Software Verification

Wednesday, January 15th 2025, 3 hours

This assignment contains three independent parts: the first part deals with bounded model-checking, the second part is about cartesian abstraction, and the last part addresses abstract interpretation.

All documents are authorized during the examination
Answers can be written in French

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 Principles

We start with some questions to check your understandings of the Bounded Model-Checking algorithms. We recall that given a transition system $\mathcal{T}$, the Bounded Model-Checking at depth n explores all executions of length at most n and checks if one of them reaches an undesirable state (such an execution is called *faulty*).

Question 1 *A Bounded Model-Checking search can return three answers: Counter-example found, No counter-example found (exhaustive), No counter-example found (non-exhaustive).*

For each possible answer, explain what the answer means about the presence of a faulty execution, its size, and the size of all executions of the model.

Question 2 *We have seen in the course two algorithms: Depth-First Search, and Global. Recall briefly how the executions are explored in the two algorithms and what guarantee they give on the faulty execution they return if they return one.*

1.2 Backward versus Forward

We consider the following program:

```
x := 0;
y := 0;
if(z > 2){
  while(z > 0){
    z := z-1;
    if (*) {
      x := x + 1;
    }
    else{
```

```
        y := y + 1;
      }
    }
    assert(x >= 2 || y >= 2);
}
```

We recall that `if (*)` is an non-deterministic branching, meaning that both branch are always possible to take.

Question 3 *Give the control-flow automaton corresponding to that code. If you have skip edges of the form $q \xrightarrow{\text{skip}} q'$ such that q has no other outgoing edge or q' has no other incoming edge, merge q and q' (in order to get a smaller automaton).*

In the same spirit, you might merge the two initial affectation in a single transition.

You should get an automaton with 8 states and 10 transitions, with no skip edges if you minimise your automaton (but with two transitions having the same source and the same target).

Question 4 *Apply the bounded model-checking algorithm in forward to the previous system up to bound 7: draw the exploration tree displaying the formulæ added (only the added one not the complete formula) at each step in the Depth-First Search algorithm, highlight the unreachable nodes, and give the result of the algorithm.*

Is there a bound for which the answer would be different? Justify your answer.

Question 5 *Apply the bounded model-checking algorithm in backward to the previous system up to bound 7 (in the same style as the previous question).*

Is there a bound for which the answer would be different?

If the results are differents in the two directions, explain why.

Question 6 *Consider a control-flow automaton $\mathcal{A}$. If the forward bounded model-checking returns a counter-example at bound k, is it also the case for the backward Bounded-model checking? Why?*

Question 7 *Can the forward bounded model-checking returns Exhaustive while the backward one returns Non-Exhaustive? If so, give an example of such a system, if no, justify.*

2 Monotone Completion (8pts)

We first recall some notations introduced during the lecture. We denote by $\mathbb{B}$ the set of *boolean values* $\mathbb{B} = \{\text{false}, \text{true}\}$. We fix a natural number $n > 0$. The set $\mathbb{B}_n = \mathbb{B}^n$ denotes the set of *bivectors*. We denote by $v_1, \ldots, v_n$ a sequence of distinct variables ranging over $\mathbb{B}$. We put $V = \{v_1, \ldots, v_n\}$. Given a propositional formula ϕ over V and a bivector $b \in \mathbb{B}_n$, we write $b \models \phi$ if by replacing v_i by b_i for every $1 \leq i \leq n$ we get a true sentence. We say that a set $B \subseteq \mathbb{B}_n$ is denoted by a formula ϕ if ϕ is a propositional formula over V such that $B = \{b \in \mathbb{B}_n \mid b \models \phi\}$.

Example 1 $(1,0) \models v_1 \wedge \neg v_2$.

We denote by $v'_1, \ldots, v'_n$ distinct variables not in V and we let $V' = \{v'_1, \ldots, v'_n\}$. Given a propositional formula ϕ over $V \cup V'$ and a pair $(b, b') \in \mathbb{B}_n \times \mathbb{B}_n$, we write $(b, b') \models \phi$ if by replacing v_i by b_i and v'_i by b'_i for every $1 \leq i \leq n$ we get a true sentence. We say that a binary relation $\rightarrow$ over $\mathbb{B}_n$ is denoted by a formula ϕ if ϕ is a propositional formula over $V \cup V'$ such that $b \rightarrow b'$ iff $(b, b') \models \phi$.

Example 2 $((1,0),(1,1)) \models v_1 \Leftrightarrow v'_1$.

Question 8 *Provide a propositional formula over $V \cup V'$ denoting the identify binary relation over $\mathbb{B}_n$, i.e. the binary relation $\rightarrow_{id}$ satisfying $b \rightarrow_{id} b'$ iff $b = b'$.*

Question 9 *Assume that $\rightarrow$ is a binary relation over $\mathbb{B}_n$ denoted by a formula $\phi_{\rightarrow}$ and B, C are two subsets of $\mathbb{B}_n$ denoted respectively by the formulas ϕ_B and ϕ_C. Provide a propositional formula (so without any quantifier) computable in linear time that is satisfiable if, and only if, there exist $b \in B$, $c \in C$ such that $b \rightarrow c$.*

We put $\mathbb{R} = \mathbb{B} \cup \{\top\}$, and $\mathbb{R}_n = \mathbb{R}^n$. Notice that $\mathbb{R}_n$ is the set of trivectors that does not contain any bottom component. A vector $t \in \mathbb{R}_n$ is called a *reduced trivector*. Let t be reduced trivector. We define the binary relation $\sqsubseteq_t$ over $\mathbb{B}_n$ defined by $x \sqsubseteq_t y$ if $x_i \in \{y_i, t_i\}$ for every $i \in \{1, \ldots, n\}$.

Question 10 *Show that $\sqsubseteq_t$ is a partial order.*

A set $B \subseteq \mathbb{B}_n$ is said to be *t-monotone* if for every $x, y \in \mathbb{B}_n$ such that $x \sqsubseteq_t y$, $x \in B$ implies $y \in B$. Given a set $B \subseteq \mathbb{B}_n$, we denote by $\mathcal{M}_t(B)$ the set of $y \in \mathbb{B}_n$ such that there exists $x \in B$ satisfying $x \sqsubseteq_t y$. This set is called the *least t-monotone over-approximation* of B.

Question 11 *Show that $\mathcal{M}_t(B)$ is t-monotone for every $B \subseteq \mathbb{B}_n$.*

Question 12 *Show that for every $B \subseteq C \subseteq \mathbb{B}_n$ we have $\mathcal{M}_t(B) \subseteq \mathcal{M}_t(C)$.*

Question 13 *Assume that $B = B_1 \cup \ldots \cup B_m$ for some subsets $B_1, \ldots, B_m \subseteq \mathbb{B}_n$. Shows that $\mathcal{M}_t(B) = \mathcal{M}_t(B_1) \cup \ldots \cup \mathcal{M}_t(B_m)$.*

We associate with a reduced trivector $r \in \mathbb{R}_n$ the set $\gamma(r)$ of bivectors $x \in \mathbb{B}_n$ such that $r_i \in \{x_i, \top\}$ for every $i \in \{1, \ldots, n\}$. Notice that γ is the concretization function introduced during the lecture.

Question 14 *Provide the set* $\gamma(\top, 0, \top)$.

Question 15 *Let* $r, t \in \mathbb{R}_n$. *We introduce* $s \in \mathbb{R}_n$ *defined by:*

$$s_i = \begin{cases} \top & \text{if } r_i \in \{\top, t_i\} \\ r_i & \text{otherwise} \end{cases}$$

Show that $\mathcal{M}_t(\gamma(r)) = \gamma(s)$.

3 Abstract Interpretation (6pts)

This section deals with abstract interpretation, and is divided into two independent subsections. The first subsection applies range analysis on an example. The second subsection studies some properties of Galois connections.

3.1 Range analysis

We perform range analysis — this analysis was presented in the course — on the control-flow automaton depicted in Figure 1. 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}. Recall that range analysis uses the *abstract domain of intervals*. Like in the course, an

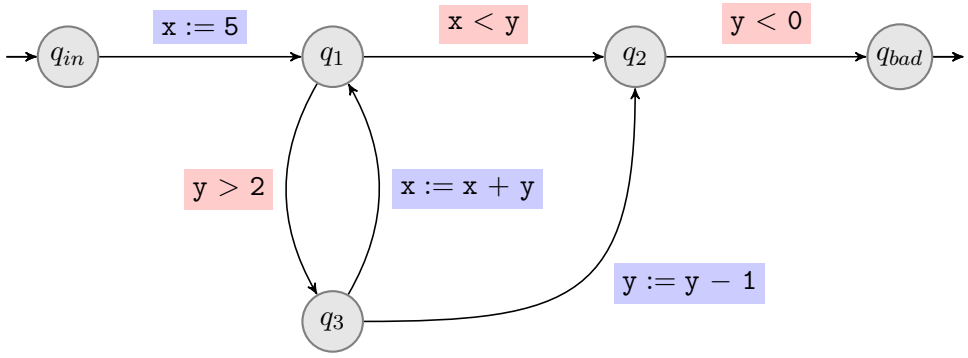

Figure 1: Control-flow automaton of Questions 16 and 17.

analysis will be called *successful* when the abstract value obtained for q_{bad} has an empty concretization.

Warning. In the questions below, **use the following order on locations** for round-robin: $q_{in}, q_1, q_2, q_3, q_{bad}$.

Question 16 *Apply the round-robin algorithm with widening. Do* not *use narrowing. Is the analysis successful?*

Question 17 *Starting from the result of the previous question, perform a decreasing iteration with narrowing. Is the analysis successful?*

3.2 Some Properties of Galois connections

We start by recalling some basic notions from the course. A *complete lattice* is a partially-ordered set $(L, \sqsubseteq)$ such that every subset $X \subseteq L$ admits a greatest lower bound and a least upper bound. We consider, for the remainder of this subsection, two complete lattices $(C, \sqsubseteq)$ and $(A, \preceq)$. As in the course, we use the symbols $\sqcap$ and $\sqcup$ for the greatest lower bound and the least upper bound in $(C, \sqsubseteq)$, and we use the symbols $\wedge$ and $\vee$ for the greatest lower bound and the least upper bound in $(A, \preceq)$.

A *Galois connection* between $(C, \sqsubseteq)$ and $(A, \preceq)$ is a pair (α, γ) of functions, with $\alpha : C \to A$ and $\gamma : A \to C$, such that the equivalence $\alpha(c) \preceq a \Leftrightarrow c \sqsubseteq \gamma(a)$ holds for every

$a \in A$ and $c \in C$. The notation $(C, \sqsubseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \preceq)$ stands for "the pair (α, γ) is a Galois connection between $(C, \sqsubseteq)$ and $(A, \preceq)$".

We also recall the characterization of Galois connections that was given in the course. Given a pair of functions $\alpha : C \to A$ and $\gamma : A \to C$, we have $(C, \sqsubseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \preceq)$ if, and only if, α is monotonic ($c_1 \sqsubseteq c_2$ implies $\alpha(c_1) \preceq \alpha(c_2)$), γ is monotonic ($a_1 \preceq a_2$ implies $\gamma(a_1) \sqsubseteq \gamma(a_2)$), $\alpha \circ \gamma$ is reductive ($\alpha(\gamma(a)) \preceq a$), and $\gamma \circ \alpha$ is extensive ($c \sqsubseteq \gamma(\alpha(c))$).

Question 18 *Prove that for every pair (α, γ) of functions verifying $(C, \sqsubseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \preceq)$, and for every $a \in A$ and $c \in C$, the two following equalities hold:*

$$\begin{aligned} \alpha(c) &= \wedge\{a \in A \mid c \sqsubseteq \gamma(a)\} \\ \gamma(a) &= \sqcup\{c \in C \mid \alpha(c) \preceq a\} \end{aligned}$$

It follows from Question 18 that γ uniquely determines α and vice-versa. The next question provides a characterization of the functions γ such that $(C, \sqsubseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \preceq)$ for some function α.

Question 19 *Consider an arbitrary function $\gamma : A \to C$. Prove that the following assertions are equivalent:*

i) *γ is* glb-preserving*, i.e., $\gamma(\wedge X) = \sqcap\{\gamma(x) \mid x \in X\}$ for all $X \subseteq A$,*

ii) *there is a function $\alpha : C \to A$ such that $(C, \sqsubseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \preceq)$.*

Hint. For the proof of *i)* $\implies$ *ii)*, show that every glb-preserving function is monotonic.