7 Hoare Logic (MJCG)

(*a*) Consider Hoare triples of the form $\{\mathtt{T}\}\ V\mathtt{:=}E\ \{V = E\}$ where $\mathtt{T}$ is the atomic formula 'true' and V and E range over variables and expressions, respectively.

(*i*) Write down an instance of such a triple that cannot be proved using Hoare logic and explain why not. [2 marks]

(*ii*) Write down conditions on V and E such that $\{\mathtt{T}\}\ V\mathtt{:=}E\ \{V = E\}$ can be proved and give a proof of this assuming your conditions. [2 marks]

(*b*) Write down and explain the weakest liberal precondition $\mathtt{wlp}(V\mathtt{:=}E,\ Q)$ and strongest postcondition $\mathtt{sp}(V\mathtt{:=}E,\ P)$. Comment on the relationship of these to the Hoare triple $\{P\}\ V\mathtt{:=}E\ \{Q\}$. [4 marks]

(*c*) Explain briefly how both weakest preconditions and strongest postconditions are used in mechanised program verification. [4 marks]

(*d*) Write down the Hoare assignment axiom and the Floyd assignment axiom. Explain carefully why each is true. [4 marks]

(*e*) Show how the Floyd assignment axiom can be derived from the Hoare assignment axiom and the other standard rules of Hoare logic. [4 marks]