SOLUTION NOTES

Specification and Verification I 2002 Paper 8 Question 12 (MJCG)

(*a*) Outline the steps involved in proving a specification $\{P\}C\{Q\}$ using the method of verification conditions [4 marks].

The steps are as follows

1. Add annotations to C giving invariants (and variants, if total correctness is being proved) to `WHILE`-commands, invariants to `FOR`-commands and assertions before any command in a sequence that is not an assignment [2 marks].
2. Apply the verification generation algorithm, which recursively descends through C computing verification conditions (details omitted) [2 marks].
3. Prove the resulting verification conditions [2 marks].

Since the question says "Outline", just the general idea will be sufficient (i.e. full details not needed).

(*b*) The familiar algorithm for generating verification conditions assumes that an annotation is added before a command C_2 in a sequence C_1`;`C_2 unless C_2 is an assignment. Extend this algorithm so that no annotation is required if C_2 is of the form `IF` B `THEN` X_1`:=`E_1 `ELSE` X_2`:=`E_2 [6 marks].

let R be $(B \wedge Q[E_1/X_1]) \vee (\neg B \wedge Q[E_2/X_2])$, then sufficient verification conditions for $\{P\}C$`;IF` B `THEN` X_1`:=`E_1 `ELSE` X_2`:=`$E_2\{Q\}$ are the verification conditions for $\{P\}C\{R\}$

This part requires original thought, since it was not covered in the lectures. Although the answer above is short, I'd expect candidates to spend some time thinking and experimenting before hitting on a solution.

(*c*) Justify your extended algorithm by showing that if the verification conditions it generates from $\{P\}$ C`;` `IF` B `THEN` X_1`:=`E_1 `ELSE` X_2`:=`$E_2\{Q\}$ are provable, then $\vdash$ $\{P\}$ C`;` `IF` B `THEN` X_1`:=`E_1 `ELSE` X_2`:=`$E_2\{Q\}$ [6 marks].

Let R be as above, then

$$B \ \wedge \ R \ = \ (B \wedge B \wedge Q[E_1/X_1]) \vee (B \wedge \neg B \wedge Q[E_2/X_2]) \ = \ B \wedge Q[E_1/X_1]$$

so

$$B \wedge R \;\Rightarrow\; B \wedge Q[E_1/X_1]$$

Similarly

$$\neg B \wedge R \;=\; (\neg B \wedge B \wedge Q[E_1/X_1]) \vee (\neg B \wedge \neg B \wedge Q[E_2/X_2]) \;=\; \neg B \wedge Q[E_2/X_2]$$

so

$$\neg B \wedge R \;\Rightarrow\; \neg B \wedge Q[E_2/X_2]$$

By the assignment axiom: $\{Q[E_1/X_1]\}X_1\texttt{:=}E_1\{Q\}$ and $\{Q[E_2/X_2]\}X_2\texttt{:=}E_2\{Q\}$.

Hence by precondition strengthening $\{B \wedge Q[E_1/X_1]\}X_1\texttt{:=}E_1\{Q\}$ and $\{\neg B \wedge Q[E_2/X_2]\}X_2\texttt{:=}E_2\{Q\}$.

Hence by precondition strengthening $\{B \wedge R\}X_1\texttt{:=}E_1\{Q\}$ and $\{\neg B \wedge R\}X_2\texttt{:=}E_2\{Q\}$ (using the implications derived above).

Hence by the conditional rule

$$\{R\}\texttt{IF}\ B\ \texttt{THEN}\ X_1\texttt{:=}E_1\ \texttt{ELSE}\ X_2\texttt{:=}E_2\{Q\}$$

If the verification conditions for $\{P\}C\{R\}$ are proved then $\vdash\ \{P\}C\{R\}$, hence by the sequencing rule and the result above

$$\vdash\ \{P\}C\texttt{;IF}\ B\ \texttt{THEN}\ X_1\texttt{:=}E_1\ \texttt{ELSE}\ X_2\texttt{:=}E_2\{Q\}$$

Thus a goal $\vdash\ \{P\}C\texttt{;IF}\ B\ \texttt{THEN}\ X_1\texttt{:=}E_1\ \texttt{ELSE}\ X_2\texttt{:=}E_2\{Q\}$ can be reduced to goal $\{P\}C\{R\}$.

It is hoped this question will measure the candidate's depth of understanding of the method of verification conditions. Only Part (a) is bookwork.