SOLUTION NOTES

Specification and Verification I 2002 Paper 7 Question 1 (MJCG)

(a) Describe the difference between deep and shallow semantic embedding [4 marks].

A deep embedding of a language L in a logic requires that a type representing phrases of L be defined in the logic, and then the semantics of L is specified by defining a function (or relation etc.) inside the logic.

A shallow embedding of a language L in a logic consists of a method of translating phrases of L into terms of the logic, representing the phrases meaning. A shallow embedding does not require either the syntax of L or the semantic function to be encoded inside the logic.

The distinction between "deep' and "shallow" embeddings is quite subtle and is really a spectrum. I will only give the full 4 marks if there is evidence that the candidate really grasps the idea.

(b) Describe two advantages of using deep embedding [4 marks] and two disadvantages [4 marks].

Advantage of deep embedding: quantification over the set of phrases of the embedded language can be expressed, allowing (for example) properties like "every program is equivalent to a program in normal form", "every program not containing a `WHILE`-command terminates" to be formulated.

Advantage of deep embedding: the semantic function is an object than can be explicitly reasoned about, for example the equivalence of different semantics could be formulated (*e.g.* denotational = operational).

Disadvantage of deep embedding: more effort (i.e. cost) is needed to perform a deep embedding, since the encoding of the syntax and semantics inside the logic is required.

Disadvantage of deep embedding: the logic has to be expressive enough, thus it might not be possible to use a weak logic (e.g. first-order logic). As weaker logics generally support more powerful automatic theorem-proving tools, using a deep embedding might rule out access to these tools.

Any valid answers will be acepted; the ones above are obvious examples, but others are possible.

(*c*) Outline how partial and total correctness specifications can be translated into higher order logic [4 marks].

A partial correctness specification $\{P\}C\{Q\}$ can be translated to a formula of the form

$$\forall s\ s'.\ \mathsf{AssertionMeaning}\ P\ s\ \wedge\ \mathsf{CommandMeaning}\ C\ (s, s') \Rightarrow\ \mathsf{AssertionMeaning}\ Q\ s$$

where AssertionMeaning P is the logical predicate representing P and CommandMeaning C is the transition relation representing command C. In a deep embedding AssertionMeaning and CommandMeaning would be defined inside the logic, but in a shallow embedding they would be metalanguage functions yielding terms.

A total correctness specification $[P]C[Q]$ can be translated to a formula of the form

$$\forall s.\ \mathsf{AssertionMeaning}\ P\ s \Rightarrow\ \exists s'.\ \mathsf{CommandMeaning}\ C\ (s, s') \wedge \mathsf{AssertionMeaning}\ Q\ s$$

The candidate is not required to give exactly the formulae above, but should show, more or less formally, that he/she understands the general idea.

(*d*) Give one advantage [2 marks] and one disadvantage [2 marks] of regarding Hoare Logic as a theory in higher order logic.

Advantage: enables general theorem proving tools to be applied.

Disadvantage: requires semantics of commands and assertion language to be formalised.

There are other advantages and disadvantages. Good marks will be obtained for any sensible answers.