Technische Universität München (I7) **Summer Semester 2022**
J. Křetínský / M. Azeem / K. Grover **18.07.2022**

Model Checking – Exercise sheet 12

Exercise 12.1

Consider the following program with a Boolean variable `x`. Initially, the value of `x` is `false`. The question mark stands for a nondeterministic value.

```
x = ?;
while (x)
        x = ?;
while (true) {}
```

Let $AP = \{x\}$, where x is true only in states where the variable `x` is `true`.

(a) Construct a Kripke structure $\mathcal{K} = (S, \rightarrow, r, AP, \nu)$ for the above program.

(b) Let $\approx$ be an equivalence relation on S such that for all $s \approx t$ we have $\nu(s) = \nu(t)$. Construct from $\mathcal{K}$ the abstracted Kripke structure $\mathcal{K}'$ w.r.t. $\approx$.

(c) Model check the following formulas with $\mathcal{K}'$. Refine the abstraction if necessary.

(i) $\neg x \, \mathbf{W} \, x$

(ii) $\mathbf{G}(\neg x \rightarrow \mathbf{X} \neg x)$

(iii) $\mathbf{X}(\neg x \rightarrow \mathbf{G} \neg x)$

Exercise 12.2

We consider the following program, over the integer variables x and y:

```
1 if (x >= 0) x = -x;
2 if (y >= 0) y = -y;
3 if (x + y > 0) error;
4 end
```

1. Give the set of configurations of the program (some may not be reachable).
2. Draw the abstract transition system with the predicates l_1, l_2, l_3, l_4 and “error”.
3. Give a path ρ in the abstract transition system reaching a state where “error” holds.
4. What is the longest prefix (denoted ρ') of ρ that can be concretized?
5. Denote q the state in the abstract transition system reached by ρ'. Give a predicate that separates configurations reachable by ρ' from configurations that admit a successor.
6. Draw the abstract transition system with that additional predicate.

7. How many times do we have to repeat the abstraction refinement technique to exhibit an abstract transition system that does not reach the error state? Draw that transition system, how many predicates have we introduced?