Exercise

2025/02/28

Reference: https://www.sosy-lab.org/research/pub/2018-HBMC.Combining_Model_Checking_and_Data-Flow_Analysis.pdf

1 (Bounded) Model Checking (30 minutes)

Jupyter Notebook: 03_BMC.ipynb

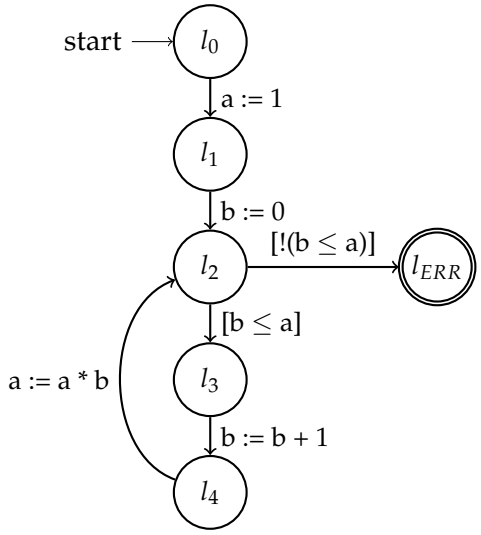
Solution:
Solution

2 Theory

2.1 Observer Automata (30 minutes)

```
1 int a = 1;
2 int b = 0;
3
4 while (b <= a) {
5     b = b + 1;
6     a = a * b;
7 }
8 ERR:;
```

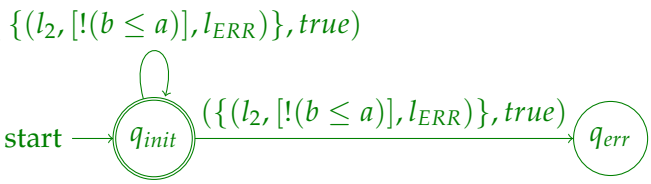
Program



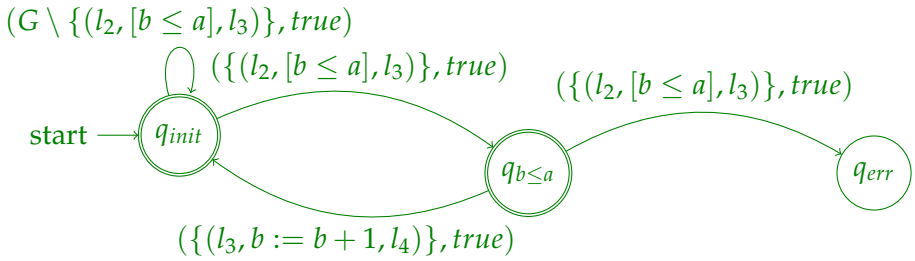
CFA $P = (L, E, l_0)$

1. Define an observer automaton for the given program $P = (L, E, l_0)$ and program variables X, for each of the following specifications:

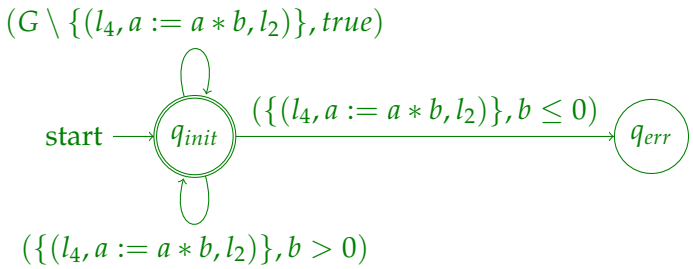
   a) $\square(l' \neq l_{ERR})$ (for $g = (l, op, l')$)



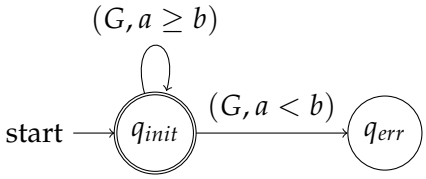
b) $\forall x \in X.\, \forall z \in X.\, \square(op = [x \leq z] \implies \circ(\forall y \in X \cup \mathbb{Z}.\, op \neq [x \leq y]\ \mathcal{W}\ op = x := x + 1))$



c) $\forall x \in X.\, \forall y \in X. \square(op = x := x * y \implies y > 0)$



2. Consider the following observer automaton A:



a) State the LTL-formula equivalent of A.

$\square a \geq b$

b) Consider observer analysis $\mathbb{O}$ for observer automaton A and precision π:

$$\begin{aligned}\pi = &\{x = n \mid x \in X, n \in \mathbb{Z}\} \cup \{x \geq n \mid x \in X, n \in \mathbb{N}\} \\ &\cup \{b \leq a, b \leq a + 1\} \cup \{false\}\end{aligned}$$

Apply the CPA algorithm with composite analysis $\mathbb{L} \times \mathbb{P} \times \mathbb{O}$ and initial state $e_0 = (l_0, \emptyset, (q_{init}, true))$ to program P. State the final reached set and whether the specification is violated, according to the algorithm.

$$
\begin{aligned}
reached = \{ & \\
& (l_0, \emptyset, (q_{init}, true)), \\
& (l_1, \{a = 1, a \geq 1\}, (q_{init}, a \geq b)), (l_1, \{a = 1, a \geq 1\}, (q_{err}, a < b))), \\
& (l_2, \{a = 1, b = 0, a \geq 1, b \leq a, b \leq a + 1, a \geq b\}, (q_{init}, a \geq b)), \\
& (l_3, \{a = 1, b = 0, a \geq 1, b \leq a, b \leq a + 1, a \geq b\}, (q_{init}, a \geq b)), \\
& (l_4, \{a = 1, b = 1, a \geq 1, b \geq 1, b \leq a, b \leq a + 1, a \geq b\}, (q_{init}, a \geq b)), \\
& (l_2, \{a = 1, b = 1, a \geq 1, b \geq 1, b \leq a, b \leq a + 1, a \geq b\}, (q_{init}, a \geq b)), \\
& (l_3, \{a = 1, b = 1, a \geq 1, b \geq 1, b \leq a, b \leq a + 1, a \geq b\}, (q_{init}, a \geq b)), \\
& (l_4, \{a = 1, b = 2, a \geq 1, b \geq 1, b \geq 2, b \leq a + 1, a < b\}, (q_{err}, a < b)), \\
& \}
\end{aligned}
$$

3 Configurable Program Analyses (120 minutes)

Jupyter Notebook: 09_Verifier-Design-part-1.ipynb

Solution:
Solution

General notes:

- The given solution is just a proposal. We do not guarantee correctness.