Software Verification

Monday, January 6th 2014, 3 hours

This assignment contains four independent parts: the first part deals with binary decision diagrams, the second part applies range analysis to a given example program, the third part is about Galois connection, and the last part deals with Craig interpolation.

1 Binary Decision Diagrams (BDD)

Question 1 *Draw the two BDDs using negated edges, representing the formula*

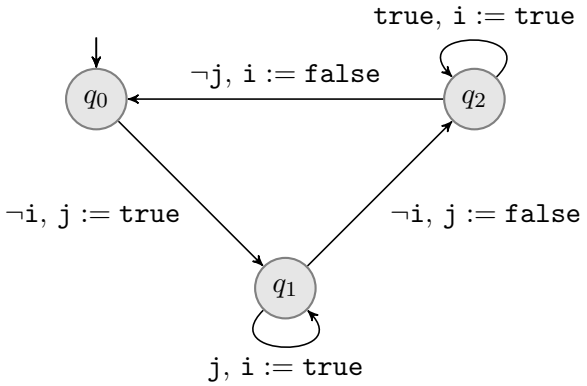
$$(x_1 \Leftrightarrow y_1) \wedge (x_2 \Leftrightarrow y_2) \wedge (x_3 \Leftrightarrow y_3)$$

using the two orderings $x_1 > y_1 > x_2 > y_2 > x_3 > y_3$ *and then* $x_1 > x_2 > x_3 > y_1 > y_2 > y_3$

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.*

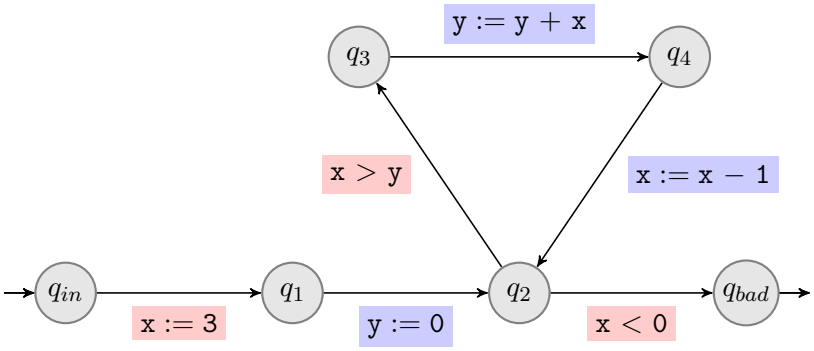
Question 4 *Choose an ordering on variables, and give the BDD associated with the formula of the previous question. It is up to you to use negated edges or not.*



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 Range Analysis

We consider the control-flow automaton depicted below, with variables $\mathtt{X} = \{\mathtt{x}, \mathtt{y}\}$, both ranging over integers, with initial location q_{in} and bad location q_{bad}.



This section performs range analysis on this control-flow automaton. 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: $q_{in}, q_1, q_2, q_3, q_4, q_{bad}$. The first two questions are independent. The third question depends on the result of the second question.

Question 5 *Apply the round-robin algorithm to compute the minimal fixpoint solution. Do* not *use widening nor narrowing. Is the analysis successful?*

Question 6 *Apply the round-robin algorithm with widening applied in location q_2 only. Do* not *use narrowing. Is the analysis successful?*

Question 7 *Starting from the result of the previous question, perform a decreasing iteration with narrowing. Is the analysis successful?*

3 Galois Connections and Minimal Elements

In this section $(S, \leq)$ denotes a partially ordered set, and $\mathcal{P}(S)$ the set of subsets of S. We introduce the function $\gamma : \mathcal{P}(S) \mapsto \mathcal{P}(S)$ that maps a set $X \subseteq S$ on the set $\gamma(X)$, called the *upward closure* of X, and defined by:

$$\gamma(X) = \bigcup_{x \in X} \{s \in S \mid x \leq s\}$$

We introduce the partial order $\sqsubseteq$ over $\mathcal{P}(S)$ defined by $X \sqsubseteq Y$ iff $\gamma(X) \subseteq \gamma(Y)$.

An element x is said to be *minimal* for a set $X \subseteq S$, if $x \in X$ and the following assertion holds:

$$\forall y \in X \quad y \leq x \quad \Rightarrow \quad y = x$$

The set of *minimal elements* of a set $X \subseteq S$ is denoted by $\alpha(X)$.

In this section, we are interested by a necessary and sufficient condition such that (α, γ) forms a Galois connection from $(\mathcal{P}(S), \subseteq)$ to $(\mathcal{P}(S), \sqsubseteq)$.

Question 8 *Provide an example of a poset $(S, \leq)$ for which $\alpha : (\mathcal{P}(S), \subseteq) \mapsto (\mathcal{P}(S), \sqsubseteq)$ is not monotonic.*

Question 9 *Show that if (α, γ) is a Galois connection from $(\mathcal{P}(S), \subseteq)$ to $(\mathcal{P}(S), \sqsubseteq)$, then $\alpha(X)$ is non empty for every non-empty set $X \subseteq S$.*

For the reminder, we assume that $\alpha(X)$ is not empty for every non empty set $X \subseteq S$.

Question 10 *Show that for every set $X \subseteq S$ and for every $x \in X$, there exists $y \in \alpha(X)$ such that $y \leq x$. Tips : Introduce $Y = \{y \in X \mid y \leq x\}$.*

Question 11 *Deduce that $X \subseteq \gamma \circ \alpha(X)$ for every $X \subseteq S$.*

Question 12 *Shows that (α, γ) is a Galois connection from $(\mathcal{P}(S), \subseteq)$ to $(\mathcal{P}(S), \sqsubseteq)$.*

4 Craig Interpolation

We consider the clauses $C_1 = (\neg a \vee \neg b)$, $C_2 = (a \vee c)$, $C_3 = (b \vee \neg c)$, $C_4 = (\neg c \vee \neg d)$, $C_5 = (c \vee e)$, $C_6 = (c \vee \neg e)$, $C_7 = (\neg b \vee d)$.

Question 13 *Shows that the conjunction of these clauses is unsatisfiable.*

Question 14 *With respect to your previous proof, which clauses can be removed in such a way the conjunction is still unsatisifiable.*

Question 15 *Provide a Craig interpolant for the pair $(C_1 \wedge C_2 \wedge C_3 \wedge C_4 \ , \ C_5 \wedge C_6 \wedge C_7)$.*