Prof. Dr. Andreas Podelski
Dr. Matthias Heizmann
Christian Schilling

Preference deadline: May 21, 2017
Discussion: May 23, 2017

Tutorial for Program Verification
Exercise Sheet 4

Exercise 1: Hoare logic 2 Points

In this exercise we consider very simple Hoare triples over Boolean variables where

- the precondition *precond*(X1,...,Xn) is a Boolean expression over the Boolean variables X1,...,Xn and does not contain the Boolean variable Y,
- the program consists of the single line

  Y:= *expr*(X1,...,Xn),

  where Y is a Boolean variable and *expr*(X1,...,Xn) is a Boolean expression over the Boolean variables X1,...,Xn that does not contain Y, and
- the postcondition *postcond*(X1,...,Xn) is a Boolean expression over the variables Y,X1,...,Xn.

(a) State a propositional logical formula

$$vc(\texttt{Y,X1,...,Xn})$$

that is valid if and only if a Hoare triple that has the following form is valid.

$$\{\ \textit{precond}(\texttt{X1,...,Xn})\ \}\ \texttt{Y := } \textit{expr}(\texttt{X1,...,Xn})\ \{\ \textit{postcond}(\texttt{Y,X1,...,Xn})\ \}$$

(b) Compute your propositional logical formula $vc(\texttt{Z,U,V})$ for the following concrete program.

$$\{\ \texttt{U} \leftrightarrow \texttt{V}\ \}\ \texttt{Z:= U} \land \texttt{V}\ \{\ \texttt{Z} \leftrightarrow \texttt{U}\ \}$$

Is your formula valid?

(c) Now we drop the restriction that *precond*(X1,...,Xn) does not contain the Boolean variable Y. Find a Hoare triple that is not valid but where your formula $vc(\texttt{U,V,Z})$ is valid.

Exercise 2: Hoare logic derivation 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 syntax for while programs introduced in the lecture.

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

Exercise 3: Hoare triples 2 Points

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

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

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

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

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

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

Exercise 4: Loop Invariant, Invariant, Inductive Invariant 2 Points

(a) Consider the following while command

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

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

(i) Find a state assertion θ_1 that implies $x \geq 0$ and is a loop invariant but not an invariant. (Be careful! It is not the one given for the program in the lecture, even though the program may look similar.)

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

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

(b) Consider the following scheme of a while command

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

and precondition $\phi \equiv x = 1 \land y = 1$. Furthermore, let $\theta \equiv x \geq 0$.

(i) Find an expression `b` such that θ is a loop invariant but not an invariant.

(ii) Find an expression `b` such that θ is an invariant but not an inductive invariant.

(iii) Find an expression `b` such that θ is an inductive invariant.