

OLLSCOIL NA hÉIREANN, GAILLIMH
NATIONAL UNIVERSITY OF IRELAND, GALWAY

SEMESTER I
WINTER EXAMINATIONS 2002/2003

Third University Examination in Information Technology

FORMAL METHODS (CT306)

Professor P. Nixon;
Professor G. Lyons;
Dr S. Flynn.

Time allowed: **Two hours.**

Candidates should attempt three questions.
All questions carry equal marks.

1. (a) What strategy would you use to prove a formula of the form: (4)

$$\vdash \{Q\} C_1; \text{ WHILE } S \text{ DO } C \{R\}$$

- (b) Use this strategy to outline a proof of the Floyd-Hoare formula:

```

 $\vdash \{X = n \wedge n \geq 0\}$ 
 $Y := 0 ;$ 
 $\text{WHILE } X > 0 \text{ DO}$ 
   $\text{BEGIN } X := X - 1 ; Y := Y + 3 \text{ END}$ 
 $\{Y = 3 \times n\}$ 

```

State clearly your invariant. (12)

- (c) In (b), what if the precondition is simply $\{X = n\}$? Would partial correctness still hold? Why? (4)

2. (a) You are given the following facts about \max

$$\vdash x \geq y \Rightarrow (\max(x, y) = x)$$

$$\vdash x < y \Rightarrow (\max(x, y) = y)$$

Now, given the specification:

$$\{True\} C \{Y = \max(X, Y)\}$$

prove that the following programs satisfy the specification. (10)

(i) IF $X \geq Y$ THEN $Y := X$

(ii) IF $X \geq Y$ THEN $X := Y$

(iii) $Y := X$

(iv) $X := 0 ; Y := 0$

- (b) In (a), the intended specification was probably not properly captured by

$$\{True\} C \{Y = \max(X, Y)\}$$

Rewrite the specification to say that, in the final state, Y holds the maximum of the original values of X and Y . Demonstrate that only program (i) satisfies this new specification. (10)

3. (a) A naive generalisation of the assignment axiom for arrays would look like:

$$\vdash \{P[E_2/A[E_1]]\} A[E_1] := E_2 \{P\}$$

Explain, using examples, why this rule does not work. (4)

- (b) Using the correct array assignment axiom, prove the following partial correctness formula: (6)

$$\begin{aligned} &\vdash \{(\forall i. N \leq i \leq n \Rightarrow A[i] = i) \wedge N > 0\} \\ &\quad N := N - 1 ; A[N] := N \\ &\quad \{(\forall i. N \leq i \leq n \Rightarrow A[i] = i)\} \end{aligned}$$

- (c) Prove the following formula of Floyd-Hoare logic:

$$\begin{aligned} &\vdash \{N = n\} \\ &\quad A[N] := N ; \\ &\quad \text{WHILE } N > 0 \text{ DO} \\ &\quad \quad \text{BEGIN } N := N - 1 ; A[N] := N \text{ END} \\ &\quad \{(\forall i. 0 \leq i \leq n \Rightarrow A[i] = i)\} \end{aligned}$$

State clearly your invariant. Note that your answer to part (b) will help you. (10)

4. (a) Distinguish between total correctness and partial correctness, giving the notation for each. Use examples to illustrate your answer. (4)
- (b) The WHILE-rule for total correctness is given by:

$$\frac{\vdash P \wedge S \Rightarrow 0 \leq E \quad \vdash [P \wedge S \wedge E = n] C [P \wedge E < n]}{\vdash [P] \text{ WHILE } S \text{ DO } C [P \wedge \neg S]}$$

Explain the role being played by E in this formula. (4)

- (c) Outline a proof of the following formula using the rules of Floyd-Hoare logic for total correctness:

```

 $\vdash [N = i + M \wedge M \leq K]$ 
  WHILE  $M \neq K$  DO
    BEGIN  $N := N + 1$  ;  $M := M + 1$  END
   $[N = i + K]$ 

```

Hint : use $(N = i + M \wedge M \leq K)$ as loop invariant, and $(K - M)$ as the variant. (12)

5. Based on your research into Formal Methods this semester, discuss the following topic:

The importance of Formal Methods in the undergraduate Computing curriculum.

Marks will be awarded for well-informed arguments. State clearly any references you make. (20)

Supplementary Material – Axioms and Inference Rules

Assignment Axiom $\vdash \{P[E/I]\} I := E \{P\}$

Array Assignment Axiom $\vdash \{P[A\{E_1 \leftarrow E_2\}/A]\} A[E_1] := E_2 \{P\}$

Precondition Strengthening $\frac{\vdash P \Rightarrow Q \quad \vdash \{Q\} C \{R\}}{\vdash \{P\} C \{R\}}$

Postcondition Weakening $\frac{\vdash \{P\} C \{Q\} \quad \vdash Q \Rightarrow R}{\vdash \{P\} C \{R\}}$

Sequencing $\frac{\vdash \{P\} C_1 \{Q\} \quad \vdash \{Q\} C_2 \{R\}}{\vdash \{P\} C_1; C_2 \{R\}}$

Blocks $\frac{\vdash \{P\} C \{Q\}}{\vdash \{P\} \text{ BEGIN } VAR I_1; \dots VAR I_n; C \text{ END} \{Q\}}$

Two-Armed Conditional $\frac{\vdash \{P \wedge S\} C_1 \{Q\} \quad \vdash \{P \wedge \neg S\} C_2 \{Q\}}{\vdash \{P\} \text{ IF } S \text{ THEN } C_1 \text{ ELSE } C_2 \{Q\}}$

One-Armed Conditional $\frac{\vdash \{P \wedge S\} C \{Q\} \quad \vdash (P \wedge \neg S) \Rightarrow Q}{\vdash \{P\} \text{ IF } S \text{ THEN } C \{Q\}}$

While $\frac{\vdash \{P \wedge S\} C \{P\}}{\vdash \{P\} \text{ WHILE } S \text{ DO } C \{P \wedge \neg S\}}$

Specification Conjunction $\frac{\vdash \{P_1\} C \{Q_1\} \quad \vdash \{P_2\} C \{Q_2\}}{\vdash \{P_1 \wedge P_2\} C \{Q_1 \wedge Q_2\}}$

Specification Disjunction $\frac{\vdash \{P_1\} C \{Q_1\} \quad \vdash \{P_2\} C \{Q_2\}}{\vdash \{P_1 \vee P_2\} C \{Q_1 \vee Q_2\}}$