Résolution modulo une théorie équationnelle

I. Résolution modulo E

On note $s \approx t$ l'équation entre s et t — une formule —, pour la différencier de $s = t$, qui est une expression mathématique signifiant que s et t sont égaux.

Soit E une théorie équationnelle. On note $=_E$ la relation d'égalité modulo E, c'est-à-dire $s =_E t$ si et seulement si tout modèle de E donne les mêmes valeurs à s et à t.

Un *unificateur modulo* E de l'équation $s \approx t$ est une substitution σ telle que $s\sigma =_E t\sigma$. On dit aussi que σ *unifie* $s \approx t$, ou bien unifie s et t, modulo E. Un unificateur modulo E d'un ensemble $E' = \{s_i \approx t_i \mid 1 \leq i \leq n\}$ fini d'équations est une substitution σ qui unifie $s_i \approx t_i$ modulo E pour tout i, $1 \leq i \leq n$.

On dit que σ est *plus général* que σ' modulo E, en notation $\sigma \preceq_E \sigma'$, si et seulement s'il existe une substitution σ'' telle que $x\sigma\sigma'' =_E x\sigma'$ pour toute variable x. On note $\equiv_E$ la relation définie par $\sigma \equiv_E \sigma'$ ssi $\sigma \preceq_E \sigma'$ et $\sigma' \preceq_E \sigma$. On note $\prec_E$ la relation définie par $\sigma \prec_E \sigma'$ ssi $\sigma \preceq_E \sigma'$ mais $\sigma \not\equiv_E \sigma'$.

1. Un *mgu* de E' modulo E est un unificateur σ de E' modulo E qui est minimal pour $\preceq_E$, c'est-à-dire tel qu'il n'existe aucun unificateur σ' de E' modulo E avec $\sigma' \prec_E \sigma$.

   On dit que E est *unitaire* si et seulement si tout ensemble fini d'équations a au plus un unificateur modulo E. La théorie vide ($E = \emptyset$) est-elle unitaire ?

2. Montrer que la théorie $E = \mathrm{C}$ d'un symbole binaire $+$ commutatif ($\mathrm{C} = \{\forall x, y \cdot x + y \approx y + x\}$) n'est pas unitaire. On insiste sur le fait de trouver l'exemple le plus simple possible.

3. Se limiter aux théories unitaires est donc une restriction trop forte. On dira qu'une théorie E est *finitaire* si et seulement si, pour tout ensemble fini d'équations E', il existe un ensemble *fini* $csu_E(E')$ d'unificateurs de E' modulo E tel que : pour tout unificateur σ de E' modulo E, il existe un élément σ' de $csu_E(E')$ tel que $\sigma' \preceq_E \sigma$. On appellera un tel ensemble $csu_E(E')$ un *ensemble complet d'unificateurs* de E' modulo E, ou un csu modulo E ("complete set of unifiers").

   Montrer que si E' a un csu modulo E, alors il en a un qui n'est composé que de mgus.

4. De nombreuses théories équationnelles utiles sont finitaires, comme par exemple la théorie AC d'un symbole associatif et commutatif. Montrer en revanche que la théorie A d'un symbole $+$ qui n'est qu'associatif n'est pas finitaire. De nouveau, on exhibera un exemple le plus simple possible.

5. On considère le problème de la *satisfiabilité modulo* E d'un ensemble de clauses S du premier ordre. On dit que I est un *modèle modulo* E de S si et seulement si $I \models S$ et $I \models E$. S est *satisfiable modulo* E si et seulement si S a un modèle modulo E.

   On dit qu'un modèle est *de Herbrand modulo* E si et seulement si l'ensemble de ses valeurs est formé exactement des classes d'équivalence $[t]_E$ des termes clos t modulo E. De façon équivalente, un modèle de Herbrand modulo E est un ensemble de classes d'équivalence $[A]_E$ d'atomes clos modulo E.

   Montrer que S est satisfiable modulo E si et seulement si S a un modèle de Herbrand modulo E.

6. Montrer le théorème de compacité pour les clauses modulo E : si S est un ensemble (en général infini) de clauses du premier ordre, et S est insatisfiable modulo E, alors il existe un sous-ensemble fini S_{fin} de S qui est insatisfiable modulo E.

7. Montrer le théorème de Herbrand modulo E : S est insatisfiable modulo E si et seulement si l'ensemble $S\downarrow$ des instances closes de S est insatisfiable modulo E, si et seulement s'il existe un ensemble fini S_0 d'instances closes de S qui est insatisfiable modulo E.

8. Soit $\succ$ un ordre strict stable sur les atomes, et qui est *compatible* à la théorie équationnelle E, c'est-à-dire que si $A =_E A'$, $A' \succ B'$ et $B' =_E B$, alors $A \succ B$. Un atome A est maximal dans une clause C ssi il n'existe aucun atome B dans C tel que $B \succ A$. Soit sel une fonction de sélection.

   On considère la règle de résolution ordonnée avec sélection, adaptée au cas modulo E :

$$\frac{\overbrace{C_i \vee +A_{i1} \vee \ldots \vee +A_{in_i}}^{1 \leq i \leq \ell} \quad C' \vee -A'_1 \vee \ldots \vee -A'_\ell}{C_1\sigma \vee \ldots \vee C_\ell\sigma \vee C'\sigma}$$

   où :

   (i) $n_i \geq 1$ pour tout i, $1 \leq i \leq \ell$;

   (ii) $\sigma \in csu_E(\{A_{ij} \doteq A'_i | 1 \leq i \leq \ell, 1 \leq j \leq n_i\})$;

   (iii) $\mathrm{sel}\,(C_i \vee +A_{i1} \vee \ldots \vee +A_{in_i}) = \emptyset$ et $A_{i1}, \ldots, A_{in_i}$ sont maximaux dans $C_i \vee +A_{i1} \vee \ldots \vee +A_{in_i}$, pour tout i, $1 \leq i \leq \ell$;

   (iv) $\mathrm{sel}\,(C' \vee -A'_1 \vee \ldots \vee -A'_\ell) = \{-A'_1, \ldots, -A'_\ell\}$ et $\ell \geq 1$, ou bien aucun littéral n'est sélectionné, $\ell = 1$ et $-A'_1$ est maximal dans $C' \vee -A'_1 \vee \ldots \vee -A'_\ell = C' \vee -A'_1$.

   (Exercice à la "où est Charlie ?" : quelle est la différence avec la règle de résolution ordonnée avec sélection du cours ?)

   Comme d'habitude, cette règle s'entend après renommage éventuel des prémisses, de sorte qu'elles n'aient aucune variable en commun.

   Montrer que cette règle est correcte, au sens où si l'on peut déduire la clause vide à partir de S, alors S est insatisfiable modulo E.

9. Montrer qu'elle est complète : si S est insatisfiable modulo E, alors on peut déduire la clause vide de S en un nombre fini d'applications de la règle de résolution ordonnée avec sélection.

II. Résolution à contraintes

On considère le cas où E n'a plus nécessairement d'ensemble *fini* complet d'unificateurs. Pour ceci, on change le calcul de résolution. On fixe de nouveau un ordre strict $\succ$ stable sur les atomes, et compatible à E.

On appelle *contrainte élémentaire* toute expression de la forme $A \approx A'$ ou bien $A > A'$, où A et A' sont des atomes. On définit $\models_E A \approx A'$ si et seulement si $A =_E A'$, et $\models_E A > A'$ si et seulement si $A \succ A'$.

On appelle *contrainte* toute expression Γ telle que définie par la grammaire :

$$\begin{array}{rcl} \Gamma & ::= & A \approx A' \mid A > A' \\ & \mid & \top \\ & \mid & \bot \\ & \mid & \Gamma \wedge \Gamma \\ & \mid & \exists x \cdot \Gamma \end{array}$$

et l'on pose $\models_E \top$ (toujours), $\not\models_E \bot$ ($\bot$ est toujours faux), $\models_E \Gamma_1 \wedge \Gamma_2$ si et seulement si $\models_E \Gamma_1$ et $\models_E \Gamma_2$, $\models_E \exists x \cdot \Gamma$ si et seulement s'il existe un terme clos t tel que $\models_E \Gamma[x := t]$.

On dira que Γ est *satisfiable* si et seulement s'il existe une substitution close σ telle que $\models_E \Gamma\sigma$.

Une *clause contrainte* est une expression de la forme $C|\Gamma$, où C est une clause et Γ une contrainte. On dit que l'interprétation I satisfait $C|\Gamma$ modulo E si et seulement si $I \models E$, et pour toute substitution close σ telle que $\models_E \Gamma\sigma$, on a $I \models C\sigma$.

On plongera les clauses dans l'ensemble des clauses contraintes en lisant chaque clause non contrainte C comme la clause contrainte $C|\top$.

1. On considère la règle de *résolution contrainte* :

$$\frac{C \vee +A_1 \vee \ldots \vee +A_n|\Gamma \quad C' \vee -A'|\Gamma'}{C \vee C'|\Gamma \wedge \Gamma' \wedge \Gamma_\approx \wedge \Gamma_>}$$

   où $n \geq 1$, $\Gamma_\approx$ est la contrainte $A_1 \approx A' \wedge \ldots \wedge A_n \approx A'$, et $\Gamma_>$ est la contrainte formée de la conjonction des contraintes élémentaires $A_i > B$ ($1 \leq i \leq n$, B atome de C) et $A' > B'$ (B' atome de C').

   Montrer que cette règle est correcte, au sens où, si S est un ensemble de clauses contraintes tel que l'on peut en déduire une clause de la forme $\square|\Gamma$ avec Γ satisfiable, alors S est insatisfable modulo E.

2. Montrer que, si $\succ$ est total sur les atomes clos (pour tous atomes clos A et A', soit $A =_E A'$, soit $A \succ A'$, soit $A' \succ A$), alors la règle est aussi complète, c'est-à-dire que si S est un ensemble de clauses contraintes qui est insatisfable modulo E, alors on peut déduire de S une clause de la forme $\square|\Gamma$ avec Γ satisfiable.

3. La règle de résolution contrainte reste-t-elle complète lorsque $\succ$ n'est pas total sur les atomes clos ? On demande bien sûr une démonstration dans l'affirmative, et un contre-exemple dans la négative.