

7 Hoare Logic (MJCG)

In this question we consider a semantics of FOR-commands in which

FOR  $V := E_1$  UNTIL  $E_2$  DO  $C$

is defined to be equivalent to

$V := E_1$ ; WHILE  $V \leq E_2$  DO ( $C$ ;  $V := V + 1$ )

- (a) How does this semantics of FOR-commands differ from the one given in the lectures? [4 marks]
- (b) The following FOR-rule is similar to one proposed by John Wickerson:

$$\frac{\vdash P \Rightarrow R[E_1/V] \quad \vdash R \wedge V > E_2 \Rightarrow Q \quad \vdash \{R \wedge V \leq E_2\} C \{R[V+1/V]\}}{\vdash \{P\} \text{ FOR } V := E_1 \text{ UNTIL } E_2 \text{ DO } C \{Q\}}$$

Assuming the semantics of FOR-commands given above, derive this Wickerson-style FOR-rule from the standard axioms and rules of Hoare logic. [10 marks]

- (c) Is the FOR-axiom:

$$\vdash \{P \wedge E_2 < E_1\} \text{ FOR } V := E_1 \text{ UNTIL } E_2 \text{ DO } C \{P\}$$

sound with the semantics given above? Justify your answer either with a proof of this axiom, or with a counterexample. [6 marks]