Unification dans les anneaux Booléens

Documents autorisés (en particulier le poly).

Les questions sont annotées par un niveau de difficulté, variant de (0) (facile) à (3) (difficile). En comptant 3 minutes passées par problème facile, 6 minutes par problème de difficulté (1), 9 minutes par problème de difficulté (2), et 12 minutes par problème de difficulté (3), vous aurez besoin de 2h39 pour tout faire — 3h32 pour 4, 8, 12 et 16 minutes. Il peut y avoir plusieurs réponses aux questions; dans ce cas, n'en donnez qu'une. Les parties II et III sont indépendantes.

Le but de ce problème est d'étudier l'unification modulo la théorie d'un anneau Booléen.

Partie I.

On considère la logique classique propositionnelle sur le langage suivant. Les formules propositionnelles F, G, ... sont les variables propositionnelles A, B, C, ..., les constantes **0** (faux), **1** (vrai), les connecteurs logiques binaires $\oplus$ (ou exclusif) et $\wedge$ (et logique). Les tables de vérité de ces opérateurs sont les suivantes:

$\oplus$	faux	vrai
faux	faux	vrai
vrai	vrai	faux

$\wedge$	faux	vrai
faux	faux	faux
vrai	faux	vrai

d'où l'on déduit la sémantique des formules.

On note $F \equiv G$ le fait que F et G soient deux formules sémantiquement équivalentes (i.e., $\rho \models F$ si et seulement si $\rho \models G$).

On considérera dans cette partie des substitutions qui envoient des variables propositionnelles sur des formules. On appelle substitution close toute substitution ς telle que $\varsigma(A)$ est une formule close (sans variable libre) pour toute variable propositionnelle A. En particulier, pour toute formule F, $F\varsigma$ est une formule close.

Pour toutes substitutions closes ς et ς', on dit que $\varsigma \equiv \varsigma'$ si et seulement si pour toute variable A, $A\varsigma \equiv A\varsigma'$.

Pour toute substitution close ς, on définit $r(\varsigma)$ comme étant l'affectation qui à toute variable A associe vrai si $\models \varsigma(A)$, et faux sinon. (Ceci fabrique une affectation à partir d'une substitution close.)

Réciproquement, our toute affectation ρ, on définit $s(\rho)$ comme étant la substitution qui à toute variable A associe **1** si $\rho(A)$ est vrai, et **0** si $\rho(A)$ est faux.

1. (1) Proposer une méthode permettant de décider si une formule F dans le langage ci-dessus est satisfiable ou non, et si oui, de retourner une affectation satisfaisant F.

2. (0) Montrer que pour toute affectation ρ, $r(s(\rho)) = \rho$.

3. (0) Montrer que pour toute substitution close ς, $s(r(\varsigma)) \equiv \varsigma$.

4. (1) Montrer que pour toute formule F, pour toute substitution close ς, $F\varsigma$ est une formule close telle que $\models F\varsigma$ si et seulement si $r(\varsigma) \models F$.

5. (0) En déduire un algorithme décidant si une formule F admet une substitution close ς telle que $\models F\varsigma$, et si oui, qui en retourne une. (On se ramènera au cas de la question I.1.)

6. (2) Pour toute formule F, pour toute substitution close ς, on définit $S(F, \varsigma)$ comme étant la substitution qui à toute variable A associe $A\varsigma \oplus (F \wedge (A \oplus A\varsigma))$.

   Montrer que si $\models F\varsigma$, alors pour toute substitution ς', $\models F\ S(F, \varsigma)\varsigma'$. (Indication: examiner les valeurs de vérité de $A\ S(F, \varsigma)\varsigma'$ en fonction de celles de $F\varsigma'$, pour toutes les variables A.)

7. (1) Montrer que pour toutes substitutions closes ς, ς' telles que $\models F\varsigma$ et $\models F\varsigma'$, alors $\varsigma' \equiv S(F,\varsigma)\varsigma'$.

Partie II.

La langage des anneaux Booléens est un langage du premier ordre formé sur les constantes 0, 1, ainsi que des symboles de fonction binaires $+$ et $*$, et du symbole de prédicat binaire $\doteq$.

Les anneaux Booléens sont les anneaux commutatifs dont la multiplication est idempotente et l'addition est 2-nilpotente. Autrement dit, ce sont les modèles équationnels (c'est-à-dire dans lesquels $\doteq$ est interprété par la relation d'égalité) de la théorie $\mathcal{B}$ suivante :

$$
\begin{array}{llll}
(\mathcal{B}1)\ (u+v)+w\doteq u+(v+w) & (\mathcal{B}2)\ u+v\doteq v+u & (\mathcal{B}3)\ u+0\doteq u & (\mathcal{B}4)\ u+u\doteq 0 \\
(\mathcal{B}5)\ (u*v)*w\doteq u*(v*w) & (\mathcal{B}6)\ u*v\doteq v*u & (\mathcal{B}7)\ u*1\doteq u & (\mathcal{B}8)\ u*u\doteq u \\
(\mathcal{B}9)\ (u+v)*w\doteq (u*w)+(v*w) & & &
\end{array}
$$

pour tous termes u, v, w du langage.

Pour tous termes u, v, on notera $\models_{\mathcal{B}} u\doteq v$ pour dire que les valeurs de u et de v sont les mêmes dans tous les anneaux Booléens.

Le problème de l'unification modulo $\mathcal{B}$ est le suivant: étant donné deux termes u et v dans le langage de $\mathcal{B}$, trouver les substitutions σ telles que $\models_{\mathcal{B}} u\sigma\doteq v\sigma$.

1. (0) Montrer que $\models_{\mathcal{B}} u\doteq v$ si et seulement si $\models_{\mathcal{B}} u+v\doteq 0$. En déduire qu'on peut réduire le problème de l'existence d'un $\mathcal{B}$-unificateur à la question de l'existence d'une substitution σ telle que $\models_{\mathcal{B}} w\sigma\doteq 0$, pour un certain terme w.

2. (0) Montrer qu'il existe σ tel que $\models_{\mathcal{B}} u\sigma\doteq v\sigma$ si et seulement s'il existe une substitution σ close (envoyant les variables libres de u et de v vers des termes clos) telle que $\models_{\mathcal{B}} u\sigma\doteq v\sigma$.

3. (2) On considère la théorie suivante Eq, dite théorie de l'égalité sur le langage de $\mathcal{B}$:

   $$
   \begin{array}{lll}
   (E1)\ u\doteq u & (E2)\ u\doteq v \Rightarrow v\doteq u & (E3)\ u\doteq v \wedge v\doteq w \Rightarrow u\doteq w \\
   (E4)\ u\doteq u' \wedge v\doteq v' \Rightarrow u+v\doteq u'+v' & (E5)\ u\doteq u' \wedge v\doteq v' \Rightarrow u*v\doteq u'*v' &
   \end{array}
   $$

   pour tous termes u, v, w, u', v'.

   Démontrer que dans tout modèle de $\mathcal{B}+Eq$ (la théorie ayant comme axiomes ceux de $\mathcal{B}$ et ceux de Eq), les formules suivantes sont valides:

   $$(\mathcal{B}10)\ 0+u\doteq u \quad (\mathcal{B}11)\ 0*u\doteq 0 \quad (\mathcal{B}12)\ u*0\doteq u$$

4. (1) Vérifier que l'interprétation canonique I^C est un modèle de $\mathcal{B}+Eq$, où I^C est définie comme suit : le domaine D est celui des formules closes de la partie I, $I^C(0)=\mathbf{0}$, $I^C(1)=\mathbf{1}$, $I^C(+)(x,y)=x\oplus y$, $I^C(*)(x,y)=x\wedge y$, $I^C(\doteq)$ est la relation $\equiv$.

5. (2) Vérifier que tout modèle équationnel de $\mathcal{B}$ est un modèle de $\mathcal{B}+Eq$. Réciproquement, montrer que, pour tout modèle I de domaine D de $\mathcal{B}$, on peut fabriquer une interprétation $I/I(\doteq)$, que l'on appellera modèle quotient, et qui est un modèle équationnel de $\mathcal{B}$.

6. (2) On appelle modèle de Herbrand équationnel de $\mathcal{B}$ tout modèle de la forme $I/I(\doteq)$, où I est un modèle de Herbrand de $\mathcal{B}$.

   Montrer que tous les modèles de Herbrand équationnels de $\mathcal{B}$ sont finis, et les décrire. (Indication: montrer que dans tous les modèles de Herbrand I de $\mathcal{B}+Eq$, pour tout élément u de l'univers de Herbrand, $I\models u\doteq 0$ ou $I\models u\doteq 1$.)

7. (3) On suppose donnée une correspondance bijective $x\mapsto A_x$ entre variables du premier ordre x et variables propositionnelles.

   On définit la traduction canonique suivante des termes de $\mathcal{B}$ vers les formules de la partie I par : $T(0)=\mathbf{0}$, $T(1)=\mathbf{1}$, $T(x)=A_x$, $T(u+v)=T(u)\oplus T(v)$, $T(u*v)=T(u)\wedge T(v)$. On remarquera que, si u est clos, $T(u)$ est la valeur de u dans le modèle canonique de la question II.4.

   Déduire des questions précédentes que, pour tous termes clos u et v, $\models_{\mathcal{B}} u\doteq v$ si et seulement si $\models T(u+v)\oplus\mathbf{1}$.

8. (1) On définit $\vec{T}$ par: $\vec{T}(\sigma)$ est la substitution qui à toute variable propositionnelle A_x associe $T(x\sigma)$. Montrer que T et $\vec{T}$ sont bijectives, et que pour tous termes u, toutes substitutions σ, $T(u\sigma) = T(u)\,\vec{T}(\sigma)$.

9. (2) Déduire des questions précédentes et de la question I.5 un algorithme décidant si deux termes de $\mathcal{B}$ ont un $\mathcal{B}$-unificateur, et si oui, qui en retourne un. Existe-t-il un algorithme en temps polynomial pour résoudre ce problème ? (On admettra que le problème de la satisfiabilité dans la logique de la partie I est NP-complet.)

10. (3) On dit de deux substitutions σ et σ' qu'elles sont $\mathcal{B}$-équivalentes, et on note $\sigma \equiv_{\mathcal{B}} \sigma'$, si et seulement si pour toute variable x, $\models_{\mathcal{B}} x\sigma \doteq x\sigma'$. On dit que σ est plus $\mathcal{B}$-général que σ', et on note $\sigma \leq_{\mathcal{B}} \sigma'$, si et seulement s'il existe une substitution σ'' telle que $\sigma\sigma'' \equiv_{\mathcal{B}} \sigma'$.

    Déduire des constructions précédentes et des questions I.6 et I.7 que la $\mathcal{B}$-unification est unitaire, c'est-à-dire que pour tous termes u et v dans le langage de $\mathcal{B}$, soit u et v ne sont pas unifiables, soit ils ont un unificateur le plus $\mathcal{B}$-général.

Partie III.

Le but de cette partie est de montrer que le langage de la partie I permet de trouver une structure aux propriétés analogues aux BDD, et analogies aux formes de Reed-Muller.

On se place donc dans le langage des formules propositionnelles de la partie I.

1. (1) Montrer que pour toute formule F, pour toute variable propositionnelle A, il existe deux formules F_1 et F_2 uniques à équivalence ($\equiv$) près, telles que $F \equiv (F_1 \wedge A) \oplus F_2$, et A n'est libre ni dans F_1 ni dans F_2.

2. (1) On dit qu'une formule F est indépendante d'une variable A si et seulement s'il existe une formule G dans laquelle A n'est pas libre, et telle que $F \equiv G$.

   Soient F_1 et F_2 deux formules dans lesquelles A n'est pas libre. Montrer que $(F_1 \wedge A) \oplus F_2$ est indépendante de A si et seulement si $F_1 \equiv \mathbf{0}$.

3. (2) On appelle forme de Reed-Muller ordonnée réduite une structure de style BDD définie comme suit. On se fixe un ordre total strict $<$ sur les variables propositionnelles. Les formes de Reed-Muller ordonnées réduites (RMO) sont définies inductivement comme étant $\mathbf{0}$, $\mathbf{1}$, et $A/\Phi_1;\Phi_2$, où Φ_1 et Φ_2 sont des RMO n'utilisant que des variables B telles que $A < B$, et $\Phi_1 \neq \mathbf{0}$.

   On définit la fonction suivante, qui retrouve une formule à partir d'un RMO: $f(\mathbf{0}) = \mathbf{0}$, $f(\mathbf{1}) = \mathbf{1}$, $f(A/\Phi_1;\Phi_2) = (f(\Phi_1) \wedge A) \oplus f(\Phi_2)$, et on définit la sémantique des RMO par: $\rho \models \Phi$ si et seulement si $\rho \models f(\Phi)$.

   Montrer que, pour deux RMO Φ_1 et Φ_2, $\Phi_1 \equiv \Phi_2$ si et seulement si $\Phi_1 = \Phi_2$. (Autrement dit, les RMO sont des formes canoniques de formules Booléennes.)

4. (3) Écrire des fonctions $+$ et $*$ prenant deux RMO en argument et retournant un RMO telles que $f(\Phi_1 + \Phi_2) \equiv f(\Phi_1) \oplus f(\Phi_2)$ et $f(\Phi_1 * \Phi_2) \equiv f(\Phi_1) \wedge f(\Phi_2)$, et en déduire un algorithme de construction du RMO représentant une formule donnée. (Autrement dit, trouver une fonction f^{-1} qui à toute formule F associe un RMO $f^{-1}(F)$, tel que $f(f^{-1}(F)) \equiv F$.)

5. (3) Soient F_1 et F_2 deux formules dans lesquelles A n'apparaît pas libre. Montrer que l'équation $(F_1 \wedge A) \oplus F_2 \equiv \mathbf{0}$ a une solution en A si et seulement si $(F_1 \wedge F_2) \oplus F_2 \equiv \mathbf{0}$, et qu'alors ses solutions sont exactement les formules équivalentes à $((F_1 \oplus \mathbf{1}) \wedge F) \oplus F_2$, pour F quelconque.

   En déduire un algorithme de $\mathcal{B}$-unification travaillant directement sur les RMO.