TD 9. Modélisation en logique du premier ordre

Exercice 1. Problème du rendu de monnaie

Le *problème du rendu de monnaie* est le problème algorithmique suivant : étant donnée une liste $v_1, \dots, v_k$ de valeurs de pièces et une somme S, trouver le nombre minimal de pièces nécessaire pour atteindre exactement la somme S.

Dans cet exercice, nous modélisons ce problème comme un problème SMT, plus précisément, comme un problème de satisfiabilité modulo la théorie de $(\mathbb{N}, +, \cdot, <, =)$.

Commençons par un exemple. Supposons que nous avons des pièces de 10, 20 et 50 centimes, et que nous voulons rendre une somme de 1,10 euro. Dans la notation ci-dessus : $k = 3$, $v_1 = 10$, $v_2 = 20$, $v_3 = 50$, et $S = 110$.

(a) Trouver le nombre minimal de pièces nécessaire pour atteindre exactement la somme $S = 110$ donnée.

(b) Écrire une formule atomique qui exprime que la combinaison linéaire positive de x_1 pièces de 10, x_2 pièces de 20, et x_3 pièces de 50 donne la somme S.

(c) Généraliser la formule trouvée dans la question précédente pour le cas d'une liste de valeurs quelconque, de longueur k quelconque.

(d) Écrire une formule atomique qui exprime que, si pour tout $1 \leq i \leq k$, x_i dénote le nombre de pièces de valeur v_i utilisé, nous avons utilisé exactement m pièces.

(e) Écrire une formule existentielle, $\varphi(m)$ à une variable libre, m, qui exprime qu'il existe une manière de rendre la somme S en utilisant exactement m pièces.

(f) En utilisant la formule $\varphi(m)$ de la question précédente, écrire une formule $\psi(m)$ à une variable libre, m, qui exprime que m est le nombre minimal de pièces nécessaire pour atteindre exactement la somme S.

Exercice 2. Nombres de Ramsey

Théorème 1 (Ramsey, version finie)**.** *Pour tout entier c et toute suite d'entiers $(n_1, n_2, \dots, n_c)$ il existe un entier m tel que pour toute coloration en c couleurs des arêtes du graphe complet K_m, il existe une couleur $1 \leq i \leq c$ et une clique de K_m d'ordre n_i qui soit monochromatique de couleur i.*

On considère la signature $L = (\emptyset, \{<, =, A, B_1, \dots, B_c\})$ où tous les symboles de relation sont binaires. L'interprétation escomptée est l'interprétation normale sur $(\mathbb{N}, <)$ où les nombres naturels dénotent les sommets du graphe, la relation $A(x, y)$ est vraie si les sommets x et y sont reliés par une arête, et, pour $1 \leq i \leq c$, $B_i(x, y)$ est vraie si les sommets x et y sont reliés par une arête, et cette arête porte la couleur n_i. Dans les questions suivantes, les formules sont des formules de la logique du premier ordre sur L.

(a) Écrire une formule à une variable libre m qui exprime le fait que le graphe ayant $\{0, \dots, m-1\}$ comme sommets est complet. On nomme $C(m)$ cette formule.

(b) Écrire une formule à une variable libre m qui exprime le fait que le graphe ayant $\{0, \dots, m-1\}$ comme sommets est complet, et que toutes ses arêtes sont coloriées (et chaque arête l'est de manière unique). On nomme $D(m)$ cette formule.

(c) Écrire une formule existentielle qui exprime le théorème de Ramsey fini, si on fixe $c = 2$, $n_1 = 3$ et $n_2 = 3$.

(d) Trouver le plus petit entier m qui vérifie la formule du point précédent.

(e) Est-ce qu'il existe une formule permettant d'exprimer le théorème de Ramsey fini ?

(f) * Est-ce qu'il existe une formule permettant d'exprimer le théorème de RAMSEY fini, si on fixe $c = 2$?

Exercice 3. Invariants de boucle

On souhaite synthétiser un invariant de boucle comme expliqué dans la section 16.4 des notes de cours. On considère pour cela le fragment de programme suivant :

```
int i = 1, s = 0;
while (i<6) {
    s=s+i;
    i=i+1;
}
assert(s = 15)
```

(a) Donner l'ensemble *Reach* $\subseteq \mathbb{Z}^2$ des configurations accessibles, c'est-à-dire des valeurs des variables `i` et `s` au cours de l'exécution du fragment de programme.

(b) Donner l'ensemble *Error* $\subseteq \mathbb{Z}^2$ des valeurs des variables `i` et `s` qui contredisent l'assertion.

(c) On se place dans une signature $(\{+^{(2)}, (i^{(0)})_{i\in\mathbb{N}}\}, \{<^{(2)}, =^{(2)}, \mathit{Inv}^{(2)}\})$ où les symboles de fonctions et de relation différents de *Inv* auront leur interprétation escomptée. Donnez les formules qui expriment le fait que *Inv* est un invariant inductif sûr du fragment de programme.

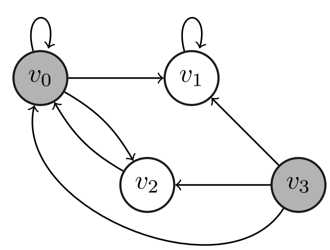
(d) Est-ce que $\mathit{Inv}^I = \mathit{Reach}$ est un modèle des formules du point précédent ? Proposer une autre interprétation qui soit un modèle.

Exercice 4. Examen 2019

On considère dans cet exercice la signature du premier ordre $L \stackrel{\text{def}}{=} (\emptyset, \mathcal{P})$ où $\mathcal{P} \stackrel{\text{def}}{=} \{E^{(2)}, =^{(2)}, G^{(1)}\}$. Soit l'interprétation I de domaine $D_I \stackrel{\text{def}}{=} \{v_0, v_1, v_2, v_3\}$ avec

$$
\begin{aligned}
E^I &\stackrel{\text{def}}{=} \{(v_0, v_0), (v_0, v_1), (v_0, v_2), (v_1, v_1), (v_2, v_0), (v_3, v_0), (v_3, v_1), (v_3, v_2)\} ,\\
=^I &\stackrel{\text{def}}{=} \{(v_0, v_0), (v_1, v_1), (v_2, v_2), (v_3, v_3)\} ,\\
G^I &\stackrel{\text{def}}{=} \{v_0, v_3\} .
\end{aligned}
$$

On peut voir I comme le graphe dirigé colorié ci-dessous, où « E » dénote la relation d'adjacence, « G » dénote les sommets gris et « $=$ » est l'égalité.



(a) Est-ce que I est un modèle de la formule $\varphi_{4,a} \stackrel{\text{def}}{=} \big(E(x, y) \land E(y, z)\big) \Rightarrow E(x, z)$? Justifiez.

(b) Est-ce que I est un modèle de la formule $\varphi_{4,b} \stackrel{\text{def}}{=} G(x) \Leftrightarrow \big(\forall y . (E(x, y) \land \neg(x = y)) \Rightarrow \neg G(y)\big)$? Justifiez.

(c) Écrivez une formule $\varphi_{4,c}$ qui exprime le fait que tous les sommets non gris de I ont un degré sortant de 1. L'interprétation I est-elle un modèle de votre formule ? Justifiez.