Exam – Initiation à la vérification

January 12, 2017

Duration: 2 hours. All course materials can be used. Answers can be given in either French or English. Justify all your answers.

1. **Petri nets**

   Let $N = \langle P, T, F, W, m_0 \rangle$ be a Petri net, and let R be the set $reach(m_0)$, i.e. the set of markings reachable from m_0 in N. With $N(m)$ we denote the net that is like N but with m as the intitial marking. We write $m \geq m'$ if $m(p) \geq m(p')$ for all $p \in P$. An *invariant* of N is a vector I with one entry for each place such that $C^T x = 0$, where C is the incidence matrix of N. An invariant is called *positive* if $I(p) > 0$ for every place $p \in P$.

   We define the following properties of nets:

   - N is *live* if for every marking $m \in R$ and every transition $t \in T$, m can reach a marking m' such that m' enables t (intuitively, every transition t can always occur again).
   - N is *bounded* if there exists some $K \in \mathbb{N}$ such that for all places $p \in P$ and all reachable markings $m \in R$, $m(p) \leq K$.
   - N is *cyclic* if every marking $m \in R$ can reach m_0.

   (a) Consider the eight different combinations of these three properties and their negations:

   i. not live, not bounded, not cyclic
   ii. not live, not bounded, cyclic
   iii. not live, bounded, not cyclic
   iv. not live, bounded, cyclic
   v. live, not bounded, not cyclic
   vi. live, not bounded, cyclic
   vii. live, bounded, not cyclic
   viii. live, bounded, cyclic

   For each case, either give an example of a Petri net *with one single place* that exhibits these properties or explain why it is not possible to construct such a net.

   (b) Prove or refute the following properties:

   i. If N has a positive invariant, then N is bounded.
   ii. If N is live and $m \geq m_0$, then $N(m)$ is live.

2. **BDDs and Abstraction**

   In logic, an "interpolant" between two formulas F and G is a formula that is implied by F, implies G, and uses on variables that occur in both F and G. In the context of counterexample-guided abstraction refinement (CEGAR), it is interesting to compute such interpolant, p.ex. to refine an equivalence class that was too coarse and led to a spurious counterexample. We shall study interpolants in the context of propositional logic.

   So, let F, G be two formulae of propositional logic (PL) such that $F \to G$, and let V_F, V_G the variables appearing syntactically in F, G, respectively. Formally, an *interpolant* for (F, G) is another PL-formula H such that $F \to H$, $H \to G$, and $V_H \subseteq V_F \cap V_G$.

(a) Prove or refute that the following formulae are interpolants for (F, G) where $Y = V_F \setminus V_G$ and $Z = V_G \setminus V_F$:
(i) $\forall Y : F$; (ii) $\exists Z : G$; (iii) $\forall Z : G$

(b) Show that $I := \exists Y : F$ is the strongest interpolant for (F, G). (I.e., I is an interpolant, and for any other interpolant J, we have $I \to J$.)

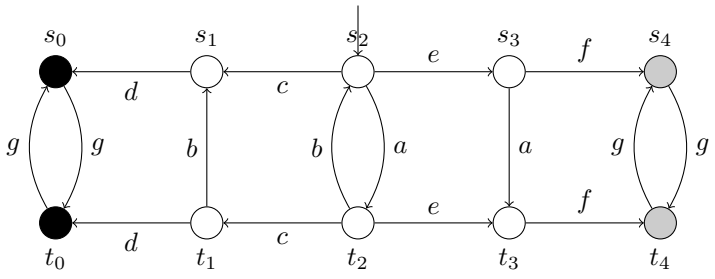
(c) Let B, C be BDDs representing F, G respectively, with $F \to G$. Write a procedure (in pseudo-code) that takes B, C as input and outputs the BDD of an interpolant H for (F, G).

- Your algorithm should be in the style of the intersection algorithm seen in the course, i.e. consider a pair of root nodes and specify the result as a either a base case or some recursion.
- The result of your algorithm should not simply compute the strongest interpolant. Use the fact that the models of H include those of F and are included in those of G.
- When the root of B is labelled by a variable, use $top(B)$, B_1, B_0 to denote the label and the two children, respectively. Use $mk(x, D_1, D_0)$ to obtain a BDD whose root is labelled by x and whose children are D_1, D_0, respectively.
- You may test BDDs for equality among each other or to a constant, and compute intersections and conjunctions.

(d) Let $F := \neg x_1 \wedge \neg x_2 \wedge x_3$ and $G := \neg x_2 \vee \neg x_3 \vee x_4$. Draw BDDs for F and G. What is the result of your algorithm in this case?

3. **Partial-order reduction**

Consider the structure shown below, where states with identical shades indicate that they satisfy the same atomic properties.



(a) Which pairs of actions are independent of each other? (It suffices to examine those that actually appear together at some state.) Which actions are visible and invisible?

(b) According to the rules of reduction C0–C3, which transitions can be eliminated from the system?

(c) Ignoring C0–C3, propose a maximal set of transitions that can be removed while maintaining stuttering equivalence.

Reminder: **C0** = no additional deadlocks may be introduced; **C1** = for every state s, every path starting at s in the original system satisfies the following: no action that depends on some action in $red(s)$ occurs before an action from $red(s)$; **C2** = when reducing, only invisible actions can be kept; **C3** = for all cycles in the reduced system: if $a \in en(s)$ for some state s in the cycle, then $a \in red(s')$ for some state s' in the cycle.