Dr. Matthias Heizmann
Dominik Klumpp

Hand in until 10:00 on June 21, 2021
Discussion: June 21, 2021

Tutorial for Program Verification
Exercise Sheet 15

In this exercise sheet we work with control flow graphs, executions and reachability graphs.

Submit your solution by uploading it as PDF in ILIAS.

Exercise 1: From Programs to CFGs — 3 Points

For each of the programs given below, draw a control-flow graph.

(a) Code of program P_{pow}:

```
e := 1;
z := 0;
while (z < y) {
    e := e * x;
    z := z + 1;
}
```

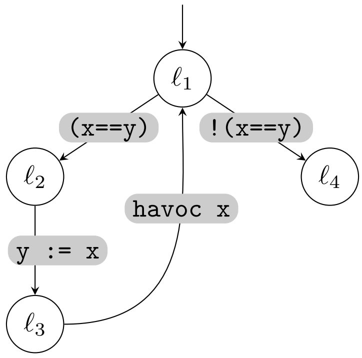
(b) Code of program P_{findmin}:

```
i := lo;
min := a[lo, lo];
while (i <= hi) {
    j := lo;
    while (j <= hi) {
        if (a[i, j] < min) {
            min := a[i, j];
        }
        j := j + 1;
    }
    i := i + 1;
}
```

Exercise 2: Program Configurations 2 Points

Consider the program $P = (V, \mu, \mathcal{T})$ with $V = \{x, y\}$, $\mu(x) = \mu(y) = \{\textbf{true}, \textbf{false}\}$ and $\mathcal{T}$ a derivation tree for the statement below on the left. On the right, a CFG for P is shown.

```
while (x == y) {
    y := x;
    havoc x;
}
```



Draw the reachability graph for this control-flow graph and the precondition-postcondition-pair $(x, x \to \neg y)$.

Exercise 3: Existence of Program Executions 2 Points

Recall the following lemma from the lecture slides:

> **Lemma** (RelAndExec) Let st be a statement, and let $G = (Loc, \Delta, \ell_{\mathsf{init}}, \ell_{\mathsf{ex}})$ be a control-flow graph for st. Then there exists a program execution $(\ell_0, s_0), \ldots, (\ell_n, s_n)$ with $\ell_0 = \ell_{\mathsf{init}}$ and $\ell_n = \ell_{\mathsf{ex}}$, iff $(s_0, s_n) \in [\![st]\!]$.

In order to prove this result, we formulated several helper lemmas. For this exercise, prove the following:

> **Lemma** (RelAndExec.2) Let st_1, st_2 be statements. Assume that for st_1 as well as for st_2, the lemma *RelAndExec* holds.
>
> Let now $G = (Loc, \Delta, \ell_{\mathsf{init}}, \ell_{\mathsf{ex}})$ be a control-flow graph for the sequential composition $st_1 st_2$. Then there exists a program execution $(\ell_0, s_0), \ldots, (\ell_n, s_n)$ with $\ell_0 = \ell_{\mathsf{init}}$ and $\ell_n = \ell_{\mathsf{ex}}$, iff $(s_0, s_n) \in [\![st_1 st_2]\!]$.