2010 Paper 8 Question 12

Specification and Verification I

Consider the following formal specification of a program that is intended to reverse an array `A` from `A`[0] up to `A`[`N`].

```
{0 ≤ N ∧ ∀i.  0 ≤ i ∧ i < N ⇒ A[i] = a[i]}
 I:=0; J:=N;
 WHILE I<J DO
  BEGIN
   VAR TEMP;
   TEMP:=A[I]; A[I]:=A[J]; A[J]:=TEMP;
   I:=I+1; J:=J-1
  END
{∀i. 0 ≤ i ∧ i < N ⇒ A[i] = a[N-i]}
```

(*a*) What is the purpose of the array variable `a` occurring in the precondition and postcondition? [2 marks]

(*b*) How does the program work? Explain your answer in English, using diagrams or example runs to make your description as clear as possible (marks will be given for clarity). [6 marks]

(*c*) Write down and carefully explain an invariant for the `WHILE`-loop that could be used to verify that the program meets its specification (marks will be given for clarity). [8 marks]

(*d*) Does the program always terminate? Justify your answer. [4 marks]