GX1305

OLLSCOIL NA hÉIREANN
The National University of Ireland, Galway

SEMESTER II
SPRING EXAMINATIONS 1998/99

Third University Examination in Information Technology

FORMAL METHODS (CT306)

Professor D. Bell
Dr. G. Lyons
Dr. S. Flynn

Time Allowed : **Two Hours**

Answer any three questions
All questions carry equal marks

1. (a) What strategy would you use to prove a formula of the form:

$$\vdash [R] \textbf{ while } S \textbf{ do } C [Q]$$

Justify your strategy by referring to the while rule for total correctness. (8)

(b) Use the strategy postulated in (a) to prove the following: (12)

$\vdash [X = 2*i]$
while $(X \neq 0)$ **do**
if $(X > 0)$ **then** $X := X - 2$
else $X := X + 2$
$[X = 0]$

2. (a) Distinguish between total correctness and partial correctness, giving the notation for each. (6)

(b) Prove the following formula of Hoare logic: (12)

$\vdash \{X = n \wedge Y = m \wedge Y \geq 0\}$
$A := Y; Z := 1;$
while $(A > 0)$ **do**
begin $Z := X * Z; A := A - 1$ **end**
$\{X = n \wedge Y = m \wedge Z = exp(n,m)\}$

You may use the facts:
$\vdash exp(m,0) = 1$
$\vdash exp(m, n+1) = m * exp(m,n)$, if $n \geq 0$

(c) What would you use as the variant if you were asked to prove total correctness of the above? (2)

3. (a) Write a short note, giving examples, on the meaning of the notation wp(C,Q), where C is a program, and Q is a condition. (4)

(b) What general method would you use to derive a program PROG satisfying

[P] PROG [Q]

where P and Q are boolean conditions. (6)

(c) Illustrate the method you described in (b) to derive a program *Abs* that satisfies the following specification:

[X = i]
Abs
[X = **abs** i]

where the function **abs** is defined by:

(i) $\vdash (i < 0) \Rightarrow$ (**abs** i = -1 * i)
(ii) $\vdash (0 \leq i) \Rightarrow$ (**abs** i = i)

Your program may not use the **abs** function. (10)

4. (a) The **do-while** statement, which takes the form **do** C **while** S, where C is a program and S is a condition, can be described by the following behaviour:

(1) execute statements C
(2) if S evaluates to True, then goto (1)
(3) finish

Based on your knowledge of Hoare logic, propose an inference rule to prove partial correctness of **do-while** statements. (Hint : note that **do** C **while** S can be equivalently written as C; **while** S **do** C.) (8)

(b) Using the rule you postulated in (a), prove the following formula of Hoare logic: (12)

$\vdash \{X = n \wedge Y = 0 \wedge n > 0\}$
do begin X := X - 1; Y := Y + 1 **end**
while $(X \neq 0)$
$\{Y = n\}$

5. (a) The assignment axiom is given as follows:

$$\vdash \{P[A\{E1 \leftarrow E2\}/A]\}\ A[E1] := E2\ \{P\}$$

Explain what is meant by the notation $A\{E1 \leftarrow E2\}$, giving examples. (4)

(b) Prove the following formula of Hoare logic: (8)

$$\vdash \{(\forall i.(0 \le i \le N) \Rightarrow A[i]=a[i]) \wedge (\forall i.(N<i \le n) \Rightarrow A[i]=2*a[i]) \wedge N \ge 0\}$$
$$A[N] := 2*A[N]\ ;\ N := N-1$$
$$\{(\forall i.(0 \le i \le N) \Rightarrow A[i]=a[i]) \wedge (\forall i.(N<i \le n) \Rightarrow A[i]=2*a[i])\}$$

(c) Prove the following formula of Hoare logic: (8)

$$\vdash \{N=n \wedge A=a\}$$
while $(N \ge 0)$ **do**
begin $A[N] := 2*A[N]\ ;\ N := N-1$ **end**
$$\{\forall i.(0 \le i \le n) \Rightarrow A[i]=2*a[i]\}$$

Note that your answer to part (b) will help you.