Software Verification

Monday, January 14th 2013, 3 hours

This assignment contains three independent parts: the first part deals with binary decision diagrams, the second part addresses abstract interpretation for congruence analysis, and the last part applies abstraction refinement to the verification of a given program.

1 Binary Decision Diagrams (BDD)

Question 1 *Draw the two BDDs representing the formula*

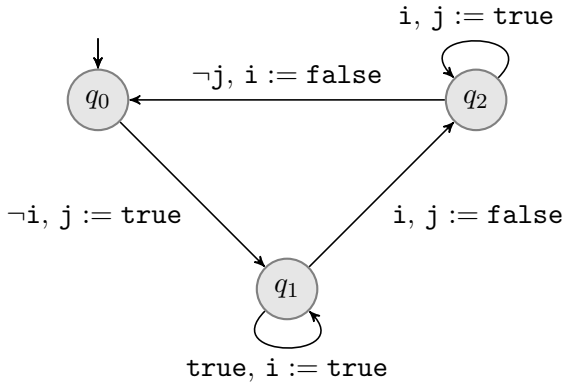
$$(x_1 \Leftrightarrow y_1) \wedge (x_2 \Leftrightarrow y_2) \wedge (x_3 \Leftrightarrow y_3)$$

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

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.*



2 Abstract Interpretation-based Congruence Analysis

This section addresses program analysis based on arithmetical congruence classes. In this analysis, the values taken by a variable of a program are abstracted by congruence classes. Program variables are assumed to range over the set $\mathbb{Z}$ of integers.

It is well-known that the set $(\mathcal{P}(\mathbb{Z}), \subseteq)$ is a complete lattice, with greatest lower bound $\cap$ and least upper bound $\cup$. We recall that a *Moore family* is a subset $\mathcal{M}$ of $\mathcal{P}(\mathbb{Z})$ that is closed under arbitrary intersection, i.e., $\bigcap X \in \mathcal{M}$ for every subset X of $\mathcal{M}$. Note that a Moore family necessarily contains $\mathbb{Z}$, since $\bigcap \emptyset = \mathbb{Z}$.

Question 5 *Prove that, for every Moore family $\mathcal{M}$, the partially-ordered set $(\mathcal{M}, \subseteq)$ is a complete lattice, with greatest lower bound $\cap$ and least upper bound $\vee$ verifying*

$$\bigvee X \quad = \quad \bigcap \{m \in \mathcal{M} \mid \forall x \in X \cdot m \supseteq x\}$$

An *arithmetical congruence class* is a subset $H \subseteq \mathbb{Z}$ of the form $c + m\mathbb{Z}$, where $c \in \mathbb{Z}$ and $m \in \mathbb{N}$. We let $\mathcal{H}$ denote the set of all arithmetical congruence classes.

Question 6 *Prove that the set $\{m\mathbb{Z} \mid m \in \mathbb{N}\}$ is a Moore family. Deduce that the set $\{\emptyset\} \cup \mathcal{H}$ is a Moore family.*

For the remainder of this section, we let $\vee$ denote the least upper bound of the complete lattice $(\{\emptyset\} \cup \mathcal{H}, \subseteq)$.

Question 7 *Let $c_1, c_2 \in \mathbb{Z}$ and $m_1, m_2 \in \mathbb{N}$. Give a simple expression, in terms of c_1, m_1, c_2, m_2, of the arithmetical congruence $(c_1 + m_1\mathbb{Z}) \vee (c_2 + m_2\mathbb{Z})$.*

Question 8 *Prove that the lattice $(\{\emptyset\} \cup \mathcal{H}, \subseteq)$ satisfies the ascending chain condition.*

3 Predicate Abstraction

We consider the control-flow automaton depicted Figure 1 where variables $\{\mathtt{x}, \mathtt{y}\}$ are valued over the reals. We are interested in proving that whatever the initial valuation of $\mathtt{x}$ and $\mathtt{y}$, the location q_{bad} is not reachable from q_{in}.

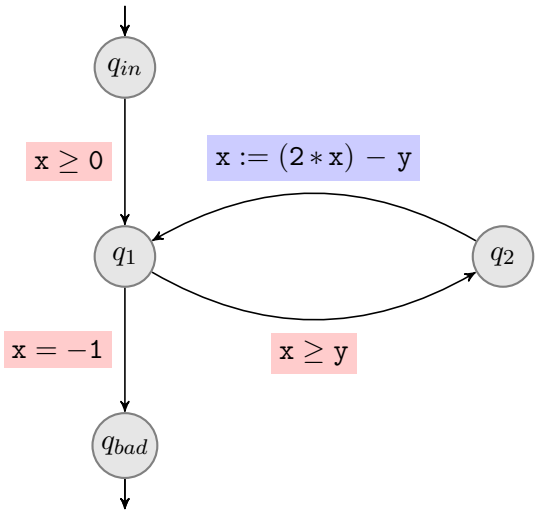


Figure 1: A control-flow automaton.

Question 9 *Provide the logical semantics of each operation labeling a transition of the control-flow automaton.*

Question 10 *Draw the finite graph obtained with the boolean abstraction with the unique predicate* $(x \geq 0)$.

Question 11 *Provide a spurious trace.*

Question 12 *Provide an additional predicate in such a way the boolean abstraction becomes precise enough and draw the finite graph obtained with the boolean abstraction based on* $(x \geq 0)$ *and this additional predicate.*