1995 Paper 9 Question 14

Semantics

The language IMP$'$ comprises integer and boolean expressions and commands, defined by

$$\begin{array}{rclcl} ie & \in & Iexp & ::= & \underline{n} \mid x \mid ie_1 \ \underline{iop}\ ie_2 \\ be & \in & Bexp & ::= & \underline{b} \mid ie_1 \ \underline{bop}\ ie_2 \\ C & \in & Com & ::= & \texttt{skip} \mid x := \ ie \mid (C_1; C_2) \mid \\ & & & & \texttt{if}\ be\ \texttt{then}\ C_1\ \texttt{else}\ C_2 \mid \texttt{repeat}\ C\ \texttt{until}\ be \end{array}$$

where $n \in \mathbb{Z}$, $b \in \{true, false\}$, $iop \in \{+, \times, -\}$, $bop \in \{<, =\}$ and $x \in Pvar$, a set of program variables.

(a) Give an annotated evaluation semantics for IMP$'$, expressing the usual behaviour of each command and expression form, which derives statements of the forms

$$ie, S \Rightarrow_I n; R \qquad be, S \Rightarrow_B b; R \qquad C, S \Rightarrow_C S'; R, W$$

for $S, S' \in States = (Pvar \to \mathbb{Z})$ and $R, W \subseteq Pvar$. $C, S \Rightarrow_C S'; R, W$ means 'in state S, command C executes to state S' whilst reading the set of variables R and writing the set of variables W'. Similarly, if $e \in Iexp \cup Bexp$ then $e, S \Rightarrow v; R$ means 'in state S, e reads variables R in evaluating to v'.

[5 marks]

(b) For $be \in Bexp$, $ie \in Iexp$, $C \in Com$ use induction on the structure of phrases to give simple definitions of sets

$$\mathcal{R}(ie), \mathcal{R}(be), \mathcal{PR}(C), \mathcal{PW}(C) \ \subseteq \ Pvar$$

where $\mathcal{R}(e)$ is the set of variables accessed by e, $\mathcal{PR}(C)$ is a set of variables possibly read during the execution of C and $\mathcal{PW}(C)$ is a set of variables possibly written to during the execution of C. Give an example to show that it is *not* in general true that

$$C, S \Rightarrow_C S'; R, W \quad \text{implies} \quad W = \mathcal{PW}(C).$$

[5 marks]

(c) Prove that for any C, S, S', R, W

$$C, S \Rightarrow_C S'; R, W \quad \text{implies} \quad (\forall x \in Pvar.\ x \notin W \Rightarrow S(x) = S'(x))$$

and that for any be, S, S', b, R

$$(\forall x \in \mathcal{R}(be). S(x) = S'(x)) \quad \text{implies} \quad (be, S \Rightarrow_B b; R \iff be, S' \Rightarrow_B b; R)$$

[5 marks]

(d) Prove that for any C_1, C_2, C_3 and be that if $\mathcal{R}(be) \cap \mathcal{PW}(C_1) = \emptyset$ then

$$(C_1; \texttt{if}\ be\ \texttt{then}\ C_2\ \texttt{else}\ C_3) \ \approx\ \texttt{if}\ be\ \texttt{then}\ (C_1; C_2)\ \texttt{else}\ (C_1; C_3)$$

You may assume without proof that if $C, S \Rightarrow_C S'; R, W$ then $W \subseteq \mathcal{PW}(C)$.

[5 marks]