Prof. Dr. Andreas Podelski
Matthias Heizmann

23.11.2011
Submission: 29.11.2011
at the beginning of the lecture

Tutorials for Program Verification
Exercise sheet 5

Exercise 1: Axioms for Update

1+2 points

(a) Consider the following Hoare logic axiom for the update statement

$$\overline{\{\phi\}\ x := t\ \{\phi \wedge x = t\}}$$

Show that this axiom is not correct.

(b) Consider the following Hoare logic axiom for the update statement

$$\overline{\{\phi\}\ x := t\ \{\exists y.\ \phi[y/x] \wedge x = t[y/x]\}}$$

Prove that this axiom is correct. You can either use the operational semantics of commands or derive this axiom using the Hoare calculus axioms and rules from the lecture.

Exercise 2: Hoare Logic Derivation

3 points + 2 bonus points

(a) Annotate the program below with a suitable loop invariant θ and then do what a tool is supposed to do: construct a derivation for the annotated program and the given pre- and postcondition.

$\{true\}$
$x := i;$
$y := j;$
while $x \neq 0$ **do** $\{\theta\}$ {
    $x := x - 1$
    $y := y - 1$
}
$\{i = j \rightarrow y = 0\}$

(b) Name two cases where the annotation with a loop invariant θ is not sufficient to derive the annotated program and give two loop invariants θ to exemplify the two cases.

Exercise 3: Derivations in $\mathcal{N}_{PL}$ 1+2 points

Construct a derivation of the following sequents in the natural deduction system $\mathcal{N}_{PL}$.

(a)

$$\frac{}{\vdash A \to B \to A}\,1$$

(b)

$$\frac{}{\neg A \vee (B \to C) \vdash (A \wedge B) \to C}$$

[1] $\to$ is a right associative connective, i.e. $A \to B \to A \;=\; A \to (B \to A)$