CS 70 Discrete Mathematics and Probability Theory
Fall 2021 Ayazifar and Rao Midterm

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/fgAom53YWLYGh9HT6`**
- **Clarification Doc:** `https://docs.google.com/document/d/1240jC66ZIkkHlyDQAOOJaAnadzlllzKpyUPKeuCtQow/edit`
- For emergencies, email fa21@eecs70.org or use the disruption form at: `https://forms.gle/aE85kLZrGVQKREfx5`. Again, keep working as best as possible, as we cannot respond in real time.

Advice.

- The questions vary in difficulty. In particular, some of the proof questions at the end are quite accessible, and even those are in not necessarily in order of difficulty. All short answers and true false questions are worth 3 points and each written problem is worth 15 unless otherwise stated. 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 $x = i(d)$ for some integer i" is a definition.**

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.

2. Warmup, Propositions, Proofs

1. Consider a universe, U, of students, let $B(x)$ denote that "x is a Berkeley student", and $S(x)$ denote that "x is a Stanford student." Furthermore, let $W(x)$ denote "student x wants to save the world", and $R(x)$ denote that "student x wants to have a billion dollars by the time they are 30". Finally, in this world, we have the following implications $\forall x \in U, B(x) \implies W(x)$ and $\forall x \in U, S(x) \implies R(x)$.

   Which of the following are always true or possibly false?

   (a) $\forall x \in U, W(x) \implies B(x)$.

   Always True ○

   Possibly False ○

   (b) $\forall x \in U, W(x) \wedge R(x)$.

   Always True ○

   Possibly False ○

   (c) $\forall x \in U, (S(x) \vee B(x) \implies W(x) \vee R(x))$.

   Always True ○

   Possibly False ○

   (d) $\forall x \in U, (S(x) \wedge B(x) \implies W(x) \wedge R(x))$.

   Always True ○

   Possibly False ○

   (e) $\exists x \in U, \neg R(x) \implies \neg S(x)$.

   Always True ○

   Possibly False ○

   (f) $\forall x \in U, \neg R(x) \implies \neg S(x)$.

   Always True ○

   Possibly False ○

2. If $4 \nmid a^3$ then $2 \nmid a$. (By $a \nmid b$, we mean a does not divide b.)

   True ○

   False ○

3. For an integer a, if $2 \nmid a$ then $4 \nmid a^3$.

   True ○

   False ○

3. Stable Matchings.

By a stable matching instance we mean the input to a stable matching problem; a set of jobs and candidates with preference lists. Recall a *matching* is a set of job-candidate pairs which contains all jobs and candidates exactly once. The "favorite" partner of an entity, job or candidate, is the first on their preference list.

1. For any two job, two candidate stable matching instance, a matching where both jobs have their favorite candidate is stable.

   Always True ◯

   Possibly False ◯

2. For any stable matching instance, any matching is stable if for each pair in the matching either the job has their favorite candidate or the candidate has their favorite job.

   Always True ◯

   Possibly False ◯

3. For any stable matching instance, every stable matching has at least one candidate who gets their favorite job.

   Always True ◯

   Possibly False ◯

4. In any job optimal pairing for a stable matching instance with n jobs, at least ____ job(s) must get their favorite partner.

5. At most how many rogue pairs could there be for an unstable matching for an n job, n candidate stable matching instance?

4. Fibonacci

Recall the Fibonacci numbers are defined by $F_0 = 0, F_1 = 1, F_i = F_{i-1} + F_{i-2}$ for all $i \geq 2$.

1. What is $\gcd(F_n, F_{n-1})$?

2. What is the multiplicative inverse of $F_n \pmod{F_{n-1}}$, for $n \geq 3$? (Hint: use extended gcd, the iterative version is easier to see. Answer should not have summations.)

3. Show that for all integers $n \geq 1$, $\sum_{i=1}^{n} F_i = F_{n+2} - 1$.

Reminder: Use your answer sheet!!

5. Proofs.

1. **10 points** Show that if $a+b+c > 2100$, then $a > 700$ or $b > 700$ or $c > 700$.

   Reminder: Use your answer sheet!!

2. Show that any multiple of 5 cents larger than 25 cents can be achieved with a combination of quarters (which are worth 25 cents) and dimes (which are worth 10 cents). (For example, 40 cents can be formed with with 4 dimes, and 45 cents can be formed using two dimes and a quarter.)

   Reminder: Use your answer sheet!!

3. Given two stable matchings M_1 and M_2, we say that M_1 is *job-preferred* to M_2 if every job prefers M_1 at least as much as M_2. In other words, every job is matched to a candidate in M_1 that is at least as high on the job's preference list as its candidate in M_2. Similarly, we say that M_1 is *candidate-preferred* to M_2 if every candidate prefers M_1 at least as much as M_2.

   Prove that if M_1 is job-preferred to M_2, then M_2 is candidate-preferred to M_1.

   Reminder: Use your answer sheet!!

6. Graphs: 2 pts/box on two box questions

For the following assume all graphs are simple (i.e., have at most one edge between any two vertices).

For parts 1-5, answers are a range: $L \leq m \leq U$ where m is the quantity that is asked for. Give as tight a range as possible, e.g., in some cases $L = U$.

For example, the "Number of edges in a 3-vertex graph" has L: 0, and U : 3.

1. How many edges are in a graph with the following properties?

   (a) In an n-vertex graph where every vertex has degree 3, where $n \geq 4$ and n is even.

   L: $\square$

   U: $\square$

   (b) For a complete graph on n vertices.

   L: $\square$

   U: $\square$

   (c) For a hypercube of dimension n.

   L: $\square$

   U: $\square$

   (d) If a graph is acyclic and has c connected components and n vertices, how many edges does it have?

   L: $\square$

   U: $\square$

   (e) In a connected graph with average degree < 2 on n vertices.

   L: $\square$

   U: $\square$

   (f) In a connected planar bipartite graph on n vertices, where $n \geq 3$.

   L: $\square$

   U: $\square$

   (g) In a connected planar bipartite graph on n vertices, where the minimum length cycle is at least 5.

   L: $\square$

   U: $\square$

For the following, a cut is a partition of V into S and $V-S$, and the edges in the cut are edges with one endpoint in S and one in $V-S$.

2. Consider a hypercube with N vertices and a cut in the hypercube where both sides of the cut have $N/2$ vertices. How many edges are in the cut?

   L: ☐

   U: ☐

3. How many edges in any cut, $(S, V-S)$ where $|S|=1$, in a tree on n vertices and maximum degree d?

   L: ☐

   U: ☐

4. The number of colors to vertex color a graph on n vertices with maximum degree $d \geq 1$.

   L: ☐

   U: ☐

5. The number of colors to *edge* color an acyclic graph on n vertices with maximum vertex degree d.

   L: ☐

   U: ☐

6. Let a "Big Chungus" graph be any connected graph with exactly 105 edges and 100 vertices and contains K_5 as a subgraph, i.e., there are five vertices with all possible edges between them.

   (a) True or False: All Big Chungus graphs are non-planar.

   True ◯

   False ◯

   (b) What is the largest number of edges that can be removed without disconnecting Big Chungus?

   ☐

7. True of False: For a graph with $c > 1$ components, where each component is bipartite, adding any edge between any pair of vertices in different components produces a bipartite graph.

   True ◯

   False ◯

8. Adding a vertex, v, of degree $>$ ___ to any graph with a Hamiltonian cycle on n vertices always yields a graph with a Hamiltonian cycle. (Give the smallest value which makes the statement true regardless of the particular set of neighbors of v.)

9. Every bipartite planar graph has an Eulerian tour.

True ○

False ○

7. More Short answer: modular arithmetic and polynomials

1. What is the multiplicative inverse of $5 \pmod{24}$?

2. What is $(a^5)^5 \pmod{35}$? (Simplify as much as possible for credit.)

3. For prime p, let $k(x) = x^1 + x^2 + \cdots + x^{p-1} \pmod{p}$.

   (a) For $x \in \{1, 2, 3, \ldots, p-1\}, k(x) = x^{-1}k(x) \pmod{p}$.

   True ◯

   False ◯

   (b) **6 points**
   Prove: For $x \in \{2, 3, \ldots, p-1\}$, $k(x) = 0 \pmod{p}$.

   Reminder: Use your answer sheet!!

4. True or False: If $\gcd(m,n) = d$, then $\frac{mn}{d} = 0 \pmod{m}$.

   True ◯

   False ◯

5. What is the number of solutions $\pmod{mn}$ for the equations $x = a \pmod{m}$ and $x = b \pmod{n}$ where $\gcd(m,n) = \gcd(a,m) = \gcd(b,n) = d$?

6. What is $a \times n(n^{-1} \pmod{m}) \pmod{m}$ if $gcd(n,m) = 1$?

7. Alice and Bob play a cooperative game. Each round (starting at round 1), they will each shoot a basketball, and they win when both of them make a shot on the same round. Alice will miss her first 2 shots (rounds 1 and 2), and starting with round 3 she will make every 5th shot (she will make shots 3, 8, etc). Bob will make every 4th shot starting with shot 1 (makes 1, 5, etc).

   (a) On what round number will the duo win the game?

   (b) What is the next round where they will both score again?

8. Given a secret of 6 bits that needs to be shared among 47 people where any 21 of the people can reconstruct the secret using polynomials over arithmetic $\pmod{p}$ (for p prime), what is the smallest possible value for p?

9. Give a degree 2 polynomial that passes through $(1,1),(2,0)$ and $(3,0)$ over $GF(5)$ (or $\pmod 5$.)

10. **6 points**
    Show that $x^{p!} = 1 \pmod{p}$ for $x \not\equiv 0 \pmod{p}$.

    Reminder: Use your answer sheet!!

11. Working $\pmod 7$, consider the polynomial:

$$4 + \sum_{k=0}^{100} x^{k!} \pmod 7.$$

    (a) Evaluate $x^{3!} \pmod 7$ for $x \neq 0 \pmod 7$.

(b) Give a degree 2 polynomial that is equivalent to $4+\sum_{k=0}^{100} x^{k!} \pmod 7$ for $x \neq 0 \pmod 7$. (Recall that $0! = 1$.)

(c) What are the roots of the resulting polynomial? (Maybe useful: $4 = -3 \pmod 7$.)

12. A common test for determining if a natural number is divisible by 7 is to take the last digit, multiply it by 2, and subtract it from the rest of the number. If the resulting number is divisible by 7, then the original number is also divisible by 7. For example, the number 553 is divisible by 7 because $55 - 2(3) = 49$, which is a multiple of 7.

(a) Give an $x \in \{7, \ldots, 14\}$ where $x \equiv (-2)^{-1} \pmod 7$.

(b) We can come up with a similar divisibility rule for any number that is relatively prime to 10. Let $n = 10a + b$ where b is the last digit of n and a is the number represented by the other digits. Given any d such that $\gcd(d, 10) = 1$, there exists a multiplier x such that the following statement holds:

$n = 10a + b$ ***is divisible by*** d ***if and only if*** $a + xb$ ***is divisible by*** d***.***

Find a general expression for x. Your answer may be expressed in terms of d.

13. Consider any k points $(x_1, y_1), (x_2, y_2), \ldots, (x_k, y_k)$. If there exists a unique degree k polynomial over a finite field that contains the points and whose leading coefficient is 1, it has the form $P(x) = x^k + Q(x)$, for some polynomial $Q(x)$.

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

(b) What is the value of $Q(x_i)$?

(c) Prove that there exists a unique $P(x)$ with leading coefficient 1 that goes through the k points.

Reminder: Use your answer sheet!!

14. Alice has 3 packets to send to Bob and Charlie. She uses Berlekamp-Welch to protect against 2 general errors, so she sends 7 packets in total. While reconstructing Alice's message, Bob finds the error-locater polynomial $E(x) = (x-1)(x-2)$. Charlie receives the same packets Bob did, but instead finds the error-locater polynomial $E(x) = (x-1)(x-3)$. Assuming *at most* 2 general errors occurred, and Bob and Charlie did not make any mistakes, which of the following must be true?

(a) A corruption occurred on packet 1.

Always True ○

Possibly False ○

(b) No corruption occurred on packets 2 and 3.

Always True ○

Possibly False ○

(c) No corruption occurred on packets 4 through 7.

Always True ○

Possibly False ○

15. In the Berlekamp-Welch scheme, for an n packet message where $n+2k$ points were sent and exactly k packets are corrupted, the resulting equations have exactly 1 solution.

True ○

False ○

8. Counting

1. How many ways are there to put n distinguishable balls into m distinguishable bins?

2. How many ways are there to put n distinguishable balls into m distinguishable bins where the first m balls go into different bins and the remaining $n-m$ balls can go into any of the bins?

3. How many ways are there to put n distinguishable balls into m distinguishable bins such that bin 1 contains 5 balls and bin 2 contains 4 balls? Assume $n \geq 9$.

4. How many ways are there to put n indistinguishable balls into m distinguishable bins?

5. Alberto has two original and very funny Among Us memes that he wants to send to the 5 CS70 slack channels. He wants to post exactly one of the two memes in every channel. If the order in which Alberto posts the memes matter, in how many ways can Alberto post the memes?

6. **6 points.** How many ways are there to put n indistinguishable balls into m distinguishable bins where bin 1 contains at most 5 balls and bin 2 contains at most 4 balls? (Full credit answers should not use summations.)

Reminder: Use your answer sheet!!

9. Staff

Consider making a staff consisting of k_1 TA's, k_2 readers, and k_3 academic interns (AI's) out of n people.

1. Argue using a combinatorial proof that the following expressions are equal.

$$\binom{n}{k_1}\binom{n-k_1}{k_2}\binom{n-k_1-k_2}{k_3} = n!\left(\frac{1}{k_1!}\right)\left(\frac{1}{k_2!}\right)\left(\frac{1}{k_3!}\right)\left(\frac{1}{(n-k_1-k_2-k_3)!}\right)$$

Reminder: Use your answer sheet!!

2. Give a secret sharing scheme where either 3 TAs or a combination of 1 TA, 2 readers, and 3 AI's can reconstruct the secret that decodes the midterm exam. (Each person should only receive one point on any polynomial.)

Reminder: Use your answer sheet!!