CS 70 Discrete Mathematics and Probability Theory
Spring 2023 Rao and Ayazifar

Midterm

PRINT Your Name: _____, _____
(last) (first)

PRINT Your Student ID: _____

PRINT Your Exam Room: _____

SID of the person sitting to your left: _____

SID of the person sitting to your right: _____

SID of the person sitting in front of you: _____

SID of the person sitting behind you: _____

Read This.

- There will be no clarifications. We will correct any mistakes post-exam in as fair a manner as possible. Please just answer the question as best you can and move on even if you feel it is a mistake.
- Due to the above. Please move on. There are lots of problems to get points from. Do not get stuck. This is good advice anyway. In fact, we repeat it below.
- Anything written outside the boxes provided will not be graded.

Advice.

- The questions vary in difficulty. In particular, the exam is not in the order of difficulty and quite accessible short answer and proof questions are late in the exam. All blanks are worth 3 points each unless otherwise specified. No negative points on true/false. **So do really scan over the exam.**
- The question statement is your friend. Reading it carefully is a tool to get to your "rational place".
- You may consult only *one sheet of notes on both sides*. Apart from that, you may not look at books, notes, etc. Calculators, phones, computers, and other electronic devices are NOT permitted.
- **You may, without proof, use theorems and lemmas that were proven in the notes and/or in lecture, unless otherwise stated. That is, if we ask you to prove a statement, prove it from basic definitions, e.g., "$d \mid x$ means $x = kd$ for some integer k" is a definition.**
- There are a total of 239 points on this exam, with 16 total questions.

1. Pledge.

Berkeley Honor Code: As a member of the UC Berkeley community, I act with honesty, integrity, and respect for others.

In particular, I acknowledge that:

- I alone am taking this exam. Other than with the instructor and GSI, I will not have any verbal, written, or electronic communication about the exam with anyone else while I am taking the exam or while others are taking the exam.
- I will not refer to any books, notes, or online sources of information while taking the exam, other than what the instructor has allowed.
- I will not take screenshots, photos, or otherwise make copies of exam questions to share with others.

SIGN Your Name: _____

2. Warmup

(1 point) What is the product of **all** numerical student answers for this question?

3. Propositional Logic

True means always true regardless of the choice of predicates $P(\cdot)$ and $Q(\cdot)$ or the values of the propositions P and Q.

1. $(\neg Q \implies (P \implies Q)) \equiv (P \implies Q)$

   ◯ True ◯ False

2. $(\neg P \vee (P \implies Q)) \equiv (P \implies Q)$

   ◯ True ◯ False

3. Write an equivalent expression for $\neg(\forall x \in S)(P(x) \implies \neg Q(x))$ that does not use the negation symbol, "¬".

4. Consider the following implication:

$$(\forall y \in S)(\exists x \in S)(Q(x) \wedge P(y)) \implies (\exists x \in S)(\forall y \in S)(Q(x) \wedge P(y))$$

   (a) Is the implication true or false?

   ◯ True ◯ False

   (b) Give a counterexample or a proof of the implication.

4. Proofs

1. (5 points) Prove that if a number does not leave a remainder of 0 or 1 when divided by 4, then it is not a perfect square.

2. (10 points) Prove for any $N > 0$ integers, $a_1 \leq \cdots \leq a_N$, there is a subset of them that sums to a multiple of N.
   (Hint: Let $S_i = \sum_{k=1}^{i} a_k$, and consider the remainders of S_1 to S_N when divided by N.)

5. Induction I.

Recall the Fibonacci numbers: $F_1 = 1$, $F_2 = 1$, and $F_m = F_{m-1} + F_{m-2}$ for $m \geq 2$.

Consider the following theorem.

> **Theorem:** Any natural number n can be written in the form
>
> $$n = \sum_{i=1}^{k} F_{m_i},$$
>
> where the m_i are distinct positive integers such that **no two m_i, m_j are consecutive**. For example, $12 = 8 + 3 + 1 = F_6 + F_4 + F_1$.

Here is a partial proof of the above theorem.

Base cases: For $n = 0$, the statement is vacuously true. For $n = 1$, this is true since $1 = F_1$.

Inductive hypothesis: For any $m \geq 2$, suppose that every number from $0 \leq n \leq m - 1$ can be written in the form above.

Inductive step: We will prove that m can be written in the form above.

Let k be the largest integer such that $F_k \leq m$. Then by the inductive hypothesis, $m - F_k$ can be written as a sum of nonconsecutive Fibonacci numbers.

1. (6 points) Prove that $m - F_k < F_{k-1}$.

2. (6 points) Finish the proof of the theorem using the fact above.

6. Induction II

(12 points) Prove for all $n \geq 2$ that

$$\sqrt{2\sqrt{3\sqrt{4\cdots\sqrt{n}}}} < 3.$$

(Hint: Try proving

$$\sqrt{k\sqrt{(k+1)\cdots\sqrt{n}}} < k+1$$

for all $2 \leq k \leq n$.)

7. Stability in Matchings.

1. The only stable matchings are the job optimal and candidate optimal stable matchings.

   ◯ True ◯ False

2. If in a matching, candidate c is paired with the first job on its preference list, it cannot be in a rogue pair.

   ◯ True ◯ False

3. If in a matching, candidate c is paired with the last job on its preference list, it must be in a rogue pair.

   ◯ True ◯ False

4. If a candidate is paired with the kth job on its preference list in a stable matching, this candidate must not be first in the preference list for at least ___ jobs.

5. Explain why the number of rejected proposals in the job-propose stable matching algorithm for an instance with n jobs and n candidates is at most $n(n-1)$.

8. Graphs

All graphs are simple and undirected unless otherwise specified.

1. The 3-dimensional hypercube has an odd number of vertices.

   ◯ True ◯ False

2. How many faces are in a planar drawing of a n-vertex tree? (Possibly in terms of n.)

3. How many faces are in a planar drawing of an n-vertex connected graph with exactly one cycle?

4. What is the minimum degree of any vertex in an n-vertex tree when $n \geq 2$? (Possibly in terms of n.)

5. Recall a bipartite graph is a graph, $G = (V, E)$, where $V = A \cup B$, $A \cap B = \varnothing$, and $E \subseteq A \times B$.

   (a) What is the maximum number of edges in a bipartite graph? (Possibly in terms of $|V|$, $|A|$ and $|B|$?)

   (b) Every graph where every vertex has degree at most 2 is bipartite.

   ◯ True ◯ False

   (c) Every bipartite planar graph with n vertices has a vertex of degree at most _____. (Give a tight bound, possibly in terms of n.)

   (d) A 3-dimensional hypercube $G = (V, E)$ is bipartite. Recall that the vertices correspond to bit-strings, e.g., $000, 011, 010$ are vertices in V. Describe a set A (where $B = V - A$) such that $E \subseteq A \times B$.

6. The *maximum* degree of any vertex in an n-vertex planar graph is _____.

7. Consider an n-vertex graph where $n \geq 3$, with vertices u and v that have degrees d_u and d_v respectively. The vertices u and v must have a common neighbor when $d_u + d_v \geq$ _____. (Answer could be in terms of n. A common neighbor of u and v is a vertex x where (u,x) and (v,x) are edges.)

8. (5 points) Prove or disprove: There are at least 3 vertices of degree less than 6 in any connected planar graph with more than 100 vertices.

9. Consider a n-vertex graph $G = (V,E)$. Suppose we create a new graph $G' = G - v$ by removing a vertex v of degree d from G. If G' can be vertex-colored with k colors, then G can be vertex-colored with at most _____ colors.

   (Give a tight bound, possibly in terms of d, k, and n. Max and/or min might be useful as d and k are possibly different.)

9. Graph: proof.

All graphs are simple and undirected unless otherwise specified.

1. Consider a graph with n vertices where every vertex has degree exactly 3.
   (a) n must be even.

   ◯ True ◯ False

   (b) Give a short proof or counterexample.

2. Consider a graph with n vertices where every vertex has degree exactly 4.
   (a) n must be odd.

   ◯ True ◯ False

   (b) Give a short proof or counterexample.

3. (5 points) Prove every n-vertex graph with $n \geq 2$ has at least 2 vertices with the same degree.

10. Sets and (modular) functions.

A *k-uniform* function $f : A \to B$ is a function where for each $y \in B$, either

1. there are exactly k distinct values, $x_1, \ldots, x_k \in A$, where $y = f(x_i)$
2. or $(\forall x \in A)(y \neq f(x))$.

For each of the following functions, $f : A \to B$, indicate the value of k for which f is k-uniform, or "Unknown" if there is not enough information to determine k.

1. $A = \{0,1,2,3\}$, $B = \{0,1,2\}$, and $f : A \to B$ is defined as $f(0) = 0$, $f(1) = 0$, $f(2) = 1$, $f(3) = 1$.

2. For $f(x) = g(h(x))$ for a k_1-uniform function $g : X \to B$ and a k_2-uniform function $h : A \to X$. (Possibly in terms of k_1 and/or k_2.)

3. Below, $A = B = \{0, \ldots, m-1\}$ under arithmetic modulo m.
   (a) $f(x) = ax \pmod{m}$ for a prime m where $a \neq 0 \pmod{m}$. (Possibly in terms of a and/or m.)

   (b) $f(x) = ax \pmod{m}$ where $\gcd(a,m) = d$. (Possibly in terms of a, m and/or d.)

4. $f(x) = ax \pmod{m}$ where $m = pq$ for primes p and q, $A = \{x \mid \gcd(x,m) = 1\}$, and $\gcd(a,m) = 1$. (Possibly in terms of a, m, p and/or q.)

5. $f(x) = ax \pmod{m}$ where $m = pq$ for primes p and q, $A = \{x \mid \gcd(x,m) = 1\}$, and $\gcd(a,m) = p$. (Possibly in terms of a, m, p, and/or q.)

11. A bit more modular arithmetic.

1. If $x \equiv 3 \pmod 5$ and $x \equiv 2 \pmod{11}$, what is $x \pmod{55}$?

2. Consider the system of equivalences

$$\begin{cases} x \equiv a \pmod{10} \\ x \equiv b \pmod{15}. \end{cases}$$

   (a) If $b-a$ is a multiple of 5, what is the number of solutions for $x \pmod{150}$?

   (b) If $b-a$ is *not* a multiple of 5, what is the number of solutions for $x \pmod{150}$?

3. Let p be a prime and a be an integer. Then $a^p - a$ is a multiple of p.

   ◯ True ◯ False

4. Let a be an integer and p and q be primes. Then $a(a^{(p-1)(q-1)} - 1)$ is a multiple of _____. (Answer should be as large as possible and cannot be 1 or involve a. It may involve p and q.)

5. Consider an RSA scheme with public key (N, e) and private key d. Let $y_1 = x_1^e \pmod N$ and $y_2 = x_2^e \pmod N$.

   (a) How should the message $x_1 x_2 \pmod N$ be encrypted? Express your answer in terms of y_1, y_2, N, e, and/or d.

   (b) Express $x_1 x_2 \pmod N$ in terms of y_1, y_2, N, e, and/or d.

12. Proof: modular arithmetic.

A prime number p is called a *Mersenne prime* if it is one less than a power of two. In other words, it is in the form $2^n - 1$ for some integer $n \geq 2$.

1. For Mersenne prime $p = 2^n - 1$, what is the smallest natural number congruent to $2^n \pmod{p}$?

2. For any positive integer a, what is the smallest natural number congruent to $(2^a)^n \pmod{p}$?

3. (5 points) Using the previous parts, prove that there are at least n distinct values of $x \pmod{p}$ such that $x^n \equiv 1 \pmod{p}$.

13. Polynomials.

1. Give an expression for a polynomial under arithmetic modulo 7 that passes through $(1,0)$ and $(2,5)$.

2. Given that you are working over arithmetic modulo a prime p, how many polynomials of degree at most d pass through a given $d-1$ points? (Assume p is much larger than d. Answer possibly in terms of p and d.)

3. The Lagrange interpolation scheme from the notes for $d+1$ points, $(x_1,y_1),\ldots,(x_{d+1},y_{d+1})$, defines the polynomials $\Delta_1(x),\ldots,\Delta_{d+1}(x)$.

   (a) How many roots does $\Delta_1(x)$ have? (Possibly in terms of d, or state "Unknown" if there is insufficient information.)

   (b) Consider the polynomial $P(x) = \Delta_1(x)\Delta_2(x)$.

      i. What is the degree of $P(x)$? (Possibly in terms of d, or state "Unknown" if there is insufficient information.)

      ii. How many values of x are there where $P(x) = 0$? (If the number of values can vary, answer "Unknown", otherwise provide a number or expression possibly in terms of d.)

   (c) True or false: Every polynomial of degree d over the reals has exactly d real roots.

   ◯ True ◯ False

14. Polynomial: applications.

1. Consider a channel that has at most e erasure errors and k corruptions. How many packets should one send to ensure that an n packet message can be recovered?

2. Consider the Berlekamp-Welch error correction scheme where the error polynomial is $E(x) = x^2 - 1 \pmod{13}$. Where are the errors? That is, for which x-values do you have $P(x) \neq r_x$? (Answer should be a list of value(s) from $\{0, 1, \ldots, 12\}$.)

3. Consider using the polynomial scheme from class to share the secret number 5 with 10 people such that any 3 people can recover the secret. What is the smallest modulus that one can work in?

4. (5 points) Describe a secret-sharing scheme in which two groups of 5 and 7 people can retrieve the secret when there is at least a majority of both groups present.

15. Computability/Countability.

1. The set of all finite subsets of a countably infinite set is uncountable.

   ◯ True ◯ False

2. The set of all subsets of a countably infinite set is uncountable.

   ◯ True ◯ False

3. A real number is computable if there is a program $P(n)$ that runs in finite time that computes the nth digit of the number.

   (a) True or false: Every real number is computable.

   ◯ True ◯ False

   (b) (5 points) Prove or disprove the statement from part (a).

16. Counting.

You may leave your answer as an expression using factorial notation, e.g., $n!$, or the choose notation, e.g., $\binom{n}{k}$, unless otherwise specified.

1. How many permutations of the word ABRACADABRA are there?

2. How many ways are there to form a string with exactly 4 A's and 3 B's?

3. How many ways are there to split n_1 indistinguishable apples and n_2 indistinguishable bananas among k people? (An expression possibly involving n_1, n_2 and k.)

4. You have a drunken sailor walking along the real line starting at 0 and ending at n and the sailor takes steps forward or backward of size 1. The sailor uses $n+2k$ steps in total. How many possible ways could this happen? For example, for $n = 2$ and $k = 1$, one of the possible ways is "backward, forward, forward, forward" or "forward,forward,forward,backward". (Note that the sailor went below 0 in the first example and past 2 in the second which is allowed.)

5. Let S_n be the number of ways to add up 1's and 2's to obtain n, where order matters. (For example, $S_3 = 3$, with the possible ways being $1+1+1$, $1+2$ and $2+1$.)

   (a) Give an expression involving a summation for S_n. (Hint: consider summing over cases.)

   (b) Give a recursive expression for S_n for $n \geq 2$. (You may assume that $S_0 = 1$, and $S_1 = 1$.)