8 Hoare Logic and Model Checking (AM)

This question considers a language \( L \) 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), \( \text{IF } B \text{ THEN } C \text{ ELSE } C' \) (conditional) and \( \text{WHILE } B \text{ DO } C \) (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 \( \models \{ P \} C \{ Q \} \).

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

(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 \( \{ T \} C \{ R = X + Y \} \) but not \( \{ X = x \land Y = y \} C \{ R = x + y \} \).

(d) Give the axioms and rules of an inference system \( \vdash \{ P \} C \{ Q \} \) for Hoare logic.

(e) Are your rules sound? To what extent are they complete?

(f) Give a formal proof, using your inference system, of
\( \{ X = x \land Y = 3 \} X := X + 1 \{ X - 1 = x \land Y < 10 \} \).

(g) Consider the command \( C \) given by \( \text{WHILE } X > 0 \text{ DO } (X := X - 1; Y := Y + 3) \), and let \( P \) be the precondition \( X = x \land Y = y \land x \geq 0 \). 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 \( C \).