CS70 Discrete Mathematics and Probability Theory, Fall 2018

Midterm 1

8:00-10:00pm, 24 September

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, without proof, use theorems and lemmas that were proven in the notes and/or in lecture.

(i) You have 120 minutes: there are 6 questions on this exam worth a total of 135 points.

[exam starts on next page]

1. True/False [*No justification; answer by shading the correct bubble. 2 points per answer; total of 32 points. No penalty for incorrect answers.*]

(a) Let $P(x), Q(x)$ be propositions involving a natural number x. Suppose you are asked to prove that the following statement is FALSE: $(\forall x \in \mathbb{N})(P(x) \Rightarrow Q(x))$. Which of the following would constitute a valid proof strategy? Answer **YES** or **NO** for each by shading the appropriate bubble.

YES	NO		
●	○	Find some x for which $P(x)$ holds and $Q(x)$ does not hold.	*2pts*
○	●	Find some x for which both $P(x)$ and $Q(x)$ hold.	*2pts*
○	●	Show that $P(x)$ holds for all x.	*2pts*
●	○	Show that $Q(x)$ doesn't hold for any x, and find some x for which $P(x)$ holds.	*2pts*
○	●	Show that $Q(x)$ holds for all x, and find some x for which $P(x)$ doesn't hold.	*2pts*

(b) The following True/False questions concern the stable marriage problem. The term "traditional SMA" denotes the propose-and-reject algorithm described in class, in which men propose to women. Answer **TRUE** or **FALSE** for each by shading the appropriate bubble.

TRUE	FALSE		
●	○	A non-stable pairing can have more than one rogue couple.	*2pts*
○	●	For every problem instance, there exist at least two distinct stable pairings.	*2pts*
●	○	In the man-optimal stable pairing, it is possible for a man to be paired with his least favorite woman.	*2pts*
○	●	In the man-optimal stable pairing, it is possible for two men to be paired with their least favorite women.	*2pts*
○	●	If man M and woman W are each other's respective least favorite choices, then M cannot be matched with W in any stable pairing.	*2pts*
○	●	If the traditional SMA terminates after exactly k days on a given instance, then the women-optimal SMA (in which the women propose to the men) also terminates after exactly k days on the same instance.	*2pts*

[Q1 continued on next page]

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

TRUE	**FALSE**		
●	○	Every hypercube is bipartite.	*2pts*
○	●	A 10-dimensional hypercube has a cycle of length 5.	*2pts*
●	○	The complete bipartite graph $K_{2,n}$ is planar for every n. [Recall that, for integers $m, n \geq 1$, $K_{m,n}$ is the bipartite graph with m vertices in one part, n in the other part, and all possible edges between the two parts.]	*2pts*
●	○	For any integer a, the equation $3x \equiv a \pmod{101}$ always has a solution for x.	*2pts*
○	●	For any integer a, the equation $3x \equiv a \pmod{102}$ always has a solution for x.	*2pts*

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 42 points. No penalty for incorrect answers.*]

(a) Suppose that $P(x, y)$ is a proposition that involves real numbers x and y. Write down quantified propositions that express each of the following statements:

(i) For some x, $P(x, y)$ holds for all y. *3pts*

$(\exists x)(\forall y)P(x, y)$

(ii) For every x, there is exactly one y such that $P(x, y)$ holds. [Note: The only quantifiers you may use are $\forall$ and $\exists$.] *3pts*

$(\forall x)((\exists y)P(x, y) \wedge (\forall y \forall z)((P(x, y) \wedge P(x, z)) \Rightarrow (y = z)))$

(iii) For all x and y, if $P(x, y)$ holds then $P(y, x)$ does not hold. *3pts*

$(\forall x \forall y)(P(x, y) \Rightarrow \neg P(y, x))$

(b) What is the minimum possible number of edges in a *connected* graph on n vertices (with no self-loops or multiple edges between any pair of vertices)? *3pts*

$n - 1$. [Such a graph is a tree.]

(c) What is the maximum possible number of edges in a *disconnected* graph on n vertices (with no self-loops or multiple edges between any pair of vertices)? *3pts*

$(n - 1)(n - 2)/2$. [K_{n-1} plus an isolated vertex.]

(d) A connected planar graph G with 6 vertices and 11 edges is drawn in the plane. How many faces does it have? *3pts*

7. [Use Euler's formula: $f = e - v + 2$.]

(e) A connected planar graph G has 100 vertices. What is the maximum possible number of edges in G? *3pts*

294. [$e \leq 3v - 6$. Note that this bound is attainable.]

[Q2 continued on next page]

(f) Find the rightmost (least significant) digit of 7^{93}. *3pts*

7. [Note that $7^2 = 49 \equiv 9 \equiv -1 \pmod{10}$. Hence $7^{93} = 7 \cdot (7^2)^{46} \equiv 7 \cdot (-1)^{46} \equiv 7 \pmod{10}$.]

(g) Solve the equation $3x \equiv 7 \pmod{8}$ for x. *3pts*

5. [The inverse of 3 mod 8 is 3. Multiplying both sides by 3 gives: $x \equiv 21 \equiv 5 \pmod{8}$.]

(h) Suppose the 25th day of this year is a Monday. Which day of the week is the 50th day of next year (assuming that this year has 365 days)? *3pts*

Saturday. [Number of intervening days is $365 + 25 = 390 \equiv 5 \pmod{7}$. 5 days after Monday is Saturday.]

(i) What is $14^{201} \pmod{15}$? *3pts*

14. [$14 \equiv -1 \pmod{15}$, so $14^{201} \equiv (-1)^{201} \equiv -1 \equiv 14 \pmod{15}$.]

(j) Find $1! + 2! + 3! + 4! + \ldots + 100! \pmod{24}$. *3pts*

9. [Since $4! = 24$, we have $24 \mid k!$ for all $k \geq 4$. Hence the sum reduces to $1! + 2! + 3! \equiv 9 \pmod{24}$.]

(k) Find $\gcd(481, 91)$. *3pts*

13. [$\gcd(481, 91) = \gcd(91, 26) = \gcd(26, 13) = \gcd(13, 0) = 13$.]

(l) Find the inverse of 27 mod 32. Your answer should be an integer in $\{0, 1, \ldots, 31\}$. *3pts*

19. [Use extended-gcd algorithm. Sequence of returned triples is: $(1, 1, 0) \to (1, 0, 1) \to (1, 1, -2) \to (1, -2, 11) \to (1, 11, -13)$. Hence inverse is $-13 \equiv 19 \pmod{32}$. Check: $19 \times 27 = 513 \equiv 1 \pmod{32}$.]

3. Proofs [*All parts to be justified. Total of 18 points.*]

(a) Prove that $\sqrt{6}$ is irrational. *6pts*

We follow the same strategy as the proof in lecture that $\sqrt{2}$ is irrational. Assume for the sake of contradiction that $\sqrt{6}$ is rational, so we can write

$$\sqrt{6} = \frac{a}{b}, \tag{1}$$

where a, b are positive integers that share no common factors.
Squaring both sides of (1) gives $6 = \frac{a^2}{b^2}$, and hence

$$a^2 = 6b^2. \tag{2}$$

Now this implies that $6 \mid a^2$, which in turn implies that $6 \mid a$ (see Lemma below). Hence we may write $a = 6k$ for some positive integer k, and substituting this into (2) gives

$$36k^2 = 6b^2.$$

Therefore, $b^2 = 6k^2$, so $6 \mid b^2$ and hence, using the Lemma again, $6 \mid b$.
Finally, we have shown that 6 is a common factor of a and b, which is a contradiction to our initial assumption that a, b have no common factors. $\square$

Twice in the above proof, we used the following lemma, which we need to prove.

Lemma: *For a natural number a, if a^2 is divisible by 6 then a is divisible by 6.*

Proof: We prove the contrapositive. Suppose that a is not divisible by 6. Then at least one of 2 and 3 (the prime factors of 6) must not be a factor of a. But this means that at least one of 2 and 3 must not be a factor of a^2, so a^2 is not divisible by 6. $\square$

(b) Prove by induction that, for all odd $n \geq 1$, $2^n + 1$ is divisible by 3. *6pts*

For $n \geq 0$, let $P(n)$ denote the following proposition: "$2^{2n+1} + 1$ is divisible by 3." We will prove $(\forall n \in \mathbb{N})P(n)$ by induction on n. Note that this proves the statement in the question as the sequence $P(0), P(1), P(2), \ldots$ covers all odd powers of 2.

Base Case: $n = 0$: The statement $P(0)$ says that $2^1 + 1 = 3$ is divisible by 3, which is obviously true.

Inductive Step: We assume $P(n)$ holds for all $n \leq k$ and prove $P(k+1)$. $P(k+1)$ asserts that the number $2^{2(k+1)+1} + 1$ is divisible by 3. But we can write

$$2^{2(k+1)+1} + 1 = 4 \cdot 2^{2k+1} + 1 = 4 \cdot (2^{2k+1} + 1) - 3.$$

By the induction hypothesis $P(k)$, $2^{2k+1} + 1$ is divisible by 3, and hence the entire number above is also divisible by 3. This completes the induction step.

[Q3 continued on next page]

(c) The so-called "Tribonacci" sequence $T(n)$ is defined as follows: *6pts*

$$T(0) = T(1) = 0; \quad T(2) = 1; \quad T(n) = T(n-1) + T(n-2) + T(n-3) \text{ for } n \geq 3.$$

Prove by induction that $T(n) \leq 2^n$ for all $n \geq 0$.

We proceed by strong induction on n.

Base Case: There are three base cases, $n = 0, 1, 2$. Thus we need to prove:

$$T(0) \leq 2^0 = 1; \qquad T(1) \leq 2^1 = 2; \qquad T(2) \leq 2^2 = 4.$$

All of these follow immediately from the given values $T(0) = T(1) = 0$ and $T(2) = 1$.

Inductive Step: For any $k \geq 3$, we assume that $T(n) \leq 2^n$ for all $n \leq k$ and prove that $T(k+1) \leq 2^{k+1}$ also holds. To see this, note that

$$\begin{aligned} T(k+1) &= T(k) + T(k-1) + T(k-2) \\ &\leq 2^k + 2^{k-1} + 2^{k-2} \quad \text{by induction hypothesis} \\ &= 2^{k-2}(4+2+1) \\ &= 7 \cdot 2^{k-2} \\ &\leq 2^{k+1}. \end{aligned}$$

This verifies that the inequality also holds for $T(k+1)$, and hence completes the induction proof.

4. Stable Marriage [*All parts to be justified unless otherwise stated. Total of 13 points.*]

Consider the following set of marriage preferences for four men 1, 2, 3, 4 and four women A, B, C, D.

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

Woman	Men			
A	3	4	1	2
B	2	4	3	1
C	1	2	3	4
D	2	3	4	1

(a) Use the Propose-and-Reject algorithm to find a male-optimal pairing. Show your work in the table below: you should indicate in each column the proposals received by each woman on each day. Note: The algorithm may terminate in fewer than the 6 days provided! *4pts*

To ensure a male-optimal pairing, we run the propose-and-reject algorithm with the men proposing. The following table shows the proposals received by each woman on each day.

Woman	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6
A				1		
B	1, 3	3, 4	4	4		
C	2, 4	2	2	2		
D		1	1, 3	3		

The algorithm terminates with the male-optimal pairing $(1, A)$, $(2, C)$, $(3, D)$, $(4, B)$.

(b) Is it possible for man 4 to be paired with woman C in a stable pairing? Briefly justify your answer using the optimality/pessimality properties of stable pairings. *3pts*

No. The above pairing is male optimal, so the best possible woman that man 4 can be paired with in any stable pairing is B. Since C is above B in his preference list, he can't be paired with C.

(c) Is it possible for man 2 to be paired with woman A in a stable pairing? Briefly justify your answer using the optimality/pessimality properties of stable pairings. *3pts*

No. The above pairing is female pessimal, so the worst man that woman A can be paired with in any stable pairing is 1. Since 2 is below 1 on her preference list, she can't be paired with 2.

[Q4 continued on next page]

(d) Suppose we add k new men and k new women to the above instance. The preference lists of these new people are completely arbitrary orderings on the $k+4$ people of the opposite gender. The preference list of each of the original four men and four women starts off exactly as above, followed by an arbitrary ordering of the new people of the opposite gender. Prove that any stable pairing of the larger instance must include a stable pairing of the original 4-man, 4-woman instance above. [Note: This proof is fairly short; you probably won't need all the space below.] *3pts*

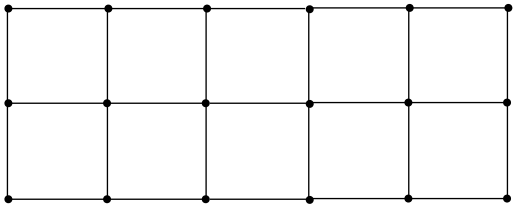
Consider any pairing for the larger instance in which some man $M \in \{1,2,3,4\}$ is paired with some woman $W \notin \{\mathrm{A},\mathrm{B},\mathrm{C},\mathrm{D}\}$. Then there must exist some man $M' \notin \{1,2,3,4\}$ who is paired with a woman $W' \in \{\mathrm{A},\mathrm{B},\mathrm{C},\mathrm{D}\}$. We claim that (M,W') is a rogue couple, so no such pairing can be stable.

To see that (M,W') is a rogue couple, note that M prefers all the women in $\{\mathrm{A},\mathrm{B},\mathrm{C},\mathrm{D}\}$ to all the other women, so he certainly prefers W' to his current partner W. Similarly, W' prefers all the men in $\{1,2,3,4\}$ to all the other men, so she prefers M to her current partner M'. Hence (M,W') is indeed a rogue couple, as claimed.

We have proved that any stable pairing for the larger instance must match men in $\{1,2,3,4\}$ with women in $\{\mathrm{A},\mathrm{B},\mathrm{C},\mathrm{D}\}$. Clearly this pairing restricted to these four men and women must itself be stable, since any rogue couple within this group would be a rogue couple for the whole pairing on the larger instance.

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

For integers $m, n \geq 2$, an $m \times n$ *grid graph* is an undirected graph drawn in the plane, with mn vertices positioned at the integer points (i, j) for $1 \leq i \leq n$ and $1 \leq j \leq m$. An edge is drawn between each pair of points whose distance in the plane is exactly 1. The figure below shows a 3×6 grid graph.



(a) How many *edges* are there in an $m \times n$ grid graph? Write your answer in the box provided; no justification is needed. *2pts*

$2nm - m - n$ total. [$n(m-1)$ vertical edges + $m(n-1)$ horizontal edges.]

(b) How many *faces* are there in an $m \times n$ grid graph? Write your answer in the box provided; no justification is needed. *2pts*

$(n-1)(m-1)+1$. [$(n-1)(m-1)$ interior square faces + 1 outer face.]

(c) Verify that the grid graph satisfies Euler's formula. *2pts*

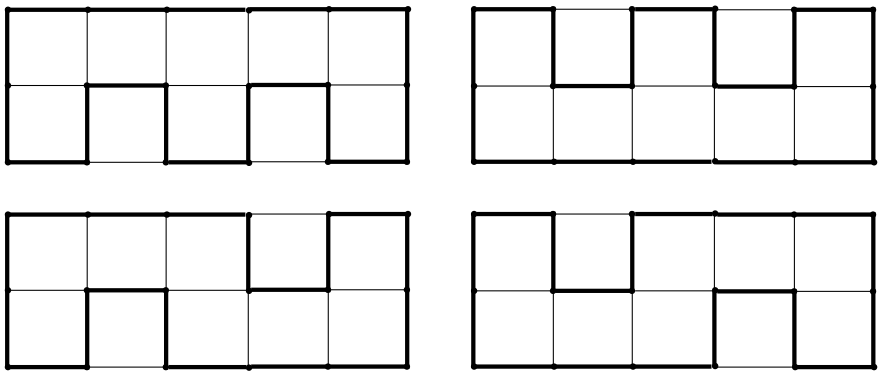
$v - e + f = nm - (2nm - m - n) + (n-1)(m-1) + 1 = 2.$

(d) For which values of n and m does the grid graph have an Eulerian tour? Write your answer in the box provided; no justification is needed. *2pts*

For $n = m = 2$ only. [For all other values of n, m, the graph has odd-degree vertices.]

(e) Recall that a *Hamiltonian cycle* in a graph is a (simple) cycle that visits every vertex exactly once. Draw a Hamiltonian cycle in the 3×6 grid graph below. [Note: You may use the diagram at the top of the page to experiment; please clearly show your final answer on the diagram below!] *2pts*

This grid graph has four Hamiltonian cycles, as follows:



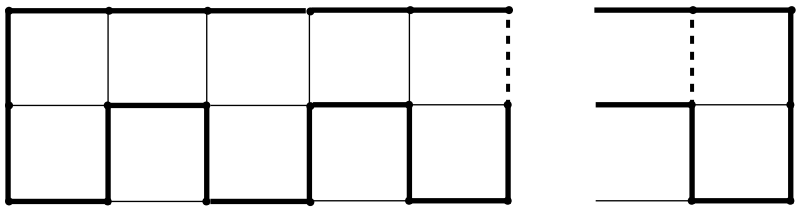
[Q5 continued on next page]

(f) Prove by induction on n that, for every *even* $n \geq 2$, every $m \times n$ grid graph has a Hamiltonian cycle. [Hint: Consider a systematic way of drawing a Hamiltonian cycle; strengthen your induction hypothesis.] *5pts*

For $\ell \geq 1$, let $P(\ell)$ denote the following proposition: "For every $m \geq 2$, the $m \times 2\ell$ grid has a Hamiltonian cycle that traverses one of the vertical edges on its rightmost boundary (i.e., a vertical edge on the line $x = m$)." We prove $(\forall \ell \geq 1)P(\ell)$ by induction on ℓ.

Base Case: $\ell = 1$: For every $m \geq 2$, the $m \times 2$ grid obviously has such a Hamiltonian cycle (just trace around the outer face).

Inductive Step: Assume that $P(\ell)$ holds for all $\ell \leq k$, and prove $P(k+1)$. If we remove the rightmost two columns of vertices from the $m \times 2(k+1)$ grid, we are left with an $m \times 2k$ grid. Note that the piece we removed is an $m \times 2$ grid, connected by m horizontal edges to the remaining $m \times 2k$ grid. By the induction hypothesis $P(k)$, this $m \times 2k$ grid has a Hamiltonian cycle that includes one of the vertical edges in its rightmost column. Also, the $m \times 2$ grid we removed has a Hamiltonian cycle running around its outer face (as argued for the base case above). Now we can splice these two cycles together (see picture below: the dotted edges are removed and replaced by the two bold horizontal edges connecting the two pieces) to obtain a Hamiltonian cycle of the entire $m \times 2(k+1)$ grid. This completes the inductive step.



(g) Prove that, if m and n are both odd, the $m \times n$ grid graph has *no* Hamiltonian cycle. [Hint: Give a direct proof, not a proof by induction.] *3pts*

The number of vertices in the grid graph is mn, which is odd if m, n are both odd. Thus any Hamiltonian cycle must have odd length. However, the grid graph is bipartite for any m, n. (To see this, color its vertices in chessboard fashion, so that each black vertex is adjacent only to white vertices and vice versa.) This means that any cycle in the graph must have even length. (An alternative way to argue that any cycle must have even length is to observe that it must have an equal number of up/down moves and left/right moves.) Hence it is not possible for a Hamiltonian cycle to exist.

6. Modular Arithmetic and Random Number Generation [*All parts to be justified unless otherwise stated. Total of 12 pts.*]

An important application of modular arithmetic is to generate a sequence of pseudo-random numbers $x_0, x_1, x_2, \ldots$, defined by the recursion

$$x_n = ax_{n-1} \pmod{p}, \text{ for } n = 1, 2, \ldots$$

Here p is a prime number, a is a positive integer such that $a \not\equiv 0 \pmod{p}$, and $x_0 \in \mathbb{Z}^+$ is a seed (initialization) satisfying $x_0 \not\equiv 0 \pmod{p}$. The *period* d is the smallest $n \in \mathbb{Z}^+$ such that $x_n \equiv x_0 \pmod{p}$; note that the sequence repeats after d numbers have been generated. We want to make d as large as possible: in this problem, you will see how large d can possibly be, using basic facts about modular arithmetic.

(a) For $n \in \mathbb{N}$, find x_n as a function of n, a, and x_0. Write your answer in the box provided; no justification is needed. *2pts*

$x_n = a^n x_0 \pmod{p}$.

(b) Prove that $a^d \equiv 1 \pmod{p}$. *2pts*

Since $x_d = a^d x_0 \equiv x_0 \pmod{p}$, we can multiply through by the inverse of x_0 mod p (which exists since p is prime and $x_0 \not\equiv 0 \pmod{p}$) to get $a^d \equiv 1 \pmod{p}$.

(c) Now let n_0 be the smallest positive integer n such that $a^n \equiv 1 \pmod{p}$. Prove that n_0 divides all positive integers n such that $a^n \equiv 1 \pmod{p}$. *4pts*

As defined in the question, let n_0 be the smallest positive integer n such that $a^n \equiv 1 \pmod{p}$, and let $n' > n_0$ be any other positive integer such that $a^{n'} \equiv 1 \pmod{p}$. We want to show that $n_0 \mid n'$.
Write $n' = qn_0 + r$, where q, r are positive integers with $0 \leq r < n_0$. (I.e., $n' \equiv r \pmod{n_0}$). Since $a^{n_0} \equiv 1 \pmod{p}$, we have $a^{qn_0} \equiv 1 \pmod{p}$, and hence $1 \equiv a^{n'} = a^{qn_0} \cdot a^r \equiv a^r \pmod{p}$. But now we have found another integer $0 \leq r < n_0$ such that $a^r \equiv 1 \pmod{p}$, which contradicts the fact that n_0 is the least such positive integer unless $r = 0$. But if $r = 0$ then $n_0 \mid n$, as required.

(d) Finally, prove that the period d divides $p - 1$. State clearly which results you used to prove this claim; in addition to earlier parts of this problem, you may use any of the theorems/lemmas from lecture. *4pts*

Since p is prime and $a \not\equiv 0 \pmod{p}$, we know by Fermat's Little Theorem that $a^{p-1} \equiv 1 \pmod{p}$. By part (b), we also know that $a^d \equiv 1 \pmod{p}$. In fact, our proof of part (b) also shows that d is the *smallest* positive integer satisfying this equivalence, since if $a^{d'} \equiv 1 \pmod{p}$ then $x_{d'} = a^{d'} x_0 \equiv x_0 \pmod{p}$, and d is the smallest integer satisfying this latter equivalence. Therefore, by part (c), we conclude that $d \mid (p - 1)$, as required.

[**Aside:** In practice, a large prime number p is used and a is carefully chosen so that the period is as large as possible, i.e., $d = p - 1$. For example, $p = 2^{31} - 1$ and $a = 7^5$ yields $d = p - 1$.]