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.

$$\{ n \geq 0 \}$$
$$f := 1;$$
$$i := 1;$$
while $$i \leq n$$ do \{ \theta \} 
$$f := f \cdot i;$$
$$i := i + 1;$$
\}
$$\{ f = \text{fact}(n) \}$$

The term $\text{fact}(n)$ denotes the factorial function applied to $n$.
In Figure you find a derivation of the given partial correctness specification in the Hoare calculus and the following loop invariant.

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

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 $u$.

$$\{ n \geq 0 \}$$
$$u := 1;$$
$$f := 1;$$
$$i := 1;$$
while $$i \leq n$$ do \{ \theta \} 
$$f := f \cdot i;$$
$$i := i + 1;$$
$$u := u + 1;$$
\}
$$\{ f = \text{fact}(n) \land u \geq 1 \}$$
(a) Transform the program (together with its pre-/postcondition) to a guarded command. Use the old \( \theta \) from the previous exercise:

\[ f = \text{fact}(i - 1) \land 1 \leq i \land i \leq n + 1 \]

(b) Why will a correctness proof using \( \text{wp} \) of your guarded command fail?

(c) Modify \( \theta \) above such that it can be used to show correctness of this program.
\[
\{1 = 1 \land n \geq 0\} f := 1 \{f = 1 \land n \geq 0\} \quad \text{asgn}
\]
\[
\{n \geq 0\} f := 1 \{f = 1 \land n \geq 0\} \quad \text{s/w}
\]
\[
\{n \geq 0\} f := 1 ; i := 1 \{f = 1 \land i = 1 \land n \geq 0\} \quad \text{seq}
\]

Proof tree for (1):

\[
\{f = \text{fact}(i + 1 - 1) \land 1 \leq i + 1 \land i + 1 \leq n + 1\} i := i + 1 \{\theta\} \quad \text{asgn}
\]
\[
\{\theta \land i \leq n\} f := f \cdot i ; i := i + 1 ; \{\theta\} \quad \text{seq}
\]
\[
\{\theta\} \text{ while } i \leq n \text{ do } \{\theta\} \{f := f \cdot i ; i := i + 1\} \{f = \text{fact}(n)\} \quad \text{whl}
\]

Proof tree for (2):

\[
\{f \cdot i = \text{fact}(i - 1) \cdot i \land 1 \leq i \land i \leq n\} f := f \cdot i \{f = \text{fact}(i - 1) \cdot i \land 1 \leq i \land i \leq n\} \quad \text{asgn}
\]
\[
\{\theta \land i \leq n\} f := f \cdot i \{f = \text{fact}(i) \land 1 \leq i \land i \leq n\} \quad \text{s/w}
\]

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