Question 1

Write a specification and derive a solution for the following problem.

Given an character array f [0..N), N ≥ 0, find the frequency of uppercase letters.

[25 marks]

Question 2

Write down the invariants **P0** and **P1** which describe the program below and hence derive the programs formal proof. An <u>annotated</u> program should be included in your answer.

```
|[ con
      N : int; { N ≥ 0 }
      f : array[0..N) of int;
   var
      n : int;
      t : int;
      n,t := 1, 0;
      do  n < N  →
         if f.t ≤ f.n →
               skip;
         [] f.t > f.n →
               t : = n;
         fi;
         n := n + 1;
      od
      { 0 ≤ t < N  ∧  ∀i : 0  ≤ i < N : f.t ≥ f.i }
]|
```

[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 int;
  var
    b : boolean;
    S
    { b ≡ ∃j : 0 ≤ j < N : f.j > 100}
$]\|$

[25 marks]

Question 4

Derive a solution for the following specification. Your answer must include a complete solution.

$\|[$ con N : int { N ≥ 0 } ;
    var f : array[0..N) of int;
      x: int;
    S
    { x = minj: 0 ≤ j < N : f.j }
$]\|$

[25 marks]

Question 5

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

$\|[$ con N : int { N ≥ 0 } ;
  var f : array[0..N) of char;
   S
  { (∃ k : 0 ≤ k ≤ N : (∀i : 0 ≤ i < k : f.i = 0) ∧
                       (∀i : k ≤ i < N : f.i = 1)}
$]\|$

  Note: Only swap operations are allowed on f.

[25 marks]

Laws of the Calculus

Let P, Q, R be propositions

1. Constants

    $P \lor true \equiv true$

    $P \lor false \equiv P$

    $P \land true \equiv P$

    $P \land false \equiv false$

    $true \Rightarrow P \equiv P$

    $false \Rightarrow P \equiv true$

    $P \Rightarrow ture \equiv true$

    $P \Rightarrow false \equiv \neg P$

2. Law of excluded middle : $P \lor \neg P \equiv true$

3. Law of contradiction: $P \land \neg P \equiv false$

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

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

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

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

    $P \land Q \equiv Q \land P$

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

    $P \land P \equiv P$

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

    $\neg (P \lor Q) \equiv \neg P \land \neg Q$

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

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

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

10. (If and only if) $\equiv$: $P \equiv Q \equiv (P \Rightarrow Q) \land (Q \Rightarrow P)$

11. Laws of distribution: $P \land (Q \lor R) \equiv (P \land Q) \lor (P \land R)$

    $P \lor (Q \land R) \equiv (P \lor Q) \land (P \lor R)$

12. Absorption: $[P \land (P \lor R) \equiv P]$

    $[P \lor (P \land R) \equiv P]$

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

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

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

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

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

Existential Quantification

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

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

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

$[Q \land (\exists x : P(x)) \equiv (\exists x : Q \land P(x))]$, 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**

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

$[\forall i : \text{false} : P \equiv \text{true}]$

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

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

$[(\forall i : R : P) \land (\forall i : S : P) \equiv (\forall i : R \lor S : P)]$

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

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

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

15. **Existential Quantification over Ranges**

$$[\exists i : R : P \equiv \exists i : R \wedge P] \quad \text{Trading}$$

$$[\exists i : \text{false} : P \equiv \text{false}]$$

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

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

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

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

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