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*

   (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*

   (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*

   (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*

   (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*

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

[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*

(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*

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

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

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

(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*

[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*

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

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

[Q3 continued on next page]

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

[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: □ Man 2 is paired with: □ Man 3 is paired with: □

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

Man 1 is paired with: □ Man 2 is paired with: □ Man 3 is paired with: □

(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: □ Man 2 is paired with: □ Man 3 is paired with: □

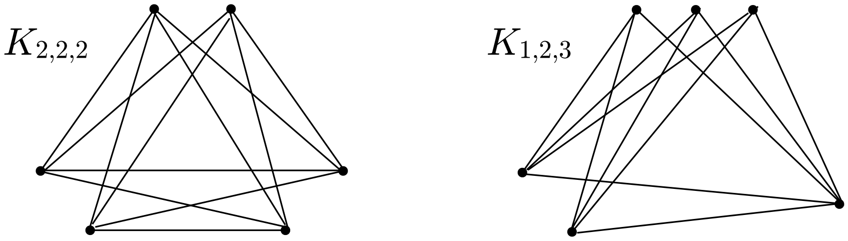
(d) Suppose now that the women know all the preference lists, and wish to collude in order to achieve the female-optimal pairing you found in part (a), even though the traditional algorithm (in which the men propose) will be used. Prove that there is no way in which the women can jointly revise their 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*

[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*

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*

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

(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*

[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*

□

(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*

[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*

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

(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*

[End of Exam!]