# Exercise session 11
# – Hoare logic –

**Exercise 36.** Division and modulo operation

Use the Hoare logic to prove that *if* statement `z:=0; while (y≤x) do (z:=z+1; x:=x-y)` executed from a state $\sigma$ with $\sigma(\mathtt{x}) > 0$ and $\sigma(\mathtt{y}) > 0$ terminates, *then* in the final state $\sigma'$, we get $\sigma'(\mathtt{z}) = \sigma(\mathtt{x})$ **div** $\sigma(\mathtt{y})$ and $\sigma'(\mathtt{x}) = \sigma(\mathtt{x})$ **mod** $\sigma(\mathtt{y})$.

**Exercise 37.** Inference rule for `repeat` S `until` b

Suggest an inference rule for `repeat` S `until` b. You are not allowed to rely on the existence of a `while`-construct in the language.

**Exercise 38.** Weakest postcondition always provable

Show that $\vdash \{\ P\ \}\ S\ \{\ \mathit{true}\ \}$ for all statements $S$ and properties $P$.

## Solutions

**Exercise 36.** Division and modulo operation

First of all, we have to determine the pre- and postcondition of the statement.
Precondition: from the informal specification we can see that in the starting state $\sigma$, `x` and `y` is greater than zero. This yields $\texttt{x} > 0 \ \wedge \ \texttt{y} > 0$. Furthermore, we see that in the final state $\sigma'$, the values of `z` and `x` depend on the initial values of `x` and `z`. Thus, we have to introduce two logical variables for the initial values of `x` and `z`.
Thus, we get the following precondition: $\{\texttt{x} > 0 \ \wedge \ \texttt{y} > 0 \ \wedge \ \texttt{x} = N \ \wedge \ \texttt{y} = M\}$

Postcondition: from the informal specification we can see that we are interested in the final values of `x` and `z`. These can be easily given by the logical variables: $\{\texttt{z} = N \ \textbf{div} \ M \ \wedge \ \texttt{x} = N \ \textbf{mod} \ M\}$

From the informal specification we can also deduce that we are interested in partial correctness only.

Before starting the proof, we have to determine the loop invariant. We do that by inspecting the iterations of the loop:

| Iteration | 0 | 1 | 2 | ... | $i$ | ... |
|---|---|---|---|---|---|---|
| `x` | $N$ | $N - M$ | $N - 2 * M$ | ... | $N - i * M$ | ... |
| `y` | $M$ | $M$ | $M$ | ... | $M$ | ... |
| `z` | 0 | 1 | 2 | ... | $i$ | ... |

From the table we can observe the following invariants: $\texttt{x} = N - \texttt{y} * \texttt{z}$, $\texttt{y} = M$, and $\texttt{z} \geq 0$. Furthermore, by inspecting the condition and the body of the loop, we can see that $\texttt{x} \geq 0$. We get our loop invariant by conjoining these four predicates (since $\texttt{z} \geq 0$ will not be used throughout the proof, we drop it from the invariant for simplicity).

Now we can start the proof by first adding the pre- and postcondition around the whole statement and adding the predicates arising from the invariant and loop condition around the `while`-statement. Then we have to complete the proof by using the Hoare rules as follows:

$\{\texttt{x} > 0 \ \wedge \ \texttt{y} > 0 \ \wedge \ \texttt{x} = N \ \wedge \ \texttt{y} = M\}$

$\Longrightarrow$

$\{\texttt{x} = N - \texttt{y} * 0 \ \wedge \ \texttt{y} = M \ \wedge \ \texttt{x} \geq 0\}$

z:=0;

$\{\texttt{x} = N - \texttt{y} * \texttt{z} \ \wedge \ \texttt{y} = M \ \wedge \ \texttt{x} \geq 0\}$

`while (y≤x) do`

$\{\texttt{y} \leq \texttt{x} \ \wedge \ \texttt{x} = N - \texttt{y} * \texttt{z} \ \wedge \ \texttt{y} = M \ \wedge \ \texttt{x} \geq 0\}$

$\Longrightarrow$

$\{\texttt{x} - \texttt{y} = N - \texttt{y} * (\texttt{z} + 1) \wedge \ \texttt{y} = M \ \wedge \ \texttt{x} - \texttt{y} \geq 0\}$

z:=z+1;

$\{\texttt{x} - \texttt{y} = N - \texttt{y} * \texttt{z} \ \wedge \ \texttt{y} = M \ \wedge \ \texttt{x} - \texttt{y} \geq 0\}$

x:=x-y;

$\{\texttt{x} = N - \texttt{y} * \texttt{z} + \wedge \ \texttt{y} = M \ \wedge \ \texttt{x} \geq 0\}$

`end`

$\{\texttt{y} > \texttt{x} \ \wedge \ \texttt{x} = N - \texttt{y} * \texttt{z} \ \wedge \ \texttt{y} = M \ \wedge \ \texttt{x} \geq 0\}$

$\Longrightarrow$

$\{0 \leq \mathtt{x} < M \ \wedge \ \mathtt{x} = N - M * \mathtt{z}\}$

$\Longrightarrow$

$\{\mathtt{z} = N \ \mathbf{div} \ M \ \wedge \ \mathtt{x} = N \ \mathbf{mod} \ M\}$

The validity of the last implication is not trivial, so we show it in more details. We prove $\mathtt{z} = N \ \mathbf{div} \ M$ and $\mathtt{x} = N \ \mathbf{mod} \ M$ separately:

A) by definition $\mathtt{z} = N \ \mathbf{div} \ M$ iff $\exists \ \mathtt{x} : \ \mathtt{z} * M + \mathtt{x} = N \ \wedge \ 0 \leq \mathtt{x} < M$. This is exactly what we have on the left-hand side of the implication.

B) $\mathtt{x} = N \ \mathbf{mod} \ M$ can be expressed as $\mathtt{x} = N - (N \ \mathbf{div} \ M) * M$. As we know that $\mathtt{z} = N \ \mathbf{div} \ M$, we get $\mathtt{x} = N - \mathtt{z} * M$, which is exactly what we have as second conjunct in the left-hand side of the implication.

**Exercise 37.** Inference rule for `repeat` S `until` b

Partial correctness: before and after the first execution of $S$ we do not know whether $b$ holds or not. Thus, we can just give the most general form of an assertion: $\{ \ P \ \} \ S \ \{ \ Q \ \}$. We know that if after the execution of $S$ condition $b$ holds then we exit the loop, thus we know that $Q \ \wedge \ b$ holds. Otherwise (i.e. $b$ does not hold), the iteration continues and $S$ will be executed again. This imposes the requirement that $Q \ \wedge \ \neg b \ \Rightarrow \ P$. This predicate can also be seen as the invariant of the loop.

So the rule looks as follows:

$$\frac{\{ \ P \ \} \ S \ \{ \ Q \ \}}{\{ \ P \ \} \ \mathtt{repeat} \ S \ \mathtt{until} \ b \ \{ \ Q \ \wedge \ b \ \}} \ Q \ \wedge \ \neg b \ \Rightarrow \ P$$

Total correctness: we have to extend the above rule with the loop variant just as we did for the `while`-rule:

$$\frac{\{ \ P \ \wedge \ V(Z+1) \ \} \ S \ \{ \ \Downarrow Q \ \wedge \ V(Z) \ \}}{\{ \ P \ \wedge \ \exists Z : V(Z) \ \} \ \mathtt{repeat} \ S \ \mathtt{until} \ b \ \{ \ \Downarrow Q \ \wedge \ b \ \}} \ Q \ \wedge \ \neg b \ \Rightarrow \ P$$

**Exercise 38.** Weakest postcondition always provable

We do the proof by structural induction on statement $S$.

**Base case:**

Skip: The antecedent is the `skip`-axiom.

$$\frac{\{ \ P \ \} \ \mathtt{skip} \ \{ \ P \ \}}{\{ \ P \ \} \ \mathtt{skip} \ \{ \ true \ \}} \ \text{consequence rule with } P \Rightarrow true$$

Assignment: The antecedent is the `assignment`-axiom with $P = true$.

$$\frac{\{ \ true[\mathtt{x} \mapsto \mathcal{A}[\![e]\!] \ \} \ \mathtt{x:=}e \ \{ \ true \ \}}{\{ \ P \ \} \ \mathtt{x:=}e \ \{ \ true \ \}} \ \text{consequence rule with } P \Rightarrow true[\mathtt{x} \mapsto \mathcal{A}[\![e]\!]$$

**Step case:**

Composition: From the induction hypothesis we know that the two triples in the antecedent can be inferred.

$$\frac{\{\ P\ \}\ S_1\ \{\ true\ \} \qquad \{\ true\ \}\ S_2\ \{\ true\ \}}{\{\ P\ \}\ S_1 ; S_2\ \{\ true\ \}}\ \text{sequential composition}$$

`If`-statement: From the induction hypothesis we know that the two triples in the antecedent can be inferred.

$$\frac{\{\ \mathcal{B}[\![b]\!]\ \wedge\ P\ \}\ S_1\ \{\ true\ \} \qquad \{\ \neg\mathcal{B}[\![b]\!]\ \wedge\ P\ \}\ S_2\ \{\ true\ \}}{\{\ P\ \}\ \texttt{if}\ b\ \texttt{then}\ S_1\ \texttt{else}\ S_2\ \texttt{end}\ \{\ true\ \}}\ \text{if rule}$$

`While`-statement: From the induction hypothesis we know that the triple in the topmost antecedent can be inferred.

$$\frac{\dfrac{\{\ \mathcal{B}[\![b]\!]\ \wedge\ true\ \}\ S\ \{\ true\ \}}{\{\ true\ \}\ \texttt{while}\ b\ \texttt{do}\ S\ \texttt{end}\ \{\ \neg\mathcal{B}[\![b]\!]\ \wedge\ true\ \}}\ \text{while rule}}{\{\ P\ \}\ \texttt{while}\ b\ \texttt{do}\ S\ \texttt{end}\ \{\ true\ \}}\ \text{consequence rule with } P \Rightarrow true \text{ and } \mathcal{B}[\![b]\!]\ \wedge\ true \Rightarrow true$$