Ollscoil na hÉireann, Gaillimh
National University of Ireland, Galway

GX _____

Semester I
Winter Examinations 2007/2008

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) Write each of the following statements using either the Floyd Hoare triple $\vdash [P]C[Q]$ or $\vdash \{P\}C\{Q\}$ and the logical constants `T` for true and `F` for false:

   (i) "If the precondition holds, the code will terminate"

   (ii) "If the code terminates, the postcondition will hold"

   (iii) "If the precondition holds, the postcondition will hold"

   (iv) "The code will terminate"

   (v) "The code will terminate and the postcondition will hold"

   (as an example, "The code will not terminate" is $\vdash \{\texttt{T}\}C\{\texttt{F}\}$). (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) Suppose we have proven $\vdash \{P\}C_1\{Q\}$, $\vdash [Q]C_2[R]$ and $\vdash [R]C_3[S]$. From these, which of the following can we conclude is true?

   (i) $\vdash \{P\}C_1; C_2\{R\}$

   (ii) $\vdash [P]C_1; C_2[R]$

   (iii) $\vdash \{P\}C_1; C_2; C_3\{S\}$

   (iv) $\vdash \{Q\}C_2; C_3\{S\}$

   (v) $\vdash \{S\}C_3; C_2; C_1\{P\}$

   (vi) $\vdash \{R\}C_3\{S\}$

   (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 either) of the two conditions is weaker.

   (i) $xy > 0$; $(x > 0) \wedge (y > 0)$

   (ii) $x > 2$; $x \neq 2$

   (iii) $A \wedge (B \vee C)$; $C \vee (A \wedge B)$

   (iv) $x < 6$; $x \neq 5$

   (v) $(\forall_x)P(x) = 7$; $(\exists_y)P(y) > 6$

   (15 marks)

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

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

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

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

   (18 marks)

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

   (12 marks)

4. (a) 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) $(Z \leq Y)[X + Z/Z][X + Z, Y/Y, X]$

   (12 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). (18 marks)

5. (a) Prove:

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

   (15 marks)

   (b) Using Weakest Precondition Semantics, determine

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

   (9 marks)

   (c) In Program Refinement suppose $\#[P, Q_1] = 5$, $\#[Q_1, R] = 6$, $\#[P, Q_2] = 7$, and $\#[Q_2, R] = 8$. Determine a lower bound for

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

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