8 Hoare Logic and Model Checking (AM)

This question considers a language $\mathcal{L}$ which has integer variables V, arithmetic expressions E and boolean expressions B, along with commands C of the forms V:=E (assignment), $C;C'$ (sequencing), `IF` B `THEN` C `ELSE` C' (conditional) and `WHILE` B `DO` C (iteration).

(*a*) Explain the syntax of the Hoare-logic partial-correctness formula $\{P\}\ C\ \{Q\}$ and give a careful definition in English of when it is valid, that is, when $\models \{P\}\ C\ \{Q\}$. [2 marks]

(*b*) How does the definition of validity for the total-correctness formula $[P]\ C\ [Q]$ differ? [1 mark]

(*c*) Preconditions and postconditions in $\{P\}\ C\ \{Q\}$ often make use of logical or auxiliary variables v in addition to program variables V. Explain why this is useful illustrating your answer with a command C which satisfies $\{\mathbf{T}\}\ C\ \{\mathtt{R} = \mathtt{X} + \mathtt{Y}\}$ but not $\{\mathtt{X} = x \wedge \mathtt{Y} = y\}\ C\ \{\mathtt{R} = x + y\}$. [3 marks]

(*d*) Give the axioms and rules of an inference system $\vdash \{P\}\ C\ \{Q\}$ for Hoare logic. [4 marks]

(*e*) Are your rules sound? To what extent are they complete? [2 marks]

(*f*) Give a formal proof, using your inference system, of $\{\mathtt{X} = x \wedge \mathtt{Y} = 3\}$ `X:=X+1` $\{\mathtt{X} - 1 = x \wedge \mathtt{Y} < 10\}$. [2 marks]

(*g*) Consider the command C given by `WHILE X>0 DO (X:=X-1; Y:=Y+3)`, and let P be the precondition $\mathtt{X} = x \wedge \mathtt{Y} = y \wedge x \geq 0$. Give the strongest postcondition Q that you can establish. Give any invariant necessary to prove $\{P\}\ C\ \{Q\}$ for your Q. Explain briefly how the structure of the proof relates to the structure of C. [6 marks]