Examen – Initiation à la vérification

29 février 2012

Duration: 2.5 hours. All course materials can be used. Answers can be given in either French or English. Justify all your answers. The numbers given in brackets indicate the estimated difficulty or length of the exercise.

1. We consider labelled transition systems \( \langle S, A, T, s_0 \rangle \), where \( S \) is a set of states, \( A \) a set of actions, \( T \subseteq S \times A \times S \) a set of transitions (we write \( s \xrightarrow{a} s' \) for \( (s, a, s') \in T \)) and \( s_0 \in S \) the initial state.

We call \( s' \in S \) a final state if \( s' \) does not have any outgoing transitions; \( S_F \subseteq S \) is the set of final states. For two states \( s, s' \), we define the language \( \mathcal{L}(s, s') := \{ a_1 \cdots a_n \mid \exists s_1, \ldots, s_{n-1} \in S : s \xrightarrow{a_1} s_1 \cdots \xrightarrow{a_n} s' \} \), i.e. the language of action sequences leading from \( s \) to \( s' \); we denote \( \mathcal{L}(s) = \bigcup_{s' \in S_F} \mathcal{L}(s') \).

Given two labelled transition systems \( \mathcal{M}_1 = \langle S_1, A, T_1, s_0^1 \rangle \) and \( \mathcal{M}_2 = \langle S_2, A, T_2, s_0^2 \rangle \), we call \( H \subseteq S_1 \times S_2 \) a bisimulation between \( \mathcal{M}_1 \) and \( \mathcal{M}_2 \) iff

1. \((s_0^1, s_0^2) \in H\);
2. if \((s, t) \in H \) and \((s, a, s') \in T_1 \), then there exists \( t' \in S_2 \) such that \((t, a, t') \in T_2 \) and \((s', t') \in H\);
3. if \((s, t) \in H \) and \((t, a, t') \in T_2 \), then there exists \( s' \in S_1 \) such that \((s, a, s') \in T_1 \) and \((s', t') \in H\).

We call \( \mathcal{M}_1 \) and \( \mathcal{M}_2 \) bisimilar if such a bisimulation exists.

A Petri net \( \mathcal{N} = \langle P, T, F, W, m_0 \rangle \) defines a labelled transition system in the usual way; we let \( \mathcal{M}(\mathcal{N}) = \langle S, T, T', m_0 \rangle \), where \( S = \{ m \mid m : P \to \mathbb{N} \} \) is the set of all markings and \( T' = \{ (m, t, m') \mid \forall p \in P : m(p) \geq W(p, t) \land m'(p) = m(p) - W(p, t) + W(t, p) \} \) represents the possible transitions between the markings. For convenience, we will sometimes denote markings as words, where each place is repeated as often as it carries tokens, i.e. \( pppq \) denotes three tokens on \( p \) and one token on \( q \).

Also, let \( \mathcal{P} = \langle P, \Gamma, \Delta, A, c_0 \rangle \) be a pushdown system (PDS) where transitions are equipped with actions from \( A \); we define \( \mathcal{M}(\mathcal{P}) = \langle S, A, T, c_0 \rangle \), where \( S = P \times \Gamma^* \) are the configurations of \( \mathcal{P} \) and \( T = \{ (p\gamma w, a, qvw) \mid \exists p \gamma \xrightarrow{a} qv \in \Delta, \forall w \in \Gamma^* \} \). We call BPA (basic pushdown automata) the subclass of PDS with only one control state, i.e. \( P = \{ p \} \). In such a case, we may omit the state \( \delta \) from the rules and configurations.

(a) Let \( H \) be a bisimulation between two systems. Show that \((s, t) \in H \) implies \( \mathcal{L}(s) = \mathcal{L}(t) \). \[2\]
(b) Consider the following Petri net $N_1$:

![Petri net N1]

Describe the language $L(X)$ of $ℳ(N_1)$. 

(c) Provide a pushdown system $P$ such that $ℳ(P)$ is bisimilar to $ℳ(N_1)$. State the corresponding bisimulation $H$.

(d) Consider the following Petri net $N_2$:

![Petri net N2]

Show that there exists no pushdown system $P$ such that $ℳ(P)$ is bisimilar to $ℳ(N_2)$. (You can exploit that the language $L(c)$ of any configuration of a PDS is context-free.)

(e) Show that there is no BPA $P$ such that $ℳ(P)$ is bisimilar to $ℳ(N_1)$.

Some hints, assuming by contradiction that such a BPA exists and $pY$ (or just $Y$, remember we can omit $p$) is its initial configuration:

i. Regard the sequence $Y \xrightarrow{a} Y_1 \xrightarrow{\alpha_1} Y_2 \xrightarrow{\alpha_2} \cdots$ in $ℳ(P)$ and show that there exists some $Z \in Γ$, $\alpha, \beta \in Γ^*$, and $m, n > 0$ such that $a^m \in L(Y, Z\alpha)$ and $a^n \in L(Z, Z\beta)$.

ii. Now show that there exist $k, \ell \leq m$ with $b^k, cb^\ell \in L(Z)$.

iii. From these facts, one has $a^m b^k, a^m cb^\ell \in L(Y, \alpha)$. Conclude.

Notes: The results proven in this section show that the class of PDS is more expressive than its subclass BPA. Moreover, the class of Petri nets (in fact, even its subclass BPP, considered in the homework) contains examples that cannot be expressed by PDS. One can also find examples showing that the analogue results hold in reverse (PN stronger than BPP, BPA containing examples that are not expressible as PN).

2. Let $AP$ be a set of atomic propositions. Recall the following definitions related to stuttering equivalence:

- Let $\sigma, \rho$ be infinite sequences over $2^{AP}$. We call $\sigma$ and $\rho$ stuttering equivalent iff there are integer sequences $0 = i_0 < i_1 < i_2 < \cdots$ and $0 = k_0 < k_1 < k_2 < \cdots$ such that for all $\ell \geq 0$:

$$\sigma(i_\ell) = \sigma(i_\ell + 1) = \cdots = \sigma(i_{\ell+1} - 1) =$$

$$\rho(k_\ell) = \rho(k_\ell + 1) = \cdots = \rho(k_{\ell+1} - 1)$$

In other words, $\sigma$ and $\rho$ can be partitioned into “blocks” of possibly differing sizes, but with the same valuations.

- Let $\phi$ be an LTL formula over $AP$. We call $\phi$ invariant under stuttering iff for all stuttering-equivalent pairs of sequences $\sigma$ and $\rho$ we have $\sigma \models \phi$ iff $\rho \models \phi$. 


(a) Prove the following theorem: Any LTL formula that does not contain an \( X \) operator is invariant under stuttering. (Hint: Proceed by induction over the structure of the formula.)

(b) Consider the Kripke structure shown below with actions \( a, b, c, d, e \), where 0 is the initial state, and \( AP = \{ p \} \) such that \( p \) holds in states 1 and 4 only.

Determine all pairs of independent actions \( I \) and indicate which actions are visible and which are not.

(c) Compute a reduction function \( red \) that satisfies the conditions C0–C3 explained in the course. Wherever possible, \( red(s) \) should be a strict subset of \( en(s) \), for each state \( s \) of \( K \). Draw the reduced structure \( red(K) \).

3. Let \( x_n, \ldots, x_0, y_n, \ldots, y_0 \) be Boolean variables. We are interested in the relation where the binary number expressed by the \( x_i \) is greater by one than the number expressed by the \( y_i \). E.g., if \( n = 2 \), then the vector \( (100, 011) \) is in the relation because \( (100)_2 = 4 \) and \( (011)_2 = 3 \).

(a) For \( n = 2 \), express the above mentioned relation as a formula of propositional logic, using the variables \( x_2, x_1, x_0, y_2, y_1, y_0 \).

(b) For general \( n \geq 0 \), give a good variable order for a BDD expressing this relation such that the resulting BDD has a size linear in \( n \). Draw the corresponding BDD for \( n = 3 \).

(c) Consider the following BDD \( B_1 \) (you may still remember it from the course):

How many different assignments for the variables \( u, w, x, y, z \) lead to the result 1?

(d) Let \( B \) be a BDD over variables \( X := \{ x_1, \ldots, x_n \} \) respecting the order \( x_1 < \cdots < x_n \). Let \( Y \subseteq X \).

In the slides on BDDs (attached) you find an algorithm for computing the intersection of two BDDs. Give an analogous algorithm for computing \( \forall Y.B \). Your algorithm may use the one for intersection as a subroutine.

Exercise your algorithm on \( \forall y, u.B_1 \), where \( B_1 \) is the BDD from above, and give the result.