Ollscoil na hÉireann, Gaillimh
National University of Ireland, Galway

GX _____

Semester I
Winter Examinations 2005/2006

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)	Dr. M. Madden
	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) Explain what is meant by the derived inference rule

$$\frac{\vdash \{P\}\ C\ \{Q\} \quad \vdash [P]\ C\ [\mathtt{T}]}{\vdash [P]\ C\ [Q]}.$$

Does the converse hold?

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

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

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

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

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

(c) For all variables in the following expressions, state whether they are free or bound:

(i) $(\forall x.(\exists y.P(x) \Rightarrow Q(y)) \wedge \neg R(z, x))$

(ii) $P(x, y) \vee (\exists z.Q(x)) \Rightarrow R(z)$

(iii) $\forall x.((y \geq 1) \wedge (x \geq y)) \wedge \forall z.(\neg(z = 1))$

2. (a) Prove:

$\vdash \quad \{A[X] = x \wedge A[Y] = y \wedge X \neq Y\}$
```
A[X] := A[X]+A[Y];
A[Y] := A[X]-A[Y];
A[X] := A[X]-A[Y]
```
$\{A[X] = y \wedge A[Y] = x\}$

(b) Explain the distinction between

(i) Specification and Implementation

(ii) Partial and Total Correctness

(iii) Axiom and Theorem

(c) Explain the meaning of the notation $wp(C, Q)$ used in Weakest Precondition Semantics, with Code C and Postcondition Q.

3. (a) Explain the meaning of the following Floyd Hoare specifications (here, `T` stands for `TRUE` and `F` stands for `FALSE`):

(i) $\vdash$ [T]C[T]

(ii) $\vdash$ {T}C{T}

(iii) $\vdash$ $\{P\}C\{\mathtt{T}\}$

(iv) $\vdash$ [F]$C[Q]$

(v) $\vdash$ [T]C[F]

Only one of these specifications actually requires further details (on precondition P, code C, postcondition Q) to verify its correctness. State which specification this is, and state whether the other four specifications are correct or not.

(b) Prove the following formulas of Floyd Hoare logic:

(i) $\{(2 \times X) > 2\}\mathtt{X} := \mathtt{X} - 1;\ \ \mathtt{X} := \mathtt{X} + \mathtt{X}\{X \geq 0\}$

(ii) $\{True\}\mathtt{A} := \mathtt{Y};\ \ \mathtt{Z} := 1\{Z = X^{Y-A}\}$

(iii) $\{Y = n \wedge X = m\}$
```
X := X + Y;  Y := X - Y;  X := X - Y
```
$\{X = n \wedge Y = m\}$

4. (a) Prove:

$\vdash$ $\{X = n \wedge X \geq 0\}$

```
Y := 1 ;
WHILE X > 0 DO
    BEGIN Y := Y * X ; X := X - 1 END
```

$\{Y = n!\}$

given that $\vdash 0! = 1$ and $\vdash \forall n.n \geq 1 \Rightarrow n! = n \times (n-1)!$.

(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).

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

(i) $x(x-1) = 0; \quad x = 0$

(ii) $x > 2 - y; \quad y - 1 > -x$

(iii) $x = 6; \quad x \neq 6$

(iv) $P(4) = 6; \quad (\exists_y)P(y) = 6$

(b) Using Weakest Precondition Semantics, determine $WP($`x:=x-1;x:=x*x` $, x = 9)$.

(c) In Program Refinement we define $[P, Q] = \{C| \vdash [P]C[Q]\}$.

(i) Prove that $[P, Q] \supseteq [R, Q]$ provided $\vdash P \Rightarrow R$.

(ii) If $[P, Q] = C_1C_2C_3$ and $\#(C_i) = i + 2$, how many distinct refinements are there?

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