Exam – Initiation à la vérification

January 13, 2015

Duration: 2 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 us consider variables with the order $u < v < w < x < y$. Let $F_1, F_2$ be propositional formulae with

$$F_1 := u \rightarrow (\neg w \land (x \leftrightarrow y)) \quad F_2 := v \land (x \rightarrow y)$$

(a) Draw BDDs for $F_1$ and $F_2$, using the given order. No justification for the construction is necessary. You may omit the 0-node and edges leading to it.

Let $F, G$ be any two formulae and $x$ a variable. Using the Shannon partitioning $F = \text{ite}(x, F[x/1], F[x/0])$ we derived the following equation for the conjunction of two formulae:

$$F \land G \equiv\begin{cases} F & \text{if } F \equiv G \\ 0 & \text{if } F = 0 \text{ or } G = 0 \\ G & \text{if } F = 1 \\ F & \text{if } G = 1 \\ \text{ite}(x, F[x/1] \land G[x/1], F[x/0] \land G[x/0]) & \text{otherwise} \end{cases}$$

(b) What is the corresponding equation for $F \rightarrow G$?

(c) Using the equation from (b), construct a BDD for $F_1 \rightarrow F_2$.

2. CBDDs are a variation of BDDs where each edge is equipped with an additional “negation” bit. If the bit of some edge is set, then the CBDD starting at the target node is interpreted as the negation of the formula it would otherwise represent. For uniformity, a CBDD starts with an (unsourced) edge to the root, which is also equipped with a negation bit. In each CBDD, there is exactly one leaf labelled by 1, the 0-node is abolished.

For example, the CBDD $A$ shown below on the left represents the formula $x$, while the CBDD $B$ represents the formula $x \lor y$. 

1
(a) Show that CBDDs as defined above are not unique.
(b) Prove that for every CBDD, one can find another, equivalent one that does not have any 0-labelled edges where the negation bit is set.
(c) Find such equivalent CBDDs without negated 0-labelled edges for the CBDDs A and C shown above.

3. Reachability in Petri nets.
Let $N = (P, T, F, W, m_0)$ be a Petri net. We say that $N$ is acyclic if the directed graph $(P \cup T, F)$ does not contain any cycles. Let $\mathcal{A}$ denote the class of Petri nets that are (i) 1-safe and (ii) acyclic.

(a) Show that the reachability problem for the class $\mathcal{A}$ is in NP.
(b) Show that the reachability problem for the class $\mathcal{A}$ is NP-hard, by reduction from the SAT problem.

4. Bisimulation
Let $\mathcal{L} = (S, A, \rightarrow)$ be a labelled transition system (LTS) with states $S$, actions $A$, and transitions $\rightarrow \subseteq S \times A \times S$ (no initial state is specified). We simplify the notion of bisimulation as follows: A relation $R \subseteq S \times S$ is called a bisimulation if for all pairs $(s, t) \in R$ and actions $a$ we have

- if $s \xrightarrow{a} s'$ for some $s'$, then there exists $t'$ such that $t \xrightarrow{a} t'$ and $(s', t') \in R$;
- if $t \xrightarrow{a} t'$ for some $t'$, then there exists $s'$ such that $s \xrightarrow{a} s'$ and $(s', t') \in R$.

We write $s \sim t$ if $(s, t) \in R$ for some bisimulation $R$.

(a) Prove that $\sim$ is an equivalence relation.
(b) Give $\sim$ for the LTS shown below.
Bisimulations often contain a large set of pairs, meaning that checking whether some relation $R$ is a bisimulation may be very time consuming. However, suppose that the relation $\sim$ is partially known (or can be easily proven for a certain subset of states). In this case, one can prove bisimulation more quickly with the concept of a bisimulation “up to” $\sim$. Let $R \subseteq S \times S$ a relation. We write $R_\sim$ for the relation $\sim \circ R \circ \sim$. Then $R$ is called a bisimulation up to $\sim$ if for all pairs $(s,t) \in R$ and actions $a$ we have

- if $s \xrightarrow{a} s'$ for some $s'$, then there exists $t'$ such that $t \xrightarrow{a} t'$ and $(s',t') \in R_\sim$;
- if $t \xrightarrow{a} t'$ for some $t'$, then there exists $s'$ such that $s \xrightarrow{a} s'$ and $(s',t') \in R_\sim$.

(c) If $R$ is a bisimulation up to $\sim$, prove that $R_\sim$ is a bisimulation.

(d) Find a minimal bisimulation up to $\sim$ for the LTS above that is (i) non-empty and (ii) does not intersect the identity relation.