Dr. Matthias Heizmann
Tanja Schindler
Dominik Klumpp

Hand in until 16:15 on June 26, 2019
Discussion: June 26, 2019

Tutorial for Program Verification
Exercise Sheet 15

In Lecture 8 we made the following definition.

Definition (Post Image) Given a binary relation R over the set X and a subset of $Y \subseteq X$, the *post image of* Y *under* R, denoted $\mathit{post}(Y, R)$, is the set $\{x \in X \mid \text{exists } y \in Y \text{ such that } (y, x) \in R\}$

We use the post image to give a formal definition of the *strongest postcondition* for a given set of program states S and a given statement st. Intuatively, the strongest postcondition is the set of states in which a program can be after executing st in some state $s \in S$.

Definition (Strongest Postcondition) Given a set of states S and a statement st the *strongest postcondition* is the post image of S under the relation $[\![st]\!]$, i.e.

$$\mathrm{sp}(S, st) = \mathit{post}(S, [\![st]\!]).$$

Exercise 1: Strongest Postcondition 3 Points

Below, you find six sets of states that are each given as a strongest postcondition. Write down each set without using the strongest postcondition operator. You may use any formalism that your have seen in the lecture. Recall that $\{\varphi\}$ denotes the set of states that satisfy the formula φ. In the formulas below, i, k, x are integer variables and a is an array whose indices and values are integers.

(a) $\mathrm{sp}(\{\mathit{select}(a, k) = 23 \land \mathit{select}(a, i) = 42\},$ `assume i==k;` $)$

(b) $\mathrm{sp}(\{0 \leq k \land k \leq i\},$ `havoc k;` $)$

(c) $\mathrm{sp}(\{\mathit{select}(a, 23) = 42\},$ `a[k]:=1337;` $)$

(d) $\mathrm{sp}(\{x \cdot x > 5\},$ `x:=k-i;` $)$

(e) $\mathrm{sp}(\{x\%2 = 0\},$ `x:=x+1;` $)$

(f) $\mathrm{sp}(\{\mathit{select}(a, i + 1) = 23\},$ `i:=2*k+i;` $)$