2003 Paper 7 Question 6

Specification and Verification I

(*a*) Explain the difference between a *variant* and an *invariant*. Briefly describe what they are used for. [4 marks]

(*b*) State and justify the verification conditions for the total correctness of `WHILE` commands. [6 marks]

(*c*) (*i*) Devise a precondition P that makes the following specification true.

```
[P]
WHILE I≤N DO SUM := SUM+(2×I); I := I+1
[SUM = N×(N+1)]
```

[2 marks]

(*ii*) Devise and justify annotations for this specification that yield provable verification conditions. [8 marks]