TD6 - Conception et vérification de programmes

Bastien Maubert et François Schwarzentruber

1 Une chose compliquée qu'on simplifie peut rester compliquée

En vous appuyant sur la preuve que le problème de satisfiabilité de K est PSPACE-complet, montrer qu'il reste PSPACE-complet pour K sans variables propositionnelles.

Soit une instance de QBF $\Phi = Q_1 p_1 \dots Q_n p_n \varphi$. On définit une formule de K dont le problème de satisfiabilité est équivalent de la manière suivante :

- $f(\psi) = \psi$ if ψ is propositional
- $f(\forall_i p_i \psi) = \Diamond(f(\psi) \wedge \Box^{n-i} p_i) \wedge \Diamond(f(\psi) \wedge \Box^{n-i} \neg p_i)$
- $f(\exists_i p_i \psi) = \Diamond(f(\psi) \wedge \Box^{n-i} p_i) \vee \Diamond(f(\psi) \wedge \Box^{n-i} \neg p_i)$

Il s'agit maintenant de transformer cette formule en une formue de K *sans variable* pour laquelle le problème de la satisfiabilité est équivalent.

2 Deux logiques équivalentes

On considère le langage suivant :

$$\varphi ::= \bot \mid p \mid \varphi \vee \varphi \mid \boxminus \varphi \mid \boxplus \varphi$$

On définit la logique $[S5; S5]$ par l'axiomatique suivante :

- les tautologies de la logique propositionnelle
- S5 pour $\boxminus$ et $\boxplus$, c'est à dire les instances de :
  - $\Box(p \to q) \to (\Box p \to \Box q)$
  - $\Box p \to p$;
  - $\Box p \to \Box\Box p$;
  - $\neg\Box p \to \Box\neg\Box p$

  où $\Box$ est soit $\boxminus$ ou $\boxplus$.
- les instances de l'axiome de commutation : $\boxminus\boxplus p \to \boxplus\boxminus p$;
- le modus ponens ;
- les règles de nécessitation.

On définit la logique $S5^2$ comme la logique des cadres $\mathcal{F} = (W_1 \times W_2, R_-, R_|)$ où :

– $(x, y)R_-(x', y')$ ssi $y = y'$;

– $(x, y)R_|(x', y')$ ssi $x = x'$.

La sémantique est naturelle.

Cet exercice a pour but de montrer que $S5^2 = [S5; S5]$, i.e. les validités de $S5^2$ sont exactement les théorèmes de $[S5; S5]$.

$Q1$) Donner une classe $\mathcal{C}_{[S5;S5]}$ de cadres pour $[S5; S5]$ telle que φ est un théorème de $[S5; S5]$ ssi φ est valide sur les modèles basés sur les cadres de $\mathcal{C}_{[S5;S5]}$. (indice : à quoi correspond la formule $\boxminus\Box p \to \Box\boxminus p$ sur les cadres ?)

Un modèle basé sur un cadre de $\mathcal{C}_{[S5;S5]}$ est appelé un modèle de $[S5; S5]$.

Le but est maintenant de montrer que si φ est satisfiable dans un modèle de $[S5; S5]$ alors φ est satisfiable dans un modèle de $[S5; S5]$ de taille au plus $2^{|\varphi|}$.

$Q2$) Expliquer pourquoi on peut se restreindre aux modèles où $R_- \circ R_| = W \times W$.

$Q3$) Donner une filtration, et montrer que le modèle filtré d'un modèle de $[S5; S5]$ est un modèle de $[S5; S5]$. Conclure.

L'objectif est ici de transformer un modèle fini de $[S5; S5]$ en un modèle de $S5^2$ qui lui est bisimilaire. Soit $\mathcal{M}$ un modèle fini de $[S5; S5]$.

$Q3$) Expliquer comment on peut transformer $\mathcal{M}$ en un modèle bisimilaire où les classes de la relation $R_- \cap R_|$ ont le même nombre de mondes.

$Q4$) Expliquer comment transformer le modèle résultat en modèle de $S5^2$ bisimilaire (le faire sur un exemple suffira).