TD7 - Conception et vérification de programmes

Bastien MAUBERT et François SCHWARZENTRUBER

1 Du parallélisme !

On considère trois processus P_1, P_2, P_3 avec une variable partagée x. Le programme du processus P_i est le suivant :

for $k_i = 1 \dots 10$
    $LOAD(x)$
    $INC(x)$
    $STORE(x)$

Autrement dit, P_i exécute 10 fois l'affectation $x := x+1$. L'affectation $x := x+1$ est réalisé avec les trois actions $LOAD(x)$, $INC(x)$ et $STORE(x)$. Considérons le programme parallèle P suivant :

$x := 0$
$P_1 \mid\mid P_2 \mid\mid P_3$

Est-ce que P a une exécution qui s'arrête avec la valeur $x = 2$?

2 Ascenseur

Consider an elevator system that services N > 0 floors numbered 0 through N-1. There is an elevator door at each floor with a call-button and an indicator light that signals whether or not the elevator has been called. For simplicity consider N $= 4$. Present a set of atomic propositions – try to minimize the number of propositions – that are needed to describe the following properties of the elevator system as LTL formulae and give the corresponding LTL formulae : (a) The doors are "safe", i.e., a floor door is never open if the elevator is not present at the given floor. (b) A requested floor will be served sometime.

(c) Again and again the elevator returns to floor 0. (d) When the top floor is requested, the elevator serves it immediately and does not stop on the way there.

3 Model-checking de LTL est... PSPACE-hard

Le $\models_\exists$-model-checking de LTL est défini de la manière suivante :

– $\mathcal{M} = (W, R, V)$ un modèle de Kripke sériel et $s \in W$, et une formule φ de LTL

– oui ssi $\mathcal{M}, s \models_\exists \varphi$.

On se propose d'encoder le problème CORRIDOR-TILING dans le model-checking de LTL. A vous de jouer ! Voici quelques indices cependant pour mener à bien la réduction :

– le chemin de $\mathcal{M}$ où φ sera vraie correspond à un balayage horizontal du pavage ;

– la formule φ peut encoder des contraintes du pavage.

4 Une formule LTL ne peut pas dire qu'il pleut un jour sur deux (en Bretagne) !

On considère LTL avec une seule proposition, p. On notera $p^i(\neg p)p^\omega$, $i \geq 0$, le chemin tel que $\{j \in \mathbb{N} \mid p \in \pi_j\} = \mathbb{N} \setminus \{i+1\}$.

Q1) Montrer que si φ a un nombre d' opérateurs "next" $\bigcirc$ inférieur ou égal à n, alors φ a la même valeur sur tous les chemins $p^i(\neg p)p^\omega$, pour $i > n$.

Q2) Conclure que, pour tout $m \geq 2$, il n'existe pas de formule de LTL φ tel que $\pi \models \varphi$ ssi $V(p) = \{\pi_{km} \mid k \in \mathbb{N}\}$.

5 LTL de profondeur 2, ça suffit !

L'objectif de cet exercice est de montrer qu'il existe une traduction tr qui traduit toute formule φ de LTL en une formule équisatisfiable $tr(\varphi)$ de LTL de profondeur modale 2. En d'autre terme, φ est satisfiable ssi $tr(\varphi)$ satisfiable. On note $\varphi[q := \psi]$ la formule φ dans laquelle on a substitué φ à q.

$Q1$) Soit φ, ψ des formules de LTL et q une proposition qui n'apparait pas dans ψ. Montrer que $\varphi[q := \psi]$ est satisfiable ssi $\varphi \wedge G(q \leftrightarrow \psi)$ est satisfiable.

$Q2$) Exhiber une traduction tr qui marche.