Semantics and Verification of Software
apl. Prof. Dr. Thomas Noll
Christoph Matheja, Kevin Batz

Lehrstuhl für Informatik 2 Softwaremodellierung und Verifikation
RWTH AACHEN UNIVERSITY

**Exercise Sheet 5**

**Due date:** May 31th. Please hand in your solutions at the start of the exercise class.

## Task 1: Applying Hoare Logic and `wlp` (30 Points)

1. Let $c$ be the following program:

$$\mathsf{if}\ (x \geq 0)\ \mathsf{then}\ \{y := x\}\ \mathsf{else}\ \{y := -x\}$$

   Calculate $\mathtt{wlp}[\![c]\!]\,(y = |x|)$. What does the result tell you about the given program?

2. Prove in Hoare logic:

$$\vdash \{x < y\}\mathsf{while}\ x < y\ \mathsf{do}\ x := x + 1\ \mathsf{end}\{x = y\}\ .$$

## Task 2: Untouched Assertions (40 Points)

Analogously to arithmetic expressions, we define the set $\mathsf{FV}\,(A)$ of free variables occurring in assertion $A$ as

$$\mathsf{FV}\,(A) \ := \ \{x \in \mathsf{Var} \mid x \text{ occurs in A}\}\ .$$

Furthermore, for $c \in \mathsf{Cmd}$, we define

$$\mathtt{Mod}(c) \ := \ \{x \in \mathsf{Var} \mid x \text{ occurs on a left-hand side of an assignment in } c\}\ .$$

Prove: For all $P, Q \in \mathsf{Assn}$ and all $c \in \mathsf{Cmd}$ with $\mathtt{Mod}(c) \cap \mathsf{FV}\,(Q) = \emptyset$, we have

$$\models\ \mathtt{wlp}[\![c]\!]\,(P) \wedge Q \ \Rightarrow\ \mathtt{wlp}[\![c]\!]\,(P \wedge Q)\ .$$

*Hint:* Recall that we identify an assertion $A$ with a set $S_A = \{\sigma \in \Sigma \mid \sigma \models A\}$.

## Task 3: `wlp` Loop Invariants (30 Points)

Given a while loop $c' = \mathsf{while}\ b\ \mathsf{do}\ c\ \mathsf{end}$ and an assertion $B \in \mathsf{Assn}$, we define

$$\Psi_B \colon \mathsf{Assn} \to \mathsf{Assn}, \quad \mathsf{Q} \ \mapsto\ (\mathsf{b} \wedge \mathtt{wlp}[\![\mathsf{c}]\!]\,(\mathsf{Q})) \vee (\neg \mathsf{b} \wedge \mathsf{B})\ .$$

That is, we have $\mathtt{wlp}[\![c']\!]\,(B) = \mathrm{FIX}(\Psi_B)$ (Lecture 10, Slide 25). Furthermore, we denote by $\leq \subseteq \mathsf{Assn} \times \mathsf{Assn}$ the partial order on assertions defined as

$$A \leq B \quad \text{iff} \quad \models A \Rightarrow B\ .$$

Now let $c' = \mathsf{while}\ b\ \mathsf{do}\ c\ \mathsf{end}$ and $A, B, I \in \mathsf{Assn}$. Prove:

$$\text{If } I \leq \Psi_B(I) \text{ and } A \leq I, \text{ then } \models \{A\}\mathsf{while}\ b\ \mathsf{do}\ c\ \mathsf{end}\{B\}\ .$$

*Hint:* You may assume that $(\mathsf{Assn}, \leq)$ is chain complete and that $\Psi_B$ is continuous. Analogously to Exercise 3.3, you may assume that for a chain complete partial order $(D, \sqsubseteq)$ and a continuous function $f \colon D \to D$ it holds that $d \sqsubseteq f(d)$ implies $d \sqsubseteq \mathrm{FIX}(f)$.