Dr. Matthias Heizmann
Tanja Schindler
Dominik Klumpp

Hand in until 10:00 on July 15, 2019
Discussion: July 15, 2019

Tutorial for Program Verification

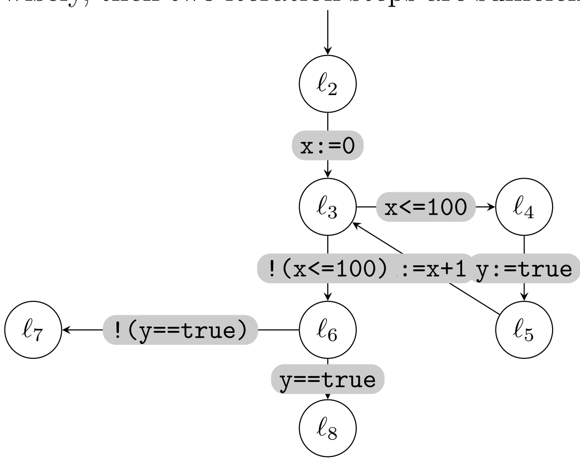
Exercise Sheet 20

Don't forget to participate in the official course evaluation which runs until Wednesday, July 17th!

Exercise 1: 5 Points

Apply the CEGAR approach to the program below. Whenever you have to provide a sequence of statements you may return any sequence, but we encourage you to take the shortest sequence.
Document all intermediate steps.
Hint: If you choose the abstraction of traces wisely, then two iteration steps are sufficient.

```
x := 0;
while (x <= 100) {
  y := true;
  x := x + 1;
}
assert y == true;
```



Exercise 2: Abstraction of a Trace 2 Points

In the lecture we defined an *abstraction* $\pi^\#$ of a trace π, derived by replacing some of the statements *st* with their abstract counterpart *abstract*(*st*). The intuition is that sometimes a few statements in π are sufficient to make it infeasible. A proof of infeasibility of $\pi^\#$ is then also a proof of infeasiblity of π.

In this exercise, we consider a modified concept of abstraction: Instead of replacing assignments with their abstraction (`havoc`), we allow them to be deleted from the trace entirely.

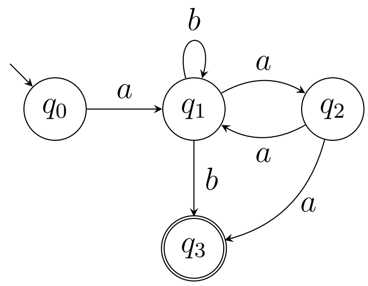
Show that this is not a good notion of abstraction. In particular, give a trace π and a corresponding abstraction $\pi^\#$, such that $\pi^\#$ is infeasible, but π is feasible. Give a proof of infeasibility for $\pi^\#$, and an execution for π.

Exercise 3: Nondeterministic Finite Automata 2 Points

A *nondeterministic finite automaton* (NFA) is a tuple $\mathcal{A} = (Q, \Sigma, \Delta, Q_0, F)$ where Q is

a finite set of states, Σ is a finite alphabet, $\Delta \subseteq (Q \times \Sigma) \times Q$ is a transition relation, $Q_0 \subseteq Q$ is a set of initial states, and $F \subseteq Q$ is a set of final (or accepting) states.
A *run* for a finite word $w = a_1 \dots a_n \in \Sigma^*$ in an NFA $\mathcal{A}$ is a finite sequence of states $q_0 q_1 \dots q_n$ such that $q_0 \in Q_0$, and $(q_i, a_{i+1}, q_{i+1}) \in \Delta$ for all $i \in \{0, \dots, n-1\}$. A run is *accepting*, if it ends in a final state $q \in F$.
A word $w \in \Sigma^*$ is *accepted* by an NFA $\mathcal{A}$ if there exists an accepting run in $\mathcal{A}$.

Let $\Sigma = \{a, b\}$. Consider the following NFA $\mathcal{A}$ given by its graphical representation, where we mark initial states by ingoing edges, and final states by double circles.



For each of the following words, state whether they are accepted by the NFA $\mathcal{A}$ or not. If a word is accepted by $\mathcal{A}$, give an accepting run.

(a) $w_1 = aaab$

(b) $w_2 = abaaba$

(c) $w_3 = abaabaa$

(d) $w_4 = abba$