Specification and Verification I

Give an example of $P$, $C$ and $Q$ such that $\vdash \{P\} C \{Q\}$ but it is not the case that $\vdash [P] C [Q]$. Justify your answer.

5 marks

Explain how to translate the partial correctness specification shown below into higher-order logic.

$$\{X = x \land Y = y\} \text{TEMP := X;} \ X := Y; \ Y := \text{TEMP} \{X = y \land Y = x\}$$

5 marks

Write down and justify an example of a correctly annotated specification $\{P\} C \{Q\}$ such that $\vdash \{P\} C \{Q\}$ but the verification conditions are not true. Comment on the significance of your example.

5 marks

Define the meaning of the notation $[P, Q]$. Write down the $\text{WHILE}$-law of refinement and justify it with respect to the $\text{WHILE}$-rule for Floyd–Hoare logic.

5 marks