Exercise Sheet 10: Correctness Properties for Execution Time

Due date: July 8th. You can hand in your solutions at the start of the exercise class.

Exercise 1 (Timed correctness in non-deterministic programs) **10%**

Extend the proof system of Hoare logic for timed correctness to incorporate a demonic model of the non-deterministic operator $c_1 \,\Box\, c_2$. (In the demonic model, all possible program executions must establish the postcondition and satisfy the time bound).

Exercise 2 (Alternative while Rule) **20%**

Suggest a rule for $\mathsf{while}\ (b)\ \mathsf{do}\ \{c\}$ that expresses that its execution time, neglecting constant factors, is the product of the number of times the loop is executed and the maximal execution time for the body of the loop.

Exercise 3 (Completeness of Hoare logic for timed correctness) **25%**

Prove or disprove: There exists a valid total correctness property $\{A\}\, c\, \{\Downarrow B\}$ such that for every $e \in \mathsf{AExp}$, the timed correctness property $\{A\}\, c\, \{e \Downarrow B\}$ is *not* valid.

Exercise 4 (Correctness Properties for Lower Execution Time Bounds) **45%**

In the lecture, we considered a calculus to prove upper bounds on the execution time of programs.

(a) [25%] Modify the Hoare logic for timed correctness from the lecture to prove *lower* execution time bounds instead of upper bounds. To be more precise, a lower bound correctness property $\{A\}c\{e \Uparrow B\}$ is valid if there exists $k > 0$ such that for each $I \in Int$, $\sigma, \sigma' \in \Sigma$ and $\tau \in \mathbb{N}$, $\langle c, \sigma\rangle \xrightarrow{\tau} \sigma'$ implies $\tau \geq k \cdot \mathfrak{A}[\![e]\!]$ and $\sigma' \models^I B$.

(b) [5%] For upper execution time bounds, we considered total correctness properties only. Why are we considering partial correctness properties instead for lower bound execution time bounds?

(c) [5%] Is there a postcondition $e \Uparrow B$ such that $\{A\}c\{e \Uparrow B\}$ universally holds regardless of the choice of A and c?

(d) [10%] Using your Hoare calculus for lower execution time bounds, prove that

$$\{\mathsf{true}\}\mathsf{while}\ (\mathsf{true})\ \mathsf{do}\ \{\mathsf{skip}\}\{2 \upuparrows N \Uparrow \mathsf{true}\}$$

is valid for each $N \in \mathbb{N}$ [1]. *Note:* You may assume $\upuparrows$ to be a given functional symbol, i.e. you do not have to define it in Hoare logic first.

[1] Knuth's arrow notation is defined recursively as $a \upuparrows 1 := a$ and $a \upuparrows (b+1) := a^{a \upuparrows b}$ where $a, b \in \mathbb{N}$.