8 Hoare Logic and Model Checking (KS)

Consider a programming language that consists of commands `C` composed from assignments `V := E` (where `E` is an expression) using sequences `C1;C2`, conditionals `IF S THEN C1 ELSE C2` (where `S` is a statement) and while-loops `WHILE S DO C`.

(*a*) Carefully explain the meaning of total correctness Hoare triples. [2 marks]

(*b*) Suggest a command C such that the following partial correctness triple holds.

$$\{X = x\}\ C\ \{1 = 2\}$$

Explain why the triple holds. [4 marks]

(*c*) Consider Hoare triples of the form $\{P\}$ `X := E` $\{P[\mathtt{E}/\mathtt{X}]\}$ where P, `X` and `E` range over formulas, variables and expressions, respectively. Recall that $P[\mathtt{E}/\mathtt{X}]$ denotes P with `E` substituted for every occurrence of `X` in P.

Write down an instance of such a triple that cannot be proved using Hoare logic and explain why it cannot be proved. [4 marks]

(*d*) Write down a partial correctness specification for a command that adds the initial values stored in variables `X` and `Y`. The command should store the result in a variable `Z`. [4 marks]

(*e*) Propose a loop invariant for proving the following partial correctness triple.

$$\{\mathtt{X} = n \wedge \mathtt{Y} = 0 \wedge n \geq 0\}$$

```
  WHILE X > 0 DO (Y := Y + X; X := X - 1)
```

$$\{\mathtt{Y} = \sum_{i=1}^{n} i\}$$

[6 marks]