Serial #

HKUST – Department of Computer Science and Engineering
COMP 2711: Discrete Math Tools for CS – Fall 2017

Fall Examination

Date: December 9, 2017 Time: 08:30 AM - 11:30 AM

Name: __________	Student ID: __________
Email: __________	Lecture Section: __________

Instructions

- This is a closed book exam. It consists of 22 pages and 14 questions.
- Please write your name, student ID, email, lecture section and tutorial 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, the $C(n,k), P(n,k)$, and $\binom{n}{k}$ notations. For example, you can write $\binom{5}{3} + \binom{4}{2}$ instead of 16. Avoid using nonstandard notation such as ${}_nP_k$ and ${}_nC_k$. Calculators may be used for the exam (but are not necessary).

Question	1	2	3	4	5	6	7	Total
Score								
Question	8	9	10	11	12	13	14	
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: [4 pts] An office manager has four employees and nine reports to be done. In how many ways can the reports be assigned to the employees so that each employee has at least one report to do?

Solution: $4^9 - \binom{4}{1}3^9 + \binom{4}{2}2^9 - \binom{4}{3}1^9$

Problem 2: [4 pts] Arrange the following functions in a list so that each is big-O of the next one in the list:

$$n^3 + 88n^2 + 3, \log n^4, 3^n, n^2 \log n, n \cdot 2^n, 10000.$$

Solution: 10000, $\log n^4$, $n^2 \log n$, $n^3 + 88n^2 + 3$, $n \cdot 2^n$, 3^n.

Problem 3: [6 pts] For each of the following parts, find the "best" big-O notation to describe the complexity of the algorithm. Choose your answers from the following:

$$O(1), O(\log n), O(n), O(n \log n), O(n^2), O(n^3), ..., O(2^n), O(n!)$$

Assume that the amount of time to print any string is a constant, i.e. $O(1)$.

(a) An algorithm that prints all bit strings of length n that end with 1.

(b) An algorithm that prints all subsets of size two of the set $\{1, 2, 3, ..., n\}$.

(c) The number of print statements in the following:

```
while $n > 1$
    print "hello";
    $n := \lfloor n/4 \rfloor$
```

Solution: (a) 2^n

(b) n^2

(c) $\log n$

Problem 4: [11 pts] Recall that in RSA, we need to choose two primes p and q, and the public key is (n, e) where $n = pq$. Let $T = (p-1)(q-1)$. The private key is d, where $ed \equiv 1 \pmod{\text{T}}$. The encryption of x is $x^e \bmod n$. This means that d must be an integer in $\mathbb{Z}_T$ that is relatively prime with T. We can find d using the following algorithm:

1. Randomly pick $d \in \mathbb{Z}_T$.
2. If d and T are relatively prime, then return d. If they are not, then pick a new d and loop from step 1.

Assume that we will never pick the same d twice.

(a) Suppose that $p = 13$, $q = 61$. In the worst case, what is the number of times we will execute step 1 (that is, the number of times we have to pick a random d)?

(b) Give an efficient algorithm to test if a single d and T are relatively prime. What is the worst case running time of your algorithm in terms of T for a single d? Express your answer in big-O notation.

(c) Bob says: "Instead of picking a random d, I will iterate over the primes from smallest to largest: I will test $d = 2, d = 3, d = 5, d = 7, \cdots$ until I get a valid d." Prove that in the worst case, this algorithm will terminate in $O(\log n)$ number of loops [1].

Solution: (a) $p - 1 = 2^2 \cdot 3$, $q - 1 = 2^2 \cdot 3 \cdot 5$. So this is equivalent to finding the number of integers from $\{0, 1, \cdots, (p-1)(q-1) - 1 = 719\}$ that are relatively prime to 2, 3, and 5. Using the inclusion exclusion principle, we first find the number of integers that are multiples of 2:360, 3:240, 5:144, 6:120, 10:72, 15:48, 30:24. The number of integers that are not relatively prime to 2, 3, and 5 would then be 360+240+144-120-72-48+24 = 528. By the pigeonhole principle, in the worst case it will take 529 tries to find a proper d.

1+ if trying to calculate the number of integers relatively prime to and less than 720. 3+ if set up the inclusion-exclusion principle. 4+ if set up the inclusion-exclusion principle correctly. 4.5 if off by one.

(b) It is the Euclidean algorithm to find gcd: start with $gcd(T, d)$, and the recursive step is to change $gcd(a, b)$ into $gcd(b, a \bmod b)$. It was shown in class that this takes $O(\log T)$ steps for the worst case of the Fibonacci numbers.

2 marks if the algorithm is less efficient than the above, but correctly analyzed (e.g. attempt to divide d and n by all integers less than d). 1 mark if either analysis or algorithm is wrong.

[1] Bob's algorithm may be much faster in the worst case, but it is very bad for cryptography!

(c) Suppose $P_{\log_2 n}$ consists of the first $\log_2 n$ primes. Then $\prod_{x \in P_{\log_2 n}} x > \prod_{x \in P_{\log_2 n}} 2 > n$. So using the fundamental theorem of arithmetic, there cannot be more than $\log_2 n$ primes which are factors of n. This means that Bob will have to try at most $\log_2 n + 1 = O(\log n)$ primes.

1 mark if the student attempts to use "the number of primes less than n is $O(\log n)$" which is not true.

Grading scheme: 5,3,3

Problem 5: [9 pts] You play against your friend in a coin flipping game, where the objective is to get the most heads after three coin flips. A player wins if they have more heads than the opponent. If the numbers of heads are equal, then no one wins; it is a tie. You will take turns flipping coins, and your friend flips first.

You want to cheat, so you created a fake coin that looks identical to a real, fair coin. The fake coin has a 80% chance of getting heads. Your friend is suspicious, so your friend gets to pick first from the two coins randomly, with equal probability. You are forced to take the other coin. You will both use your own coin for all three coin flips. The game begins, and your friend flips the coin once and gets heads.

(a) Given that your friend's first coin flip returns heads, what is the probability that your friend got the fake coin, to your disadvantage?

(b) Given that your friend's first coin flip returns heads, what is the probability that you will win the game? (Use your answer in part (a).)

Solution: (a) Define the following events: E_1: Your friend got the fake coin. E_2: Your friend got the real coin. H: Your friend's coin flip returns heads. T: Your friend's coin flip returns tails.

We want to know $p(E_1|H)$.

We know that $p(H) + p(T) = 1$, $p(E_1) + p(E_2) = 1$.

Then we have:

$$p(E_1|H) \cdot p(H) = p(H|E_1) \cdot p(E_1)$$

$$p(E_1|H) = 0.8 \cdot 0.5/p(H) = 0.4/(0.5 \cdot 0.8 + 0.5 \cdot 0.5) = 0.4/0.65 = 8/13$$

(b) There are two scenarios to consider: You have the real coin or the fake coin. In either case you must have at least 2 heads to consider winning.

You have real coin: Chance of friend having 1 heads = $0.2{\cdot}0.2$, multiply chance of you having 2 heads or more = $0.5 \cdot 0.5 \cdot 0.5 \cdot 4$, makes 0.02. Chance of friend having 2 heads = $0.8 * 0.2 * 2$, multiply chance of you having 3 heads = $0.5 * 0.5 * 0.5$, makes 0.04. Add the two probabilities for 0.06, multiplied with chance in (a) = 0.48/13.

You have fake coin: Chance of friend having 1 heads = $0.5{\cdot}0.5$, multiply chance of you having 2 heads or more = $0.8 \cdot 0.8 \cdot 0.2 \cdot 3 + 0.8 \cdot 0.8 \cdot 0.8$, makes 0.224. Chance of friend 2 heads = $0.5 \cdot 0.5 \cdot 2$, multiply chance of you having 3 heads = $0.8 \cdot 0.8 \cdot 0.8$, makes 0.256. Add the two probabilities for 0.48, multipled with chance in (b) = 2.4/13.

Total = $2.88/13 \approx 22\%$.

> 4 marks if the two cases are set up correctly and the student attempted to calculate most cases correctly but made minor mistakes. 3 marks if the two cases are set up correctly and the student missed some cases/mistakes or did not use combinatorics. 2 marks if there are many mistakes.

Grading scheme: 4,5

Problem 6: [7 pts] 64 fair coins are flipped independently randomly and then arranged in an 8 by 8 block randomly without looking. Each row contains eight coins and there are eight rows. If all eight coins in a row have the same symbol (heads or tails), we call it a homogeneous row. Let X denote the number of homogeneous rows in the block.

(a) If all coin flips come up heads, what is the value of X?

(b) Calculate $p(X = 1)$

(c) Calculate $E(X)$

(d) Calculate $V(X)$

Solution: (a) 8.

(b) For any given row, the chance it is homogeneous is $(1/2)^8 \cdot 2 = (1/2)^7$ (all heads or all tails). The chance that it is not homogeneous is $(1 - (1/2)^7)$. Overall, seven rows must not be homogeneous and one row must be homogeneous, so $p(X = 1) = 8(1/2)^7(1 - (1/2)^7)^7$.

(c) Consider the homogeneity of each row as its own indicator variable X_i, all X_i are mutually independent. So $E(X) = 8E(X_1) = 8(1/2)^7$.

(d) As above, $V(X) = 8V(X_1) = 8(1/2)^7(1 - (1/2)^7)$.

Grading scheme: 1,2,2,2

Problem 7: [7 pts] Ten people at a party decide to randomly choose one person to clean up. They decide to play rock, paper, scissors (R, P, S) to do so. The rules are as follows:

1. Each player will simultaneously choose one symbol in R, P, S. R beats S, S beats P, P beats R.
2. If the remaining players can be divided into exactly two sets S_1 and S_2, not necessarily the same size, such that all players in S_1 chose the same symbol and all players in S_2 chose the same symbol, and S_1's symbol beats S_2's symbol, then all players in S_2 is eliminated.
3. Otherwise, there is a tie, and no one is eliminated.
4. The above continues until only one player is left.

Assuming all players choose symbols randomly, what is the probability that no one is eliminated after ten rounds of the game?

Solution: Consider one round of the game. Consider the chance of having at least one R and at least one P, but no S. The chance of having only R and P, no S, is $(2/3)^{10}$. The chance of having only R is $(1/3)^{10}$, same for only P. So the chance of having at least one R, at least one P, but no S is $(2/3)^{10} - 2(1/3)^{10}$. The chance of having at least one R, one S, no P is the same; one R, one P, no S is the same. So each round of the game has a $3((2/3)^{10} - 2(1/3)^{10})$ chance of eliminating players; the chance of no player being eliminated would be $1 - 3((2/3)^{10} - 2(1/3)^{10})$. After ten rounds, the chance is $(1 - 3((2/3)^{10} - 2(1/3)^{10}))^{10} \approx 0.59$.

Problem 8: [6 pts] Let $P(n)$ be the statement that a postage of n cents can be formed using just 4-cent and 7-cent stamps. Prove by induction that $P(n)$ is true for $n \geq 18$.

Solution: By (weak) induction: It is easy to show that $P(18)$ is true. Now suppose that $P(k)$ is true where $k \geq 18$. We show that $P(k+1)$ is also true. Consider the postage of k cents (by inductive hypothesis, such postage can be formed). This postage either

(i) contains at least one seven-cent stamp, or

(ii) contains no seven-cent stamp. In this case, it contains at least five 4-cents stamp since $k \geq 18$.

In case (i), by simply replace that seven-cent stamp by two 4-cet stamps, we obtain a postage of $k+1$ cents. In case (ii), by replacing that five 4-cent stamps by three 7-cent stamps, we obtain a postage of $k+1$ cents. This completes the inductive step.

By strong induction: It is easy to show that $P(18), P(19), P(20), P(21)$ is true. Now suppose that $P(k-3), P(k-2), P(k-1), P(k)$ is true where $k \geq 21$. We show that $P(k+1)$ is true. Since $P(k-3)$ is true, a postage of $k-3$ cents can be formed. Adding one more 4-cent stamp, we obtain a postage of $k+1$ cents.

Problem 9: [6 pts] Use induction to prove that, for any non-negative integer n,

$$1 + rn \leq (1+r)^n, \text{ if } r > -1.$$

Solution: **Base case**: When $n = 0$,

$$\begin{aligned} \text{LHS} &= 1 + r \cdot 0 = 1 \\ \text{RHS} &= (1+r)^0 = 1 \end{aligned}$$

LHS $\leq$ RHS. So, the statement is true for $n = 0$.

Induction hypothesis: Now let $n \geq 1$. Assume the statement is true for $n - 1$, i.e.,

$$1 + r \cdot (n-1) \leq (1+r)^{n-1}$$

Induction step: Consider the case of n,

$$\begin{array}{rcll} (1+r)^n &=& (1+r) \cdot (1+r)^{n-1} & \\ &\geq& (1+r) \cdot (1 + r \cdot (n-1)) & \text{by hypothesis} \\ &=& 1 + rn + r^2 n - r^2 & \\ &=& 1 + rn + r^2(n-1) & \\ &\geq& 1 + rn & \text{since } r^2(n-1) \geq 0 \end{array}$$

So, the statement is true for the case of n.

By the principle of Mathematical Induction, we conclude that the statement is true for any non-negative integer n.

Problem 10: [7 pts] Let S be the subset of the set of ordered pairs of integers defined recursively by:

Basis step: $(0,0) \in S$

Recursive step: If $(a,b) \in S$, then $(a,b+1) \in S$, $(a+1,b+1) \in S$, and $(a+2,b+1) \in S$.

(a) List the elements of S produced by the first two applications of the recursive definition.

(b) Use structural induction to prove that $a \leq 2b$ whenever $(a,b) \in S$.

Solution: (a) First Application of Recursive step to S

Applying recursive step to (0,0) gives (0,1), (1,1), (2,1)
So $S = \{(0,0),(0,1),(1,1),(2,1)\}$

Second Application of Recursive step to S

Omit the application of the Recursive step to (0,0) again, since we already have those terms in S.
Applying recursive step to (0,1) gives (0,2), (1,2), (2,2)
Applying recursive step to (1,1) gives (1,2), (2,2), (3,2)
Applying recursive step to (2,1) gives (2,2), (3,2), (4,2)
So $S = \{(0,0),(0,1),(0,2),(1,1),(1,2),(2,1),(2,2),(3,2),(4,2)\}$

(b) Inductive Hypothesis: $P(a,b) : a \leq 2b$ whenever $(a,b) \in S$.
Basis Step: $P(0,0) : 0 \leq 0$.
Recursive Step:
$a \leq 2b$ (inductive hypothesis).
$a \leq 2b \leq 2b+2 \leq 2(b+1)$
$P(a,b+1)$ is true.
$a \leq 2b$ (inductive hypothesis)
$a+1 \leq a+2 \leq 2b+2 \leq 2(b+1)$
$P(a+1,b+1)$ is true.
$a \leq 2b$ (inductive hypothesis)
$a+2 \leq 2b+2 \leq 2(b+1)$
$P(a+2,b+1)$ is true.

Grading scheme: 3,4

Problem 11: [10 pts] In a *Double Towers of Hanoi* problem, there are three poles in a row and $2n$ disks for some positive integer n. There are two disks of size 1, two disks of size 2, and so on, up to two disks of size n. Initially one of the poles contains all the disks placed on top of each other in pairs of decreasing size. Disks are transferred one-by-one from one pole to another, but at no time may a larger disk be placed on top of a smaller disk. A disk may be placed on top of one of the same size. Let $T(n)$ be the number of moves needed to transfer a tower of $2n$ disks from one pole to another.

(a) Find $T(1)$ and $T(2)$.

(b) Find $T(3)$.

(c) Find a recurrence relation expressing $T(n)$ in terms of $T(n-1)$, for all integers $n \geq 2$.

(d) Find a closed-form solution for the recurrence.

Solution: (a) $T(1) = 2$
$T(2) = 6$

(b) $T(3) = 14$

(c) $T(n) = 2T(n-1) + 2$

(d)

$$\begin{aligned}
T(n) &= 2T(n-1) + 2 \\
&= 2(2T(n-2) + 2) + 2 \\
&= 2^2T(n-2) + 2^2 + 2 \\
&\vdots \\
&= 2^{n-1}T(n-(n-1)) + 2^{n-1} + \cdots + 2^2 + 2^1 \\
&= 2^{n-1}T(1) + 2^{n-1} + \cdots + 2^2 + 2^1 \\
&= 2^n + 2^{n-1} + \cdots + 2^2 + 2^1 \\
&= 2^{n+1} - 2
\end{aligned}$$

Grading scheme: 2,2,3,3

Problem 12: [8 pts] Suppose we want to obtain a list of all primes up to some positive integer n. The following algorithm is called the Sieve of Eratosthenes, and it returns P:

1. Initiate $L = \{2, 3, 4, \cdots, n\}$, the list of integers from 2 to n.
2. Set p to be the smallest integer of L. Remove p from L and put p in P. Also, remove $(p+k)p$ from L for all $k \geq 0$ where $(p+k)p \leq n$.
3. Repeat Step 2 unless the smallest integer of L is larger than $\sqrt{n}$.
4. Finally, put all remaining integers in L into P, and return P.

We show that this algorithm is correct by proving (a) and (b) below.

(a) Prove that P contains the set of all primes up to n.

(b) Prove that the set of all primes up to n contains P. (Hint: Equivalently, prove that P does not contain any composite number up to n.)

Solution: (a) Consider $L' = L \cup P$ throughout the algorithm, which is the same as the eventually returned P. Initially, $L' = \{2, 3, 4, \cdots, n\}$ contains P_n, the set of all primes up to n. Looking at step 2, we only remove an integer from L' if it is equal to $(p+k)p$ for $k \geq 0$ and $p \geq 2$. Such an integer is clearly not prime as p and $p+k$ divide it. Since we are only remove non-primes from L', it will always contain P_n.

(b) According to the fundamental theorem of arithmetic, n can be written as $p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$, where $p_1, p_2, \cdots, p_m$ is an ascending list of primes. Then $n = p_1 \cdot n'$, where $n' > p_1$. This means that if p_1 were selected in Step 2, n would be removed in Step 2.

Now we need to prove that p_1 would become the smallest integer of L at some point before it terminates. From part (a), we know that p_1 will never be removed from $L \cup P$ because it is prime. Also we see that $p_1^2 = p_1 \cdot p_1 < p_1 \cdot n' = n$, so the algorithm will not terminate before it reaches p_1. Therefore at some point p_1 must become the smallest integer of L. Then n will be removed.

Grading scheme: 4,4

Problem 13: [7 pts] In class we learned about several special types of graphs: complete graphs K_n, cycles C_n, and complete bipartite graphs $K_{m,n}$. Recall the definitions:

K_n For $V = \{v_1, v_2, \cdots, v_n\}$ ($n \geq 1$), there is exactly one edge between every pair of vertices in V. K_1 is a single vertex and K_2 is two vertices connected by an edge.

C_n For $V = \{v_1, v_2, \cdots, v_n\}$ ($n \geq 3$), there is exactly one edge between v_i and v_{i+1} for all $1 \leq i \leq n$, plus exactly one edge from v_n to v_1.

$K_{m,n}$ For every vertex u_i in $U = \{u_1, u_2, \cdots, u_m\}$, and v_j in $V = \{v_1, v_2, \cdots, v_n\}$ ($m \geq 1, n \geq 1$), there is exactly one edge connecting u_i and v_j. There are no edges between two vertices in U, and no edges between two vertices in V.

(a) Can a complete graph K_n be bipartite? Explain what conditions n must satisfy if it is possible.

(b) Can a cycle C_n be bipartite? Explain what conditions n must satisfy if it is possible.

(c) Can a complete bipartite graph $K_{m,n}$ have an Euler path but not an Euler circuit? Explain what conditions m and n must satisfy if it is possible.

Solution: (a) Yes, only if $n = 2$: the graph with two vertices and one edge. Consider the colouring method to determine if a graph is bipartite. If $n > 2$, then if we mark a vertex as red, all other vertices will be marked as blue, and they will be neighbours of each other, so the colouring contradicts the requirement for bipartite graphs.

(b) Yes, when n is even. Using the colouring method, if vertex 1 is red, then 2 is blue, 3 is red, and so on. Vertex n is blue if n is even, in which case there is no contradiction (all red vertices have blue neighbours, all blue vertices have red neighbours). Vertex n is red if n is odd, but it is a neighbour of vertex 1, so there is a contradiction; no colouring is possible.

(c) For a bipartite graph, the vertices in U all have degree n and the vertices in V all have degree m. We know that there exists an Euler path but not an Euler circuit if there are exactly two vertices of odd degree and all other vertices have even degree. For such a scenario to occur, this means that either $m = 2$ and n is odd, or $n = 2$ and m is odd. So it is possible.

Grading scheme: 2,2,3

Problem 14: [8 pts] In this question, we want to find the minimum number of edges in a connected graph with n vertices.

(a) Give an example of a connected graph with n vertices and $n-1$ edges.

(b) Prove that if there is a connected graph with n vertices and $k < n$ edges, then there is a connected graph with $n-1$ vertices and $k-1$ edges. (Hint: Does a vertex of degree 1 always exist? Prove it.)

(c) Using the above, prove that there is no connected graph with n vertices and fewer than $n-1$ edges.

Solution: (a) Remove any one edge from C_n.

(b) A vertex of degree 1 always exists because the total degree of all vertices is $2k < 2n$. If all vertices had degree 2 or above, then the total degree would be $\geq 2n$, which is a contradiction. So there must be such a vertex. Call this vertex v and the incident edge e. For any two vertices $v_1, v_2 \neq v$ in the graph, there must be a path between them because it is a connected graph, and the path between them does not have to contain e: if e is in such a path, then the next edge in that path must also be e since v has degree 1 (it cannot lead to any other vertex), so the two e's can be removed without affecting the path. So when we remove v from the set of vertices and e from the set of edges, the remaining graph has $n-1$ vertices and $k-1$ edges, and it is still connected.

(c) Suppose in contradiction that G is a connected graph that has n vertices and k edges where $k < n-1$. Then using part (b), we have a connected graph that has $n-1$ vertices and $k-1$ edges. We can repeat this process until we reach a connected graph with at least 2 vertices and 0 edges. This is a contradiction, as such a graph is clearly not connected.

Grading scheme: 1,3,4