Specification and Verification I 2004 – Paper 8 Question 13 (MJCG)

(a) The specification needs to say that in the state where the program, `SORT` say, terminates, the values of $A(0), A(1), \ldots, A(N)$ are a permutation of the values of $A(0), A(1), \ldots, A(N)$ had in the initial state, and are also in ascending order. This can be expressed by

$$\{A = a \ \wedge \ N = n\} \ \texttt{SORT} \ \{\mathsf{Sorted}(A, n) \ \wedge \ \mathsf{Perm}(A, a, n)\}$$

where A and n are auxiliary (ghost) variables, and $\mathsf{Sorted}(A, n)$ means $A(0) \leq A(1) \leq \ \cdots \ \leq A(n)$ and $\mathsf{Perm}(A, a, n)$ means $(A(0), \ldots, A(n))$ is a permutation of $(a(0), \ldots, a(n))$.

(b) VDM notation eliminates the needs for auxiliary variables using 'hooked variables'.
The hooked variable $\overleftarrow{X}$ denotes in a postcondition the value of the unhooked variable X in the precondition state. Thus in VDM notation `SORT` can be specified by:

$$\{T\} \ \texttt{SORT} \ \{\mathsf{Sorted}(A, \overleftarrow{N}) \ \wedge \ \mathsf{Perm}(A, \overleftarrow{A}, \overleftarrow{N})\}$$

VDM notation specifies total correctness, so the above VDM does not correspond the the specification given in (a), but to the total correctness specification:

$$[A = a \ \wedge \ N = n] \ \texttt{SORT} \ [\mathsf{Sorted}(A, n) \ \wedge \ \mathsf{Perm}(A, a, n)]$$

(c) The weakest precondition $\mathsf{Wp}(C, Q)$ denotes the weakest condition such that starting in any state satisfying the condition, the command C terminates in a state satisfying Q. For partial correctness Dijkstra defined the weakest liberal precondition $\mathsf{Wlp}(C, Q)$, which denotes the weakest condition such that starting in any state satisfying the condition, if the command C terminates, then it does so in a state satisfying Q. A Floyd-Hoare partial correctness specification $\{P\}C\{Q\}$ can be expressed as $P \Rightarrow \mathsf{Wlp}(C, Q)$, and a total correctness specification $[P]C[Q]$ as $P \Rightarrow \mathsf{Wp}(C, Q)$.

Part (a) of the question refers to the material covered in the lecture "Devising correct rules", which covers arrays. Parts (b) and (c) refer to material at the end of the course on alternative specification methods to Floyd-Hoare logic.

When marking (a) I'll give 6 marks for evidence that the candidate grasps the general idea (need for auxiliary variables, etc) and another 2 marks for good explanations and presentation.

When marking (b) and (b) I'll give 4 marks for evidence that the candidate grasps the general ideas (hooked variables for VDM, predicate transformers for weakest preconditions) and another 2 marks for good explanations and presentation.