Dr. Matthias Heizmann
Tanja Schindler
Dominik Klumpp

Hand in until 16:15 on July 3, 2019
Discussion: July 3, 2019

Tutorial for Program Verification
Exercise Sheet 17

In this exercise we will see that there are programs that have an infinite reachability graph but there exists a finite precise abstract reachability graph.

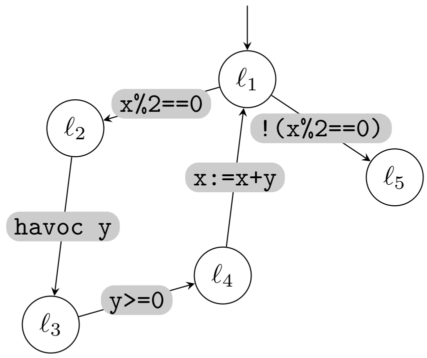
In the lecture we defined the precise abstract reachability graph as follows.
Definition (precise abstract reachability graph) A *precise abstract reachability graph* is a pair (AC, T) such that AC is a set of abstract configurations such that

- for each abstract configuration $(\ell, \{\varphi\})$ for which $\varphi \neq \mathbf{false}$ and there exists $(\ell, st, \ell') \in \Delta$, there is a an abstract configuration $(\ell', \{\varphi'\})$ such that $sp(\{\varphi\}, st) = \{\varphi'\}$ and $((\ell, \{\varphi\}), st, (\ell', \{\varphi'\})) \in T$
- $(\ell_{\mathsf{init}}, \{\varphi_{\mathsf{pre}}\}) \in AC$, and
- there is a path from $(\ell_{\mathsf{init}}, \{\varphi_{\mathsf{pre}}\})$ to each abstract configuration $(\ell, \{\varphi\})$.

Exercise 1: Precise Abstract Reachability Graph 2 Points

Consider the control flow graph depicted on the right, that was constructed for the the program $P = (V, \mu, \mathcal{T})$ with $V = \{x, y\}$, $\mu(x) = \mu(y) = \mathbb{Z}$ whose code is shown on the left.

```
while (x % 2 == 0) {
  havoc y;
  assume y >= 0;
  x := x + y;
}
```



Draw the precise abstract reachability graph for this control-flow graph and the precondition $x \geq 0$.

In the lecture it was said that the precise abstract reachability graph is unique. This is not true. For example in this exercise you could chose $(\ell_2, \{x \geq 0 \wedge x\%2 = 0\})$ or $(\ell_2, \{x\%2 = 0 \wedge x \geq 0\})$ (or even both!) as successors of the initial abstract configuration. For solving this exercise it is necessary to choose the formulas that define sets of states wisely.