p7a1
MJCG

Specification and Verification I 2001

SV1.1: Solution Notes

What is the difference between partial and total correctness. [4 marks]

> A partial correctness specification $\{P\}C\{Q\}$ requires that the postcondition Q hold *only if* the execution of the command C terminates when started in a state satisfying P.
>
> A total correctness specification $[P]C[Q]$ requires that the execution of the command C terminates when started in a state satisfying P, and also that the postcondition Q holds in the final state.

Why is the assignment axiom more problematical for total correctness than for partial correctness. [4 marks]

> An assignment X := E may not terminate if E contains errors (like division by zero) or non-terminating function calls. The assignment axiom for total correctness is only valid if assignments terminate, so this is a problematical assumption.

State the WHILE-rule for total correctness. [4 marks]

$$\frac{\vdash [P \wedge S \wedge (E = n)]\ C\ [P \wedge (E < n)], \qquad \vdash P \wedge S \Rightarrow E \geq 0}{\vdash [P]\ \texttt{WHILE}\ S\ \texttt{DO}\ C\ [P \wedge \neg S]}$$

where n is a ghost (or auxiliary) variable

What needs to be added to the method of verification conditions to make it work for total correctness. [4 marks]

> All WHILE-commands need to be annotated with variants, then the verification conditions need to be adjusted so that they are based on the rule for total correctness.

Explain how a total correctness specification $[P]C[Q]$ can be embedded as a term TotalSpec $p\ c\ q$ in higher order logic. [4 marks]

> $[P]C[Q]$ embeds as TotalSpec $[\![P]\!]\ [\![C]\!]\ [\![Q]\!]$, where $[\![P]\!]$, $[\![C]\!]$ and $[\![Q]\!]$ are the translations of P, C and Q to predicates, respectively, and TotalSpec is defined by
>
> $$\mathsf{TotalSpec}\ p\ c\ q\ ==\ \forall s.\ p\ s\ \Rightarrow\ \exists s'.\ c(s, s')\ \wedge\ q\ s'$$