Software Verification

Wednesday, January 17th 2018, 3 hours

This assignment contains three independent parts: the first part deals with bounded model-checking, the second part is about abstract interpretation, and the last part addresses the termination problem for Petri nets.

All documents are authorized during the examination

1 Bounded Model-Checking (8pts)

This section will browse a few concepts that have been seen in the first part of the course (Bounded Model-Checking).

1.1 Binary Decision Diagrams

Question 1 *Given the two ROBDD A and B (see fig.1), two propositional logic formula, build the resulting binary decision diagrams for* $(A \vee B) \Rightarrow (A \wedge B)$ *(order on variables is* $x > y > z > t$*). Try to represent the ROBDD with only the* 1 *terminal node (this form is more compact).*

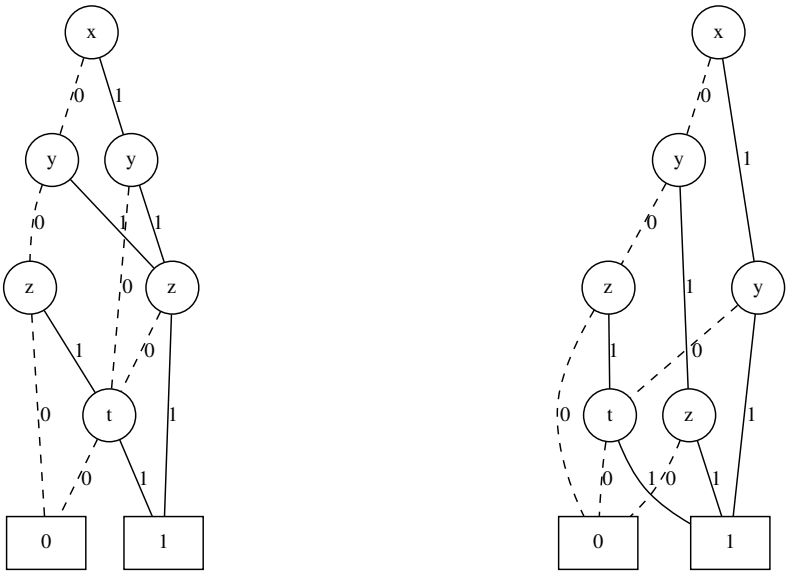


Figure 1: ROBDD A (left) and B (right).

1.2 The Bridge Crossing Problem

The goal of this exercise is to translate the "*Bridge Crossing Problem*" into a SAT decision problem (and **not** to give an effective solution). Here is the problem:

> "*Four people come to a river in the night. There is a narrow bridge, but it can only hold two people at a time. They have only one torch and, because it is night, the torch has to be used when crossing the bridge. Person A can cross the bridge in 1 minute, B in 2 minutes, C in 5 minutes, and D in 8 minutes. When two people cross the bridge together, they must move at the slower person's pace. The question is, can they all get across the bridge in 15 minutes or less?*"

Question 2 *Give the boolean variables needed to represent the problem and write the main constraints with it.*

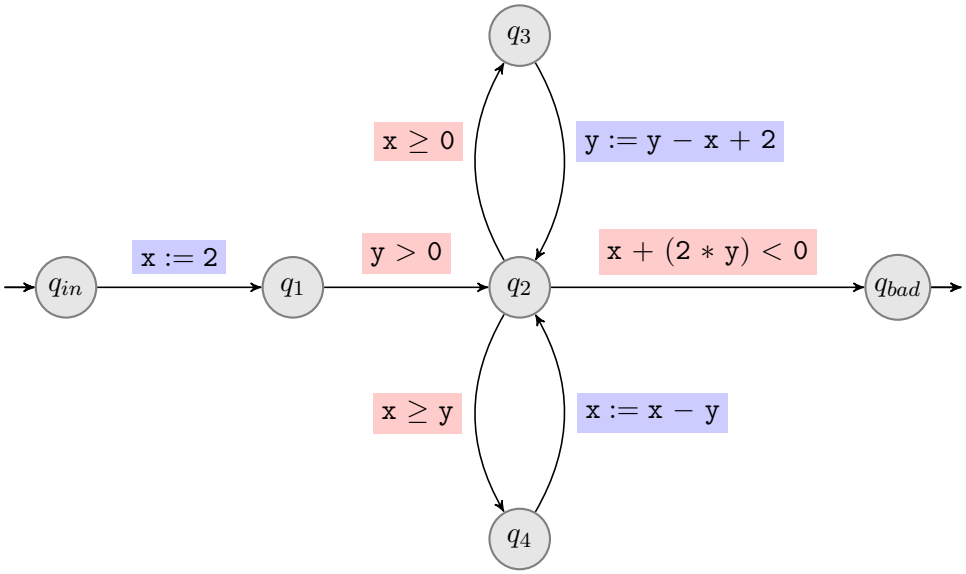
Question 3 *Describe a method to actually build the solution(s) with a SAT-solver.*

2 Abstract Interpretation (8pts)

This section deals with abstract interpretation, and is divided into two independent subsections. The first subsection focusses on range analysis and the second one is on the theory of Galois connections.

2.1 Range analysis

We perform range analysis — this analysis was presented in the course — on the control-flow automaton depicted below. This control-flow automaton has two variables `x` and `y`, both ranging over integers. The initial location is q_{in} and the bad location is q_{bad}.



Like in the course, an analysis will be called *successful* when the abstract value obtained for q_{bad} is $\bot$. Round-robin iteration shall use the following order on locations: $q_{in}, q_1, q_2, q_3, q_4, q_{bad}$.

Question 4 *Apply the round-robin algorithm with widening. Do* not *use narrowing. Is the analysis successful?*

Question 5 *Starting from the result of the previous question, perform a decreasing iteration with narrowing. Is the analysis successful?*

2.2 Least fixpoint approximation by Galois connection

We first recall some notions and notations from the course. Assume a complete lattice $(L, \sqsubseteq)$, with greatest lower bound written $\sqcap$ and least upper bound written $\sqcup$. A function $f : L \to L$ is called *monotonic* when it satisfies $(x \sqsubseteq y \implies f(x) \sqsubseteq f(y))$ for every $x, y \in L$. The *least fixpoint* of a function $f : L \to L$, if it exists, is denoted by $\mathrm{lfp}(f)$.

By the theorem of Knaster-Tarski, every monotonic function $f : L \to L$ on a complete lattice $(L, \sqsubseteq)$ has a least fixpoint that satisfies $\mathrm{lfp}(f) = \bigsqcap\{x \in L \mid f(x) \sqsubseteq x\}$.

For the remainder of this subsection, we consider two complete lattices $(C, \sqsubseteq)$ and $(A, \preceq)$ and a Galois connection $(C, \sqsubseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \preceq)$. We also assume that we are given a function $f : C \to C$ that is monotonic. Let $f^\sharp$ denote the function $f^\sharp = \alpha \circ f \circ \gamma$.

Question 6 *Prove that the function $f^\sharp$ is monotonic.*

Question 7 *Prove that* $\mathrm{lfp}(f) \sqsubseteq \gamma(\mathrm{lfp}(f^\sharp))$.

3 Petri Nets Boundeness Problem (10pts)

In this section $(P, T, \mathrm{input}, \mathrm{output})$ is a *Petri net* where P is a finite set of *places*, T is a finite set of *transitions*, and $\mathrm{input}, \mathrm{output} : T \to P \to \mathbb{N}$ are the input and output functions of the Petri net.

The *semantics* of a transition t is defined thanks to a binary relation over the markings by $x \xrightarrow{t} y$ if $x(p) \geq \mathrm{input}(t)(p)$ and $y(p) = x(p) - \mathrm{input}(t)(p) + \mathrm{output}(t)(p)$ for every $p \in P$. The *one-step* relation is the binary relation $\to$ defined by $x \to y$ if $x \xrightarrow{t} y$ for some transition t in T. The *reachability* relation is the binary relation $\xrightarrow{*}$ defined as the reflexive and transitive closure of $\to$. The *reachability set* of a Petri net from an initial marking m_{init} is the set of markings m such that $m_{init} \xrightarrow{*} m$. When this set if finite, the Petri net is said to be *bounded* from m_{init}.

The sum $x + y$ of two markings x, y is the marking defined by $(x + y)(p) = x(p) + y(p)$ for every place p in P.

Question 8 *Prove that $x + m \xrightarrow{*} y + m$ for every markings x, y, m such that $x \xrightarrow{*} y$.*

We introduce the partial order $\leq$ over the markings defined by $x \leq y$ if $x(p) \leq y(p)$ for every place p in P. We also define the relation $<$ by $x < y$ if $x \leq y$ and $x \neq y$.

Question 9 *Assume that* $m_{init} \xrightarrow{*} x \xrightarrow{*} y$ *for some markings* m_{init}, x, y *such that* $x < y$. *Prove that the Petri net is not bounded from* m_{init}.

A set W of words over a finite alphabet T is said to be *prefix-closed* if any prefix of words in W is a word in W. Let us recall the Konig's Lemma : For every infinite prefix-closed set W, there exists an infinite sequence $t_1, t_2, \ldots$ of elements in T such that $t_1 \ldots t_n \in W$ for every $n \in \mathbb{N}$.

Question 10 *Prove that if a Petri net is not bounded from an initial marking* m_{init} *then there exists an infinite sequence* $t_1, t_2, \ldots$ *of transitions, and an infinite sequence* $x_0, x_1, \ldots$ *of distinct markings such that* $x_0 = x_{init}$ *and such that* $x_{j-1} \xrightarrow{t_j} x_j$ *for every* $j \geq 1$.

Question 11 *Prove that if a Petri net is not bounded from an initial marking* m_{init} *then there exists two markings* $x < y$ *such* $m_{init} \xrightarrow{*} x \xrightarrow{*} y$

Question 12 *Explain in few lines how to decide if a Petri net is bounded from an initial marking.*