2007 Paper 7 Question 6

Specification and Verification I

(a) Describe how the meaning of {`T`} `X := Y` {`X=Y`} differs from the meaning of {`Y=y`} `X := Y` {`X=y`}. [2 marks]

(b) Is the total correctness specification `[Y=0] X := X/Y [X=X]` true? Justify your answer. [2 marks]

(c) Give an expression E such that {`T`} `X :=` E {`X` $= E$} is not true. [2 marks]

(d) Explain how specifications containing VDM's hooked variables like $\overleftarrow{X}$ can be translated to specifications that do not use hooked variables. [2 marks]

(e) What is the relationship between the provability of verification conditions and the provability of the specification from which they were generated? [2 marks]

(f) Define the weakest liberal precondition `wlp(`C`,`Q`)` in higher-order logic. [2 marks]

(g) What is the relationship between $\{P\}\ C\ \{Q\}$ and `wlp(`C`,`Q`)`? [2 marks]

(h) Explain how $\forall x.\ P(x)$ is represented in terms of λ-abstraction and function application in higher-order logic. [2 marks]

(i) Show how to derive a proof rule for the one-arm conditional from the proof rule for the two-arm conditional and the definition of `IF` S `THEN` C as `IF` S `THEN` C `ELSE SKIP`. [4 marks]