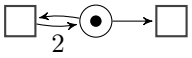
Exam solution – Initiation à la vérification

January 12, 2016

1. **Petri nets**

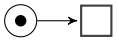
   (a) i. not live, not bounded, not cyclic

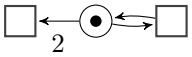
   ii. not live, not bounded, cyclic: impossible

   Suppose that a net (with place p) is cyclic and unbounded but not live, i.e. there exists a transition t and a marking $m \in R$ such that m cannot reach any m' with $m'(p) \geq W(p,t)$.
   But due to cyclicity, one can reach m_0 from any $m \in R$, and due to unboundedness, $R = \mathit{reach}(m_0)$ contains a marking m' with $m'(p) \geq W(p,t)$, a contradiction.

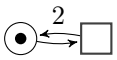
   iii. not live, bounded, not cyclic

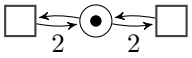
   iv. not live, bounded, cyclic

   v. live, not bounded, not cyclic

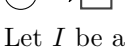
   vi. live, not bounded, cyclic

   vii. live, bounded, not cyclic: impossible

   Let p be the single place. Call a transition t *increasing* if $W(p,t) < W(t,p)$, *preserving* if $W(p,t) = W(t,p)$, and *decreasing* if $W(p,t) > W(t,p)$.
   Suppose that the net is bounded but not cyclic. Boundedness implies that no transition can be increasing. If the net had preserving transitions only, then only the initial marking is reachable, and the net would be cyclic. Thus the net must have at least one decreasing transition t. Consider the run where we repeat t until the number of tokens is less than $W(p,t)$. After this, t can never fire again, hence the net is not live.

   viii. live, bounded, cyclic

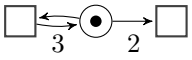
   

   (b) Let I be a positive invariant, m some reachable marking and q some place. We have

$$m(q) \leq m(q) \cdot I(q) \leq \sum_{p \in P} I(p) \cdot m(p) = \sum_{p \in P} I(p) \cdot m_0(p).$$

The first two steps are justified by the fact that I is positive and $m(p) \geq 0$ for all p. The last step follows from the fact that I is an invariant. The latter expression is a constant and provides a bound for q (and in fact for all places).

The statement is false. The net shown below is live and can reach any odd number of tokens. However, if $m(p) = 2$, the net can reach 0 tokens and is unable to continue afterwards.



2. BDDs and Abstraction

For a set of variables X, let 2^X denote the set of Boolean assignments over X. For an assignment A, $F[X/A]$ denotes the formula where occurrences of all $x \in X$ in F are replaced by $A(x)$. Models of formulae are taken to be assignments over $V_F \cup V_G$, and $M_{|X}$ denotes the restriction of an assignment M to X. $M[X \mapsto A]$ denotes the assignment that assigns $A(x)$ to x if $x \in X$ and $M(x)$ otherwise.

(a) i. Not an interpolant. P.ex., for $F = x, G = \top$, we have $\forall Y : F = \bot$, and $\bot \not\rightarrow F$.

ii. Not an interpolant. P.ex., for $F = \bot, G = x$, we have $\exists Z : G = \top$, and $\top \not\rightarrow G$.

iii. $\forall Z : G$ is an interpolant.

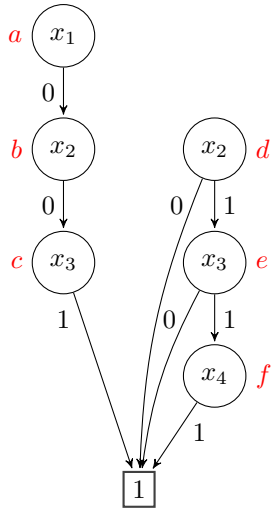
- Let M be a model of $\forall Z : G = \bigwedge_{A \in 2^Z} G[Z/A]$. So in particular $M \models G[Z/M_{|Z}]$ and hence $M \models G$.
- For any assignment M, $M \models F$ implies $M \models G$. But $M \models F$ is independent of $M_{|Z}$, so we can conclude that $\forall Z : (F \rightarrow G)$, which is logically equivalent to $F \rightarrow (\forall Z : G)$. (applying the law $a \rightarrow (b \wedge c) \equiv (a \rightarrow b) \wedge (a \rightarrow c)$).

(b)
- I is an interpolant: Let $F' := \neg G$ and $G' := \neg F$, so $F' \rightarrow G'$. From (a) we know that $F' \rightarrow \forall Y : G' \rightarrow G'$, and by contraposition $F \rightarrow \exists Y : F \rightarrow G$.
- Let J be any interpolant for (F, G); we show $I \rightarrow J$: Let $M \models I$. Then there exists $A \in 2^Y$ such that $M \models F[Y/A]$. Let $M' = M[Y \mapsto A]$, then $M' \models F$ and, since J is an interpolant, $M' \models J$. But M and M' differ only on variables that do not occur in J, hence $M \models J$.

(c) The algorithm implements the cases of the equation given below. The first three cases are trivial, and the last case is the usual recursion due to applying the *ite* operator. The cases where a variable occurs in one BDD but not the other are resolved using the lessons from (a) and (b): Variables from $V_F \setminus V_G$ are eliminated by existential quantifier, and variables from $V_G \setminus V_F$ by universal quantifier.

$$inter(F,G) \equiv \begin{cases} F & \text{if } F = 0 \text{ or } F = 1 \\ G & \text{if } G = 1 \\ F & \text{if } F = G \\ inter(F_0 \vee F_1, G) & \text{if } top(F) < top(G) \\ inter(F, G_0 \wedge G_1) & \text{if } top(F) > top(G) \\ mk(x, inter(F_1, G_1), inter(F_0, G_0)) & \text{if } x = top(F) = top(G) \end{cases}$$

(d) The drawing below gives the BDDs for F (root node a) and G (root node d).



The equation from (c) yields:

$inter(a, d) = inter(b \vee 0, d) = inter(b, d) = mk(x_2, inter(0, e), inter(c, 1)) = mk(x_2, 0, 1).$

The resulting BDD represents the formula $\neg x_2$, which is indeed implied by F and implies G.

3. **Partial-order reduction**

(a) The following states have multiple enabled actions:
- s_2 with $\{a, c, e\}$: of the three pairs, only $\langle a, e\rangle$ form a 'diamond'.
- t_2 with $\{b, c, e\}$: dito for $\langle b, c\rangle$.
- t_1 with $\{b, d\}$: we conclude that $\langle b, d\rangle$ are not independent.
- s_3 with $\{a, f\}$: dito for $\langle a, f\rangle$.

Thus, the only relevant independent pairs are $\langle a, e\rangle$ and $\langle b, c\rangle$.
Obviously, only d and f are visible, the other actions are invisible.

(b) Not a single transition can be removed according to rules C0–C3. In fact, it suffices to apply rules C0 and C1, due to the dependencies found in (a).

(c) There are three classes for stutter equivalence to preserve: a run (i) either remains in the white states, (ii) or eventually reaches the black states, (iii) or eventually reaches the grey states. The only loop in the white states is between s_2 and t_2, so these two must be kept for (i). To preserve (ii), we can eliminate either s_1 or t_1 with their adjacent transitions. For (iii), the analogue holds with s_3 and t_3. A possible result is shown below; in any case six transitions are eliminated.