Exercise Sheet 6

Due date: December 6th. You can hand in your solutions at the start of the exercise class.

Remark: We started uploading solutions to previous exercises. The password to access the solutions on our website will be announced in the next exercise class.

Hint: Notation is as in the lecture. That is, c is a program, b a Boolean expression, σ a program state, etc.

Task 1: Partial Correctess Properties (2 Points)

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.

(a) Prove that there exists a partial correctness property $\{A\}c\{B\}$ of a program c that computes a Goldbach partition of any given natural number n? (You do not have to search for such a program c, it suffices to find suitable assertions A, B.)

(b) Does the existence of a program c satisfying the partial correctness property from (a) prove Goldbach's conjecture? Justify your answer.

Task 2: Relative Completeness (4 Points)

Intuitively, the weakest precondition $wp(c, B)$ of a program c and a postcondition B in an expressive assertion language is an assertion A_0 that is implied by all assertions A such that $\{A\}c\{B\}$ is a valid partial correctness property (see Definition 10.6 from the lecture).

This exercise takes a more detailed look at the proof of relative completeness of Hoare logic.

(a) Give a formal *syntactic* definition of the weakest precondition of a `while` program c and an assertion B. *Hint:* For simplicity, you may use infinite conjunctions and disjunctions which are not allowed in the assertion language from the lecture.

(b) Prove that Hoare logic is relatively complete. That is, show for all statements $c \in \mathsf{Cmd}$ and all assertions B that $\vdash \{wp(c, B)\}c\{B\}$ holds.

Task 3: Strongest Postconditions (4 Points)

Intuitively, the *strongest postcondition* $sp(c, A)$ of a program c and a precondition A in an expressive assertion language is the strongest assertion B that holds when running c on a state satisfying A. In contrast to weakest preconditions, we thus apply forwards reasoning.

(a) Formalize the intuitive definition of strongest postconditions from above, i.e. give an exact definition of the set of states described by $sp(c, A)$.

(b) Give a formal *syntactic* definition of the strongest precondition of a `while` program c and an assertion A. *Hint:* For simplicity, you may use infinite conjunctions and disjunctions which are not allowed in the assertion language from the lecture.

(c) Apply your syntactic definition from (b) to compute the following strongest postcondition:

$$sp(x := 2 * x; y := x + 2; z := y + x, x = 1)$$

(d) Prove or disprove: For every program $c \in \mathsf{Cmd}$, $\models \{wp(c, sp(c, \mathit{false}))\}c\{sp(c, wp(c, \mathit{false}))\}$.