INSTITUTE OF TECHNOLOGY
BLANCHARDSTOWN

BACHELOR OF SCIENCE (HONOURS) IN COMPUTING BN402

Derivation of Algorithms

COMP H4018

Stage 4
Semester 2

Internal Examiner(s): Mr. Stephen Sheridan

External Examiner(s): Mr. John Dunnion
Dr. Richard Studdert

DATE: May 2007
TIME: TBA

Instructions to candidates:

1) ANSWER ANY FOUR QUESTIONS
2) ALL QUESTIONS CARRY EQUAL MARKS

DO NOT TURN OVER THIS PAGE UNTIL YOU ARE TOLD TO DO SO

(ANSWER ANY FOUR QUESTIONS)

Question 1

a) Prove that the following code fragment contains an infinite loop.

```
|[ con N : int; {N > 0}
   var x: int;
   x := N;
   do  x > 0 →
        S
        x := x + 1
   od
]|
```

(5 marks)

b) Write down an invariant **P** for the following loop and prove that the body of the loop is correct. Your answer must also show program termination.

```
|[ con N : int; {N ≥ 0}
   var n, x : int;
   n, x := 0, 1;
   do  n < N →
        { P ∧ n < N }
        x, n := 4 * x, n + 1;
        { P }
   od
   { x = 4^N }
]|
```

(10 marks)

c) Write down an invariant and a complete solution to the given specification.

```
|[ con N : int; { N ≥ 0 }
   var t : int;
    S
   { t = #j: 0 ≤ j < N : j mod 2 ≠ 0}
]|
```

Note: It is not necessary to prove your solution correct.

(10 marks)
(Total 25 marks)

Question 2

Write down the invariants **P0** and **P1** which describe the program below and hence derive the program's formal proof. An annotated program should be included in your answer.

```
|[ con
     N : int; { N  ≥ 0 }
     f : array[0..N) of boolean;
  var
      h : int;
      k : int;
      h,k := 0, 0;
      do  k < N   →
        if f.k  →
                 h := h + 1
        []  ¬f.k →
                 skip
        fi;
        k := k + 1;
     od
  { h = #j : 0 ≤ j < N : f.j }
]|
```

(25 marks)

Question 3

Formally derive a solution to the given specification. Your answer should include a complete solution.

```
|[ con
     N : int; { N ≥ 0 }
     f : array[0 .. N ) of char;
  var
     k : int;
     S
     { k =  #j : 0 ≤ j < N : f.j ≥ 'a' ∧ f.j ≤ 'z'}
 ]|
```

(25 marks)

Question 4

Write a specification and derive a solution for the following problem. Your answer must include a complete solution.

Given an integer array f [0..N), N ≥ 0, find the index of the smallest element in f.

(25 marks)

Question 5

a) Use an invariant diagram to derive an $O(N)$ solution to the following specification. Your answer should include a complete solution.

$$
\begin{array}{l}
|[\ \text{con } N, k : \text{int } \{ N \geq 0 \} ; \\
\quad \text{var } f : \text{array}[0..N) \text{ of int}; \\
\quad S \\
\quad \{ (\exists p,q : 0 \leq p \leq q \leq N : (\forall i : 0 \leq i < p : f.i < k) \wedge \\
\qquad\qquad\qquad\qquad\qquad\qquad (\forall i : p \leq i < q : f.i = k) \wedge \\
\qquad\qquad\qquad\qquad\qquad\qquad (\forall i : q \leq i < N : f.i > k))\} \\
]|
\end{array}
$$

Note: Only swap operations are allowed on f.

(25 marks)

APPENDIX

Laws of the Calculus

Let P, Q, R be propositions

1. Constants

   $P \vee true \equiv true$

   $P \vee false \equiv P$

   $P \wedge true \equiv P$

   $P \wedge false \equiv false$

   $true \Rightarrow P \equiv P$

   $false \Rightarrow P \equiv true$

   $P \Rightarrow ture \equiv true$

   $P \Rightarrow false \equiv \neg P$

2. Law of excluded middle : $P \vee \neg P \equiv true$
3. Law of contradiction: $P \wedge \neg P \equiv false$

4 Negation : $\neg\neg P \equiv P$

5. Associativity: $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$

   $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$

6. Commutativity: $P \vee Q \equiv Q \vee P$

   $P \wedge Q \equiv Q \wedge P$

7. Idempotency: $P \vee P \equiv P$

   $P \wedge P \equiv P$

8. De Morgan's laws : $\neg (P \wedge Q) \equiv \neg P \vee \neg Q$

   $\neg (P \vee Q) \equiv \neg P \wedge \neg Q$

9. Implication $P \Rightarrow Q \equiv \neg P \vee Q$

   $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$

   $(P \wedge Q) \Rightarrow R \equiv P \Rightarrow (Q \Rightarrow R)$

10. (If and only if) $\equiv$: $P \equiv Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$
11. Laws of distribution: $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$

    $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$

12. Absorption: $[P \wedge (P \vee R) \equiv P]$

    $[P \vee (P \wedge R) \equiv P]$

13. **Predicate Calculus**

Negation

$\forall x \neg P(x) \equiv \neg \exists x P(x)$

$\exists x \neg P(x) \equiv \neg \forall\ P(x)$

$\exists x P(x) \equiv \neg(\forall x \neg P(x))$

Universal Quantification

$[(\forall x : P(x)) \ \wedge\ (\forall x : Q(x)) \ \equiv\ (\forall x : P(x) \wedge\ Q(x))\ ]$

$[(\forall x: P(x)) \ \vee\ (\forall x : Q(x)) \Rightarrow (\forall x: P(x) \vee Q(x))\ ]$

$[Q \vee (\forall x : P(x)) \ \equiv\ (\forall x: Q \vee P(x))\ ]$, where x not free in Q

$[Q \wedge\ (\forall x: P(x)) \ \equiv\ (\forall x: Q \wedge\ P(x))\ ]$, where x not free in Q

Existential Quantification

$[(\exists x: P(x) \wedge Q(x)) \ \Rightarrow (\ \exists x : P(x)) \ \wedge\ (\ \exists x : Q(x))\ ]$

$[(\ \exists x : P(x)) \ \vee\ (\ \exists x: Q(x)) \ \equiv\ (\ \exists x: P(x) \vee Q(x))\ ]$

$[Q \vee (\ \exists x: P(x)) \ \equiv\ (\ \exists x : Q \vee P(x))\ ]$, where x not free in Q

$[Q \wedge\ (\ \exists x: P(x)) \ \equiv\ (\ \exists x : Q \wedge\ P(x))\ ]$, where x not free in Q

$[\ (\exists x : P(x)) \ \equiv \neg(\forall x: \neg P(x))]$

$[\ (\neg \exists x : P(x)) \ \equiv (\forall x: \neg P(x))]$

14. **Universal Quantification over Ranges**

$[\forall i : R : P \ \equiv \forall i : \neg R \vee P\ ]$ Trading

$[\forall i : false : P \ \equiv true\ ]$

$[\forall i : i = x : P \ \equiv\ P(\ i\ :=\ x)\ ]$ One-point rule

$[(\forall i : R : P) \ \wedge\ (\forall i : R : Q) \ \equiv\ (\forall i : R : P \wedge\ Q)\ ]$

$[(\forall i : R : P) \ \wedge\ (\forall i : S : P) \ \equiv\ \ (\forall i : R \vee S : P)\ ]$

$[(\forall i : R : P) \ \vee\ (\forall i : R : Q) \Rightarrow (\forall i : R : P \vee Q)\ ]$

$[Q \vee (\forall i : R : P) \ \equiv\ (\forall i : R : Q \vee P)\ ]$

$[Q \wedge\ (\forall i : R : P) \ \equiv\ (\forall i : R : Q \wedge\ P)\ ]$

15. **Existential Quantification over Ranges**

$[\ \exists i : R : P \ \equiv\ \exists i : R \wedge P\ ]$ Trading

$[\ \exists i : false : P \ \equiv false]$

$[\ \exists i : i = x : P \ \equiv\ P(i := x)\ ]$ One-point rule

$[(\exists i : R : P \wedge Q) \Rightarrow (\exists i : R : P) \wedge (\exists i : R : Q)\ ]$

$[(\exists i : R : P) \vee (\exists i : R : Q) \equiv (\exists i : R : P \vee Q)\ ]$

$[Q \vee (\exists i : R : P) \equiv (\exists i : R : Q \vee P)\ ]$

$[Q \wedge (\exists i : R : P) \equiv (\exists i : R : Q \wedge P)\ ]$