UNIVERSITY OF EDINBURGH

COLLEGE OF SCIENCE AND ENGINEERING

SCHOOL OF INFORMATICS

DISCRETE MATHEMATICS AND MATHEMATICAL REASONING

Tuesday 1st April 2014

00:00 to 00:00

INSTRUCTIONS TO CANDIDATES

1. **Answer all five questions in Part A, and two out of three questions in Part B. Each question in Part A is worth 10% of the total exam mark; each question in Part B is worth 25%.**
2. **Use a single script book for all questions.**
3. **CALCULATORS MAY NOT BE USED FOR THIS EXAM.**

THIS EXAMINATION WILL BE MARKED ANONYMOUSLY

PART A

ANSWER ALL QUESTIONS IN PART A

1. A relation R over A is called circular if for all $a, b, c \in A$, aRb and bRc imply cRa.

   (a) Recall the definition of a reflexive relation. [*1 mark*]

   (b) Recall the definition of a transitivity relation. [*1 mark*]

   (c) Recall the definition of a symmetric relation. [*1 mark*]

   (d) Prove that R is reflexive and circular if and only if R is an equivalence relation. [*7 marks*]

2. Let $\{0,1\}^*$ denote the set of all binary strings. Write $y \cdot z$ for the concatenation of the strings y and z. Prove by induction that every string $x \in \{0,1\}^*$ can be written in the form $x = y \cdot z$ where the number of 0's in y is the same as the number of 1's in z. x, y and z can be the empty string denoted ε. For instance, $01001 = 01 \cdot 001$; $111011 = 11101 \cdot 1$; and $00000 = \varepsilon \cdot 00000$.

   (a) Prove the base step. [*2 marks*]

   (b) State the inductive hypothesis. [*2 marks*]

   (c) Prove the inductive step. [*6 marks*]

3. Consider the following algorithm

```
procedure ex3([a_1, ..., a_n])
    i:= 1
    while i<n
        j:= i+1
        while j≤n
            if a_i = a_j
            then return i
            else j:= j+1
        i:= i+1
    return -1
```

   (a) Apply the procedure `ex3` to the sequences [*2 marks*]

$$\bar{a} = [5, 6, 1, 21, 3, 5, 7]$$
$$\bar{c} = [5, 6, 1, 21, 3, 9, 7]$$

   (b) What does this procedure do? [*1 mark*]

(c) Given an input sequence $\bar{\mathtt{i}}$ of size n, we let A_n denote the number of comparisons (tests $\leq$ or $=$) performed by the procedure `ex3` on $\bar{\mathtt{i}}$. Give a closed formula for A_n. Justify your answer. *[2 marks]*

(d) Prove that $A_n \in \Theta(n^2)$:

i. give the witnesses k and C for $A_n \in \mathcal{O}(n^2)$, and justify your answer; *[2 marks]*

ii. give the witnesses k and C for $A_n \in \Omega(n^2)$, and justify your answer. *[3 marks]*

4. (a) Prove the following pigeonhole principle. If $N \geq 0$ objects are placed in $k \geq 1$ boxes, then at least one box contains at least $\left\lceil \frac{N}{k} \right\rceil$ objects. *[5 marks]*

(b) During a three week period of 21 days a shinty team play at least one game a day, but no more than 30 games. Show that there must be a period of some consecutive days during which the team plays exactly 11 games. *[5 marks]*

5. (a) Show that if 7 integers are selected from the first 10 positive integers, there must be at least two pairs of these with the sum 11 *[3 marks]*

(b) Is the conclusion in part a) still true if six integers are selected rather than seven *[2 marks]*

(c) Assume you have a set S of $2k$ numbers, which are partitioned into k disjoint pairs. Prove that selecting $k+n$ (with $n \geq 1$) of the numbers from S will select both numbers of at least n of the pairs. *[5 marks]*

PART B

ANSWER TWO QUESTIONS FROM PART B

6. Let p be a prime number. The purspose of this exercice is to prove that $(p-1) \equiv (p-1)! \pmod{p}$

   (a) Let $(\mathbb{Z}_p)^* = \{1, \ldots, p-1\}$. Prove that any integer $x \in (\mathbb{Z}_p)^*$ has an inverse mod p. [*3 marks*]

   (b) What is the multiplicative inverse of 21 in mod 31 arithmetic? [*3 marks*]

   (c) Prove that the only integers in $(\mathbb{Z}_p)^*$ that are their own inverse in mod p arithmetic are 1 and $p-1$. [*3 marks*]

   (d) Prove that no two distinct integers in $(\mathbb{Z}_p)^*$ have the same multiplicative inverse.

   [**Hint:** Prove this by contradition] [*8 marks*]

   (e) Using items 6a, 6c and 6d, prove that $(p-1) \equiv (p-1)! \pmod{p}$

   [**Hint:** Distinguish the case $p = 2$ from the case $p > 2$] [*8 marks*]

7. Let G be an undirected graph with vertices V and edges E.

   (a) Give the definition of Graph G is connected *[4 marks]*

   (b) Show that if we can make G connected by inserting $k-1$ edges, then G can have at most k connected components. *[5 marks]*

   (c) Assume G is connected. Choose a vertex x and remove it from the set of vertices along with any edge connecting to x. This operation transforms the connected graph G into a set of connected components. We call this graph $G-x$. Show an upper and a lower bound of the number of connected components created by this step in terms of the degree of x. Show that your bounds are exact by giving an example graph G and an example vertex x where $G-x$ has exactly that many components. *[8 marks]*

   (d) Show the following theorem Every connected graph $G=(V,E)$ with $|V| \geq 2$ has at least two vertices x_1, x_2 such that both $G-x_1$ and $G-x_2$ are connected. *[8 marks]*

8. Recall that the expected value of the random variable X on a sample space S is equal to

$$E(X) = \sum_{s \in S} P(s)X(s)$$

where P is the probability distribution on S.

(a) Consider an octal dice which has eight faces and when rolled gives any value from 1 to 8. What is the expected number that appear when a fair octal dice is rolled ? Show your calculations. *[5 marks]*

(b) Prove the following that expected values are linear. For any random variables $X, X_1, \ldots, X_n$ on S and $a, b \in \mathbb{R}$ *[7 marks]*

i. $E(X_1 + X_2 + \ldots + X_n) = E(X_1) + \ldots + E(X_n)$.

ii. $E(a\,X + b) = a\,E(X) + b$.

(c) What is the expected sum of the numbers that appear when five fair octal dice are rolled ? Show your calculations. *[5 marks]*

(d) The variance of X, $V(X)$, is defined by:

$$V(X) = E((X - E(X))^2) = \sum_{s \in S}(X(s) - E(X))^2 P(s)$$

.

Prove the following property of variance. *[8 marks]*

$$V(X) = E(X^2) - E(X)^2$$