Prof. Dr. Andreas Podelski
Dr. Matthias Heizmann

Preference deadline: May 31, 2018
Discussion: June 4, 2018

Tutorial for Program Verification
Exercise Sheet 5

Exercise 1: Hoare logic derivation – Multiplication 1 Point

Solve Exercise 3c from the last exercise sheet whose solution has not yet been discussed in the exercise group.

Exercise 2: Hoare logic derivation – Factorial function 2 Points

Consider the annotated program Fact.

$$\begin{array}{l} \{n \geq 0\} \\ f := 1; \\ i := 1; \\ \textbf{while } i \leq n \textbf{ do } \{\theta\} \ \{ \\ \quad f := f \cdot i; \\ \quad i := i + 1; \\ \} \\ \{f = \mathit{fact}(n)\} \end{array}$$

The term $\mathit{fact}(n)$ denotes the factorial function applied to n.

In Figure 1 you find a derivation of the given partial correctness specification in the Hoare calculus and the following loop invariant.

$$\theta := f = \mathit{fact}(i-1) \wedge 1 \leq i \wedge i \leq n+1$$

Collect all side conditions from the strengthening/weakening rule applications (marked with "s/w") and show that they are valid (you can skip trivial proofs). Note that one of the proofs requires a case split.

Exercise 3: Guarded commands 2 Points

Consider the following modified version of Fact where we added the variable u.

$$\begin{array}{l} \{n \geq 0\} \\ u := 1; \\ f := 1; \\ i := 1; \\ \textbf{while } i \leq n \textbf{ do } \{\theta\} \ \{ \\ \quad f := f \cdot i; \\ \quad i := i + 1; \\ \quad u := u + 1; \\ \} \\ \{f = \mathit{fact}(n) \wedge u \geq 1\} \end{array}$$

(a) Transform the program (together with its pre-/postcondition) to a guarded command. Use the old θ from the previous exercise:

$$f = \mathit{fact}(i-1) \wedge 1 \leq i \wedge i \leq n+1$$

(b) Why will a correctness proof using **wp** of your guarded command fail?

(c) Modify θ above such that it can be used to show correctness of this program.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\{1=1\wedge n\geq 0\}\, f:=1\,\{f=1\wedge n\geq 0\}}\,\text{asgn}}{\{n\geq 0\}\, f:=1\,\{f=1\wedge n\geq 0\}}\,\text{s/w} \qquad \dfrac{\dfrac{}{\{f=1\wedge 1=1\wedge n\geq 0\}\, i:=1\,\{f=1\wedge i=1\wedge n\geq 0\}}\,\text{asgn}}{\{f=1\wedge n\geq 0\}\, i:=1\,\{f=1\wedge i=1\wedge n\geq 0\}}\,\text{s/w}}{\{n\geq 0\}\, f:=1\,;\, i:=1\,\{f=1\wedge i=1\wedge n\geq 0\}}\,\text{seq} \qquad (1)}{\{n\geq 0\}\,\texttt{Fact}\,\{f=\mathit{fact}(n)\}}\,\text{seq}$$

Proof tree for (1):

$$\dfrac{\dfrac{\dfrac{(2) \qquad \dfrac{\dfrac{}{\{f=\mathit{fact}(i+1-1)\wedge 1\leq i+1\wedge i+1\leq n+1\}\, i:=i+1\,\{\theta\}}\,\text{asgn}}{\{f=\mathit{fact}(i)\wedge 1\leq i\wedge i\leq n\}\, i:=i+1\,\{\theta\}}\,\text{s/w}}{\{\theta\wedge i\leq n\}\, f:=f\cdot i\,;\, i:=i+1;\,\{\theta\}}\,\text{seq}}{\{\theta\}\,\textbf{while}\ i\leq n\ \textbf{do}\ \{\theta\}\ \{f:=f\cdot i\,;\, i:=i+1\}\,\{\theta\wedge\neg(i\leq n)\}}\,\text{whl}}{\{f=1\wedge i=1\wedge n\geq 0\}\,\textbf{while}\ i\leq n\ \textbf{do}\ \{\theta\}\ \{f:=f\cdot i\,;\, i:=i+1\}\,\{f=\mathit{fact}(n)\}}\,\text{s/w}$$

Proof tree for (2):

$$\dfrac{\dfrac{}{\{f\cdot i=\mathit{fact}(i-1)\cdot i\wedge 1\leq i\wedge i\leq n\}\, f:=f\cdot i\,\{f=\mathit{fact}(i-1)\cdot i\wedge 1\leq i\wedge i\leq n\}}\,\text{asgn}}{\{\theta\wedge i\leq n\}\, f:=f\cdot i\,\{f=\mathit{fact}(i)\wedge 1\leq i\wedge i\leq n\}}\,\text{s/w}$$

Figure 1: Hoare derivation for `Fact` function and $\theta\equiv f=\mathit{fact}(i-1)\wedge 1\leq i\wedge i\leq n+1$. Due to space constraints the proof tree is split into three subtrees and we have not substituted θ. On the web page you can find a full picture of the proof tree.