_2 + s'_1 \equiv t'$$

et finalement

$$s \overset{\neq\Lambda}{\underset{C}{\longleftrightarrow}}{}^{*} t.$$

Question 2 : Si $s_1 + t_1 =_C s_2 + t_2$, alors il y une preuve équationnelle entre ces deux termes avec 0 ou 1 étape en tête. Dans le cas 0, $(s_1 =_C s_2 \wedge t_1 =_C t_2)$, et dans le cas 1, $(s_1 =_C t_2 \wedge s_2 =_C t_1)$.

Question 3 : Il suffit dans l'algorithme pour l'unification standard donné en cours, de remplacer la règle de décomposition par la règle

$$\text{Mutate} \quad \frac{s_1 + t_1 = s_2 + t_2}{(s_1 = s_2 \wedge t_1 = t_2) \vee (s_1 = t_2 \wedge s_2 = t_1)}$$

Cette règle est correcte et complète d'après la question ci-dessus. Les autres règles restent correctes et complètes. Les arguments de décroissance de la mesure vue en cours restent les mêmes pour ces règles. Quant à la règle Mutate, elle ne fait pas croître le nombre de variables non résolues du problème, et fait décroître strictement le multiensemble des tailles des équations. Les arguments selon lesquels un problème en forme normale pour l'ensemble des règles est en forme résolue restent identiques.

Question 5 : L'ensemble $Ue(f,g,\{x_1,\dots,x_{n+m}\},E')$ est fini, car par définition d'une présentation résolvante, E' est fini.

Par définition, si μ est dans $Ue(f,g,\{x_1,\dots,x_{n+m}\},E')$, $f(x_1,\dots,x_n)\mu =_{E'} g(x_{n+1},\dots,x_{n+m})\mu$, donc μ est une solution de $Ge(f,g,\{x_1,\dots,x_{n+m}\})$.

Soit σ modulo une solution de $Ge(f,g,\{x_1,\dots,x_{n+m}\})$, montrons que c'est une instance modulo E' d'un élément de $Ue(f,g,\{x_1,\dots,x_{n+m}\},E')$ sur les variables du problème initial *i. e.* $\{x_1,\dots,x_{n+m}\}$.

Comme E' est une présentation résolvante, il existe une preuve équationnelle de $f(x_1,\dots,x_n)\sigma =_{E'} g(x_{n+1},\dots,x_{n+m})\sigma$ avec 0 ou 1 étape en tête.

- S'il n'y a pas d'étape en tête, alors $f=g$ et $n=m$. On a alors une preuve équationelle de la forme

$$f(x_1,\dots,x_n)\sigma \equiv f(x_1\sigma,\dots,x_n\sigma) \xleftrightarrow[E']{\neq\Lambda} f(x_{n+1},\dots,x_{2n})\sigma \equiv f(x_{n+1}\sigma,\dots,x_{2n}\sigma)$$

  Donc $x_i\sigma =_{E'} x_{n+i}\sigma$ pour $i=1,\dots,n$. Soient μ et θ les substitutions respectivement définies par $\mu=(x_{n+i}\mapsto x_i)_{i=1,\dots,n}$ et $\theta\equiv(x_i\mapsto x_i\sigma)_{i=1,\dots,n}$. D'après ce qui précède, il est clair que $x_i\sigma =_{E'} x_i\mu\theta$ pour $i=1\dots 2n$. σ est donc une instance d'un élément de $Ue(f,f,\{x_1,\dots,x_{2n}\},E')$ (*i. e.* μ).
- S'il y a une étape en tête, elle utilise une égalité de E', $f(t_1,\dots,t_n)=g(t_{n+1},\dots,t_{n+m})$. On a alors une preuve équationnelle de la forme

$$\begin{array}{lll} f(x_1,\dots,x_n)\sigma & \equiv & f(x_1\sigma,\dots,x_n\sigma) \\ & \xleftrightarrow[E']{\neq\Lambda} & f(t_1\theta,\dots,t_n\theta) \\ & \xleftrightarrow[f(t_1,\dots,t_n)=g(t_{n+1},\dots,t_{n+m})]{\Lambda} & g(t_{n+1}\theta,\dots,g_{n+m}\theta) \\ & \xleftrightarrow[E']{\neq\Lambda} & g(x_{n+1},\dots,x_{n+m})\sigma \\ & \equiv & g(x_{n+1}\sigma,\dots,x_{n+m}\sigma) \end{array}$$

  Donc $x_i\sigma =_{E'} t_i\theta$ pour $i=1,\dots,n+m$. Soit μ la substitution de $Ue(f,g,\{x_1,\dots,x_{n+m}\},E')$ définie par $(x_i\mapsto t_i)_{i=1,\dots,n+m}$. Il est clair que $x_i\sigma =_{E'} x_i\mu\theta$ pour $i=1,ldots,n+m$.

Question 6 : Montrons tout d'abord que la règle est correcte. Soit donc σ une solution de $\bigvee_{\mu\in Ue(f,g,\{x_1,\dots,x_{n+m}\},E')}((\exists\vec{z})\bigwedge_{i=1}^{n+m} x_i\mu = s_i \wedge P)$. C'est une solution d'une disjonction, donc solution de l'un des membres $((\exists\vec{z})\bigwedge_{i=1}^{n+m} x_i\mu = s_i\wedge P)$ associé à une substitution μ de $Ue(f,g,\{x_1,\dots,x_{n+m}\},E')$. Il existe des valeurs pour les éléments de $\vec{z}$, données par la substitution θ de domaine $\vec{z}$ telles que σ est solution de $\bigwedge_{i=1}^{n+m} x_i\mu\theta = s_i\theta\wedge P\theta$. Par hypothèse sur la façon de construire les problèmes, les $\vec{z}$ n'apparaîssent pas dans les s_i ni dans P. σ est donc solution de $\bigwedge_{i=1}^{n+m} x_i\mu\theta = s_i\wedge P$. σ est solution de P. Il reste à montrer que σ est solution de $f(s_1,\dots,s_n)=g(s_{n+1},\dots,s_{n+m})$:

$$\begin{array}{llll} f(s_1,\dots,s_n)\sigma & \equiv & f(s_1\sigma,\dots,s_n\sigma) & \\ & =_{E'} & f(x_1\mu\theta\sigma,\dots,x_n\mu\theta\sigma) & \text{car } x_i\mu\theta\sigma =_{E'} s_i\sigma \\ & \equiv & f(x_1\mu,\dots,x_n\mu)\theta\sigma & \\ & =_{E'} & g(x_{n+1}\mu,\dots,x_{n+m}\mu)\theta\sigma & \text{car } f(x_1\mu,\dots,x_n\mu)=g(x_{n+1}\mu,\dots,x_{n+m}\mu)\in E' \\ & \equiv & g(x_{n+1}\mu\theta\sigma,\dots,x_{n+m}\mu\theta\sigma) & \\ & =_{E'} & g(s_{n+1}\sigma,\dots,s_{n+m}\sigma) & \text{car } x_i\mu\theta\sigma =_{E'} s_i\sigma \\ & \equiv & g(s_{n+1},\dots,s_{n+m})\sigma & \end{array}$$

Montrons maintenant que la règle est complète : soit donc σ une solution de $f(s_1, \ldots, s_n) = g(s_{n+1}, \ldots, x_{n+m}) \wedge P$. Soit ρ la substitution définie par $(x_i \mapsto s_i)_{i=1,\ldots,n+m}$, en supposant que les variables $x_1, \ldots, x_{n+m}$ n'apparaissent pas dans le problème de départ. σ est solution de

$$f(x_1\rho, \ldots, x_n\rho) = g(x_{n+1}\rho, \ldots, x_{n+m}\rho) \wedge \bigwedge_{i=1}^{i=n+m} x_i\rho = s_i \wedge P$$

$\rho\sigma$ est en particulier solution de $f(x_1, \ldots, x_n) = g(x_{n+1}, \ldots, x_{n+m})$, donc d'après la question précédente, instance sur $\{x_1, \ldots, x_{n+m}\}$ d'un élement μ de $Ue(f, g, \{x_1, \ldots, x_{n+m}\}, E')$ par une substitution θ :

$$\forall x_i \in \{x_1, \ldots, x_{n+m}\} \quad x_i\rho\sigma =_{E'} x_i\mu\theta$$

Soient $\vec{z}$ les variables introduites par μ. On peut sans perte de généralité les renommer de façon qu'elles n'apparaîssent pas dans le problème de départ. Or $x_i\rho = s_i$, donc

$$\forall x_i \in \{x_1, \ldots, x_{n+m}\} \quad s_i\sigma =_{E'} x_i\mu\theta$$

Comme les variables $\vec{z}$ n'apparaîssent pas dans les s_i ni dans P, θ donne aux variables $\vec{z}$ des valeurs telles que σ est solution de

$$\bigwedge_{i=1}^{i=n+m} s_i\theta = x_i\mu\theta \wedge P\theta$$

donc solution de

$$\exists \vec{z}, \bigwedge_{i=1}^{i=n+m} x_i\mu = s_i \wedge P$$

Question 7 : Par hypothèse $R(E)$ est fini. E et $R(E)$ définissent la même théorie équationnelle car $E \subset R(E)$ et pour toute équation de $R(E)$ soit elle est dans E, soit de la forme

$$f(x_1, \ldots, x_n)\mu = g(x_{n+1}, \ldots, x_{n+m})\mu$$

avec μ dans $CSU(f, g, \{\vec{x}\}, E)$, donc par définition

$$f(x_1, \ldots, x_n)\mu =_E g(x_{n+1}, \ldots, x_{n+m})\mu$$

Il reste à montrer que toute preuve entre deux termes E-égaux peut se faire avec au plus une étape en tête dans $R(E)$. Puisque la théorie est sans effondrement, aucun théorème équationnel n'est de la forme $x = t$ où x est une variable et t un terme non variable. La forme générale d'un théorème (avec au moins une étape) est donc

$$f(t_1, \ldots, t_n) = g(t_{n+1}, \ldots, t_{n+m}).$$

La substitution $\sigma = (x_i \mapsto t_i)_{i=1,\ldots,n+m}$ est solution de l'équation générale $f(x_1, \ldots, x_n) = g(x_{n+1}, \ldots, x_{n+m})$, donc instance de l'un des éléments μ de $CSU(f, g, \{\vec{x}\}, E)$. Il existe donc θ telle que

$$\forall x_i \in \{x_1, \ldots, x_{n+m}\} \quad x_i\sigma =_E x_i\mu\theta$$

On a donc

$$
\begin{array}{rcll}
f(t_1, \ldots, t_n) & \equiv & f(x_1\sigma, \ldots, x_n\sigma) & \text{car } t_i = x_i\sigma \\
& \overset{\neq\Lambda}{\underset{R(E)}{\longleftrightarrow}} & f(x_1\mu\theta, \ldots, x_n\mu\theta) & \text{car } E \subset R(E) \\
& \overset{\Lambda}{\underset{R(E)}{\longleftrightarrow}} & g(x_{n+1}\mu\theta, \ldots, x_{n+m}\mu\theta) & \text{car } f(x_1, \ldots, x_n)\mu = g(x_{n+1}, \ldots, x_{n+m})\mu \in R(E) \\
& \overset{\neq\Lambda}{\underset{R(E)}{\longleftrightarrow}} & g(x_{n+1}\sigma, \ldots, x_{n+m}\sigma) & \\
& \equiv & g(t_{n+1}, \ldots, t_{n+m}) &
\end{array}
$$