CS 70 Discrete Mathematics and Probability Theory
Spring 2022 Sen and Rao

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: _____

Advice.

- The questions vary in difficulty. In particular, some of the proof questions at the end are quite accessible, and even those are not necessarily in order of difficulty. All blanks are worth 3 points each unless otherwise specified. No negative points on true/false. **So do really scan over the exam a bit.**
- 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.**

Remote Proctoring Instructions.

- Gradescope assignment with the PDF **entire exam** will be available on the "Midterm" assignment (on either the regular or Alternate Gradescope).
- **Be sure** to **download** the PDF from the Midterm Gradescope assignment.
- There will be no clarifications made directly to individuals. We will listen to issues, but if a problem is identified to be in error, we may choose to address it during the midterm or after the midterm. Please keep moving through the exam.
- **Remote: You have 120 minutes to do the exam and then an extra twenty minutes to scan your answer sheet to the Midterm assignment.**
- **Remote: Clarification Request form:** https://forms.gle/EMYnKgyiahoG6BBVA
- **Clarification Doc:** https://tinyurl.com/cs70-sp22-mt-clarifications
- For emergencies, email sp22@eecs70.org or use the disruption form at: https://forms.gle/hwXJ3ZWaxUsgszNs7.
  Again, keep working as best as possible, as we cannot respond in real time.

Major Gradescope Issues. If there is a global issue and it is not affecting you, please continue. If you are experiencing difficulties with Gradescope or Zoom, you may check your email, and we will post a global message on Piazza and bypass email preferences to inform you of what to do.

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 have any other browsers open while 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: Shoeless.

There are 70 people. An even number of them wear one shoe. One-half of the remainder wear no shoes, and the rest wear two shoes.

1. How many shoes are worn in total by the 70 people? (2 points.)

2. Briefly justify your answer. (2 points.)

3. Propositional Logic

Let A, B, and C be statements, where A is always true, B is always false, C is always true, and let $P(x)$ and $Q(x)$ be predicates over a nonempty set S, where the statements $\forall x \in S, P(x)$; $\exists x \in S, Q(x)$; and $\exists x \in S, \neg Q(x)$ are always true.

1. $A \implies B$

   ◯ Always True ◯ Always False ◯ Depends

2. $B \implies A$

   ◯ Always True ◯ Always False ◯ Depends

3. $A \implies C$

   ◯ Always True ◯ Always False ◯ Depends

4. $(A \vee B) \implies \neg C$

   ◯ Always True ◯ Always False ◯ Depends

5. $\neg A \vee C$.

   ◯ Always True ◯ Always False ◯ Depends

6. $\forall x \in S, Q(x)$

   ◯ Always True ◯ Always False ◯ Depends

7. $\exists x \in S, P(x)$

   ◯ Always True ◯ Always False ◯ Depends

8. $\exists x \in S, Q(x) \wedge P(x)$

   ◯ Always True ◯ Always False ◯ Depends

9. $\forall x \in S, Q(x) \vee P(x)$

   ◯ Always True ◯ Always False ◯ Depends

4. To Prove or Disprove, that is the question.

First, say whether statement is true or false, and then prove or disprove. The proof or counterexamples should be brief.

1. Prove or disprove: for $x, y, d \in \mathbb{Z}$, if $d \mid (x - y)$ then $d \mid x$.

◯ True ◯ False

2. Prove or disprove: $2x^2 = 4$ has no solutions in the rationals.

◯ True ◯ False

5. Stability in Matchings. 2 points/part.

1. For any stable matching instance, the job optimal stable matching has at least one job that is paired with their favorite candidate.

   ○ Always True

   ○ Possibly False

2. For any stable matching instance, the job optimal stable matching has no job paired with their least favorite candidate.

   ○ Always True

   ○ Possibly False

3. For any stable matching instance, the job optimal stable matching has at least one candidate that does not get their favorite job.

   ○ Always True

   ○ Possibly False

4. For any stable matching instance, all matchings have an even number of rogue couples. (Recall, a stable matching has 0 rogue couples.)

   ○ Always True

   ○ Possibly False

5. Consider an output from running the Propose-and-Reject algorithm on a stable matching instance with n jobs and n candidates. We then arbitrarily permute one job's preference list.

   (a) What is the maximum number of jobs that can participate in a rogue couple in the outputted matching with respect to the permuted preference list?

   (b) What is the maximum number of rogue couples in the outputted matching with respect to the permuted preference list?

6. Graphs

You may assume all graphs in this section are simple (as defined in the notes) unless otherwise specified.

1. For all $n \geq 3$, any connected graph with n vertices and n edges is planar.

   ◯ True ◯ False

2. How many colors are needed to vertex color a bipartite graph of maximum vertex degree d? (Recall that a valid vertex coloring assigns colors to the vertices such that the vertices in an edge have different colors.)

3. Consider that $G = (V, E_1)$ and $G' = (V, E_2)$ are bipartite, how many colors are sufficient to vertex color $G'' = (V, E_1 \cup E_2)$? (You should give as small as bound as possible.)

4. Consider bipartite graphs $(V, E_1), (V, E_2), (V, E_3), \ldots, (V, E_k)$ are bipartite, how many colors are sufficient to color $(V, E_1 \cup \cdots \cup E_k)$? (You should give as small as bound as possible that is in terms of k.)

5. There is always a vertex of degree at most _____ in a connected bipartite planar graph. Recall that any bipartite planar graph $G = (V, E)$ satisfies $|E| \leq 2|V| - 4$. (You should give as tight of a bound as possible.)

6. The complete graph K_n on $n > 3$ vertices can be made to contain an Eulerian tour by deleting a minimum of _____ edges. (Answer(s) should be as small as possible and possibly in terms of n.)

   even n: odd n:

7. Consider a connected n-vertex graph G with exactly k cycles. Provide as tight of a bound as possible for each part. (You may assume $n > 4k$.)

   (a) Removing $2k$ edges from G produces a graph with at least ___ connected components.

   (b) Removing $2k$ edges from G produces a graph with at most ___ connected components.

8. At least d colors are *required* for a valid vertex coloring for any graph with maximum vertex degree d.

   ◯ True ◯ False

9. Removing any degree 2 vertex (and its incident edges) in a connected acyclic graph leaves a graph with two connected components.

   ◯ True ◯ False

10. Consider a walk in a connected graph $G = (V, E)$ with $|V| \geq 4$ formed by starting at a vertex u and proceeding by choosing an arbitrary unused edge at the current vertex to get to the next vertex. The process terminates when it reaches a vertex where all incident edges have already been used.

    (a) The walk always terminates at the vertex u if and only if the degree of every vertex is ____.

    (b) For a tree, the walk always terminates at a vertex with degree that is ___. (Give as specific of an answer as possible.)

    (c) For a complete graph on n vertices where n is odd, the walk always forms a Hamiltonian tour.

    ◯ True ◯ False

    (d) For a hypercube of dimension n, the walk terminates at an odd degree vertex or at u.

    ◯ True ◯ False

7. Modular Arithmetic: what number (or expression)?

1. Give all the solutions to $5x \equiv 3 \pmod{24}$ or write "none".

2. Give all the solutions to $15x \equiv 3 \pmod{24}$ or write "none".

3. Give all the solutions to $15x \equiv 13 \pmod{24}$ or write "none".

4. Compute $21^{141} \pmod{71}$.

5. Consider an RSA scheme with public key $N = 77$ and $e = 7$.
   (a) What is the private key?

   (b) What is the decoding of the encrypted message 76? (Give an answer in $\{0, \ldots, 76\}$. Also, notice that 76 is one less than 77.)

6. What is $304^{2022} \pmod{70}$? (Answer should be from $\{0, \ldots, 69\}$.) Please clearly circle/box your final answer. (Hint: $70 = 2 \times 5 \times 7$.) (10 points.)

8. When the Midterm has Proofs. (15 points.)

Given a positive integer n, we define the digital root of n, $\mathrm{DR}(n)$, to be the positive integer attained from repeatedly summing the base 10 digits of n until n is a single digit number. For example, $\mathrm{DR}(191) = 2$ because $191 \to 1+9+1 = 11 \to 1+1 = 2$.

Prove that $\mathrm{DR}(n) \equiv n \pmod 9$.

9. Polynomial and Applications.

1. Consider non-zero polynomials $P(x)$ of degree d_p and $Q(x)$ of degree d_q, where d_p and d_q are nonnegative integers.

   (a) What is the maximum degree of $P(x)Q(x)$?

   (b) What is the maximum degree of $P(Q(x))$?

   (c) What is the maximum degree of $P(xQ(x))$?

2. If a polynomial $P(x)$ has a root at r, then $P(x) = (x-r)Q(x)$ for some polynomial $Q(x)$.

   ◯ True ◯ False

3. Given a degree d polynomial $P(x)$ and k values $x_1, \ldots, x_k$ with $k \leq d$, how many polynomials of degree at most d over arithmetic modulo prime p have the same value as $P(x)$ on $x_1, \ldots, x_k$?

4. For this problem, consider the Berlekamp-Welch scheme for a message of size n that tolerates k errors.

   (a) What is the degree of the polynomial $P(x)$ used to encode the message?

   (b) What is the degree of the error locator polynomial $E(x)$ in the reconstruction algorithm?

   (c) What is the degree of $Q(x) = P(x)E(x)$ in the reconstruction algorithm?

   (d) If there were $i \leq k$ errors, the recovered $E(x)$ has at least ___ roots. Give the largest lower bound you can.

10. Polynomials and Functions.

1. Consider any function $f(x)$ where the domain and range is arithmetic modulo a prime p,

   (a) Prove that $f(x)$ corresponds to a polynomial expression modulo p. (5 points.)

   (b) Give a tight upper bound on the minimum degree of a polynomial that represents $f(x)$. (Your proof above may be useful.)

2. Consider a composite number $m = p_1 p_2$, with p_1 and p_2 different primes, and a polynomial $P(x)$ over arithmetic modulo m.

   (a) Give a tight upper bound on the minimum degree of a polynomial expression equivalent as functions to $P(x)$ (i.e. gives the same value when evaluated at all x). (Hint: Think about question 1(b) and CRT.)

   (b) Justify your answer above. That is, show that any polynomial over arithmetic modulo m can be represented by an expression of degree at most your answer above. (10 points)

   (c) Any function under arithmetic modulo m corresponds to a polynomial.

   ◯ True ◯ False

11. Count the Ways.

Jonathan is playing a game called 70rdle. In this game, the 70 staff has a secret string of five upper-case English letters, and Jonathan must guess exactly what the string is. Assume each subpart is independent of the other subparts. The English alphabet has 26 letters.

1. With no restrictions, how many strings are possible?

2. If no letter is allowed to appear in the string more than once, how many strings are possible?

3. If the letters in the string must be sorted in alphabetical order, how many strings are possible? For example, AABCD is valid, but ABCDA is not.

4. How many strings contain at least one J?

5. How many strings contain at least one J in the first two letters?

6. How many strings contain exactly four J's?

7. How many strings contain exactly five J's?

12. A little bit of Fermat from Induction.

Suppose p is a prime.

1. Prove that for any $1 \leq k \leq p-1$, $p \mid \binom{p}{k}$. (5 points.)

2. Prove Fermat's Little Theorem via induction: in other words, prove that for all integers a,

$$a^p \equiv a \pmod{p}.$$

(Hint: You may find the Binomial Theorem helpful: $(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i$.) (15 points.)

13. Rare Scheme for Alice.

Bob is trying to send a message m to $\text{Alice}_1, \ldots, \text{Alice}_M$, such that if k of the Alices' agree, they can reconstruct the message. However, he wants to prevent Eve from reconstructing the message, even if she is able to determine all of the Alices' points.

The Alices use the same RSA scheme, broadcasting the public key (N, e). Bob then uses the polynomial secret sharing scheme (over arithmetic modulo a sufficiently large prime p), sending points $(1, x_1), \ldots, (M, x_M)$ to $\text{Alice}_1, \ldots, \text{Alice}_M$, respectively, such that if $P(x)$ is the polynomial determined by the points, then $P(0)$ is m^e.

(a) After completing the interpolation, how can the Alices reconstruct m? (5 points.)

(b) Eve doesn't know the Alices' private key d, but knows N, e, and p. She manages to trick all of the Alices into revealing $(1, x_1^d), \ldots, (M, x_M^d)$. Prove that if $M > (k-1)d$, then Eve can find the message m without figuring out the value of d. (15 points.)