M1 MPRI
Exam on the first part of the Verification module

Thursday 3rd November, 2016

Lecture and exercise notes are allowed. Answers can be written in English or French.

Question 1 *(6 points)*

For each of the following LTL formulae ϕ_i, give a Büchi automaton (over the alphabet $\Sigma = 2^{\{a,b\}}$) whose language is the language of ϕ_i. Give each time a short explanation.

ϕ_1: $\mathsf{F}(a \implies \mathsf{F}\, b)$

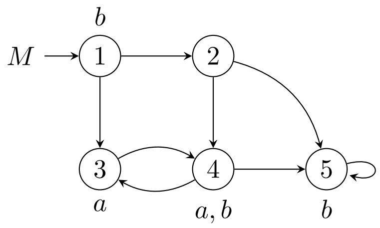
ϕ_2: $(\mathsf{F}\, a) \implies (\mathsf{F}\, b)$

ϕ_3: $\mathsf{G}(a \implies \mathsf{G}\, b)$

ϕ_4: $(\mathsf{G}\, a) \implies (\mathsf{G}\, b)$

Question 2 *(4 points)*

For each ϕ_i of the previous question, give the set of states of M which satisfy $\mathsf{A}\phi_i$ and the set of states which satisfy $\mathsf{E}\phi_i$. No explanation needed.



Question 3 *(7 points)*

The goal of this question is to prove some PSPACE-hardness results.

For this we will use the following tiling ("pavage" in French) problem. We consider a finite list of tiles $\mathsf{T} = \{T_1, \ldots, T_k\}$ and two binary relations $H, V \subseteq \mathsf{T}^2$ on these tiles to indicate which tiles match horizontally and vertically. We write $\mathbb{N}^* = \{1, 2, ..\}$ for the strictly positive integers and, given $n \in \mathbb{N}^*$, use $[n]$ to denote the interval $\{0, 1, \ldots, n-1\}$. For $n, m \in \mathbb{N}^*$, an (n, m) *tiling* is a mapping $p : [n] \times [m] \to \mathsf{T}$ that puts a tile from T on each discrete cell of the $n \times m$ rectangle (a same tile can be used several times). Here is an example of a $(4, 2)$ tiling:

$p_{\texttt{example}} =$

T_3	T_3	T_1	T_2
T_1	T_1	T_4	T_2

An (n, m) tiling p is *correct* iff the following three conditions hold:

$$p(0,0) = T_1 \ \wedge \ p(n-1, m-1) = T_k \ , \tag{P1}$$
$$\forall i \in [n]: \quad \forall j \in [m]: \quad i = 0 \vee \langle p(i-1, j), p(i, j)\rangle \in H \ , \tag{P2}$$
$$\forall i \in [n]: \quad \forall j \in [m]: \quad j = 0 \vee \langle p(i, j-1), p(i, j)\rangle \in V \ . \tag{P3}$$

Informally, a tiling is correct if the tiles that are horizontal neighbours are allowed by H, if the tiles that are vertical neighbours are allowed by V, and if the tiles used in the south-west and north-east corners are T_1 and T_k.

The decision problem we consider is:

Rectangular_Tiling

Input: A set of tiles T and two relations H, V as above; a *width* $w \in \mathbb{N}^*$ represented in base 1 (thus we consider that the size of the input is $k^2 + w$).

Output: yes iff there exists a *height* $h \in \mathbb{N}^*$ and a correct tiling of the $w \times h$ grid.

It is admitted that Rectangular_Tiling is PSPACE-complete.

With an instance $I = (\mathsf{T}, H, V, w)$ of the tiling problem, we associate the following set of $k+1$ propositions $AP = \mathsf{T} \cup \{\mathtt{edge}\}$. Given an (n, m) tiling $p : [n] \times [m] \to \mathsf{T}$, we associate an infinite word $\pi(p) = v_0 v_1 v_2 \ldots$ given by

$$T_j \in v_i \text{ iff } i < n \times m \text{ and } T_j = p(\mathrm{mod}(i, n), \mathrm{div}(i, n)),$$
$$\mathtt{edge} \in v_i \text{ iff } i < nm \text{ and } \mathrm{mod}(i+1, n) = 0,$$

for all $i \in \mathbb{N}$ and $j \in \{1, \ldots, k\}$ (mod and div denote the rest and the quotient of the Euclidian division). For example, the $(4, 2)$ tiling above has

$$\pi(p_{\mathtt{example}}) = \{T_1\} \cdot \{T_1\} \cdot \{T_4\} \cdot \{T_2, \mathtt{edge}\} \cdot \{T_3\} \cdot \{T_3\} \cdot \{T_1\} \cdot \{T_2, \mathtt{edge}\} \cdot \emptyset \cdot \emptyset \cdot \emptyset \cdots$$

3.1. Give a polynomial-sized LTL formula ϕ_0 (depending on I) such that $\pi \models \phi_0$ iff π is $\pi(p)$ for some $x \in \mathbb{N}^*$ and some (w, h) tiling p. (NB: Here and in the next question, you should briefly explain how your formula works but a mathematical proof of correctness is not needed.)

Is the size of ϕ_0 linear, quadratic, cubic, ..., in $|I|$?

3.2. Give a polynomial-sized LTL formula (depending on I) ϕ_1 such that, for all $h \in \mathbb{N}^*$ and (w, h) tilings p, $\pi(p) \models \phi_1$ iff p is a correct tiling.

Is the size of ϕ_1 linear, quadratic, cubic, ..., in $|I|$?

3.3. Conclude and prove that the problem to say if an LTL formula given as input is valid (i.e., holds in all words $\pi : \mathbb{N} \to 2^{AP}$) is PSPACE-hard.

3.4. In questions 3.2 and 3.3 above can you give formulae ϕ_0 and ϕ_1 that use X and F (and propositions and boolean combinators) but not the U, "until", modality? What do we conclude?

Question 4 *(4 points)*

Here are four CTL* formulae, where a is an atomic proposition:

$$\mathsf{AF}\,\mathsf{AX}\,a \quad (\phi_1) \qquad \mathsf{AX}\,\mathsf{AF}\,a \quad (\phi_2) \qquad \mathsf{AFX}\,a \quad (\phi_3) \qquad \mathsf{AXF}\,a \quad (\phi_4)$$

4.1. Which of these four formulae are CTL formulae? Are LTL formulae?

4.2. Two CTL* formulae ϕ and ψ are *equivalent* when $M, \pi \models (\phi \iff \psi)$ for all finite Kripke structures M and all runs π in M.

Say which formulae among $\phi_1, \phi_2, \phi_3, \phi_4$ are equivalent. (For equivalent formulae, give a proof of equivalence. For non-equivalent formulae, give a witness structure and run).