Ollscoil na hÉireann, Gaillimh
National University of Ireland, Galway *GX* _____

Semester I
Winter Examinations 2006/2007

Exam Code(s)	3IF1
Exam(s)	IF1 B.Sc. (Information Technology)
Module Code(s)	CT306
Module(s)	Formal Methods
Paper No.	1
Repeat Paper	_____ Special Paper _____
External Examiner(s)	Professor J. Keane
Internal Examiner(s)	Professor. G. Lyons
	Dr. M. Mc Gettrick
Instructions	Answer 3 questions. All questions will be marked equally.
Duration	2hrs
No. of Answer Books	1
Requirements	
Handout	
MCQ	
Statistical Tables	
Graph Paper	
Log Graph Paper	
Other Material	
No. of Pages	
Department(s)	

1. (a) Let α represent the statement "the program starts in a state satisfying the precondition", β represent the statement "the program terminates" and γ "the final program state satisfies the postcondition". Using α, β, and γ and the standard connectives in logic ($\wedge, \vee, \rightarrow$, etc.) write (in the simplest form possible - i.e. using the fewest number of connectives) the following Floyd Hoare Triples:

   (i) $\vdash [\mathtt{T}]C[\mathtt{T}]$
   (ii) $\vdash \{\mathtt{T}\}C\{\mathtt{F}\}$
   (iii) $\vdash \{P\}C\{\mathtt{T}\}$
   (iv) $\vdash [P]C[\mathtt{F}]$
   (v) $\vdash [\mathtt{T}]C[Q]$

   (note here that T stands for TRUE and F stands for FALSE). (15 marks)

   (b) Explain the distinction between

   (i) Specification and Implementation
   (ii) An Axiom and an Inference Rule
   (iii) An Axiom and a Theorem

   (9 marks)

   (c) If $\vdash \{P\}\, C_1\, \{Q\}$ and $\vdash \{Q\}\, C_2\, \{P\}$, write down a simplified version of the program $C_1; C_2$. Can you simplify the program $C_2; C_1$? (6 marks)

2. (a) Prove the derived inference rules

   (i)
   $$\frac{\vdash \{P\}\, C\, \{Q_1\} \quad \vdash \{P\}\, C\, \{Q_2\}}{\vdash \{P\}\, C\, \{Q_1 \leftrightarrow Q_2\}}$$

   (ii)
   $$\frac{\vdash \{P_1\}\, C\, \{Q_1\} \quad \vdash \{P_2\}\, C\, \{Q_2\}}{\vdash \{P_1 \wedge P_2\}\, C\, \{\neg Q_1 \rightarrow Q_2\}}$$

   (15 marks)

   (b) In each of the following state which (if any) condition is stronger.

   (i) $y(x-1) = 0; \quad x = 0$
   (ii) $x > 2; \quad 1 < x$
   (iii) $x = 6; \quad x \neq 5$
   (iv) $P(4) = 6; \quad (\forall_y)P(y) = 6$
   (v) $(x > 1) \wedge (y > 1); \quad (x > 2) \vee (y > 2)$

   (15 marks)

3. (a) Prove the following formulas of Floyd Hoare logic:

(i) $\vdash \{X \leq Y\}$ `WHILE X < Y DO X := X + 1` $\{X = Y\}$

(ii) $\vdash [X = 0]$ `WHILE X > 0 DO X := X + 1` $[X = 0]$

(iii) $\vdash [TRUE]$ `WHILE X > 0 DO X := X - 1` $[TRUE]$

(18 marks)

(b) Calculate the results of carrying out the following substitutions:

(i) $(X^3 - 3 * X)[Y - 1/X]$

(ii) $(X + Y - Z)[Y, X, Y/X, Y, Z]$

(iii) $(X + Y - Z)[Y/X][X/Y][Y/Z]$

(iv) $(Z \leq Y)[X + Y, Y/Z, X][X + Z, Y/Y, X]$

(12 marks)

4. (a) Prove:

$\vdash \{(A[x] = m) \wedge (A[y] = n)\}$

```
BEGIN VAR T;
  T:=A[x];
  A[x]:=A[y];
  A[y]:=T;
END
```

$\{(A[x] = n) \wedge (A[y] = m)\}$

Is this program also totally correct? If so, state why this should be the case. (14 marks)

(b) Prove:

$\vdash$ $[Y > 0]$

```
R := X ; Q := 0 ;
WHILE Y ≤ R DO
    BEGIN R := R - Y ; Q := Q + 1 END
```

$[X = Y \times Q + R \wedge R < Y]$

(N.B.: this is a **total** correctness specification). (16 marks)

5. (a) Use the loop invariant $(Y = X!) \wedge (X \leq N)$ to prove

$\vdash$ $\{X = 0 \wedge Y = 1\}$

```
WHILE X < N DO
    BEGIN X := X + 1 ; Y := Y * X END
```

$\{Y = N!\}$.

Explain how weakening the loop guard `X < N` to `X` $\neq$ `N` would affect your choice of loop invariant. (15 marks)

(b) Using Weakest Precondition Semantics, determine

$$WP(\mathtt{y} := 5; \mathtt{x} := \mathtt{x} - 1; \mathtt{x} := -\mathtt{x} * \mathtt{y}, x > 10).$$

(9 marks)

(c) In Program Refinement suppose $\#[P, Q] = 5$ and $\#[Q, R] = 7$. Determine

$$\#\{C \mid \vdash [P]C[R]\}.$$

(6 marks)

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 $\dfrac{\vdash P \Rightarrow Q \quad \vdash \{Q\}\, C\, \{R\}}{\vdash \{P\}\, C\, \{R\}}$

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

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

Blocks $\dfrac{\vdash \{P\}\, C\, \{Q\}}{\vdash \{P\}\, BEGIN\, VAR\, I_1; \ldots VAR\, I_n;\, C\, END\{Q\}}$

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

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

While $\dfrac{\vdash \{P \wedge S\}\, C\, \{P\}}{\vdash \{P\}\, WHILE\, S\, DO\, C\, \{P \wedge \neg S\}}$

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

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