HKUST – Department of Computer Science and Engineering
COMP 2711: Discrete Math Tools for Computer Science
Lecture Sessions L1 & L3

Fall 2018 Midterm Examination

Date: 31st October 2018 Time: 19:00–21:00

Name: _____	Student ID: _____
Email: _____	Lecture: _____

Instructions

- This is a closed book exam. It consists of **10** pages and 8 questions. You are allowed to bring a single-page cheat sheet.
- Please write your name, student ID, email, lecture section in the space provided at the top of this page.
- Please sign the honor code statement on page 2.
- Answer all the questions within the space provided on the examination paper. You may use the back of the pages for your rough work. Each question is on a separate page. This is for clarity and is not meant to imply that each question requires a full page answer. Many can be answered using only a few lines.
- Solutions can be written in terms of binomial coefficients, factorials, and the $C(n,k)$, $P(n,k)$ notation. For example, you can write $\binom{5}{3}+\binom{4}{2}$ instead of 16. Avoid use of nonstandard notation such as ${}_nP_k$ or ${}_nC_k$. Calculators may be used for the exam (but are not necessary).

Questions	1	2	3	4	5	6	7	8	Total
Points	8	7	7	8	6	10	7	7	60
Score									

As part of HKUST's introduction of an honor code, the HKUST Senate has recommended that all students be asked to sign a brief declaration printed on examination answer books that their answers are their own work, and that they are aware of the regulations relating to academic integrity. Following this, please read and sign the declaration below.

I declare that the answers submitted for this examination are my own work.

I understand that sanctions will be imposed, if I am found to have violated the University regulations governing academic integrity.

Student's Name: _____

Student's Signature: _____

Problem 1: Knights and Knaves [8 pts]

There are only two kinds of inhabitants on an island: knights, who always tell the truth; and knaves, who always lie. You encounter two of the island's inhabitants, Alice and Bob. Alice tells you, "Bob is a knave." Bob clarifies, "Actually, Alice and I are both knaves."

(a) Let p be the proposition "Alice is a knight", and q be the proposition "Bob is a knight". Write a single compound proposition constructed from p and q which contains all the information given or implied in the question. (Hint: Consider that Alice could be a knight or a knave, and Bob could be a knight or a knave.)

(b) Solve your proposition in (a) to show whether Alice is a knight or a knave, and Bob is a knight or a knave. (There may be multiple or no correct answers; list all of them.)

Solution: (a)

$$((p \wedge \neg q) \vee (\neg p \wedge q)) \wedge ((q \wedge (\neg q \wedge \neg p) \vee (\neg q \wedge (p \vee q))$$

(XOR can be used to connect Alice's two cases and Bob's two cases. Some other answers are possible. Using implication is generally not correct.)

(b) Simplifying Bob's two cases:

$$\begin{aligned} & ((q \wedge (\neg q \wedge \neg p) \vee (\neg q \wedge (p \vee q)) \\ \equiv \; & F \vee (\neg q \wedge (p \vee q)) \\ \equiv \; & \neg q \wedge (p \vee q) \\ \equiv \; & \neg q \wedge p \end{aligned}$$

This is in fact the first of Alice's cases, so Alice must be a knight and Bob must be a knave.

This question should be marked leniently. Suggested marking schemes:

- 7 marks for correct solution and correct explanation (-1 for missing compound propositions)
- 4-6 marks for correct solution but incorrect explanation, depending on quality of explanation
- 2 marks for correct solution but no explanation
- 0-4 marks for incorrect solution, depending on quality of explanation

Problem 2: Tautologies [7 pts]

Some of the following propositions and predicates are **tautologies**. For each statement that is **not** a tautology, prove it by providing a counterexample. For each statement that is a tautology, just state it is a tautology; no proof is required.

(a) $(p \wedge q) \vee (q \wedge \neg p) \vee \neg q \vee (r \wedge T)$

(b) $((p \to q) \to r) \to p$

(c) $\Big(\forall x P(x)\Big) \to \Big(\exists x (P(x) \to Q(x))\Big)$

(d) In the domain of real numbers:
$$\Big(\exists x \forall y (x > 2 \to x^2 + y^2 > 10)\Big) \wedge \Big(\forall x \exists y (x > 2 \to x^2 + y^2 > 10)\Big)$$

Solution: (a) Tautology. (No proof required.)

(b) Not a tautology. It is false when p is false, q is true and r is True:

$$\begin{aligned} & ((p \to q) \to r) \to p \\ \equiv\ & ((F \to T) \to T) \to F \\ \equiv\ & (T \to T) \to F \\ \equiv\ & T \to F \\ \equiv\ & F \end{aligned}$$

(c) Not a tautology. It is false if $Q(x)$ is always false and $P(x)$ is always true.

$$\begin{aligned} & \Big(\forall x P(x)\Big) \to \Big(\exists x (P(x) \to Q(x))\Big) \\ \equiv\ & T \to \Big(\exists x (T \to F)\Big) \\ \equiv\ & T \to F \\ \equiv\ & F \end{aligned}$$

(d) Tautology.

Problem 3: Pigeonhole principle [7 pts]

Consider the set $S = \{1, 2, \ldots, 2n\}$, and subsets $P = \{p_1, p_2, \ldots, p_m\} \subseteq S$ such that they satisfy the following criterion:

$$\forall p_i \in P \, \forall p_j \in P \, (i \neq j \rightarrow p_i \nmid p_j)$$

In the above, $p_i \nmid p_j$ means p_j is not divisible by p_i.

(a) Find a subset $P \subseteq S$ satisfying the above criterion such that $|P| = n$.

(b) For any subset P satisfying the above criterion, we can write every $p_i \in P$ as $c_i \cdot 2^{k_i}$, where c_i is odd. Prove that the following is true:

$$\forall p_i \in P \, \forall p_j \in P \, (i \neq j \rightarrow c_i \neq c_j)$$

(c) Prove that there is **no** $P' \subseteq S$ satisfying the above criterion such that $|P'| > n$. (Hint: By contradiction, suppose $|P'| = n + 1$ satisfies the above criterion. Following (b), put each p_i in the pigeonhole c_i.)

Solution: (a) $P = \{n+1, n+2, \ldots, 2n\}$. Answer for a specific n is not accepted. (2 marks) Other answers are possible.

(b) WLOG consider $p_i < p_j \in P$. If $i \neq j$, then $p_i \nmid p_j$. However, if $c_i = c_j$, then $p_i = c_i \cdot 2^{k_i} | c_i \cdot 2^{k_i + (k_j - k_i)} = c_i \cdot 2^{k_j} = p_j$. This is a contradiction, so $c_i \neq c_j$. (3 marks)

(c) Let each hole be an odd number in S. The largest odd number in S is $2n-1$, so the holes are $\{1, 3, 5, \ldots, 2n-1\}$, so there are n holes, and the odd factor of each number in P' fits into one of these holes. Therefore, there are $n + 1$ numbers for n holes, and by the pigeonhole principle, there exists two different $p_i, p_j \in P'$ in the same hole, i.e. $c_i = c_j$. But we know that this is impossible from (b), giving a contradiction. (2 marks)

Problem 4: Sets and functions [8 pts]

(a) Consider finite sets S and T, and a function $f : S \to T$. Write down the contrapositive of "If f is injective, then $|T| \geq |S|$." Then, prove the contrapositive directly.

(b) For functions on finite sets $f : S \to T$, $g : T \to U$, if f is injective, and g is surjective, is it true that $g \circ f$ must be injective? Prove it.

(c) Consider a lossless data compression algorithm, like `zip` or `rar`: compressed files can always be de-compressed to obtain the original files. Prove that it is impossible for a lossless data compression algorithm to reduce the size of every file. (Hint: Use (a), and prove by contradiction on the set of all files of size n bits or less.)

Solution: (a) The contrapositive is "If $|T| < |S|$, then f is not injective". We can prove it by the pigeonhole principle. f maps pigeons in S to holes in T. Since $|T| < |S|$, there must be two pigeons that share a same hole, say $a, b \in S$. Then $a \neq b$ but $f(a) = f(b)$, so f is not injective.

(b) False. Students can provide any counterexample such that f is injective, g is surjective, and $g \circ f$ is not injective. For example: $S = T = \{a, b\}$, $U = \{0\}$, $f(x) = x$, $g(y) = 0$, then $g(f(x)) = 0$. It is not injective because $g(f(a)) = g(f(b)) = 0$.

(c) By contradiction, consider such a function f defined on $F_n \to T$, where F_n is the set of all files of size n bits or less. As f reduces the sizes of all files, T satisfies $T \subseteq F_{n-1}$, the size of all files of size $n-1$ bits or less. Clearly $F_{n-1} \subset F_n$, so $|T| < |F_n|$. However, since f is invertible, f must be injective. Therefore, using (a), we have $|T| \geq |F_{n-1}|$. This is a contradiction.

Problem 5: Divisibility [6 pts]

(a) Let x, y, z be positive integers. Show that, if $z|xy$ and y, z are relatively prime, then $z|x$.

(b) Let x, y be positive integers and p be a positive prime integer. Show that, if $p|xy$ then $p|x$ or $p|y$. (*Note:* You may use the result from (a) even if you did not solve that part.)

Answer: (a) Since y, z are relatively prime, $gcd(y, z) = 1$. Using the extended Euclidean algorithm, we can calculate integers s, t such that

$$sy + tz = 1 \qquad (1)$$

Multiplying both sides of (1) with x, we get

$$syx + tzx = x \qquad (2)$$

From the problem statement, $z|xy$, thus $z|syx$. Moreover, it is obvious that $z|tzx$. We know that from this it follows that z divides their sum, that is, $z|(syx + tzx)$. But, from (2), $(syx + tzx) = x$, therefore $z|x$.

Students may choose to explicitly prove the fact that if $a|b$ and $a|c$ then $a|(b + c)$. This is fine but not necessary.

(b) Since p is prime, it follows that $gcd(p, x)$ is either p or 1, because these are the only divisors of p. If $gcd(p, x) = p$, then x is a multiple of p, that is, $p|x$. Else, $gcd(p, x) = 1$, that is, x, p are relatively prime. In this case, using (a), we get that $p|y$.

Problem 6: RSA [10 pts]

Consider the RSA encryption with parameters $p = 19, q = 37$.

(a) Which one of the integers $2, 3, 11$ can be used as the encryption key e? Why? (*Note:* only one of them is an acceptable solution.)

(b) Compute the value of the decryption key d for for your choice of e from step (a). Show all intermediate steps.

(c) Assume you want to encrypt the message 3. What is the resulting encrypted ciphertext? Use repeated squaring and show all intermediate steps.

Answer: (a) $(p-1)(q-1) = 648$. For e it must be true that $gcd(e, 648) = 1$. Therefore, e cannot be 2 (since $648 = 2 \cdot 324$) or 3 (since $648 = 3 \cdot 216$). On the other hand $gcd(11, 648) = 1$, therefore $e = 11$.

(b) The private key d is the multiplicative inverse of e modulo $(p-1)(q-1)$. Using the extended Euclidean algorithm:

$$\begin{aligned} 648 &= 58 \cdot 11 + 10 \\ 11 &= 1 \cdot 10 + 1 \\ 10 &= 10 \cdot 1 \end{aligned}$$

Substituting backwards

$$1 = 11 - 10 \cdot 1 = 11 - (648 - 58 * 11) = -1 \cdot 648 + 59 \cdot 11$$

Since 59 is already in $\mathbb{Z}_{648}$ the answer is $d = 59$. Note that students can use a table form to obtain the answer, which should be accepted.

(c) The encrypted ciphertext is computed as

$$3^e \bmod pq = 3^{11} \bmod 703$$

To compute this, we first compute

$$\begin{aligned} 3^2 \bmod 703 &= 3 \cdot 3 \bmod 703 = 9 \\ 3^4 \bmod 703 &= 9 \cdot 9 \bmod 703 = 81 \\ 3^8 \bmod 703 &= 81 \cdot 81 \bmod 703 = 234 \end{aligned}$$

It holds that $11 = 8 + 2 + 1$. Hence

$$\begin{aligned} 3^{11} \bmod 703 = 3^{1+2+8} \bmod 703 &= 3 \cdot 3^2 \cdot 3^8 \bmod 703 \\ &= 3 \cdot 9 \cdot 234 \bmod 703 = 694 \end{aligned}$$

No marks for this part if the answer is correct but there are no steps, because it is easy to obtain the answer using a calculator.

Problem 7: Counting [7 pts]

A committee of 5 members needs to be formed in order to represent the employees in an office. There are 20 employees, 11 men and 9 women.

(a) How many ways are there to form the committee if there are no restrictions in the gender of the members.

(b) How many ways are there to form the committee if at least one woman and one man must be in it.

(c) How many ways are there to form the committee if there must be more women than men.

Briefly justify your answers.

Answer: (a) This is simply $C(20, 5) = 15504$.

(b) There are $C(11, 5) = 462$ ways to form a committee entirely from men and $C(9, 5) = 126$ ways to form a committee entirely from women. Note that no committee can consist entirely of women and entirely of men at the same time. Therefore the correct answer is $C(20, 5) - C(11, 5) - C(9, 5) = 14916$.

(c) Let us consider all the distinct cases that lead to more women than men. There are $C(9, 5)$ ways to form a committee from five women and no man, $C(9, 4) \cdot C(11, 1)$ ways to form a committee with four women and one man, and $C(9, 3) \cdot C(11, 2)$ ways to form a committee with three women and two men. In all other cases, there will not be more women than men in the committee. Therefore the correct answer is $C(9, 5) + C(9, 4) \cdot C(11, 1) + C(9, 3) \cdot C(11, 2) = 6132$.

Problem 8: Combinations and Permutations [7 pts]

You are given a suitcase that has a combination lock. It consists of five dials, each of which can be rotated to take a value from 0–9. The suitcase only opens if you guess the correct 5-digit solution.

(a) How many different solutions are there?

(b) How many different solutions are there, if you know that no two adjacent dials can have the same digit?

(c) Assume that the lock has a weird flaw: The exact order in which you put the digits does not matter. In this case how many different solutions are there?
(Note that all permuted versions of a given combination still count as one solution. For example, if the correct solution is *12345*, then *34125*, *51243*, *23145*, etc., all count as the same solution.)

Briefly justify your answers.

Answer: (a) All 10 digits are possible for each of the 5 dials, hence 10^5.

(b) $10 \cdot 9^4$. All digits are possible for the first dial. For each subsequent dial, the digit chosen in the previous dial is not a valid option.

(c) Since the order of the digits does not matter, this can be seen as a classic "stars-and-bars" problem. We need 10 gaps, each one for one of the digits 0–9, thus the number of bars is $10 - 1 = 9$. The numbers of stars is 5, one for the chosen digit in each of the dials. The standard formula for this problem gives $C(14, 5) = 2002$.