Basics of Verification

Written exam, November 23rd, 2010

3 hours

The lecture notes are authorized, but no other documents.
Exercises are independent.
All answers should be rigorously and clearly justified.
The number in front of each question gives an indication on its length or difficulty.

1 Mutual Exclusion

Consider the following algorithm for 3 processes `P(0)`, `P(1)` and `P(2)`.

```
P(i): loop forever
1        req[i] := true
2        if turn = i then
3           turn := i+1 mod 3
4        wait until (turn = i or not (req[i+1 mod 3] or req[i+2 mod 3]))
5        cs[i] := true
6        Critical section
7        cs[i] := false
8        req[i] := false
      end loop
```

Initially, we assume that all boolean variables are set to `false` and `turn` is set to 0.

A counter-example is an infinite run which will be given as a sequence of steps each being described by the active process and the values, after the execution of this step, of all program counters (`pc`) and all shared variables (`req` and `cs`) as shown below:

active	pc			req			cs			turn
	0	1	2	0	1	2	0	1	2	
Init	1	1	1	F	F	F	F	F	F	0
0	2	1	1	T	F	F	F	F	F	0
1	2	2	1	T	T	F	F	F	F	0
1	2	4	1	T	T	F	F	F	F	0
1	2	4	1	T	T	F	F	F	F	0

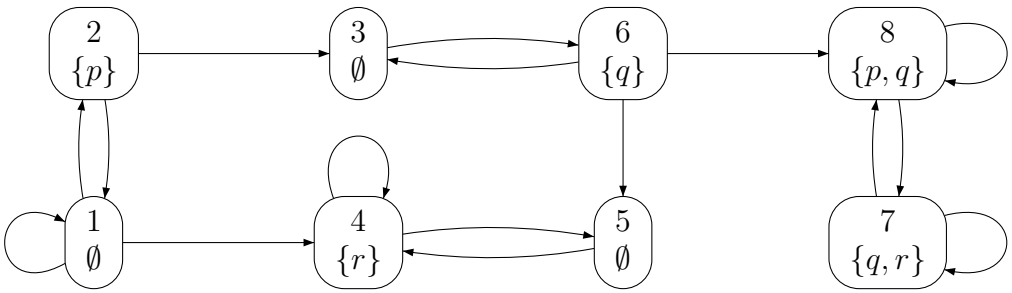
[2] **a)** Give a CTL formula expressing the mutual exclusion *safety* property (at most one process in the critical section) using the atomic propositions `cs[0]`, `cs[1]` and `cs[2]`. Show that this safety property is not satisfied.

[2] **b)** Consider the liveness property

$$\mathsf{AG}((\texttt{req[0]} \vee \texttt{req[1]} \vee \texttt{req[2]}) \longrightarrow \mathsf{AF}(\texttt{cs[0]} \vee \texttt{cs[1]} \vee \texttt{cs[2]}))$$

Show that this liveness property is not satisfied even for *fair* runs satisfying for each process `i` the formula $\texttt{fair[i]} = \mathsf{GF}\,\texttt{req[i]} \rightarrow \mathsf{GF}(\texttt{active} = \texttt{i})$.

2 Semantics of CTL*



Consider the above model M. Recall that if φ is a state formula, we denote by $[\![\varphi]\!]$ the set of states of M satisfying φ.

[4] **a)** Compute the following sets. For each state *in* $[\![\mathsf{E}\,\alpha]\!]$ give a path satisfying α and for each state *not in* $[\![\mathsf{E}\,\alpha]\!]$ explain why there are no paths satisfying α. Give dual explanations for formulæ of the form $\mathsf{A}\,\alpha$.

(i) $[\![\mathsf{EG}\,r]\!]$,

(ii) $[\![\mathsf{AX}\,q]\!]$,

(iii) $[\![\varphi_1]\!]$ where $\varphi_1 = (\mathsf{EG}\,r) \vee (\neg q \wedge \mathsf{EX}\,q)$,

(iv) $[\![\mathsf{E}\,\psi]\!]$ where ψ is the path formula $\psi = \mathsf{G}\,\mathsf{F}\,\varphi_1 \to \mathsf{G}\,\mathsf{F}(q \wedge \neg r)$,

(v) $[\![\mathsf{E}(\psi \wedge (q\,\mathsf{U}\,p))]\!]$,

(vi) $[\![\mathsf{A}(\psi \to \mathsf{F}\,p)]\!]$.

[1] **b)** For each state i of M, give a characteristic formula $\xi_i \in$ CTL such that $[\![\xi_i]\!] = \{i\}$ using only atomic propositions, boolean connectives and the modality EX.

3 Equivalences in CTL*

Let φ and ψ be arbitrary CTL* formulæ and consider the following state formulæ:

$$\varphi_1 = \mathsf{A}(\psi \to \mathsf{G}\,\mathsf{A}(\psi \to \mathsf{F}\,\varphi))$$
$$\varphi_2 = \mathsf{A}(\psi \to \mathsf{G}\,\mathsf{F}\,\varphi)$$
$$\varphi_3 = \mathsf{A}(\psi \to \mathsf{G}\,\mathsf{A}\,\mathsf{F}\,\varphi)$$

[1] **a)** Show that the formula $\varphi_3 \to \varphi_2$ is valid, i.e., for all model M and all state s, if $M, s \models \varphi_3$ then $M, s \models \varphi_2$.

[1] **b)** Show that the formula $\varphi_2 \to \varphi_3$ is not valid when $\psi = \mathsf{G}\,p$ and $\varphi = q$, i.e., find a model M and a state s such that $M, s \models \varphi_2$ and $M, s \not\models \varphi_3$.
Hint: Search a model with at most 3 states.

[1] **c)** Prove or disprove that the formula $\varphi_2 \to \varphi_1$ is valid when $\psi = q \to \mathsf{G}\,p$ and $\varphi = q$.

[2] **d)** Prove that the formula $\varphi_1 \to \varphi_2$ is valid when $\psi = q \to \mathsf{G}\,p$ and $\varphi = q$.

4 LTL and automata

Let $\mathrm{AP} = \{p, q\}$ be the set of atomic propositions and let $\Sigma = 2^{\mathrm{AP}}$ be its associated alphabet.

[4] **a)** Consider the formulæ $\alpha = \mathsf{F}(p \wedge \neg q)$, $\beta = \mathsf{F}(p \wedge \mathsf{X}\, p)$, and $\varphi = (\mathsf{G}(p \to q)) \to \mathsf{G}\,\beta$. The aim is to compute the generalized Büchi automaton (GBA) $\mathcal{A}_\varphi$ associated with φ with the construction seen during the course. The following intermediary steps are mandatory:

(i) Write the formula φ in negative normal form.

(ii) Draw the reduction graph starting from $\{\varphi\}$. Do not forget the marks $!\alpha$ and $!\beta$ on the reduction rules.

(iii) Give the sets $\mathrm{Red}(\{\varphi\})$, $\mathrm{Red}_\alpha(\{\varphi\})$ and $\mathrm{Red}_\beta(\{\varphi\})$.

(iv) Draw the transitions starting from state $\{\varphi\}$ in the GBA $\mathcal{A}_\varphi$.

(v) Complete the construction and draw the automaton $\mathcal{A}_\varphi$.
Indicate clearly the acceptance sets T_α and T_β.

5 LTL and Past

For $n > 0$, let $\mathrm{AP}_n = \{p_0, \ldots, p_{n-1}\}$ be a set of atomic propositions and let $\Sigma_n = 2^{\mathrm{AP}_n}$ be the associated alphabet. We want to show the existence of an $\mathcal{O}(n)$-sized LTL formula with future and past modalities such that any *initially* equivalent *pure future* LTL formula is of size $\Omega(2^n)$.

First, for $S \subseteq \mathrm{AP}_n$ we define the propositional formula $\alpha_S = \bigwedge_{p_i \in S} p_i \wedge \bigwedge_{p_j \in \mathrm{AP}_n \setminus S} \neg p_j$.

Next, consider the following *pure future* $\mathrm{LTL}(\mathrm{AP}_{n+1}, \mathsf{G})$ formula:

$$\varphi_n = \bigwedge_{S \subseteq \mathrm{AP}_n} ((\alpha_S \wedge p_n) \to \mathsf{G}(\alpha_S \to p_n)) \wedge ((\alpha_S \wedge \neg p_n) \to \mathsf{G}(\alpha_S \to \neg p_n))$$

[2] **a)** Let $w = b_0 b_1 b_2 \cdots \in \Sigma_{n+1}^\omega$ and $i \geq 0$. Show that $w, i \models \varphi_n$ if and only if for all $j \geq i$ such that $b_i \cap \mathrm{AP}_n = b_j \cap \mathrm{AP}_n$ we have $p_n \in b_i \iff p_n \in b_j$.

[2] **b)** Prove that there is a formula $\psi_n \in \mathrm{LTL}(\mathrm{AP}_{n+1}, \mathsf{Y}, \mathsf{S}, \mathsf{X}, \mathsf{U})$ of size $\mathcal{O}(n)$ which is *initially* equivalent to φ_n.

Fix a word $w = a_0 \cdots a_{2^n-1} \in \Sigma_n^{2^n}$ which is a permutation of the symbols in Σ_n (each letter of Σ_n occurs once in w). For each subset $K \subseteq \{0, \ldots, 2^n - 1\}$, define the word $w_K = b_0 \cdots b_{2^n-1} \in \Sigma_{n+1}^{2^n}$ whose projection on Σ_n is w and such that $K = \{i \mid p_n \notin b_i\}$:

for each $i \in \{0, \ldots, 2^n - 1\}$ we have $b_i = \begin{cases} a_i & \text{if } i \in K \\ a_i \cup \{p_n\} & \text{otherwise.} \end{cases}$

Recall that $\mathcal{L}(\mathsf{G}\,\varphi_n) = \{v \in \Sigma_{n+1}^\omega \mid v \models \mathsf{G}\,\varphi_n\}$.

[3] **c)** Prove that for all $K \subseteq \{0, \ldots, 2^n - 1\}$, we have $w_K^\omega \models \mathsf{G}\,\varphi_n$. Prove next that any generalized Büchi automaton recognizing $\mathcal{L}(\mathsf{G}\,\varphi_n)$ has at least 2^{2^n} states.

[1] **d)** Prove that any *pure future* formula $\varphi'_n \in \mathrm{LTL}(\mathrm{AP}_{n+1}, \mathsf{X}, \mathsf{U})$ which is *initially* equivalent to φ_n is of size $\Omega(2^n)$.