Exercise Sheet 6: Axiomatic Semantics

Due date: June 3rd. You can hand in your solutions at the start of the exercise class.

Exercise 1 (Assertion Language) 35%

(a) [10%] Give an assertion A with a logical variable $i \in \mathsf{LVar}$ which expresses that i is a prime number. More precisely, for every $\sigma \in \Sigma$ and $I \in \mathsf{Int}$, $\sigma \models^I A$ should be valid if and only if i is prime.

(b) [10%] Give an assertion A with logical variables $i, j, k \in \mathsf{LVar}$ which expresses that k is the least common multiple of i and j.

(c) [15%] Goldbach's conjecture states that every even natural number $n \in \mathbb{N}$ can be written as the sum of two primes $p, q \in \mathbb{N}$. Such a pair (p, q) is called a Goldbach partition of n. Does there exist a partial correctness property $\{A\}c\{B\}$ of a program c that computes the Goldbach partition of any given even natural number? If yes, does the existence of a program c satisfying this property prove Goldbach's conjecture?

Exercise 2 (Axiomatic Semantics of a For-Loop) 35%

(a) [10%] Develop a proof rule for statements of the form $\mathsf{for}\, x := a_1 \,\mathsf{to}\, a_2 \mathsf{do}\{c\}$ where $x \in \mathsf{Var}$, $a_1, a_2 \in \mathsf{AExp}$, and $c \in \mathsf{Cmd}$ (without assuming the presence of a `WHILE` statement in the programming language).

(b) [25%] Using this rule (and the known proof system), establish the validity of the following partial correctness property:

$$\{y \geq 0\} z := 0; \mathsf{for}\ x := 1\ \mathsf{to}\ y \mathsf{do}\{z := z + x\} \left\{ z = \frac{y(y+1)}{2} \right\}$$

Exercise 3 (Weakest Precondition) 30%

In the lecture, the weakest precondition calculus has been introduced to show relative completeness of Hoare Logic. Informally, the weakest precondition $wp(c, B)$ is the weakest assertion A such that $\{A\}c\{B\}$ holds. Note that termination is not required.

(a) [15%] Give a formal definition of the weakest precondition $wp(c, B)$ of a `WHILE` program c and an assertion B. For simplicity, the weakest precondition may be infinite (or contain recursion).

(b) [15%] Prove that the rules Hoare Logic together with your rules to compute the weakest precondition is relative complete, i.e. show by structural induction that $\vdash \{wp(c, B)\}c\{B\}$ holds for all statements $c \in \mathsf{Cmd}$ and assertions B.

Exercise 4 (Strongest Postcondition (Bonus)) 20%

This exercise is a bonus task which considers an alternative to weakest preconditions. Informally, the strongest postcondition $sp(c, A)$ is the strongst assertion B such that $\{A\}c\{B\}$ holds.

(a) [15%] Give a formal definition of the strongst postcondition $sp(c, A)$ of a `WHILE` program c and an assertion A. Again, it is not required that the strongest postcondition is finite.

(b) [5%] What is an advantage of weakest preconditions in comparison to strongest postconditions when trying to automatically prove Hoare triples?