2002 Paper 8 Question 12

Specification and Verification I

(*a*) Outline the steps involved in proving a specification $\{P\}C\{Q\}$ using the method of verification conditions. [6 marks]

(*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]

(*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:=$E_2\{Q\}$. [8 marks]