HKUST – Department of Computer Science and Engineering
COMP2711: Discrete Math Tools for CS – Fall 2016

Final Examination

Date: Dec 7, 2016 (Wednesday)
Time: 12:30–15:30
Venues: Tsang Shiu Tim Art Hall (L1 students) and
LG4 Multi-purpose Room (L2 and L3 students)

Surname (e.g., Chan): ______________________

Given Name (e.g., Tai Man): ______________________

Student ID: ______________ Seat Number: ______________

Lecture Session (Please tick only one of the following): □ L1 □ L2 □ L3

Instructions

- You are allowed to bring a calculator and an A4-sized cheating sheet hand-written on both sides.
- Answer all the questions within the space provided on the examination paper. You may use the back of the pages for your rough work.
- **Unless otherwise specified you *must* always explain how you derived your answer. A number without an explanation will be considered an incorrect answer.**
- Solutions can be written in terms of binomial coefficients and falling factorials. For example, $\binom{5}{3} + \binom{4}{2}$ may be written instead of 16, and $5^{\underline{3}}$ instead of 60.
- Please *do not* use the $_nP_k$ and $_nC_k$ notation. Use $n^{\underline{k}}$ and $\binom{n}{k}$ instead.

Questions	1	2	3	4	5	6	7	8	Total
Points	13	12	15	15	10	15	10	10	100
Score									

Seat Number: ______________

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: [13 pts] You are given **two** fair dice where each dice has the number 1 to 6 printed on it. You are also given **one** wheel so that a random spin of the wheel returns an integer from 2 to 12 in a uniform distribution. Answer the following questions.

(a) What is the probability to have a sum larger than 5 (excluding 5) when the two dice are tossed at the same time?

(b) You are now playing a boardgame. Each time you move your token x steps forward if you spin the wheel and obtain a number x. What is the expected number of steps moved if you spin the wheel 5 times?

(c) In the same boardgame mentioned in part (b), assume that you win the game if and only if you can move your token 10 steps or more with only 2 spins or fewer. What is your winning probability? (You win if you have moved the token **10 steps or more**.)

(d) In the same boardgame mentioned in part (b) and part (c), but you roll a pair of dice and take the sum of the two dice as the number x instead of spinning the wheel. Assume that you win the game if and only if you can move your token 10 steps or more with only 2 rolls or fewer, is your winning probability the same? If yes, **briefly explain** your answer. If no, please **identify** whether spinning wheel or rolling a pair of dice has a higher probability of winning and **briefly explain** your answer.

Solution: (a) $\frac{5+6+5+4+3+2+1}{36} = \frac{26}{36}$

(b) $E(5x) = 5E(x) = 5\frac{2+3+4+5+6+7+8+9+10+11+12}{11} = 35$

(c) $P(\text{Win}) = P(\text{Win with one spin only}) + P(\text{Win with exactly two spins})$

Win with one spin only: The first spin has to be 10, 11, or 12.

$$P(\text{Win with one spin only}) = \frac{3}{11}$$

Win with exactly two spins: The first spin is s where s can be 2 to 9. The second spin has to be at least $10 - s$. If $s = 2$, the second spin can be 8, 9, 10, 11, 12; if $s = 3$, the second spin can be 7, 8, 9, 10, 11, 12, etc.

$$\begin{aligned} P(\text{Win with exactly two spins}) &= \sum_{s=2}^{8}(\frac{1}{11})(\frac{s+3}{11}) + \frac{1}{11}\cdot\frac{11}{11} \\ &= \frac{67}{121} \\ P(\text{Win}) &= \frac{100}{121} \end{aligned}$$

(d) The probability is not the same. For spinning wheel, it is more likely to get a small number than rolling a pair of dice despite the fact that the expected value of the spinning wheel is the same as rolling a pair of dice. Therefore, it is more likely to lose the game with the spinning wheel.

$P(\text{Win}) = P(\text{Win with one roll only}) + P(\text{Win with exactly two rolls})$
Win with one roll only: The first roll has to be 10, 11, or 12.

$$P(\text{Win with one roll only}) = \frac{3+2+1}{36}$$

Win with exactly two rolls: The first roll is s where s can be 2 to 9. The second roll has to be at least $10-s$. If $s=2$, the second roll can be 8, 9, 10, 11, 12; if $s=3$, the second roll can be 7, 8, 9, 10, 11, 12, etc.

$$P(\text{Win with exactly two rolls}) = \sum_{s=2}^{9} P(s) \sum_{t=10-s}^{12} P(t)$$

Formulate the table for different s.

s	2	3	4	5	6	7	8	9
$P(s)$	1/36	2/36	3/36	4/36	5/36	6/36	5/36	4/36
$\sum_{t=10-s}^{12} P(t)$	15/36	21/36	26/36	30/36	33/36	35/36	36/36	36/36

Thus, we have

$$\begin{aligned} P(\text{Win with exactly two rolls}) &= \frac{15+42+78+120+165+210+180+144}{36\cdot 36} \\ &= \frac{53}{72} \\ P(\text{Win}) &= \frac{53+12}{72} = \frac{65}{72} \end{aligned}$$

Thus, rolling a pair of dice is a better choice.

Suggested Marking: 2-2-4-5. Part does not require the detailed evaluation of the probability. Any valid explanation is acceptable.

Seat Number: ____________

Problem 2: [12 pts] Assume that $f(x)$ is a linear function in the form of $f(x) = ax + b$ where a and b are real numbers. Let n be a random variable with mean m and variance v. Expressing the following in terms of a, b, m, v and some constants. **Show your steps**.

(a) Variance of $f(n)$.

(b) Expectation of $f(n^2)$.

(c) Expectation of $f(n)^2$.

(d) Expectation of $f(n)f(p)$, if p is another random variable that is independent of n and has the same distribution as n.

Solution: Assume that S is the sample space of n.

(a) Variance of $f(n)$, first need to find $E(f(n))$. By the linearity of expectation, $E(f(n)) = am + b$.

$$\begin{aligned} Var(f(n)) &= \sum_{x:x\in S} p(x)(ax + b - E(f(n))^2 \\ &= \sum_{x:x\in S} p(x)(ax + b - am - b)^2 \\ &= \sum_{x:x\in S} p(x)a^2(x - m)^2 \\ &= a^2 \sum_{x:x\in S} p(x)(x - m)^2 = a^2 v. \end{aligned}$$

(b) Expectation of $f(n^2)$:

$$\begin{aligned} E(f(n^2)) &= \sum_{x:x\in S} p(x)(ax^2 + b) \\ &= a \sum_{x:x\in S} p(x) \cdot x^2 + \sum_{x:x\in S} p(x) \cdot b \\ &= a \sum_{x:x\in S} p(x) \cdot x^2 + b \\ v = Var(n) &= (\sum_{x:x\in S} p(x)x^2) - m^2 \\ E(f(n^2)) &= a(v + m^2) + b \end{aligned}$$

(c) Expectation of $f(n)^2$:

$$\begin{aligned} E(f(n)^2) &= \sum_{x:x\in S} p(x)(ax+b)^2 \\ &= \sum_{x:x\in S} p(x)(a^2x^2+2abx+b^2) \\ &= a^2(v+m^2)+2abm+b^2 \end{aligned}$$

(d) By expected product of independent random variables, mean of $f(n)f(p) = E(f(n))E(f(p))$. Thus,

$$\begin{aligned} E(f(n)f(p)) &= E(f(n))E(f(p)) \\ &= E(f(n))E(f(n)) \\ &= (am+b)^2 \end{aligned}$$

Suggested Marking: 3 pts each. Missing steps -1 pt for each part.

Problem 3: [15 pts] A bag contains two dice. One dice is a normal six-sided fair dice, while the other is a special dice also with six sides where each of the 4 sides shows one dot and each of the remaining 2 sides shows two dots. Each side of both dice is equally likely to be on top when the corresponding dice is rolled. One of the dice is picked from the bag at random (i.e., the event that the fair dice is picked and the event that the special dice is picked are equally likely to occur), and this dice is rolled 2 times. Let A_1 be the event that the number of dots on top is smaller than or equal to two dots on the first roll, and A_2 be the event that the number of dots on top is smaller than or equal to two dots on the second roll. We denote the complement of A_1 and the complement of A_2 by $\bar{A}_1$ and $\bar{A}_2$, respectively.

(a) What is $P(A_1)$ and $P(A_2)$?

(b) What is $P(A_2|A_1)$?

(c) What is $P(A_1 \cup A_2)$?

(d) What is $P(\bar{A}_1 \cap \bar{A}_2)$?

(e) Are A_1 and A_2 independent? Explain your answer.

Solution: (a) If a fair dice is picked, the probability that we get one or two dots on top is $\frac{1}{3}$. If a special dice is picked, the probability that we get one or two dots on top is 1. Therefore, $P(A_1) = \frac{1}{2} \cdot \frac{1}{3} + \frac{1}{2} \cdot 1 = \frac{2}{3}$. By the same argument, $P(A_2) = \frac{2}{3}$.

(b)

$$\begin{aligned} P(A_2|A_1) &= \frac{P(A_2 \cap A_1)}{P(A_1)} \\ &= \frac{\frac{1}{2} \cdot \frac{1}{3} \cdot \frac{1}{3} + \frac{1}{2} \cdot 1 \cdot 1}{\frac{2}{3}} \\ &= \frac{\frac{1}{18} + \frac{1}{2}}{\frac{2}{3}} \\ &= \frac{30}{36} = \frac{5}{6} \end{aligned}$$

(c) By the principle of the inclusion-exclusion, we have

$$\begin{aligned} P(A_1 \cup A_2) &= P(A_1) + P(A_2) - P(A_1 \cap A_2) \\ &= \frac{2}{3} + \frac{2}{3} - \frac{5}{9} \\ &= \frac{12}{9} - \frac{5}{9} = \frac{7}{9} \end{aligned}$$

(d) $\bar{A}_1 \cap \bar{A}_2$ is just the complement of $A_1 \cup A_2$, so the answer is $1 - \frac{7}{9} = \frac{2}{9}$.

(e) No, A_1 and A_2 are dependent because $P(A_2|A_1) \neq P(A_2)$.

Suggested Marking: 3 pts each.

Problem 4: [15 pts]

(a) Evaluate $6^{1161} \mod 602$.

(b) Is each of the following true? Please explain.

(i) Is "$(178^{88} \mod 89) = [(401^{3,243,554} + 1,197,491) \mod 97]$"?

(ii) Is "$(21^{70} \mod 71) = (21^{71} \mod 72)$"?

Solution: *(a)*

$$\lfloor \log_2 1161 \rfloor = 10$$

$R_1 = 6^2 \mod 602 = 6 \times 6 \mod 602 = 36$
$R_2 = 6^4 \mod 602 = R_1 \times R_1 \mod 602 = 92$
$R_3 = 6^8 \mod 602 = R_2 \times R_2 \mod 602 = 36$
$R_4 = 6^{16} \mod 602 = R_3 \times R_3 \mod 602 = 92$
$R_5 = 6^{32} \mod 602 = R_4 \times R_4 \mod 602 = 36$
$R_6 = 6^{64} \mod 602 = R_5 \times R_5 \mod 602 = 92$
$R_7 = 6^{128} \mod 602 = R_6 \times R_6 \mod 602 = 36$
$R_8 = 6^{256} \mod 602 = R_7 \times R_7 \mod 602 = 92$
$R_9 = 6^{512} \mod 602 = R_8 \times R_8 \mod 602 = 36$
$R_{10} = 6^{1024} \mod 602 = R_9 \times R_9 \mod 602 = 92$

$$\begin{aligned} 6^{1161} \mod 602 &= 6^{1024+128+8+1} \mod 602 \\ &= 6^{1024} \cdot 6^{128} \cdot 6^{8} \cdot 6^{1} \mod 602 \\ &= 92 \cdot 36 \cdot 36 \cdot 6 \mod 602 \\ &= 216 \end{aligned}$$

(b) *(i) No.*

Consider LHS.

$$\begin{aligned} 178^{88} \mod 89 &= (178 \mod 89)^{88} \mod 89 \\ &= 0^{88} \mod 89 \\ &= 0 \end{aligned}$$

Consider RHS.

$$\begin{aligned} & (401^{3,243,554} + 1,197,491) \mod 97 \\ = & [((401 \mod 97)^{3,243,554} \mod 97) + (1,197,491 \mod 97)] \mod 97 \\ = & [(13^{3,243,554} \mod 97) + 26] \mod 97 \\ = & [(13^{3,243,554 \mod (97-1)} \mod 97) + 26] \mod 97 \\ & \textit{(By Fermat's Little Theorem)} \\ = & [(13^{2} \mod 97) + 26] \mod 97 \\ = & (72 + 26) \mod 97 \\ = & 1 \end{aligned}$$

Thus, LHS is not equal to RHS.

(ii) *No.*
Consider LHS. We have

$$21^{70} \mod 71 = 1$$

Consider RHS $= 21^{71} \mod 72$*.*
By Euclid's Division Theorem, the above expression could be written as follows.

$$21^{71} = 72q + r$$

where q and r are two unique integers.
Note that $r = 21^{71} \mod 72$*. Thus,*

$$\begin{aligned} 21^{71} &= 72q + (21^{71} \mod 72) \\ 21^{71} \mod 72 &= 21^{71} - 72q \\ &= 3(7 \cdot 21^{70} - 24q) \end{aligned}$$

which is divisible by 3. Thus, RHS is divisible by 3.
Note that LHS is equal to 1 which is not divisible by 3.
Thus, LHS is not equal to RHS.

Suggested Marking:
(a) 5 pts
(b) 10 pts

Problem 5: [10 pts] Consider the RSA cryptosystem where the public key is represented in the form of (e, n). We know that the public key of Raymond is $(7, 247)$ and the public key of Kenneth is $(13, 187)$.

(a) Is it possible to find the secret key of Raymond and the secret key of Kenneth? If yes, please find the two secret keys. If no, please explain the reason.

(b) Suppose that Kenneth wants to send an encrypted message to Raymond. The message is represented by a number 20. What is the value of the encrypted message? Please show your steps.

Solution: *(a) Yes.*
Consider Raymond's case.
Note that $13 \times 19 = 247$.
Thus, $p = 13$ *and* $q = 19$.
So, $T = (13-1)(19-1) = 12 \times 18 = 216$
Secret key of Raymond = the multiplicative inverse of 7 *in* Z_{216} *= 31*

Consider Kenneth's case.
Note that $11 \times 17 = 187$.
Thus, $p = 11$ *and* $q = 17$.
So, $T = (11-1)(17-1) = 10 \times 16 = 160$
Secret key of Kenneth = the multiplicative inverse of 13 *in* Z_{160} *= 37*

(b) Since the encrypted message is sent to Raymond, we should use the public key of Raymond for encryption.

$$\begin{aligned} \textit{The encrypted message} &= 20^7 \mod 247 \\ &= 1280000000 \mod 247 \\ &= 58 \end{aligned}$$

Suggested Marking:
(a) 7 pts
(b) 3 pts

Problem 6: [15 pts]

(a) Consider the following two modular equations.

$$\begin{aligned} x \bmod 990 &= 733 \\ x \bmod 693 &= 40 \end{aligned}$$

Does there exist a solution for $x \in Z_{3000}$ such that x satisfies the above two modular equations? If yes, please give all possible solutions in Z_{3000} and show your steps. If no, please explain why there is no solution in Z_{3000}.

(b) Consider the following two modular equations.

$$\begin{aligned} x \bmod 991 &= 752 \\ x \bmod 997 &= 40 \end{aligned}$$

Does there exist a solution for $x \in Z_{3000}$ such that x satisfies the above two modular equations? If yes, please give all possible solutions in Z_{3000} and show your steps. If no, please explain why there is no solution in Z_{3000}.

Solution: *(a) Yes.*

Based on the two modular equations, we express them as follows.

$$\begin{aligned} x &= 990q_1 + 733 \text{..........(*)} \\ x &= 693q_2 + 40 \text{..........(**)} \end{aligned}$$

where q_1 and q_2 are two integers.

We derive as follows.

$$\begin{aligned} 990q_1 + 733 &= 693q_2 + 40 \\ 693 &= 693q_2 - 990q_1 \\ 99 \cdot 7 &= 99 \cdot 7q_2 - 99 \cdot 10q_1 \\ 7 &= 7q_2 - 10q_1 \\ 7q_2 &= 7 + 10q_1 \\ q_2 &= 1 + \frac{10}{7}q_1 \end{aligned}$$

Since both q_1 and q_2 are integers, we derive that q_1 is a multiple of 7.

Consider (*).

When $q_1 = 0$, $x = 990 \cdot 0 + 733 = 733$.

Thus, all solution in Z_{3000} is 733.

(b) No.

Since $gcd(991, 997) = 1$, by Chinese Reminder Theorem, we know that *there exists a unique solution in* Z_{988027} *where* $988027 = 991 \times 997$. *However, this unique solution in* Z_{988027} *is equal to 447,693 which is greater than or equal to 3000.*

By Euclid's Extended GCD algorithm, we derive the following.

$$991(166) + 997(-165) = 1$$

The multiplicative inverse of 991 in Z_{997} *is* $166 \mod 997 = 166$.

The multiplicative inverse of 997 in Z_{991} *is* $-165 \mod 991 = 826$.

Construct $y = 752 \cdot 997 \cdot 826 + 40 \cdot 991 \cdot 166 = 625868784$.

The unique solution x *in* Z_{988027} *is* $625868784 \mod 988027 = 447,693$, *which is greater than or equal to 3000. Thus, there is no solution in* Z_{3000}.

Suggested Marking:
(a) 8 pts
(b) 7 pts

Question 7: [10 pts] Assume that a party of n people wants to select some of their members to form a committee. The committee must have at least one member. Let $T(n)$ be the total number of possible committees that can be formed from a party of n people.

(a) Define $T(n)$ as a recurrence equation, and prove that your recurrence equation is correct by induction.

(b) Iterate the recurrence equation $T(n)$ in part (a) to obtain a closed form solution.

(c) Prove that the closed form solution in part (b) is correct by induction.

Solution: (a) $T(1) = 1$, and $T(n) = 2T(n-1) + 1$ for $n > 1$.

The base case $T(1)$ is obviously true.

Assume that $T(n-1)$ counts the number of committees that are formed from $n-1$ people correctly for $n > 1$.

When there are n people, the number of possible committees that are formed without the n-th person is counted by $T(n-1)$. On the other hand, each committee without the n-th person union with the n-th person forms another possible committee. So, we have $2T(n-1)$ possible committees. There is only one case is missed, which is the committee that contains only the n-th person. Therefore, when there are n people, $T(n) = 2T(n-1)+1$ counts all possible committees with at least one member from n people. By the principle of induction, we have proved that the recurrence equation is correct.

(b)

$$\begin{aligned}
T(n) &= 2T(n-1) + 1 \\
&= 2^2T(n-2) + 2 + 1 \\
&= 2^3T(n-3) + 2^2 + 2 + 1 \\
&\vdots \\
&= 2^{n-1}T(1) + 2^{n-2} + \cdots + 2^1 + 2^0 \\
&= 2^{n-1} + 2^{n-2} + \cdots + 2^1 + 2^0 \\
&= 2^n - 1
\end{aligned}$$

(c) Base case ($n = 1$): $T(1) = 1 = 2^1 - 1$, so the base case is true.

Assume that $T(n-1) = 2^{n-1} - 1$ is true for $n > 1$,

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

By the principle of mathematical induction, we have proved that $T(n) = 2^n - 1$ is true for $n \geq 1$.

Suggested Marking: 4-3-3 pts.

Problem 8: [10 pts] For this problem, you may assume that n is a non-negative power of 3. Suppose that function $T(n)$ satisfies $T(1) = 7$ and, for $n > 1$,

$$T(n) \leq 9T(\frac{n}{3}) + 5n$$

Prove that $T(n) = O(n^2)$ by advanced induction.

Solution: *We want to prove that $T(n) = O(n^2)$.*

By the definition of big O, we need to show the following.

$$\exists n_0 \in Z \text{ and } k_1, k_2 \in R \text{ such that } \forall n > n_0, T(n) \leq k_1 n^2 - k_2 n$$

Suppose that $n > n_0$.

Let $P(n)$ be "$T(n) \leq k_1 n^2 - k_2 n$".

Consider $P(1)$. We want to see whether $P(1)$ is true. That is, we want to show that $T(1) \leq k_1 \cdot 1^2 - k_2 \cdot 1$......(*).

Consider the RHS of (*). It is equal to $k_1 \cdot 1^2 - k_2 \cdot 1 = k_1 - k_2$.

In other words, according to (*), we need to prove

$$T(1) \leq k_1 - k_2$$

Currently, we do not know the values of k_1 and k_2. In order to prove $T(1) \leq k_1 - k_2$, we should set the values of k_1 and k_2 such that

$$k_1 - k_2 \geq T(1)$$

That is,

$$k_1 - k_2 \geq 7$$

Thus, $P(1)$ is true. Thus, we guess that n can be $1, 3^1, 3^2, ...,$. Since $n > n_0$, we have "$n_0 \geq 0$".

Thus, we guess that $P(1), P(3^1), P(3^2), ...$ are also true. The base case is when $n = 1$.

Next, we want to show that "$P(n/3) \Rightarrow P(n)$" is true for all $n > 1$.

Assume that $P(n/3)$ is true for $n > 1$. That is, $T(n/3) \leq k_1(n/3)^2 - k_2(n/3)$.

Next, we want to show that $P(n)$ is true.

Consider

$$\begin{aligned}
T(n) &\le 9T(\frac{n}{3}) + 5n \\
&\le 9 \cdot (k_1(n/3)^2 - k_2(n/3)) + 5n \\
&= 9 \cdot (k_1 n^2/9 - k_2 n/3) + 5n \\
&= k_1 n^2 - 3k_2 n + 5n \\
&= k_1 n^2 - k_2 n - 2k_2 n + 5n \\
&= k_1 n^2 - k_2 n + (5 - 2k_2)n
\end{aligned}$$

Currently, we don't know the value of k_1 *and the value of* k_2*.*

In order to prove $T(n) \le k_1 n^2 - k_2 n$*, we should set a value of* k_1 *and a value of* k_2 *such that*

$$5 - 2k_2 \le 0$$

We deduce that

$$k_2 \ge 5/2$$

Thus, $P(n)$ *is true.*

We prove that "$P(n/3) \Rightarrow P(n)$*" is true for all* $n > 1$*. By Mathematical Induction,* $\forall n \ge 1, T(n) \le k_1 n^2 - k_2 n$*.*

We should set some values for n_0, k_1, k_2*.*

Since $n_0 \ge 0$*, we set* $n_0 = 0$*.*

Since $k_2 \ge 5/2$*, we set* $k_2 = 5/2$*.*

Since $k_1 - k_2 \ge 7$ *(i.e.,* $k_1 \ge 7 + k_2$*), we set* $k_1 = 7 + 5/2 = 19/2$*.*

Suggested Marking:
10 pts

Seat Number: ____________

[SCRAP PAPER]

Seat Number: ____________

[SCRAP PAPER]

Seat Number: ____________

[SCRAP PAPER]