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

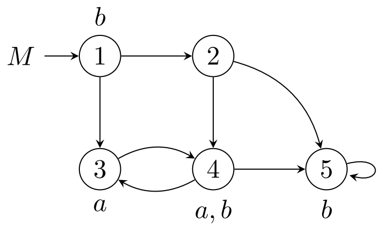
ϕ_2: $(\mathsf{F}\, a) \implies (\mathsf{F}\, b)$

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 $\pi(p) = v_0 v_1 v_2 \dots$ 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 $j \in \{1, \dots, k\}$ (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?

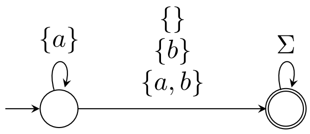
4.2. Two CTL* formulae ϕ and ψ are *equivalent* when $M, \pi \models (\phi \iff \psi)$ for all finite Kripke structures M and all runs π in M.

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).

Answers

Question 1

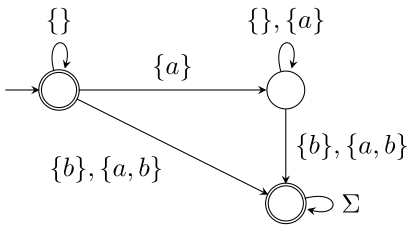
ϕ_1**:** $\mathsf{F}(a \implies \mathsf{F}\, b) \equiv \mathsf{F}(\neg a \vee \mathsf{F}\, b) \equiv (\mathsf{F}\neg a) \vee (\mathsf{F}\,\mathsf{F}\, b) \equiv (\mathsf{F}\neg a) \vee (\mathsf{F}\, b) \equiv \mathsf{F}(\neg a \vee b)$



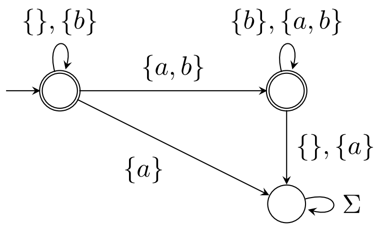
ϕ_2**:** $(\mathsf{F}\, a) \implies (\mathsf{F}\, b) \equiv (\neg\mathsf{F}\, a) \vee (\mathsf{F}\, b) \equiv (\mathsf{G}\,\neg a) \vee (\mathsf{F}\, b)$

A nondeterministic Büchi automaton with two initial states:

A deterministic version is also possible:



ϕ_3**:** $\mathsf{G}(a \implies \mathsf{G}\, b) \equiv (\mathsf{G}\,\neg a) \vee [(\neg a)\,\mathsf{U}\,(a \wedge \mathsf{G}\, b)] \equiv (\neg a)\,\mathsf{W}\,(a \wedge \mathsf{G}\, b)$ (W stands for "weak until".)



ϕ_4**:** $(\mathsf{G}\, a) \implies (\mathsf{G}\, b) \equiv \neg(\mathsf{G}\, a) \vee (\mathsf{G}\, b) \equiv (\mathsf{F}\,\neg a) \vee (\mathsf{G}\, b)$

Question 2

$\mathsf{E}\phi_1$**:** 1, 2, 3, 4, 5

$\mathsf{A}\phi_1$**:** 1, 2, 3, 4, 5

$\mathsf{E}\phi_2$**:** 1, 2, 3, 4, 5

$\mathsf{A}\phi_2$**:** 1, 2, 3, 4, 5

$\mathsf{E}\phi_3$**:** 1, 2, 4, 5

$\mathsf{A}\phi_3$**:** 5

$\mathsf{E}\phi_4$**:** 1, 2, 3, 4, 5

$\mathsf{A}\phi_4$**:** 1, 2, 5

$\phi_1 \equiv \mathsf{F}(\neg a \vee b)$. State 3 is the only one which does not satisfy $(\neg a \vee b)$, and no execution stays in 3 forever.

Every execution from every state satisfies $\mathsf{F}b$. Hence every execution from every state satisfies ϕ_2.

ϕ_3 means "once a is satisfied, b is satisfied forever (including in the first position satisfying a)." The executions which visit state 3 do not satisfy ϕ_3. All the others do: when a is satisfied in state 4, b is satisfied too, and, if we avoid state 3, we go to 5 (which satisfies b) and stay there forever.

Only the executions alternating between 3 and 4 satisfy $\mathsf{G}a$. They do not satisfy $\mathsf{G}b$, so they do not satisfy ϕ_4.

Question 3

3.1. We introduce some abbreviations:

$$\texttt{tiled} \stackrel{\text{def}}{=} \bigvee_{0<i\leq k} T_i \tag{1}$$

$$\texttt{nothing} \stackrel{\text{def}}{=} \neg(\texttt{tiled} \vee \texttt{edge}) \tag{2}$$

ϕ_0 is obtained as the conjunction of the following subformulae:

"π is in T^+ and ends with an $\texttt{edge}$":

$$\mathsf{G}\Big[\bigwedge_{0<i<j\leq k} \neg(T_i \wedge T_j)\Big] \bigwedge \texttt{tiled}\ \mathsf{U}\ \big(\texttt{tiled} \wedge \texttt{edge} \wedge \mathsf{XG}\,\texttt{nothing}\big)$$

"edges occur every wth position:

$$\Big[\bigwedge_{0\leq i<w-1} \mathsf{X}^i\neg\texttt{edge}\Big] \wedge \mathsf{G}\left[\begin{array}{ll} & \texttt{edge} \implies \mathsf{X}^w(\texttt{edge} \vee \texttt{nothing}) \\ \wedge & \neg\texttt{edge} \implies \mathsf{X}^w\neg\texttt{edge} \end{array}\right]$$

The size of $\texttt{tiled}$ and $\texttt{nothing}$ is $O(k)$, the size of the first subformula is $O(k^2)$, the size of the second subformula is $O(w^2+k)$. Hence the formula has quadratic size.

3.2. Since we assume that π is some $\pi(p)$, ϕ_1 just needs, e.g., the conjunction of the following subformulae:

"tiles respect H and V":

$$\mathsf{G}\bigwedge_{\substack{0<i,j\leq k\\ \langle T_i,T_j\rangle\notin H}} \Big[\neg(T_i \wedge \mathsf{X}\,T_j) \vee \texttt{edge}\Big] \quad \wedge \quad \mathsf{G}\bigwedge_{\substack{0<i,j\leq k\\ \langle T_i,T_j\rangle\notin V}} \neg(T_i \wedge \mathsf{X}^w T_j)$$

"they start with T_1 and end with T_k":

$$T_1 \quad\wedge\quad \mathsf{F}(T_k \wedge \mathsf{X}\,\texttt{nothing})$$

The size of the first subformula is $O(wk^2)$, the size of the second subformula is $O(k)$. Hence the formula has quadratic size.

3.3. The conjunction $\phi_0 \wedge \phi_1$ is satisfiable iff a correct tiling exists. This provides a reduction from $\mathsf{Rectangular\_Tiling}$ to LTL satisfiability. The reduction is obviously logspace and shows that LTL satisfiability is PSPACE-hard. Since validity is dual to satisfiability and since PSPACE coincides with coPSPACE, we conclude that LTL validity is PSPACE-hard.

3.4. In our first answer, we used only one U, in "$\texttt{tiled}\,\mathsf{U}\,(\texttt{tiled} \land \texttt{edge} \land \mathsf{XG}\,\texttt{nothing})$". We can define a version of ϕ_0 that does not use U:

$$\mathsf{G}\left[\begin{array}{ll} & \bigwedge_{0<i<j\leq k} \neg(T_i \land T_j) \\ \land & \texttt{nothing} \implies \mathsf{X}\,\texttt{nothing} \\ \land & \texttt{edge} \implies \texttt{tiled} \end{array}\right] \land \mathsf{F}\big[\texttt{tiled} \land \texttt{edge} \land \mathsf{X}\,\texttt{nothing}\big]$$

We conclude that the validity problem for LTL is already PSPACE-hard when restricted to the $L(\mathsf{F}, \mathsf{X})$ fragment.

Question 4

4.1 The first two formulae are CTL. The last two do not respect the syntax of CTL nor LTL formulae (but they are made of an LTL formula with an explicit "A" path quantifier so that they behave like LTL global specifications).

4.2 $\mathsf{XF}\,\psi$ and $\mathsf{FX}\,\psi$ are equivalent LTL formulae (trivial), hence ϕ_3 and ϕ_4 are equivalent.

These are in turn equivalent to ϕ_2:

- To see that ϕ_4 implies ϕ_2, assume $q \models \mathsf{AXF}\,a$ and pick any successor state q' of q. If π is any run from q' then $q \cdot \pi$ is a run from q, hence satisfies $\mathsf{XF}\,a$ hence $\pi \models \mathsf{F}\,a$. Since this holds for all π, we get $q' \models \mathsf{AF}\,a$. Since this holds for all $q \to q'$, we get $q \models \mathsf{AX}\,\mathsf{AF}\,a$.
- To see that ϕ_2 implies ϕ_4, assume $q \models \phi_2$ and take a run π from q. Since π has the form $q\,q'\,q'' \cdots$, the suffix run $\pi' = q'\,q'' \cdots$ is a run from q', a successor state of q. From $q \models \phi_2$, we get $q' \models \mathsf{AF}\,a$. Hence $\pi' \models \mathsf{F}\,a$. Hence $\pi \models \mathsf{XF}\,a$. This holds for all runs starting from q hence $q \models \phi_4$.

Now ϕ_1 and ϕ_2 are not equivalent. In the following structure s_1 does not satisfy $\mathsf{AX}\,a$. Thus the run $\pi = s_1^\omega$ that remains forever in s_1 does not satisfy $\mathsf{F}\,\mathsf{AX}\,a$. Hence $s_1 \not\models \phi_1$. However all runs satisfy $\mathsf{F}\,a$ hence all states satisfy $\mathsf{AF}\,a$. Thus all states satisfy ϕ_2.