Solution notes

Specification and Verification I 2005 – Paper 7 Question 6 (MJCG)

(a) State and explain Hoare's assignment axiom for simple assignments $V{:=}E$, where V is a variable. [5 marks]

The assignment axiom consists of all instances of:

$$\{Q[E/V]\}\ V{:=}E\ \{Q\}$$

where $Q[E/V]$ denotes the result of substituting E for V in Q.

If a formula "$\cdots E \cdots$" holds and the assignment $V{:=}E$ is executed, then in the state after the assignment, the value of the variable V will be the value of E and hence the formula "$\cdots V \cdots$" will hold.

(b) Is Hoare's assignment axiom valid for assignments $V := E$ if the expression E can have side effects? Justify your answer. [5 marks]

Hoare's assignment axiom will not in general hold if E can have side effects. An example that illustrates why not is:

$$\{X = 1 \wedge Y = 1\}\ X{:=}\texttt{BEGIN}\ 2;\ Y{:=}2\ \texttt{END}\ \{X = 2 \wedge Y = 1\}$$

where $\texttt{BEGIN}\ 2;\ Y{:=}2\ \texttt{END}$ *is an expression that evaluates to 2 and has a side-effect of setting variable Y to 2. The assignment axiom fails to predict that Y is changed. Furthermore, the precondition $\{Q[E/V]\}$ that Hoare's axiom would produce: $\{\texttt{BEGIN}\ 2;\ Y{:=}2\ \texttt{END} = 2 \wedge Y = 1\}$ doesn't make sense in first-order logic!*

(c) State and explain the assignment axiom for array assignments $V(E_1) := E_2$, where V is an array variable. [5 marks]

The array assignment axiom is the normal assignment axiom applied to the assignment $V := V[E_1 \leftarrow E_2]$, where $V[E_1 \leftarrow E_2]$ is the array identical to V except that the value at E_1 has been changed to E_2 (and all other components of the array unchanged).

(d) The following alternative "forward" rule for assignments has been proposed:

$$\vdash \{P\}\ V{:=}E\ \{\exists v.\ V = E[v/V]\ \wedge\ P[v/V]\}$$

Explain informally why this rule is valid. [5 marks]

If P holds, then after executing $V{:=}E$ the variable V will have the value of E in the state before the assignment, which is the value of $E[v/V]$ in the state after the assignment, where v is the value of V in the state before the assignment. This value v will satisfy $P[v/V]$ because we assumed P held in the state before the assignment.

Context

This question is about Hoare Logic and was covered near the beginning of the course.

Marking Scheme

For each section:

5 marks : well-written answer that goes beyond pure regurgitation of course material and shows evidence of understanding.

4 marks : complete answer, but lacking in the flair needed for 5 marks;

3 marks : evidence of basic grasp of material, but some omissions or inaccuracies;

2 marks : partial answer lacking some key material or serious inaccuracies;

1 mark : something at least vaguely relevant detectable.