# Software Verification

Thursday, January 8th 2015, 3 hours

This assignment contains three independent parts: the first part deals with binary decision diagrams, the second part is about Galois connections and range analysis, and the last part addresses the coverability problem for Petri nets.

## 1 Binary Decision Diagrams (BDD)

**Question 1** *Draw the two BDDs representing the formula*

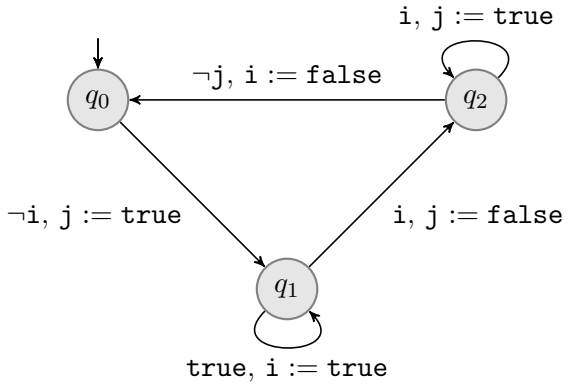
$$(x_1 \Leftrightarrow y_1) \wedge (x_2 \Leftrightarrow y_2) \wedge (x_3 \Leftrightarrow y_3)$$

*using the two orderings* $x_1 > y_1 > x_2 > y_2 > x_3 > y_3$ *and then* $x_1 > x_2 > x_3 > y_1 > y_2 > y_3$*. It is up to you to use negated edges or not.*

**Question 2** *Draw the graph representing the operational semantics of the control flow automaton represented in the figure below. Only the part of the operational semantics reachable from the configuration* $(q_0 \wedge \texttt{i} = \texttt{false} \wedge \texttt{j} = \texttt{false})$ *will be drawn.*

**Question 3** *Choose and explain variable names you will need and give a formula encoding the transition relation of the whole operational semantics of the same control flow automaton, using these variables.*

**Question 4** *Choose an ordering on variables, and give the BDD associated with the formula of the previous question. It is up to you to use negated edges or not.*




In this variant of control flow transition systems, transitions are labelled by a guard and an assignment. The transition can be taken only if the guard evaluates to `true`.

## 2 Galois Connections and Range Analysis

This section first establishes some properties of Galois connections, and then applies range analysis to an example. These two sub-parts are independent.

Let $(A, \preceq)$ and $(C, \sqsubseteq)$ be arbitrary complete lattices. The greatest lower bound and least upper bound are respectively denoted by $\wedge$ and $\vee$ in $(A, \preceq)$, and by $\sqcap$ and $\sqcup$ in $(C, \sqsubseteq)$.

**Question 5** *Prove that for every Galois connection* $(C, \sqsubseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \preceq)$*, 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 5 that $\gamma$ uniquely determines $\alpha$ and vice-versa. The next question provides a characterization of the $\gamma$ such that $(C, \sqsubseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \preceq)$ for some $\alpha$.

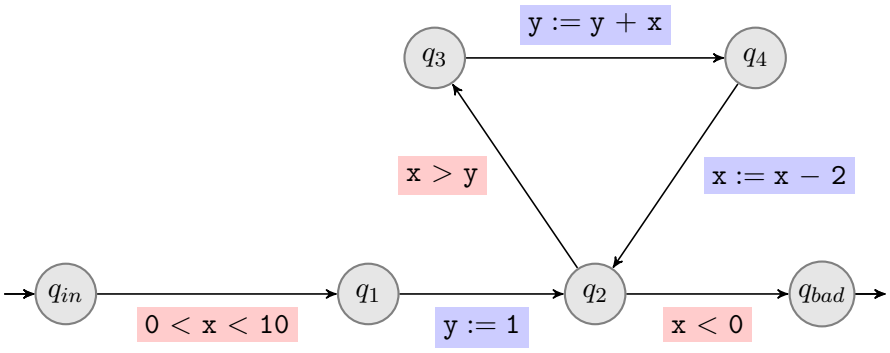
**Question 6** *Consider an arbitrary function* $\gamma : A \to C$*. Prove that the following assertions are equivalent:*

*i)* $\gamma$ *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* $(C, \sqsubseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \preceq)$ *is a Galois connection.*

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

We now perform range analysis on the control-flow automaton depicted below, with variables $\mathtt{X} = \{\mathtt{x}, \mathtt{y}\}$, 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 7** *Apply the round-robin algorithm with widening applied in location* $q_2$ *only. Do* not *use narrowing. Is the analysis successful?*

**Question 8** *Starting from the result of the previous question, perform a decreasing iteration with narrowing. Is the analysis successful?*

# 3 A Backward Algorithm For The Coverability Problem

We show the correctness of an algorithm deciding the coverability problem for Petri nets based on upward closed sets.

## 3.1 Upward Closed Sets

Vectors in $\mathbb{N}^d$ are called *configurations*. Given a configuration $\vec{c} \in \mathbb{N}^d$, we denote by $\uparrow \vec{c}$ the set $\{\vec{c} + \vec{n} \mid \vec{n} \in \mathbb{N}^d\}$. Given a set $\vec{C} \subseteq \mathbb{N}^d$, we also introduce $\uparrow \vec{C}$ the set $\bigcup_{\vec{c} \in \vec{C}} \uparrow \vec{c}$. Observe that $\uparrow \vec{C} = \{\vec{c} + \vec{n} \mid \vec{c} \in \vec{C} \ \wedge \ \vec{n} \in \mathbb{N}^d\}$. A set $\vec{C} \subseteq \mathbb{N}^d$ is said to be *upward closed* if $\uparrow \vec{C} = \vec{C}$.

**Question 9** *Provide two examples of sets : one that is upward closed and one that is not upward closed.*

Let us recall that for every upward closed set $\vec{C} \subseteq \mathbb{N}^d$ there exists a finite set $\vec{B} \subseteq \vec{C}$ such that $\vec{C} = \uparrow \vec{B}$.

**Question 10** *Provide an algorithm that takes as input two finite sets $\vec{X}, \vec{Y} \subseteq \mathbb{N}^d$ and decides if $\uparrow \vec{X} \subseteq \uparrow \vec{Y}$.*

Let us consider an infinite sequence $(\vec{C}_i)_{i \geq 0}$ of upward closed sets. Let us introduce $\vec{C}_\infty = \bigcup_{i \geq 0} \vec{C}_i$.

**Question 11** *Show that $\vec{C}_\infty$ is upward closed.*

We deduce that there exists a finite set $\vec{B} \subseteq \mathbb{N}^d$ such that $\vec{C}_\infty = \uparrow \vec{B}$.

**Question 12** *Deduce that there exists $i \geq 0$ such that $\vec{C}_\infty = \vec{C}_0 \cup \ldots \cup \vec{C}_i$.*

The following question is independant of the previous questions. The result will be usefull in the next section.

**Question 13** *Let $\vec{b}, \vec{u}, \vec{v} \in \mathbb{N}^d$. Provide an algorithm that computes a vector $\vec{b'} \in \mathbb{N}^d$ such that:*

$$\uparrow \vec{b'} \ = \ (\uparrow \vec{v} \cap \uparrow \vec{b}) - \vec{v} + \vec{u}$$

## 3.2 The Coverability Problem

A Petri net is a tuple $(\vec{c}_{\text{ini}}, T)$ where $\vec{c}_{\text{ini}} \in \mathbb{N}^d$ is the *initial configuration*, and $T \subseteq \mathbb{N}^d \times \mathbb{N}^d$ is a finite set of *transitions*.

We associate to a transition $t = (\vec{u}, \vec{v})$ a binary relation $\xrightarrow{t}$ over the configurations defined by $\vec{x} \xrightarrow{t} \vec{y}$ if, and only if, there exists $\vec{n} \in \mathbb{N}^d$ such that $\vec{x} = \vec{u} + \vec{n}$ and $\vec{y} = \vec{v} + \vec{n}$. We also introduce the binary relation $\rightarrow$ over the configurations defined by $\vec{x} \rightarrow \vec{y}$ if, and only if, there exists a transition $t \in T$ such that $\vec{x} \xrightarrow{t} \vec{y}$. The reflexive and transitive closure of $\rightarrow$ is denoted by $\xrightarrow{*}$. Notice that $\vec{x} \xrightarrow{*} \vec{y}$ if, and only if, there exists a sequence $\vec{c}_0, \ldots, \vec{c}_k$ of configurations, and a sequence $t_1, \ldots, t_k \in T$ such that:

$$\vec{x} = \vec{c}_0 \xrightarrow{t_1} \vec{c}_1 \cdots \xrightarrow{t_k} \vec{c}_k = \vec{y}$$

The coverability problem takes as input a Petri net $(\vec{c}_{\text{ini}}, T)$ and a configuration $\vec{c}_{\text{bad}}$ and it returns true if, and only if, there exists $\vec{n} \in \mathbb{N}^d$ such that $\vec{c}_{\text{ini}} \xrightarrow{*} (\vec{c}_{\text{bad}} + \vec{n})$.

Given a set $\vec{C} \subseteq \mathbb{N}^d$ of configurations, and a transition $t$, we denote by $\text{pre}_t(\vec{C})$ the following set of configurations:

$$\text{pre}_t(\vec{C}) = \{\vec{x} \in \mathbb{N}^d \mid \exists \vec{c} \in \vec{C}\ \vec{x} \xrightarrow{t} \vec{c}\}$$

**Question 14** *Assume that $t = (\vec{u}, \vec{v})$ is a transition and let $\vec{b} \in \mathbb{N}^d$. Show the following equality:*

$$\text{pre}_t(\uparrow \vec{b}) = (\uparrow \vec{v} \cap \uparrow \vec{b}) - \vec{v} + \vec{u}$$

We introduce the set $\text{pre}_T(\vec{C}) = \bigcup_{t \in T} \text{pre}_t(\vec{C})$.

**Question 15** *Deduce an algorithm that takes as input a finite set of transtions $T \subseteq \mathbb{N}^d \times \mathbb{N}^d$ and a finite set $\vec{B} \subseteq \mathbb{N}^d$ and returns a finite set $\vec{B}' \subseteq \mathbb{N}^d$ such that:*

$$\uparrow \vec{B}' \ = \ \text{pre}_T(\uparrow \vec{B})$$

Now, let us consider a bad configuration $\vec{c}_{\text{bad}}$ and let us consider the sequence $(\vec{C}_i)_{i \geq 0}$ defined by $\vec{C}_0 = \uparrow \vec{c}_{\text{bad}}$ and by induction for every $i \geq 0$ by:

$$\vec{C}_{i+1} = \text{pre}_T(\vec{C}_i)$$

We introduce $\vec{C}_\infty = \bigcup_{i \geq 0} \vec{C}_i$.

**Question 16** *Show that there exists $i \geq 0$ such that $\vec{C}_{i+1} \subseteq \vec{C}_0 \cup \ldots \cup \vec{C}_i$.*

**Question 17** *Show that if $\vec{C}_{i+1} \subseteq \vec{C}_0 \cup \ldots \cup \vec{C}_i$ then $\vec{C}_i = \vec{C}_\infty$.*

**Question 18** *Show that there exists $\vec{n} \in \mathbb{N}^d$ such that $\vec{c}_{ini} \xrightarrow{*} (\vec{c}_{bad} + \vec{n})$ if, and only if, $\vec{c}_{ini} \in \vec{C}_\infty$.*

**Question 19** *Deduce an algorithm for deciding the coverability problem.*