

2000 Paper 7 Question 1

Specification and Verification I

Explain why the Assignment Axiom of Floyd–Hoare logic is valid only for assignments whose right-hand sides have no side effects. [4 marks]

Illustrate your explanation with an example. [4 marks]

Suppose expressions of the form $(C;E)$ are allowed, where C is a command and E is an ordinary expression (E has no embedded commands). $(C;E)$ is evaluated by first executing the command C (with possible side-effects) and then returning the value of the expression E .

Discuss how Floyd–Hoare logic might be extended to handle such expressions. [6 marks]

Illustrate your discussion by giving a proof in the extended logic of

$$\begin{aligned} & \{Y \leq X\} \\ & R := X; Q := 0; \\ & \text{WHILE (BEGIN } R := R - Y; Q := Q + 1 \text{ END; } Y \leq R) \text{ DO SKIP} \\ & \{X = R + (Y \times Q) \wedge R < Y\} \end{aligned}$$

[6 marks]