IMPERIAL COLLEGE LONDON

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
EXAMINATIONS 2009

EEE PART III/IV: MEng, BEng and ACGI

Corrected Copy

Q2 (b)

DISCRETE MATHEMATICS AND COMPUTATIONAL COMPLEXITY

Tuesday, 26 May 2:30 pm

Time allowed: 3:00 hours

There are FIVE questions on this paper.

Answer Question One (40 marks), Question Two (40 marks), and TWO of Questions Three to Five (30 marks each). Note that this paper is marked out of 140.

Any special instructions for invigilators and information for candidates are on page 1.

Examiners responsible First Marker(s) : G.A. Constantinides
Second Marker(s) : M.M. Draief

NOTATION

The following notation may be used throughout this paper:

$\mathbb{R}$: The set of real numbers.

$\mathbb{R}_+$: The set of positive real numbers.

$\mathbb{Z}$: The set of integers.

$\mathbb{Z}_+$: The set of positive integers.

$\mathbb{N}$: The set of natural numbers.

$\mathbb{Q}$: The set of rational numbers.

$\mathbb{Q}_+$: The set of positive rational numbers.

$\mathscr{P}(S)$: The power set of set S.

The Questions

1. **[Compulsory]**

a) Show that $|\mathbb{Z}_+| = |\mathbb{N}|$.

[2]

b) State whether each of the following relations are (i) reflexive, (ii) symmetric, (iii) transitive.

i) "is a sibling of" on the set of all people. (Note: sibling means brother or sister).

ii) "is the son of" on the set of all people.

iii) "is the same sex as" on the set of all people.

iv) "is greater than" on the set of all integers.

[8]

c) Which of the following functions are (i) injective, (ii) surjective? Prove your answer in each case.

i) $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defined by $f(x,y) = x + y$.

ii) $f : \mathbb{N} \to \mathbb{N}$ defined by $f(n) = n + 1$.

iii) $f : \mathscr{P}(X) \to X \cup \{0\}$ defined by $f(x) = |x|$, where $X = \{x | x \in \mathbb{Z}_+ \wedge x \leq 10\}$.

[8]

d) State the truth value of each of the following statements, first using $\mathbb{R}$ as the universe of discourse, and then using $\mathbb{Z}$ as the universe of discourse.

i) $\exists x \forall y (y + (-y) = x)$.

ii) $\forall x (x \leq 0 \vee x \geq 1)$.

iii) $\forall x \exists y (xy = 1)$.

[8]

e) Let $R(p,b)$ denote the predicate 'Person p has borrowed book b from the library'. Let $O(b)$ denote the predicate 'Book b is overdue'. Let the set of people be P and the set of books be B. Write the following sentences in predicate logic, using predicates $R(p,b)$ and $O(b)$.

i) Steven has borrowed a book.

ii) "Crime and Punishment" has been borrowed.

iii) No book has been borrowed by more than one person.

iv) If a book is overdue, then it must have been borrowed.

[6]

f) State the predicate logic definitions of '$f(x)$ is $O(g(x))$' and '$f(x)$ is $\Omega(g(x))$'. Use these definitions to show that x^2+1 is $\Theta(x^2)$ from first principles.

[8]

2. **[Compulsory]**

a) Two integers m and n are said to be *relatively prime* if they have no common factor except 1. Express that P(m,n) is the predicate "m and n are relatively prime", using a composite predicate logic formula. The universe of discourse should be the set $\mathbb{Z}_+$, and you may use a predicate $=$ and the multiplication operator over integers, both with the usual meaning.

[2]

Let F be the set of all functions from $\mathbb{Z}_+$ to $\mathbb{N}$. Let p_i be the ith prime number, so $p_1 = 2$, $p_2 = 3$, *etc.* Let $g : \mathbb{Z}_+ \rightarrow F$ be the function mapping a positive integer n into a function f such that $n = p_1^{f(1)} p_2^{f(2)} \dots$.

b) Find $g(1), g(2), g(3)$ and $g(4)$, and show that $\forall n \exists k \forall i((i > k) \rightarrow (g(n)\overset{(i)}{\cancel{(k)}} = 0))$, where the universe of discourse is $\mathbb{Z}_+$.

[6]

Define $h : \mathbb{Z}_+ \rightarrow \mathbb{Z}_+$ by $h(n) = p_1^{2g(n)(1)} p_2^{2g(n)(2)} \dots$.

c) Calculate $h(1), h(2), h(3)$ and $h(4)$.

[2]

d) Show that $\forall n(h(n) = n^2)$. Show further that h is an injection but not a bijection.

[4]

Let $q : \mathbb{N} \rightarrow \mathbb{N}$ be the function $q(0) = 0$ and $q(n) = 2n - 1$ for $n > 0$. Now define $v : A \rightarrow \mathbb{Z}_+$ by $v(n) = p_1^{q(g(n)(1))} p_2^{q(g(n)(2))} \dots$.

e) Calculate $v(1), v(2), v(3)$ and $v(4)$.

[4]

f) Show that v is an injection but not a bijection. *Hint: You may use the fact that q is an injection.*

[6]

Let $r: A \to \mathbb{Z}_+$ be defined by $r(m,n) = h(m)v(n)$, where $A \subseteq \mathbb{Z}_+ \times \mathbb{Z}_+$.

g) For $A = \mathbb{Z}_+ \times \mathbb{Z}_+$, show that r is not an injection, but it is a surjection.

[6]

h) For $A = \{(m,n) | m \in \mathbb{Z}_+ \wedge n \in \mathbb{Z}_+ \wedge P(m,n)\}$, show that r is a bijection.

[6]

Define $s: A \to \mathbb{Q}_+$ as the bijection $s(m,n) = m/n$, for the choice of A from part (h).

i) Explain why, since s is a bijection, it follows that $r \cdot s^{-1}$ is a bijection.

[2]

j) Note that $r \cdot s^{-1}$ is a function with domain $\mathbb{Q}_+$ and co-domain $\mathbb{Z}_+$. Hence comment on the countability of the positive rationals, justifying your comment with reference to your answers to this question.

[2]

3. Let $X = \{x | x \in \mathbb{Z}_+ \wedge x \leq 20\}$, and let Y be the set of non-empty character strings of length up to twenty characters. Define $f : X \to Y$ where $f(x)$ is the string representing the English word for x, *e.g.* $f(1) =$ "*one*".

Let $g : Y \to X$ be a function where $g(y)$ is the number of characters in the string y, *e.g.* $g(\text{"}one\text{"}) = 3$. Let R be a relation on the set X defined by $R = g \cdot f$.

a) State, with justification, whether:

i) f is injective,

ii) f is surjective,

iii) f^{-1} exists,

iv) g is injective,

v) g is surjective,

vi) g^{-1} exists.

[12]

b) Evaluate $f(X)$ and $g(Y)$.

[4]

c) i) Compute the elements of R.

ii) State, with justification, whether R is reflexive, R is symmetric, and R is transitive.

iii) Show that $\exists y \in X \exists k \in \mathbb{Z}_+ (R^k = \{(x,y) | x \in X\})$ is true.

[14]

4. Consider the function $f : \mathbb{R}^3 \rightarrow \mathbb{R}$ defined by $f(n,a,b) = a \cdot b^n$.

a) Show that $f(n, 10^3, 10^{-1}) \leq 1$ for all n greater than some value N.

[4]

b) Show further that for any positive ε, $f(n, 10^3, 10^{-1}) \leq \varepsilon$ for all n greater than some value N (which may depend on ε).

[5]

c) Express as a predicate $P(b)$ the English statement "for every positive real number a there is another real number N such that for all values of n greater than N, $f(n,a,b)$ can be bounded from above by as small a positive number as you wish" using predicate logic. You should use $\mathbb{R}$ as the universe of discourse.

[8]

d) Show that $P(0.5)$ is true.

[9]

e) The proposition $\forall b \in \mathbb{R}(b \in X \rightarrow P(b))$ is true for a variety of sets X. Find the largest set X for which this proposition is true, in the sense that if the proposition is also true for X', it follows that $X' \subseteq X$.

[4]

5. This question concerns two C/C++ methods to evaluate a polynomial $c[0]+c[1]x+c[2]x^2+\ldots+c[n]x^n$. Algorithm 1 is shown in Fig. 5.1, and Algorithm 2 is shown in Fig. 5.2. In both algorithms, the first argument is a pointer to an array of length $n+1$ of real coefficients, the second argument is the value of n, and the third argument is a real value of x.

a) Let p_i denote the value of p at entry to iteration i of the i loop in Algorithm 1.

i) What is p_1?

ii) Express p_{i+1} in terms of p_i as a first order homogeneous recurrence relation. Solve the recurrence relation, and hence find the value of p at the exit of the i loop in Algorithm 1 as a function of k and x.

[6]

b) Explain why Algorithm 2 correctly evaluates the polynomial at x.

[6]

c) Let $f(n)$ denote the number of multiplications executed by a call to **evalpoly1**(c,n,x).

i) Find a formula for $f(n)$ in terms of n only.

ii) Hence show that $f(n)$ is $\Omega(n^2)$.

[9]

d) Let $g(n)$ denote the number of multiplications executed by a call to **evalpoly2**(c,n,x).

i) Find a recurrence relation for $g(n)$.

ii) Hence find a suitable big-O expression for $g(n)$.

[6]

e) Contrast the efficiency of the two algorithms.

[3]

```
float evalpoly1( float *c, int n, float x ) {
  float f = 0.0;
  float p;
  int k,i;

  for(k = 0; k <= n; k++) {
    p = 1.0;
    for(i = 1; i <= k; i++) {
      p *= x;
    }
    f += c[k]*p;
  }
  return(f);
}
```

Figure 5.1 Algorithm 1.

```
float evalpoly2( float *c, int n, float x ) {
  if(n == 0)
    return(c[0]);
  else
    return(c[0] + x*evalpoly2(c+1, n-1, x));
}
```

Figure 5.2 Algorithm 2.

Discrete Maths + Computational Complexity

Answers 2009
E2.17 + 3.20
1/12

1. a) A suitable bijection is $f(x) = x - 1$, $f: \mathbb{Z}_+ \to \mathbb{N}$.

[2]

b) (i) symmetric, transitive (excluding half-siblings)
(ii) none
(iii) reflexive, symmetric & transitive
(iv) transitive

[8]

c) (i) Not injective, e.g. $f(0,1) = f(1,0)$ but $(1,0) \neq (0,1)$.
Surjective, e.g. $f(x, 0) = x$ for any $x \in \mathbb{R}$.

(ii) Injective: $f(n) = f(m)$
$\Rightarrow n+1 = m+1 \Rightarrow n = m$
Not surjective, as $0 \notin f(\mathbb{N})$.

(iii) Not injective, e.g. $f(\{1,2\}) = f(\{2,3\})$ but
$\{1,2\} \neq \{2,3\}$.
Surjective, as we may choose any $x \subseteq X$.
Since $|X| = 10$, $|x|$ may be any integer $0, 1, \ldots, 10$
$= X \cup \{0\}$.

[8]

d) (i) True in both cases ($x = 0$).
(ii) True for $\mathbb{Z}$ but not for $\mathbb{R}$ (e.g. $x = \frac{1}{2}$)
(iii) True for $\mathbb{R}$ but not for $\mathbb{Z}$ (e.g. $x = 2$).

[8]

1\. e) (i) $\exists b \in B \quad R(\text{Steven}, b)$

(ii) $\exists p \in P \quad R(p, \text{"Crime and Punishment"})$

(iii) $\forall b \in B \quad \forall p_1 \in P \ \forall p_2 \in P \ \left(R(p_1, b) \wedge R(p_2, b) \rightarrow p_1 = p_2 \right)$

(iv) $\forall b \in B \ \left(O(b) \rightarrow \exists p \in P \quad R(p, b) \right)$.

[6]

f) $f(x)$ is $O(g(x)) \equiv$

$$\exists c \in \mathbb{R}_+ \ \exists k \in \mathbb{R}_+ \ \forall x \left((x > k) \rightarrow \left(|f(x)| \leq c|g(x)| \right) \right)$$

$f(x)$ is $\Omega(g(x)) \equiv$

$$\exists c \in \mathbb{R}_+ \ \exists k \in \mathbb{R}_+ \ \forall x \left((x > k) \rightarrow \left(|f(x)| \geq c|g(x)| \right) \right)$$

Let $f(x) = x^2 + 1$

For $x > 1$, $f(x) \leq x^2 + x^2$

$= 2x^2$

So $f(x)$ is $O(x^2)$

For $x > 1$ (say),

$f(x) \geq x^2$

So $f(x)$ is $\Omega(x^2)$

$\therefore f(x)$ is $\Theta(x^2)$.

[8]

2. a) $\forall c\, \exists x\, \exists y \left(cx = m \wedge cy = n \rightarrow c = 1 \right)$

[2]

b) $g(1)(n) = 0$ for all n

$g(2)(1) = 1, \quad g(2)(n) = 0$ for $n > 1$

$g(3)(1) = 0, \quad g(3)(2) = 1, \quad g(3)(n) = 0$ for $n > 2$

$g(4)(1) = 2, \quad g(4)(n) = 0,$ for $n > 1$

Note that not every integer is prime, so $p_i < i$ always.

We may then take $k = n$, as if $g(n)(n) \geqslant 1$ then $n > n$ (contradiction).

[6]

c) $h(1) = 1$

$h(2) = 2^2 = 4$

$h(3) = 3^2 = 9$

$h(4) = 2^4 = 16$

[2]

d) $$h(n) = p_1^{2\, g(n)(1)}\, p_2^{2 g(n)(2)} \cdots$$
$$= \left[p_1^{g(n)(1)}\, p_2^{\cancel{2} g(n)(2)} \cdots \right]^2$$
$$= n^2.$$

$h(n) = h(m) \Rightarrow n^2 = m^2$

$\Rightarrow n = m$ (n & m are positive)

There is no n s.t. $n^2 = 2$ ($\pm\sqrt{2}$ not integer).

[4]

2 e) $q_p^V(1) = 1$

$q_p^V(2) = 2^{2-1} = 2$

$q_p^V(3) = 3^{2-1} = 3$

$q_p^V(4) = 2^{4-1} = 8$ [4]

f) $v(n) = v(m)$

$\Rightarrow p_1^{q(g(n)(1))} p_2^{q(g(n)(2))} \cdots = p_1^{q(g(m)(1))} p_2^{q(g(m)(2))} \cdots$

Since p_i is prime, this requires

$q(g(n)(1)) = q(g(m)(1))$

$\vdots$

i.e. $q(g(n)(i)) = q(g(m)(i))$ for all i.

q is an injection, so we need

$g(n)(i) = g(m)(i)$ for all i.

$\Rightarrow n = m$.

There is, however no n s.t. $v_{q_p}(n) = 4$, as this would require $q(g(n)(1)) = 2$

i.e. $2g(n)(1) - 1 = 2$

$\Rightarrow g(n)(1) = 3/2$ which is non-integral.

[6]

2 g) r is not an injection as, for example,

$$r(2,4) = 4 \times 8 = 32$$

but also $r(1,8) = 1 \times 2^{2\times 3-1} = 32$.

But $(2,4) \neq (1,8)$.

Any $z \in \mathbb{Z}_+$ can be written as

$$z = p_1^{\alpha_1} p_2^{\alpha_2} \cdots$$

Note also that $r(m,n) = p_1^{2g(m)(1) + q(g(n)(1))} \cdot p_2^{2g(m)(2) + q(g(n)(2))} \cdots$

If α_i is even, choose $q(g(n)(i)) = 0$

$\Rightarrow g(n)(i) = 0$.

and $g(m)(i) = \alpha_i / 2$.

If α_i is odd, choose $q(g(n)(i)) = 1$

$\Rightarrow g(n)(i) = 1$

and $g(m)(i) = \lfloor \alpha_i / 2 \rfloor$.

Then $r(m,n) = z$. So r is a surjection.

[6]

2.h) $r(a,b) = r(c,d)$

$$\Rightarrow h(a)v(b) = h(c)v(d)$$

$$\Rightarrow p_1^{2g(a)(1)+q(g(b)(1))} p_2^{2g(a)(2)+q(g(b)(2))} \ldots = p_1^{2g(c)(1)+q(g(d)(1))} p_2^{2g(c)(1)+q(g(d)(2))} \ldots$$

$$\Rightarrow 2g(a)(i) + q(g(b)(i)) = 2g(c)(i) + q(g(d)(i)) \quad \text{for all } i$$

Because ~~p(m,n~~ $p(a,b)$ is true and
$p(c,d)$ is true

either (i) $g(a)(i) = 0$ and $g(c)(i) = 0$
(ii) $g(a)(i) = 0$ and $g(d)(i) = 0$
(iii) $g(b)(i) = 0$ and $g(c)(i) = 0$
(iv) $g(b)(i) = 0$ and $g(d)(i) = 0$

For (i), $q(g(b)(i)) = q(g(d)(i))$
$\Rightarrow g(b)(i) = g(d)(i)$
& $g(a)(i) = g(c)(i)$ from (i)

For (ii) $q(g(b)(i)) = 2g(c)(i)$
$\Rightarrow g(b)(i) = g(c)(i) = 0$
so $g(b)(i) = g(d)(i)$
& $g(a)(i) = g(i)$

For (iii), ~~g(b)(i~~ $2g(a)(i) = q(g(d)(i))$
$\Rightarrow g(a)(i) = g(d)(i) = 0$
so $g(b)(i) = g(d)(i)$
& $g(a)(i) = g(c)(i)$

For (iv), $2g(a)(i) = 2g(c)(i)$ so $g(b)(i) = g(d)(i)$
& $g(a)(i) = g(c)(i)$

2 (h) [cont'd]

Hence in all four cases

$$g(a) = g(c)$$
$$\& \; g(b) = g(d)$$

Thus $a = b \wedge b = d \Rightarrow$ INJECTION.

We have already established surjectivity.

[6]

i) s is a bijection $\Rightarrow$ s^{-1} is a bijection

r is a bijection $\Rightarrow$ $r \cdot s^{-1}$ is a bijection (composition)

[2]

j) This establishes $|\mathbb{Z}_+| = |\mathbb{Q}_+|$, as we have an explicit bijection between the sets.

Since $|\mathbb{Z}_+| = |\mathbb{N}|$, we have that $\mathbb{Q}_+$ is countable.

[2] ~~[6]~~

3. a) (i) Yes – no two integers have the same English word.
(ii) No, e.g. there is no integer with English word "xxx".
(iii) No, from (ii). Inverse only exists for bijections.
(iv) No, e.g. $g(\text{"one"}) = g(\text{"xxx"})$ but "one" $\neq$ "xxx".
(v) Yes, one can construct a string consisting of x "a"s, for any $1 \leq x \leq 20$. This is a non-empty character string of length ≤ 20.
(vi) No, from (iv). Inverse only exists for bijections.

[12]

b) $f(X) = \{$"one", "two", "three", "four", ..., "twenty"$\}$.
$g(Y) = \{1, 2, \ldots, 20\} = X$.

[4]

c) $R = g \cdot f$
$= \{(1,3), (2,3), (3,5), (4,4), (5,4), (6,3), (7,5), (8,5), (9,4), (10,3), (11,6), (12,6), (13,8), (14,8), (15,7), (16,7), (17,9), (18,8), (19,7), (20,6)\}$

R is not reflexive: $(1,1) \notin R$
R is not symmetric: $(1,3) \in R$ but $(3,1) \notin R$
R is not transitive: $(1,3) \in R$, $(3,5) \in R$, but $(1,5) \notin R$.

$R^2 = \{(1,5), (2,5), (3,4), (4,4), (5,4), (6,5), (7,4), (8,4), (9,4), (10,5), (11,3), (12,3), (13,5), (14,5), (15,5), (16,5), (17,4), (18,5), (19,5), (20,3)\}$

$R^3 = \{(1,4), (2,4), (3,4), (4,4), (5,4), (6,4), (7,4), (8,4), (9,4), (10,4), (11,5), (12,5), (13,4), (14,4), (15,4), (16,4), (17,4), (18,4), (19,4), (20,5)\}$

3.(c) $R^4 = \{(x,4) \mid x \in X\}$.
[contd]

So with $y=4$ $(\in X)$ and $\kappa = 4$ $(\in \mathbb{Z}_+)$,
we have via existential generalisation,

$$\exists y \, \exists \kappa \; (R^\kappa = \{(x,y) \mid x \in X\}).$$ [14]

4. a) $f(n, 10^3, 10^{-1}) = 10^{3-n}$

$10^{3-n} \leq 1$ for $n \geq 3$ [4]

b) Choose $3-n \leq \log_{10} \epsilon$

i.e.

$n \geq 3 - \log_{10} \epsilon$. [5]

c) $\forall a \forall \epsilon \exists N \forall n \left(\epsilon > 0 \wedge a > 0 \wedge n > N \rightarrow f(n,a,b) \leq \epsilon \right)$

$\equiv P(b)$. [8]

d) $f(n, a, 0.5) = a(0.5)^n$

Since we may take $\epsilon > 0$, $a > 0$, choose

$$N = \frac{\log \epsilon - \log a}{\log(0.5)}$$

In the case $a \leq 0$ or $\epsilon \leq 0$, take arbitrary N.

Then $n > N \Rightarrow n \log(0.5) < \log \epsilon - \log a$

$\Rightarrow a(0.5)^n < \epsilon$

$\Rightarrow f(n,a,b) \leq \epsilon$. [9]

e) $X = \{ x \mid x \in \mathbb{R} \wedge -1 < x < 1 \}$. [4]

5. a) (i) $p_1 = 1.0$

(ii) $p_{i+1} = x\,p_i$

$\Rightarrow \; p_i = x^{i-1}$

Value at exit is $p_{k+1} = x^k$.

[8]

b) If $n=0$ then evalpoly2 returns $c[0]$, which is the zero-order (constant) polynomial.

Induction hypothesis: evalpoly2$(c+1, n-1, x)$ returns the desired result, i.e. $c[1] + c[2]x + \ldots + c[n]x^{n-1}$.

Then evalpoly2 (c, n, x) returns

$$c[0] + x\left(c[1] + c[2]x + \ldots + c[n]x^{n-1}\right)$$

= the desired polynomial.

[6]

c) (i) One mult per iteration of i loop + one extra per iteration of k loop

$$\Rightarrow \#\text{mults} = n+1 + \sum_{k=0}^{n} k$$

$$= n+1 + \tfrac{1}{2}n(n+1)$$

$$= \tfrac{1}{2}(n+1)(n+2)$$

(ii) $\#\text{mults} = \tfrac{1}{2}n^2 + \tfrac{3}{2}n + 1$

$\geq \tfrac{1}{2}n^2$ for $n > 0$

$\Rightarrow$ #mults is $\Omega(n^2)$ [$c = \tfrac{1}{2}$, $k=1$, say].

[9]

5. d) (i) $g(0) = 0$

$g(n) = 1 + g(n-1)$ for $n > 0$.

(ii) This is an A.P.

$g(n) = n$

$g(n)$ is a $O(n)$ function

[6]

e) One is $\Omega(n^2)$ and one is $O(n)$

$\Rightarrow$ quadratic versus linear time. Alg 2 is preferable.

[3]