SS 2025 05.06.2025

Exercises to the lecture
Semantics
Sheet 6

Prof. Dr. Roland Meyer
Jan Grünke Delivery until 19.04.2025 at 16:45

Exercise 6.1 (Transition Invariants)
Consider the program p, given by

1: **while** $x > 0$ **and** $y > 0$ **do**
2:   **if** $*$ **then**
3:     $x := x - 1$
4:   **else**
5:     $x := *$
6:     $y := y - 1$
7:   **end if**
8: **end while**

and the following transition invariant $T := T_x \cup T_y \bigcup_{\substack{i \neq j \\ i,j \in [1,8]}} T_{ij}$ with

$$T_{ij} := pc = i \wedge pc' = j$$
$$T_x := x \geq 0 \wedge x' < x$$
$$T_y := y \geq 0 \wedge y' < y.$$

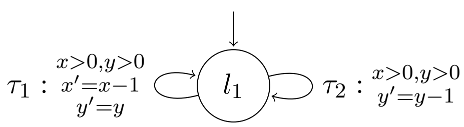
(a) Justify why T is a disjunctive well-founded transition invariant.

(b) Is T also an inductive transition invariant? Explain.

(c) State the proof rule used to establish termination via inductive transition invariants.

(d) Demonstrate that the program p terminates by applying this rule. First, express the program p as a symbolic transition system. Then, strengthen your transition invariant and prove that it is inductive.

Exercise 6.2 (Transition Predicate Abstraction)
Consider the following control flow graph for the program from the previous exercise:



Let $\mathcal{P} := \{x' = x - 1,\ y' = y - 1,\ y' = y\}$ be the set of transition predicates.
We aim to prove that the program p terminates under any fairness condition using transition predicate abstraction. Since we are not concerned with a specific fairness condition, we treat all nodes as fair. Thus, we verify whether T_v is well-founded for every node v in the abstract transition program.

(a) Provide the set of all abstract transitions, denoted as $T^{\#}_{\mathcal{P}}$.

(b) Using the algorithm discussed in the lecture, compute the abstract transition program $p^{\#}$ for the set of transition predicates $\mathcal{P}$.

(c) Do all nodes in $p^{\#}$ represent abstract transitions that are well-founded? If not, introduce additional predicates to ensure that termination of the original program p can be proven.

Exercise 6.3 (LTL to Büchi)
Consider the formula $\varphi = (p \wedge \bigcirc\neg p)\,\mathcal{U}\,(p \wedge \bigcirc p)$.

(a) Write down the Fisher-Ladner closure $FL(\varphi)$.

(b) Does a consistent Hintikka set H exists such that $\{\neg p, \varphi\} \subseteq H$?

(c) Construct the generalized Büchi automata A_φ according to the algorithm from the lecture. You may consider only inclusion minimal Hintikka sets and leave out unreachable states.

(d) Give a reachable state in A_φ that has no successors.