Exam – Initiation à la vérification

March 12, 2014

Duration: 2.5 hours. All course materials can be used. Answers can be given in either French or English. Justify all your answers.

1. Binary decision diagrams.
   Let \( V_n = \{ x_1, \ldots, x_n \} \) be a set of variables for \( n \geq 1 \), where \( x_i < x_j \) iff \( i < j \).
   Remark: In the following, when talking about the number of nodes of a BDD, we only count those nodes that are labelled by variables.

   (a) Give a BDD with variables from \( V_4 \) that has as many nodes as possible. (Be careful to avoid redundant nodes or isomorphic subgraphs!)

   (b) What is the maximal number of nodes in a BDD if the set of variables is \( V_5 \) or \( V_6 \)?

   (c) Generally, if the set of variables is \( V_n \), for arbitrary \( n \), let \( N^*_n \) be the maximal number of nodes labelled by \( x_i \). Give a formula to compute \( N^*_n \).

2. Coverability graphs.
   (a) The construction of coverability graphs, as defined in the lecture slides, is not entirely deterministic: e.g., the order in which nodes are taken from the worklist is undefined. Give an example of a net \( N \) and two possible coverability graphs of \( N \) that are non-isomorphic to each other. In each case, indicate the order in which nodes were treated in the worklist.

   (b) A marking of a net \( N \) is said to be a deadlock if no transition can fire in it. Clearly, \( N \) contains a reachable deadlock iff the reachability graph of \( N \) contains a node with no outgoing edges. Can the same be said of \( N \) and any of its coverability graphs?

   Let \( \phi \) be an LTL-formula. We define the \( X \)-depth of \( \phi \) as the maximal nesting of \( X \)-operators in \( \phi \), i.e., \( d_X(\phi) = 0 \) if \( \phi \) does not contain any occurrence of \( X \); \( d_X(\phi) = \max\{d_X(\phi_1), d_X(\phi_2)\} \) if \( \phi = \phi_1 U \phi_2 \), and \( d_X(\phi) = d_X(\phi_1) + 1 \) if \( \phi = X \phi_1 \). The \( U \)-depth \( d_U(\phi) \) is defined analogously for the nesting depth of the \( U \)-operator. The language \( LTL(U^m, X^n) \) signifies the language of LTL formulae \( \phi \) with \( d_U(\phi) \leq m \) and \( d_X(\phi) \leq n \), where \( m = \infty \) or \( n = \infty \) indicates no restriction of the operator in question.

   Let \( \alpha \in \Sigma^\omega \) (for some alphabet \( \Sigma \)), and let \( \alpha(i) \) denote the \( i \)-th letter of \( \alpha \) (beginning at \( i = 0 \)). We say that \( \alpha(i) \) is \( n \)-redundant in \( \alpha \) (for \( n \geq 0 \)) if \( \alpha(i) = \alpha(i+1) = \cdots = \alpha(i+n+1) \) and there is \( j > i \) with \( \alpha(j) \neq \alpha(i) \). The \( n \)-canonical form of \( \alpha \) is obtained by deleting from it all \( n \)-redundant letters, and two words \( \alpha, \beta \) are \( n \)-stutter-equivalent if they have the same canonical form. A language \( L \subseteq \Sigma^\omega \) is called \( n \)-stutter-closed if it is closed under \( n \)-stutter-equivalence.

   (a) We learned in the course that every language definable in \( LTL(U^\infty, X^0) \) is \( 0 \)-stutter-closed. Prove that for any \( n \geq 0 \), the languages in \( LTL(U^\infty, X^n) \) are \( n \)-stutter-closed.
(b) A similar principle can be formulated when the $U$-depth is restricted. Let $\phi \in LTL(U^m, X^0)$, where $m \geq 1$. Prove that for all $u, v \in \Sigma^*$ and $\alpha \in \Sigma^\omega$ we have that $u^m \alpha$ satisfies $\phi$ iff $u^{m+1} \alpha$ does.

(c) Using the results above, show that the language $(aa|ab)^\omega$ cannot be defined by any LTL formula. (Remark: The language can, however, be accepted by a Büchi automaton.)

4. Bisimulation

(a) In the figure below, determine for each pair of Kripke structures $K_i, K_j$ whether $K_i \equiv K_j$, either by giving a bisimulation or reasoning that none exists. (As usual, identical colours - black and white - indicate identical labellings.)

(b) Prove or refute (by a counterexample) the following claims:

- Let $H$ be a bisimulation between structures $K_1$ and $K_2$ and $J$ a bisimulation between $K_2$ and $K_3$. Is $H \circ J$ a bisimulation between $K_1$ and $K_3$?
- Let $H, J$ be bisimulations between structures $K_1$ and $K_2$. Is $H \cup J$ a bisimulation?