

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING  
EXAMINATIONS 2010

© Imperial College London

## NOTATION

The following notation may be used throughout this paper:

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

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

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

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

# The Questions

## 1. [Compulsory]

a) For the sets  $S_1 = \{\emptyset, a\}$ , and  $S_2 = \{2, 3\}$ , list the elements of:

- i)  $S_1 \cup S_2$ ,
- ii)  $S_1 \cap S_2$ ,
- iii)  $S_1 - S_2$ ,
- iv)  $S_1 \times S_2$ ,
- v)  $\mathcal{P}(S_1)$ .

[ 9 ]

b) Provide one example of each of the following functions from  $\mathbb{N}$  to  $\mathbb{N}$ :

- i) An injection but not a surjection,
- ii) A surjection but not an injection,
- iii) A bijection,
- iv) Neither a surjection nor an injection.

[ 6 ]

c) Express each of these statements using predicate logic syntax. You may assume the existence of an addition operation “+” over integers, and an equality predicate “=”, both with the usual meaning, *e.g.*  $4 + 1 = 3 + 2$ . The universe of discourse should be the set of integers.

- i) “No matter which two integers  $a$  and  $b$  I choose,  $a + b$  has the same value as  $b + a$ ”.
- ii) “If I want to sum any three integers, it doesn’t matter whether I add the first two integers first, and then add the third, or whether I add the last two, and then add the first”.
- iii) “For every integer  $a$ , there is another integer  $b$  such that no matter which integer  $c$  I choose, if I add  $a$  to  $c$  and then add  $b$  to the result, I get back to  $c$ ”.

- iv) “There is an integer to which I can add any integer  $a$ , and I get the result  $a$ ”.

[ 6 ]

- d) Solve the following recurrence relations, in each case stating whether the resulting sequence  $a_n$  is  $O(n)$ .

- i)  $a_n = a_{n-1}$  for  $n > 1$  with  $a_1 = 1$ ,
- ii)  $a_n = 2a_{n-1} + 1$  for  $n > 1$  with  $a_1 = 1$ ,
- iii)  $a_n = a_{n-1} + a_{n-2} + 1$  for  $n > 1$  with  $a_0 = 0, a_1 = 0$ .
- iv)  $a_n = \frac{3}{4}a_{n-1} - \frac{1}{8}a_{n-2}$  for  $n > 1$  with  $a_0 = 1, a_1 = 1$ .

[ 9 ]

- e) Provide one example each of a relation on  $A = \{1, 2, 3\}$  that has each of the following properties. The cardinality of the relation should be at least 1 in all cases.

- i) reflexive but not symmetric or transitive,
- ii) transitive but not reflexive or symmetric,
- iii) symmetric but not reflexive or transitive,
- iv) reflexive and transitive but not symmetric,
- v) reflexive and symmetric but not transitive,
- vi) transitive and symmetric but not reflexive,
- vii) reflexive, symmetric, and transitive.

[ 10 ]

2. [Compulsory]

For two sets  $A$  and  $B$ , let  $A \rightarrow B$  denote the set of all functions from  $A$  to  $B$ . This question will repeatedly refer to the set  $M = (\mathbb{N} \rightarrow \{0, 1\})$ .

- a) We can define a function  $q : M \rightarrow \mathcal{P}(\mathbb{N})$  by  $q(g) = \{i \mid g(i) = 1\}$ . Show that  $q$  is a bijection.

[ 12 ]

- b) Hence comment on the relationship between the cardinality of  $M$  and the cardinality of  $\mathcal{P}(\mathbb{N})$ .

[ 2 ]

Let us assume that there exists a bijection  $h : \mathbb{N} \rightarrow M$ . Consider a set  $S = \{i \mid h(i)(i) = 0\}$ .

- c) Show that  $S \in \mathcal{P}(\mathbb{N})$ .

[ 8 ]

- d) Show that  $\neg \exists n (q(h(n)) = S)$ .

[ 12 ]

- e) Draw the appropriate conclusion about the assumption on the existence of  $h$ , and hence on the cardinality of  $\mathcal{P}(\mathbb{N})$  and the countability of  $\mathcal{P}(\mathbb{N})$ , explaining your answers carefully.

[ 6 ]

3. Let  $A$  and  $B$  be finite sets.
- a) State a formula for the number of functions from  $A$  to  $B$  in terms of the cardinalities of  $A$  and  $B$ .  
[ 3 ]
  - b) Derive a formula for the number of injections from  $A$  to  $B$  in terms of the cardinalities of  $A$  and  $B$ .  
[ 9 ]
  - c) Derive a formula for the number of surjections from  $A$  to  $B$  in terms of the cardinalities of  $A$  and  $B$ .  
[ 9 ]
  - d) Derive a formula for the number of bijections from  $A$  to  $B$  in terms of the cardinalities of  $A$  and  $B$ .  
[ 9 ]

4. a) Write a predicate logic expression for each of these statements, given that  $R$  is a relation on a set  $A$ . Use  $A$  as the universe of discourse.

- i) “ $R$  is a reflexive relation”.  
 ii) “ $R$  is a transitive relation”.

[ 4 ]

$R$  is said to be *antisymmetric* iff  $\forall a \forall b (aRb \wedge bRa \rightarrow (a = b))$ . A relation  $\preceq$  is a *partial order* iff it is reflexive, antisymmetric, and transitive. A relation  $\preceq$  is a *total order* if it is both a partial order and also  $\forall a \forall b ((a \preceq b) \vee (b \preceq a))$ .

Consider the relation  $\preceq_1 = \{(a, b) | \exists k \in \mathbb{N} (b = ka)\}$  on the set  $\mathbb{N}$  and  $\preceq_2 = \{(a, b) | \exists k \in \mathbb{N} (b = ka)\}$  on the set  $B = \{1, 2, 3, 4, 6, 8, 12\}$ .

- b) Show that  $\preceq_1$  and  $\preceq_2$  are both partial orders.

[ 12 ]

- c) Show that neither  $\preceq_1$  nor  $\preceq_2$  are total orders.

[ 6 ]

- d) Draw the digraph of  $R_1 = \{(1, 2), (1, 3), (2, 4), (2, 6), (3, 6), (4, 8), (4, 12), (6, 12)\}$ .

[ 4 ]

- e) Draw the digraph of  $\{(b, b) | b \in B\} \cup R_1^*$ , where  $R_1^*$  denotes the transitive closure of  $R_1$ , and comment on its relationship to  $\preceq_2$ .

[ 4 ]

5. a) State the Master Theorem.

[ 8 ]

- b) Write pseudo-code for four procedures, each operating on an array  $a$  of integers of length  $n$ , and respectively having execution time:
- i) that is a  $\Omega(n)$  function,
  - ii) that is a  $\Omega(2^n)$  function,
  - iii) that the Master Theorem shows to be a  $O(n)$  function,
  - iv) that the Master Theorem shows to be a  $O(n^2 \log n)$  function.

You may assume that no compiler optimizations would be performed on your code.

[ 14 ]

- c) Let  $\Pi$  denote the set of all problems. Let  $A$  denote the set of all algorithms. Let  $Q(x, y, z)$  be the predicate “Algorithm  $x$  solves problem  $y$  in worst-case time  $O(z)$ ”, where  $z$  is a function of the size,  $n$ , of the problem instance. For example,  $Q(\text{myalg}, \text{myprob}, n^2)$  states that `myalg` solves `myprob` in worst-case quadratic time. Let  $P$  be the set of all tractable problems. Define  $P$  in terms of  $Q$  using predicate logic syntax.

[ 4 ]

- d) Give one example each of: a tractable problem, an unsolvable problem, and a solvable problem not known to be tractable.

[ 4 ]



# Discrete mathematics and Computational Complexity

E3.20

1/8

1. a) (i)  $S_1 \cup S_2 = \{\emptyset, a, 2, 3\}$  solutions 2010

(ii)  $S_1 \cap S_2 = \emptyset$

(iii)  $S_1 - S_2 = \{\emptyset, a\}$

(iv)  $S_1 \times S_2 = \{(\emptyset, 2), (\emptyset, 3), (a, 2), (a, 3)\}$

(v)  $P(S_1) = \{\emptyset, \{\emptyset\}, \{a\}, \{\emptyset, a\}\}$

[9]

b) (i)  $f(n) = n + 1$

(ii)  $f(n) = \lfloor n/2 \rfloor$

(iii)  $f(n) = n$

(iv)  $f(n) = \lfloor n/2 \rfloor + 1$

[6]

c) (i)  $\forall a \forall b (a + b = b + a)$

(ii)  $\forall a \forall b \forall c ((a + b) + c = a + (b + c))$

(iii)  $\forall a \exists b \forall c (a + c) + b = c$

(iv)  $\exists b \forall a (b + a = a)$

[6]

d) (i)  $a_n = 1 \quad (n \geq 1) \quad \text{is } O(n)$

(ii)  $a_n = \alpha 2^n - 1 \quad (n \geq 1)$

$a_1 = 2\alpha - 1 = 1$

$\Rightarrow \alpha = 1 \quad \text{so} \quad a_n = 2^n - 1 \quad \text{Not } O(n)$

(iii) form  $r^2 - r - 1 = 0$

$1^2 - 4 \cdot 1 \cdot (-1) \neq 0$ , so distinct roots.

Roots are  $r_1 = \frac{1 - \sqrt{1+4}}{2} = \frac{1}{2}(1 - \sqrt{5})$

$r_2 = \frac{1}{2}(1 + \sqrt{5})$

$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n - \frac{1}{1 \mp 1 - 1}$

$= \alpha_1 r_1^n + \alpha_2 r_2^n - 1$

$\alpha_1 + \alpha_2 - 1 = 0$

$\Rightarrow \alpha_1 r_1 + \alpha_2 r_2 - r_1 = 0$

$\alpha_1 r_1 + \alpha_2 r_2 - 1 = 0$

$$\text{So } \alpha_2 = \frac{r_1 - 1}{r_1 - r_2}$$

$$\alpha_1 = \frac{1 - r_2}{r_1 - r_2}$$

$a_n$  is not  $O(n)$ .

[9]

$$(iv) \quad (r - \frac{1}{2})(r - \frac{1}{4}) = 0 \rightarrow \text{distinct roots.}$$

$$\alpha_n = \alpha_1 \left(\frac{1}{2}\right)^n + \alpha_2 \left(\frac{1}{4}\right)^n$$

$$\left. \begin{array}{l} \alpha_1 + \alpha_2 = 1 \\ 2\alpha_1 + \alpha_2 = 4 \end{array} \right\} \Rightarrow \alpha_1 = 3, \alpha_2 = -2$$

$$a_n = 3\left(\frac{1}{2}\right)^n - 2\left(\frac{1}{4}\right)^n \quad n \geq 0 \quad \underline{\text{is}} \quad O(n).$$

$$e) \quad (i) \quad R = \{(1,1), (2,2), (3,3), (1,2), (2,3)\}$$

$$(ii) \quad R = \{(1,2), (2,3)\}, (1,3)\}$$

$$(iii) \quad R = \{(1,2), (2,3), (2,1), (3,2)\}$$

$$(iv) \quad R = \{(1,1), (2,2), (3,3), (1,2)\}$$

$$(v) \quad R = \{(1,1), (2,2), (3,3), (1,2), (2,3), (2,1), (3,2)\}$$

$$(vi) \quad R = \{ \cancel{1} \} \{ (1,1), (1,2), (2,1), (2,2) \}$$

$$(vii) \quad R = \{1,2,3\} \times \{1,2,3\}.$$

[10]

2. (a) (i) Injection:

$$q(g_1) = q(g_2) \\ \Rightarrow \{i_1 \mid g_1(i_1) = 1\} = \{i_2 \mid g_2(i_2) = 1\}$$

$$\text{i.e. } g_1(i_1) = 1 \Leftrightarrow g_2(i_1) = 1$$

Since the co-domain of  $g$  is  $\{0, 1\}$ ,  
we have  $g_1(i_1) = g_2(i_1)$  for all  $i_1$ , and so  
 $g_1 = g_2$ .

(ii) Surjection.

Let the elements of  $S \in P(\mathbb{N})$  be given by  
 $S = \{s_1, s_2, \dots\}$ .

We can construct  $g$  as  
 $g(i) = \begin{cases} 0, & \text{if } i \notin S \\ 1, & \text{otherwise.} \end{cases}$

Then  $q(g) = S$ . [12]

(b) They must therefore have the same cardinality. [2]

$$(c) S = \{i \mid h(i)(i) = 0\}$$

Since the domain of  $h$  and the domain of the  
domain of  $h(i)$  are both  $\mathbb{N}$ ,  $S \subseteq \mathbb{N}$ . Hence  
 $S \in P(\mathbb{N})$ . [8]

(d) Consider  $h(n)$ . If  $h(n)(n) = 0$ , then  $n \in S$ .

But also  $n \notin q(h(n))$ , from the definition of  $q$ .

If  $h(n)(n) = 1$  then  $n \notin S$ .

But also  $n \in q(h(n))$ , from the definition of  $q$ .

Hence  $S \neq q(h(n))$ .

Since this is true for all  $n$ ,  $\neg \exists n \mid q(h(n)) = S$ . [12]

e) Hence there is no such bijection  $h$ . As a result,  $|P(\mathbb{N})|$   
 $\neq |\mathbb{N}|$ .  $P(\mathbb{N})$  is uncountable. [6]



3 a)  $|B|^{ |A| }$  (book)

[3]

b)  $\frac{|B|!}{(|B|-|A|)!}$   $\left( |B| \times (|B|-1) \times \dots \times (|B|-|A|+1) \right)$  - each time we  
 fewer co-domain element to select) [9] ~~[6]~~

c)  $\frac{|A|!}{(|A|-|B|)!}$   $\left( |A| \times (|A|-1) \times \dots \times (|A|-|B|+1) \right)$  - each time we  
 fewer domain element to select) [9] ~~[6]~~

d)  $|A|!$  (note that this is also  $|B|!$ , since  $|A|=|B|$ ) [9]

4. a) (i)  $\forall a (aRa)$   
 (ii)  $\forall a \forall b \forall c (aRb \wedge bRc \rightarrow aRc)$

b) (i) Reflexivity of  $\leq_1$   
 Consider  $a \in \mathbb{Z}$ .  $(a, a) \in \leq_1$  because  $\exists k$  ( $k=1$ )  
 s.t.  $a = k \cdot a$ .

(ii) Transitivity of  $\leq_1$

Consider  $(a, b) \in \leq_1$  and  $(b, c) \in \leq_1$

Then  $\exists k_1, k_2$  s.t.

$$b = k_1 a \quad \text{and} \quad c = k_2 b.$$

Since  $c = k_2 k_1 a$ ,  $\exists k$  s.t. ( $k = k_1 k_2$ )

$$\text{s.t. } c = k a$$

$\therefore (a, c) \in \leq_1 \Rightarrow \leq_1$  is transitive.

(iii) Antisymmetry.

$$a \leq b \quad \text{and} \quad b \leq a.$$

$$\text{Then } b = k_1 a \quad \text{and} \quad a = k_2 b$$

$$\text{So } a = k_2 k_1 a \Rightarrow k_2 k_1 = 1$$

Since  $k_1, k_2 \in \mathbb{Z}$ ,  $k_1 = 1$  and  $k_2 = 1$ .

$$\text{Thus } a = b.$$

$\therefore \leq_1$  is a partial order.

It follows that  $\leq_2$  is a partial order, since

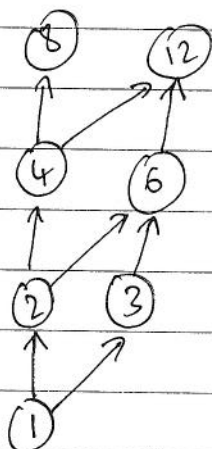
$$\{1, 2, 3, 4, 6, 8, 12\} \subseteq \mathbb{N}$$

c)  $(4, 6) \notin \leq_1$ , as  $\nexists k \in \mathbb{Z} \text{ s.t. } 4 = 6k$  is not satisfiable for  $k$  integer.

Equally,  $(6, 4) \notin \leq_1$  as  $6 = 4k$  is not satisfiable for  $k$  integer.

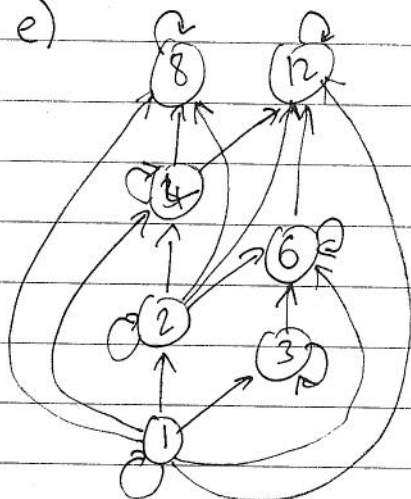
Since 4 & 6 are in the sets for both  $\leq_1$  &  $\leq_2$ , the proof holds for both.

4. d)



[4]

e)



They are equal.

[4]



5. a) let  $a \geq 1$  be a real number,  $b \geq 1$  be an integer,  
 $c \geq 0$  be a real number, and  $d \geq 0$  be a real number.  
 let  $f$  be an increasing function satisfying  $f(n) = a f(n/b) + cn^d$   
 whenever  $n = b^k$  for  $k \in \mathbb{Z}^+$ .

Then:

If  $a < b^d$ ,  $f(n)$  is  $O(n^d)$   
 If  $a = b^d$ ,  $f(n)$  is  $O(n^d \log n)$   
 If  $a > b^d$ ,  $f(n)$  is  $O(n^{\log_b a})$

(bookwork)

-8]

b) (i) proc  $p1(a[n]: \text{integer})$   
 $t := 0$   
 for  $i = 1$  to  $n$   
 $t := t + a[i]$   
 end  
 result :=  $t$

(ii) proc  $p2(a[n]: \text{integer})$   
 if  $n > 1$   
 result :=  $p2(a[1 \text{ to } n-1]) + p2(a[2 \text{ to } n])$   
 else  
 result := 1  
 end

(iii) proc  $p3(a[n]: \text{integer})$   
 if  $n > 1$   
 result :=  $p3(a[1 \text{ to } \lfloor n/2 \rfloor])$   
 for  $i = 1$  to  $n$   
 result := result + 1  
 end  
 else  
 result := 1  
 end

(iv) proc  $p_4(a[n]: \text{integer})$

if  $n > 1$   
 for  $i = 1$  to  $n$   
 $\text{result} := \text{result} + p_4(a[1 \text{ to } \lfloor n/2 \rfloor])$

end;  $i = 1$  to  $n$   
 $\text{result} := \text{result} + 1$

end  
 else

$\text{result} := 1$

end

[4]

c)  ~~$P = \{y \mid \exists x \exists p \in Q(x, y, n)$~~

c)  $P = \{y \mid \exists x \in A \exists b \in \mathbb{Z}^+ Q(x, y, n^b)\}$  [4]

d) tractable: matrix multiplication

unsolvable: halting problem

intractable(?):  $k$ -colouring of a graph.

[4]