Prof. Dr. Andreas Podelski
Matthias Heizmann

9.11.2011
Submission: 15.11.2011
at the beginning of the lecture

Tutorials for Program Verification
Exercise sheet 2

Exercise 1: Hoare logic derivation 1+1+2 points

(a) Write down a partial correctness specification (i.e. precondition and postcondition for a program `C` that computes the maximum of x and y and stores the result in z.

(b) Write down the program `C`. Use the pseudo code introduced in the lecture.

(c) Construct a Hoare logic derivation that proves that your program `C` fulfills your correctness specification.

Exercise 2: Hoare triples 2 points

Consider the following Hoare triples. Which of them are valid for any program `C` and any state assertion ϕ?

(a) $\{\ true\ \}$ `C` $\{\ \phi\ \}$

(b) $\{\ false\ \}$ `C` $\{\ \phi\ \}$

(c) $\{\ \phi\ \}$ `C` $\{\ true\ \}$

(d) $\{\ \phi\ \}$ `C` $\{\ false\ \}$

If a Hoare triple is valid for any program `C` and any state assertion ϕ explain why. If a Hoare triple is not valid for some program `C` and some state assertion ϕ give a counterexample.

Exercise 3: Loop Invariant, Invariant, Inductive Invariant 3 points

(a) Consider the following while command

$$\mathrm{C} \equiv \ \textbf{while}\ \texttt{x<42}\ \textbf{do}\ \texttt{x:=x+y}$$

and precondition $\phi \equiv\ x = 1 \wedge y = 1$.

(i) Find a state assertion θ_1 that implies $x \geq 0$ and is loop invariant but not invariant.

(ii) Find a state assertion θ_2 that implies $x \geq 0$ and is invariant but not inductive invariant.

(iii) Find a state assertion θ_3 that implies $x \geq 0$ and is is inductive invariant.

(b) Consider the following scheme of a while command

$$\mathrm{C} \equiv \quad \textbf{while } \texttt{b } \textbf{do } \texttt{x := x+y}$$

and precondition $\phi \equiv \ x = 1 \wedge y = 1$.

(i) Find an expression `b` such that $\theta = x \geq 0$ is loop invariant but not invariant.

(ii) Find an expression `b` such that $\theta = x \geq 0$ is invariant but not inductive invariant.

(iii) Find an expression `b` such that $\theta = x \geq 0$ is is inductive invariant.