CS70 Discrete Mathematics and Probability Theory, Fall 2019

Midterm 1

7:00-9:00pm, 7 October

Your First Name: **Your Last Name:**

SIGN Your Name: **Your SID Number:**

Your Exam Room:

Name of Person Sitting on Your Left:

Name of Person Sitting on Your Right:

Name of Person Sitting in Front of You:

Name of Person Sitting Behind You:

Instructions:

(a) As soon as the exam starts, please write your student ID in the space provided at the top of every page! (We will remove the staple when scanning your exam.)

(b) There are **6 double-sided** *sheets (12 numbered pages) on the exam. Notify a proctor immediately if a sheet is missing.*

(c) We will not grade anything outside of the space provided for a question (i.e., either a designated box if it is provided, or otherwise the white space immediately below the question). **Be sure to write your full answer in the box or space provided!** *Scratch paper is provided on request; however, please bear in mind that nothing you write on scratch paper will be graded!*

(d) The questions vary in difficulty, so if you get stuck on any question it may help to leave it and return to it later.

(e) On questions 1-2, you need only give the answer in the format requested (e.g., True/False, an expression, a statement.) An expression may simply be a number or an expression with a relevant variable in it. For short answer questions, correct, clearly identified answers will receive full credit with no justification. Incorrect answers may receive partial credit.

(f) On questions 3-6, you should give arguments, proofs or clear descriptions if requested. If there is a box you must use it for your answer: answers written outside the box may not be graded!

(g) You may consult one two-sided "cheat sheet" of notes. Apart from that, you may not look at any other materials. Calculators, phones, computers, and other electronic devices are NOT permitted.

(h) You may use, without proof, theorems and lemmas that were proved in the notes and/or in lecture.

(i) You have 120 minutes: there are 6 questions on this exam worth a total of 140 points.

[exam starts on next page]

1. True/False [*No justification; answer by shading the correct bubble. 2 points per answer; total of 36 points. No penalty for incorrect answers.*]

(a) Which of the following is a valid logical equivalence, for arbitrary propositions P, Q, R? Answer **YES** (for valid) or **NO** (for not valid) by shading the appropriate bubble.

YES	NO		
●	○	$(P \implies \neg Q) \equiv \neg(P \wedge Q)$	*2pts*
●	○	$((P \wedge Q) \implies R) \equiv (Q \implies (\neg P \vee R))$	*2pts*
○	●	$((P \implies R) \wedge (Q \implies R)) \equiv ((P \wedge Q) \implies R)$	*2pts*

(b) Indicate which of the following quantified statements is **TRUE** or **FALSE** by shading the appropriate bubble.

TRUE	FALSE		
○	●	$(\forall a, b \in \mathbb{N})(\exists c \in \mathbb{N})((a < b) \Rightarrow (a < c < b))$.	*2pts*
●	○	$\neg(\exists a, b \in \mathbb{N})(\sqrt{2} = \frac{a}{b})$.	*2pts*
●	○	$(\forall n \in \mathbb{N})(\exists m \in \mathbb{N})((m > n) \wedge \neg(\exists a, b \in \mathbb{N})((a > 1) \wedge (b > 1) \wedge (m = ab)))$.	*2pts*
○	●	$(\forall x, y, z \in \mathbb{Z})((x \leq y) \Rightarrow (xz \leq yz))$.	*2pts*

(c) Which of the following are valid proof strategies? Answer **YES** (for valid) or **NO** (for not valid) by shading the appropriate bubble.

YES	NO		
○	●	$P(0), P(1)$ and $P(2)$ hold, and $(\forall k \geq 2)(P(k) \Rightarrow P(k+2))$ holds. Hence $P(n)$ holds for all $n \in \mathbb{N}$.	*2pts*
●	○	$P(0)$ holds and for all $k \in \mathbb{N}$ the following two implications hold: $P(k) \Rightarrow P(2k)$; $P(2k) \Rightarrow P(2k+1)$. Hence $P(n)$ holds for all $n \in \mathbb{N}$.	*2pts*
●	○	$P(0)$ holds and for all $k \in \mathbb{N}$ the following three implications hold: $P(2k) \Rightarrow P(2k+1)$; $P(-2k+1) \Rightarrow P(-2k)$; and $P(k) \Leftrightarrow P(-k)$. Hence $P(n)$ holds for all $n \in \mathbb{Z}$.	*2pts*

[Q1 continued on next page]

(d) Answer each of the following questions **TRUE** or **FALSE** by shading the appropriate bubble.

TRUE	**FALSE**		
●	○	In a stable marriage instance, if a woman W is the least favorite in every man's preference list, then changing W's preference list cannot change the pairing output by the traditional Stable Marriage Algorithm.	*2pts*
●	○	In a stable marriage instance, if a man M is the least favorite in every woman's preference list, then changing M's preference list cannot change the pairing output by the traditional Stable Marriage Algorithm.	*2pts*
●	○	Every planar drawing of a graph G has the same number of faces.	*2pts*
●	○	If a graph has 10 vertices and 25 edges, then it cannot be planar.	*2pts*
○	●	Every tree with at least four vertices must have at least three leaves.	*2pts*
●	○	Any two longest (simple) paths in a connected, undirected graph must have at least one vertex in common.	*2pts*
●	○	The equation $5x \equiv 15 \pmod{93}$ has a unique solution for x modulo 93.	*2pts*
○	●	The equation $3x \equiv 18 \pmod{93}$ has a unique solution for x modulo 93.	*2pts*

[exam continued on next page]

2. Short Answers [*Answer is a single number or expression; write it in the box provided; no justification necessary. 3 points per answer; total of 36 points. No penalty for incorrect answers.*]

(a) Alice, Bob and Carol are called to give statements about a crime. Alice says: "Bob is guilty." Bob and Carol also give statements. Afterwards one and only one of the suspects is found guilty. The detective notes that the guilty suspect always told the truth while the other two only told lies. Which suspect is guilty? *3pts*

Carol. [Alice's statement cannot be true, since if it were then she would be guilty, which would imply Bob is not guilty, contradicting her statement. So Alice's statement is false, implying that she is not guilty and also that Bob is not guilty. This leaves Carol as the only possible guilty person.]

(b) In a sports competition, athletes from San Francisco, Los Angeles and San Diego are chosen to be part of three teams, A, B and C. Each athlete is in exactly one team. What is the minimum total number of athletes needed to ensure that there is some team containing at least 5 athletes from the same city? *3pts*

37. [The number of city-team pairs is $3 \times 3 = 9$. View these as 9 boxes. As in the proof of the pigeonhole principle, if each box contains at most 4 athletes, there can be at most 36 athletes total.]

(c) Let K_n be the complete graph on n vertices. What is the minimum number of edges that must be removed from K_n to make it disconnected? *3pts*

$n - 1$. [If we remove all $n - 1$ edges incident on any particular vertex, we will disconnect that vertex from the graph. We can't disconnect the graph by removing fewer edges, because the number of edges connecting any set of k vertices to the rest of the graph is $k(n-k)$, which is minimized when $k = 1$.]

(d) Let H_n be the n-dimensional hypercube. What is the minimum number of colors needed to color the *edges* of H_n so that no two adjacent edges receive the same color? *3pts*

n. [Each vertex has n edges incident on it, so clearly we need at least n colors. We can achieve n colors by coloring all the edges along each dimension (none of which touch each other) with the same color.]

(e) Let 0010100 and 1001110 be the bit representations of two vertices in the 7-dimensional hypercube. What is the length of a shortest path between these two vertices? *3pts*

4. [The length of a shortest path is equal to the number of positions in which the two binary strings differ.]

(f) Solve the equation $4x \equiv 7 \pmod{11}$ for x. Your answer should be an integer in $\{0, 1, \ldots, 10\}$. *3pts*

10. [The inverse of 4 (mod 11) is 3; multiplying both sides of the equation by 3 gives $x \equiv 21 \equiv 10 \pmod{11}$.]

[Q2 continued on next page]

(g) Compute $10^{11^{12^{13}}} \pmod{11}$. Your answer should be an integer in $\{0, 1, \ldots, 10\}$. *3pts*

10. [Note that $10 \equiv -1 \pmod{11}$. Furthermore the exponent $11^{12^{13}}$, being a power of 11, is odd. Hence the expression is $-1 \equiv 10 \pmod{11}$.]

(h) Compute $1^{16}+2^{16}+\cdots+99^{16}+100^{16} \pmod{17}$. Your answer should be an integer in $\{0, 1, \ldots, 16\}$. *3pts*

10. [By Fermat's Little Theorem, $a^{16} \equiv 1 \pmod{17}$ for all $a \not\equiv 0 \pmod{17}$. Hence all the terms in the sum (mod 17) are 1, except for the ones corresponding to multiples of 17, namely 17, 34, 51, 68, 85, which are all zero. Thus the sum is $100 - 5 = 95 \equiv 10 \pmod{17}$.]

(i) Let n be a positive integer. What is $\gcd(4n^2 + 1, 2n + 1)$? *3pts*

1. [Note that $4n^2 + 1 = (2n - 1)(2n + 1) + 2$, so $\gcd(4n^2 + 1, 2n + 1) = \gcd(2n + 1, 2)$. But this last gcd is 1 since $2n + 1$ is odd.]

(j) Find $\gcd(476, 153)$. *3pts*

17. [Using Euclid's algorithm: $\gcd(476, 153) = \gcd(153, 17) = \gcd(17, 0) = 17$.]

(k) Find the inverse of 24 mod 53. Your answer should be an integer in $\{0, 1, \ldots, 52\}$. *3pts*

42. [The sequence of recursive calls to the extended Euclidean algorithm is: $(53, 24) \to (24, 5) \to (5, 4) \to (4, 1) \to (1, 0)$. The corresponding sequence of returned triples is: $(1, 1, 0) \to (1, 0, 1) \to (1, 1, -1) \to (1, -1, 5) \to (1, 5, -11)$. Hence the inverse is $-11 \equiv 42 \pmod{53}$.]

(l) Bob sets up an RSA scheme based on primes $p = 5$, $q = 11$ and exponent $e = 3$. Alice wants to send Bob the message 20 (viewed as an integer mod 55). What is the encrypted message that Alice sends to Bob? *3pts*

25. [Alice's message is $20^3 \pmod{55}$, which we can compute as follows: $20^3 = 400 \times 20 \equiv 15 \times 20 = 300 \equiv 25 \pmod{55}$.]

[exam continued on next page]

3. Proofs [*All parts to be justified. Total of 20 points.*]

(a) Let a be a natural number. Prove that if $a^2 - 3a + 1$ is even then a is odd. *4pts*

Proof by contraposition: we prove that if a is even then $a^2 - 3a + 1$ is odd.
Suppose a is even, so $a = 2k$ for some $k \in \mathbb{Z}$. Then $a^2 - 3a + 1 = 4k^2 - 6k + 1 = 2(2k^2 - 3k) + 1$, which is odd.
[Incidentally, notice that in fact $a^2 - 3a + 1$ cannot be even for any a: this is because $a^2 - 3a + 1 = a(a-3)+1$, and $a(a-3)$ is always even because the parity of $a-3$ is opposite to that of a. Therefore the original claim is actually vacuously true!]

(b) Prove that $\sqrt{ab} \leq \frac{a+b}{2}$ for all positive real numbers a, b. *4pts*

Direct proof. The claim is equivalent to showing that $\frac{a+b}{2} - \sqrt{ab} \geq 0$. Let us write

$$\tfrac{a+b}{2} - \sqrt{ab} = \tfrac{1}{2}(a + b - 2\sqrt{ab}) = \tfrac{1}{2}(\sqrt{a} - \sqrt{b})^2 \geq 0,$$

where in the last step we used the fact that the square of any number is non-negative.

(c) Prove that there do not exist integers m, n such that $m^2 + 4n + 1 = 0$. *5pts*

Proof by contradiction. Suppose such integers m, n exist. Since $m^2 = -(4n + 1)$ is odd, m must be odd, so we can write $m = 2k + 1$ for some $k \in \mathbb{Z}$.
The equality can now be written $(2k + 1)^2 + 4n + 1 = 0$, or equivalently, expanding the square: $4k^2 + 4k + 4n + 2 = 0$. But this is of the form $4\ell = 2$ for some integer ℓ, which is not possible since 4ℓ is divisible by 4 but 2 is not. Contradiction.

(d) Prove by induction that, for all natural numbers n, $2^{3n+1} + 5$ is divisible by 7. *7pts*

Base case ($n = 0$)**:** The claim is that $2^1 + 5 = 7$ is divisible by 7, which is obviously true.
Inductive step: Assume for some arbitrary $k \geq 0$ that $7 \mid (2^{3k+1} + 5)$ (induction hypothesis). We need to prove that $7 \mid (2^{3(k+1)+1} + 5)$.
Now $2^{3(k+1)+1} + 5 = 8 \cdot 2^{3k+1} + 5 = 8(2^{3k+1} + 5) - 35$. The first term here is divisible by 7 by the induction hypothesis, and the second term (35) is obviously divisible by 7; hence their difference is also divisible by 7. Thus indeed $7 \mid (2^{3(k+1)+1} + 5)$, as required.
Hence the statement is true for all $n \in \mathbb{N}$ by induction.

[exam continued on next page]

4. Stable Marriage [*All parts to be justified unless otherwise stated. Total of 18 points.*]
Consider the following preference lists for three men 1, 2, 3, and three women A, B, C.

Man	Women		
1	A	B	C
2	B	A	C
3	B	C	A

Woman	Men		
A	3	2	1
B	1	2	3
C	2	3	1

(a) Find the female-optimal pairing. Write your answer in the boxes provided; no justification is needed. *3pts*

Man 1 is paired with: B Man 2 is paired with: C Man 3 is paired with: A

[This can just be read off from the women's preference lists: since the three women all have different first-choice men, giving each one her first choice is a stable pairing and obviously no woman can do better than this.]

(b) Find the female-pessimal pairing. Write your answer in the boxes provided; no justification is needed. *3pts*

Man 1 is paired with: A Man 2 is paired with: B Man 3 is paired with: C

[Female-pessimal is equivalent to male-optimal, so we can just run the traditional SMA. It is easily checked that it yields the above pairing.]

(c) There is one other stable pairing, different from both the female-optimal and female-pessimal ones. What is this pairing? Write your answer in the boxes provided; no justification is needed. [Hint: Use parts (a) and (b) to narrow your search.] *4pts*

Man 1 is paired with: B Man 2 is paired with: A Man 3 is paired with: C

[Notice from parts (a) and (b) that, in any stable pairing, B can only get paired with 1 (optimal) or 2 (pessimal), and C only with 2 or 3. (A can get paired with anyone since her optimal is 3 and her pessimal is 1, the top and bottom of her list respectively.) If B is with 2 then C must be with 3, which is (b) above. If C is with 2 then B must be with 1, which is (a) above. The only other possibility is B with 1 and C with 3.]

(d) Suppose now that the women know all the preference lists, and wish to collude in order to achieve the female-optimal pairing you found in part (a), even though the traditional algorithm (in which the men propose) will be used. Prove that there is no way in which the women can jointly revise their preference lists so as to achieve this pairing. [Hint: Note that the men's lists remain fixed. You should answer this question *without* considering all possibilities for the womens' lists. You may use without proof any result you have seen in class or in the homeworks, provided you state it clearly.] *4pts*

Consider this from the point of view of the men. Note that, in the female-optimal pairing, two men (2 and 3) are paired with their least favorite woman. But we have seen in homework that this is not possible. [Although you were not required to supply a proof here, recall that the traditional SMA terminates as soon as the first man proposes to his least favorite woman, and this can happen for only one man.] Hence, regardless of the preference lists of the women, the traditional algorithm can never produce the female-optimal pairing.

[Q4 continued on next page]

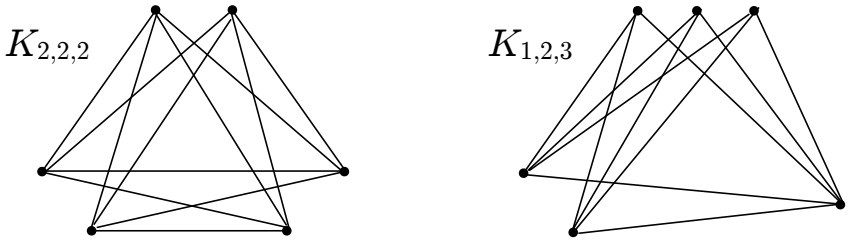
(e) Now suppose that the women are given the additional option of omitting some men from their preference lists altogether (i.e., a woman may rank only some of the men, declaring the others "unacceptable"). Suppose also that we again run the traditional (men-proposing) algorithm, except that a woman rejects all proposals from her unacceptable men (possibly leaving her with no man on a string). Explain how the women can now achieve the female-optimal pairing from part (a), and justify why this works. *4pts*

The women simply declare as unacceptable all men except for their respective optimal men. When the traditional SMA is run, each woman will reject all proposals until she receives one from her optimal man; this must happen eventually since no other woman will accept a proposal from that man. (Recall that no two women share the same optimal man, since the female-optimal pairing is a proper pairing.) Hence the algorithm will terminate with the female-optimal pairing. [Note, incidentally, that this strategy works for any instance of stable marriage; it is not specific to the example in this question.]

[exam continued on next page]

5. Complete Tripartite Graphs. [*All parts to be justified unless otherwise stated. Total of 18 points.*]

Let ℓ, m, n be positive integers with $\ell \leq m \leq n$. The complete tripartite graph $K_{\ell,m,n}$ consists of three disjoint groups of vertices, L, M, N, with $|L| = \ell$, $|M| = m$, and $|N| = n$. There are no edges between any two vertices in the same group, and there is one edge between every pair of vertices belonging to different groups. The figure below shows two examples: $K_{2,2,2}$ and $K_{1,2,3}$.



(a) How many *edges* are there in $K_{\ell,m,n}$? Write your answer as a function of ℓ, m, n in the box provided; no justification is needed. [Hint: Check your answer on the two examples above!] *3pts*

$\ell m + \ell n + mn$. [The number of edges between L and M is clearly ℓm. Similarly, there are ℓn and mn edges, respectively, between L and N, and between M and N.]

(b) For what values of ℓ, m, n does there exist an Eulerian tour in $K_{\ell,m,n}$? No justification is needed. *3pts*

ℓ, m, n are either all odd or all even. [The condition for existence of an Eulerian tour is that all vertex degrees are even. The degree of each vertex in L is $m + n$, of each vertex in M is $\ell + n$, and of each vertex in N is $\ell + m$. These are all even if and only if the parities of all of ℓ, m, n are equal.]

(c) Prove that $K_{\ell,m,n}$ does **not** have a Hamiltonian cycle if $n > \ell + m$. [Recall that a Hamiltonian cycle in a graph G is a cycle that visits every vertex of G exactly once.] *5pts*

Proof by contraposition. We show that if $K_{\ell,m,n}$ has a Hamiltonian cycle then $n \leq \ell + m$.
Since there are no edges within N, any Hamiltonian cycle must enter and leave N exactly n times (in order to visit all of its vertices). Each time the cycle leaves N, it must proceed to a vertex in $L \cup M$ that it has not yet visited (since the cycle cannot visit any vertex more than once). But the number of vertices in $L \cup M$ is $\ell + m$, so we must have $n \leq \ell + m$.

[Q5 continued on next page]

(d) It is known that $K_{2,2,2}$ is planar (even though this is not obvious from the above drawing). How many faces are there in any planar drawing of $K_{2,2,2}$? Write your answer in the box provided; no justification is needed. *2pts*

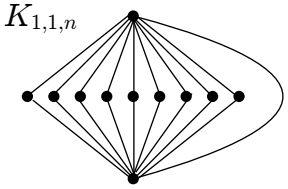
8. [$K_{2,2,2}$ has $v = 6$ vertices and $e = 12$ edges. By Euler's formula, the number of faces is $f = e - v + 2 = 8$.]

(e) For which values of ℓ, m, n is $K_{\ell,m,n}$ planar? Justify your answer. [Note: You may use the fact stated in part (d) that $K_{2,2,2}$ is planar.] *5pts*

Recall that $\ell \leq m \leq n$. We note first that if $n \geq 3$ and $\ell + m \geq 3$, then $K_{\ell,m,n}$ contains $K_{3,3}$ and hence is not bipartite. Hence in particular if $\ell \geq 3$ then the graph is not bipartite. We consider each of the remaining cases $\ell = 1, 2$.

Case 1: $\ell = 2$. Clearly if $m > 2$ or $n > 2$ then we have $K_{3,3}$, so the only possibility is $\ell = m = n = 2$. This is just $K_{2,2,2}$, which we are told is planar.

Case 2: $\ell = 1$. Again, if $m > 2$, or if $m = 2$ and $n \geq 3$, then we have $K_{3,3}$. So we only need to consider the possibilities $m = n = 2$ and $m = 1$. When $m = n = 2$ the graph is $K_{1,2,2}$, which is a subgraph of $K_{2,2,2}$ and hence also planar. When $m = 1$ the graph is $K_{1,1,n}$, which is easily seen to be planar as shown below.



To summarize: the only planar cases for (ℓ, m, n) are $(2, 2, 2)$, $(1, 2, 2)$ and $(1, 1, n)$ for any $n \geq 1$.

[exam continued on next page]

6. RSA [*All parts to be justified unless otherwise stated. Total of 12 pts.*]

Alice sends messages to Bob using his public key (N, e), where $N = pq$ is the product of two large primes, and $e = 3$. Eve (as usual) is listening in but is unable to decrypt any of the messages. One day, just for fun, Bob decides to share his private key, d, with Eve. Of course, this means that Eve is now able to decrypt all messages sent to Bob. However, Bob isn't too worried as he plans to change the value e in his public key to some other value e', reasoning that Eve won't be able to compute Bob's corresponding new private key d' because she still doesn't know p and q. In this problem, you are asked to show that Bob is mistaken, because in fact, using her knowledge of d, Eve can factor Bob's public key $N = pq$ and thus do anything Bob can do.

(a) Show that $3d - 1 = k(p-1)(q-1)$ for $k = 1$ or $k = 2$. *4pts*

By definition, $d = e^{-1} \pmod{(p-1)(q-1)}$. Since $e = 3$, we can write this as an integer equation $3d = k(p-1)(q-1) + 1$ for some integer k. Since $0 < d < (p-1)(q-1)$, the only possible values for k are $k = 1, 2$.

(b) How can Eve determine the value of k in part (a)? *4pts*

Suppose $k = 1$. Then $3d - 1 = (p-1)(q-1) < N$. Suppose $k = 2$. Then $3d - 1 = 2(p-1)(q-1) = N + pq - 2p - 2q + 2$, which is larger than N when p, q are large numbers, as we are told in the question. Hence Eve can simply test whether $3d - 1 < N$; if so she knows that $k = 1$, else $k = 2$.

[Incidentally, it turns out that in fact $k = 2$ always (though you were not expected to prove this). To see this, note that any prime $p > 3$ satisfies $p \equiv 1 \pmod 3$ or $p \equiv 2 \pmod 3$. Hence $(p-1)(q-1) \equiv 0 \pmod 3$ or $(p-1)(q-1) \equiv 1 \pmod 3$. Since $k(p-1)(q-1) + 1 = 3d \equiv 0 \pmod 3$, $k = 1$ is not possible.]

(c) Using parts (a) and (b), show how Eve can factor N efficiently. [Hint: You may want to give an explicit formula for p (or for q) in terms of N and d. Alternatively, you may write down equations that can be solved for p (or q).] *4pts*

From part (a), we have $k(p-1)(q-1) = 3d - 1$. Multiplying out, re-arranging, and writing $N = pq$, this gives us the equation

$$p + q = N + 1 - \tfrac{3d-1}{k}. \tag{1}$$

We also know that

$$pq = N. \tag{2}$$

Together, equations (1) and (2) are enough to determine the two unknowns, p and q, and hence to factor N. (Recall that we know the values of k, D and N, so they are just constants here.)

To see the solution explicitly, define $B := N + 1 - \frac{3d-1}{k}$, so that equation (1) becomes

$$p + q = B. \tag{3}$$

Multiplying equation (3) by p and substituting for pq from equation (2), we get

$$p^2 - pB + N = 0.$$

This is a quadratic equation in p which can be solved as usual. The two roots $\frac{B \pm \sqrt{B^2 - 4N}}{2}$ correspond to the values of p and q (since everything is symmetrical in p, q).

[End of Exam!]