CS 70 Discrete Mathematics and Probability Theory
Spring 2021 Parekh and Rao Midterm

Remote Proctoring Instructions.

- On questions 1-10: You need only give the answers on the **“Midterm (Short Answers)” gradescope assignment** within the 2 hour time period of the exam. All short answers and truefalse are worth 3 points. There are roughly 60 questions. (No justification is required.)
- On questions 11-14, the answers will be written on separate sheets of paper for each problem. You will need to scan **four sheets** of paper to a separate **gradescope assignment called Midterm (PDF and long answers.)**. Each problem is worth 15 points. Each problem can only use one page; the solutions use much less, so one page per problem is a **hard limit.**
- Both gradescope assignments will be available at 7:00 PM and the PDF for the **entire exam including short answers** will be available on the “Midterm(PDF and long answers)” assignment.
- **Be sure** to **download** the *PDF* from the Midterm (PDF and long answers) gradescope assignment.
- There will be no clarifications. If a problem has an error, we will address it after the midterm.
- **You have 120 minutes which includes the time to fill out the answers in the Midterm(Short Answers) gradescope assignment and then an extra twenty minutes to scan your paper solutions to the Midterm (PDF and long answers) assignment.**
- For emergencies, email sp21@eecs70.org or use the disruption form at: http://bit.ly/mtdisrupt. Keep working as best possible, we cannot respond in realtime.

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. No negative points on true/false. **So do really scan over the exam a bit.**
- On the Midterm (Short Answers) grade scope assignment, each question has its own Save button. Make sure to click this button for every question; if your page crashes, internet goes down, or anything else happens, only saved questions will be automatically submitted.
- 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., “$d|x$ 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, we will post a global message on piazza and bypass email preferences to inform you of what to do.

In particular, if the short answer gradescope becomes widely problematic we will ask you to scan one page per question with your answers **so keep paper available: one page for each of 10 short answer questions in addition to the 4 pages for the proof questions or** 14 pages in total.

Please do not email in such a global crash as we will not be able to deal with individual issues, just continue with your exam and write your answers on paper; one question per page for short answers, and one question per page for long answers.

Some Latex Commands for Gradescope.

You can (if you choose) use latex. It is fairly easy and satisfying.

Surround an expression by “$$ ... $$” on gradescope and you will be in latex.

Examples: “$$ A+B*D $$” will give: $A + B * D$.

There are useful commands:

1. “$$ A^2 $$” yields A^2
2. $$ \frac{a}{b} $$ yields $\frac{a}{b}$.
3. “\max ” yields max.
4. “a \b ” yields $a \geq b$.
5. “$$ (q^ {-1} \pmod{p})$$” yields $(q^{-1} \pmod{p})$.
6. “{n \choose k-1}” yields $\binom{n}{k-1}$.
7. Grouping with “{ }”: “$$6 ˆ{G * H}$$” yields 6^{G*H}.

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.

   Signed:______________

2. Warmup, Propositions, Proofs

1. $\forall x, y \in \mathbb{R}, \exists z \in \mathbb{R}\ ((x > y) \implies x > z > y)$

   ○ True

   ○ False

2. $\exists z \in \mathbb{R},\ \forall x, y \in \mathbb{R}\ ((x > y) \implies x > z > y)$.

   ○ True

   ○ False

3. For a function $f(x)$, Consider $X = f^{-1}(A \cup B)$ and $Y = f^{-1}(A) \cup f^{-1}(B)$. (Recall that $f(X) = \{y | y = f(x) \text{ for some } x \in X\}$ and $f^{-1}(Y) = \{x | f(x) \in Y\}$.)
   Is $X \subseteq Y$, $Y \subseteq X$, or both?

   □

4. If one has $n+1$ pigeons distributed into n holes, there always exist a hole with at least X pigeons. What is the largest value of X where the statement is true?

   □

5. If $2n+1$ pigeons are placed in an n holes numbered 0 to $n-1$, there always exists a pair of holes numbered i and $i+1 \pmod{n}$ with a total of at least X pigeons in the two holes. What is the largest value of X where the statement is true?

   □

6. The equation $x^5 = 16$ has a rational solution

   ○ True

   ○ False

3. Stable Matchings. 2 points/part.

In the following “favorite” partner means first on preference list, “optimal” partner means the most preferred partner in any stable pairing.

1. There is a stable pairing where no job is paired with the first candidate on their list.

   ○ True

   ○ False

2. If there is a stable pairing where a job j is paired with its pessimal candidate, then all jobs are paired with their pessimal candidate in that stable pairing.

   ○ True

   ○ False

3. No job can improve their final outcome in the jobs propose matching algorithm by submitting a false preference list.

   ○ True

   ○ False

4. No collection of jobs can conspire to improve the outcome of any job j in the jobs propose matching algorithm by jointly submitting false preference lists.

   ○ True

   ○ False

5. If in a run of a jobs propose algorithm, job j is rejected by candidate c because of job j' then job j' can never be rejected by a candidate c' because of job j.

   ○ True

   ○ False

4. Graphs

1. What is the least number of edges whose removal splits a 4 dimensional hypercube into two components of equal number of vertices?

2. What is the least number of edges whose removal splits K_6 into two components of equal number of vertices?

3. There is an even number of odd degree vertices in any graph.

4. A graph for which the average degree of vertices is an odd integer must have an odd number of vertices.

   ○ True

   ○ False

5. What is the length (in edges) of an Eulerian tour of $G = (V, E)$?

6. For a planar graph where every face is bounded by at least 4 edges, derive an upper bound on the number of edges e in terms of v, the number of vertices.

7. For a planar graph with v vertices where every face is bounded by at least 4 edges, there must be a vertex of degree less than or equal to X. What is the minimum value of X where the statement is true? (You may use U, the answer for part 6, or just state the correct number.)

8. For a connected graph with exactly 3 disjoint cycles, what is the minimum number of components in the graph if one removes 5 edges?

9. If a graph does not have an Eulerian tour it does not have a Hamiltonian tour.

○ True

○ False

5. Modular Arithmetic

1. For $x, y \in \mathbb{N}$, with $x < y$, what is the smallest M, where $y \pmod{x} < M$. (Your expression should be in terms of y only.)

   It should be as tight as possible though within 1 of the correct answer is fine.

2. If $gcd(a,m) = x$ and $gcd(b,m) = y$, and $gcd(x,y) = z$, what is $gcd(ab,m)$?

3. If m and n have $gcd(m,n) = 1$, and $n = m+5$, there is a unique $x \pmod{mn}$ where $x = 5 \pmod{m}$ and $y = 0 \pmod{n}$.

   ○ True

   ○ False

4. If m and n have $gcd(m,n) = 1$, and $n = m+5$, find one $x \pmod{mn}$ where $x = 5 \pmod{m}$ and $y = 0 \pmod{n}$. (Expression can possibly use m and n and should be as simple as possible for full credit.)

5. How many values of $a \in \{0, \ldots, 9\}$ is $f(x) \equiv ax \pmod{10}$ a bijection?

6. Calculate the last digit of 7^{2021}.

7. If $x = y^{32}$, and $z = y^1$, give an expression for y^{65} in terms of positive powers of x and z with minimum power of z.

For the following two questions. Consider $m,n \in \mathbb{N}$ where $m,n > 2$. Consider the graph G on mn vertices labeled $V = \{0,\ldots,mn-1\}$, with edges $\{(i, i+m \pmod{mn})$ and $(i, i+n \pmod{mn}) : i \in V\}$.

8. Credit only awarded if both answers are correct.

   (a) If $gcd(m,n) = 1$, what is the maximum degree of a vertex in G?

   (b) If $gcd(m,n) = 1$, what is the number of connected components of G?

9. Credit only awarded if both answers are correct.

   (a) If $gcd(m,n) = d$, what is the maximum degree of a vertex in G?

   (b) If $gcd(m,n) = d$, what is the number of connected components of G?

6. RSA

1. For the RSA scheme where $p = 3$ and $q = 11$, choose an appropriate e and d to complete the construction.

2. For the RSA scheme with p and q, we have that for an integer x.

   Which of the following statements are always true? If none, state none.

   (a) $p|(x^e - x)$
   (b) $p|(x^{ed} - x)$
   (c) $p|x^{ed}$
   (d) $p|x^e$

3. Given x, y, and an RSA encryption scheme with public key where $N = pq$, what is the encryption of $E(xy)$ in terms of $E(x)$ and $E(y)$?

4. To check a signature y of a message m (that is, $y = m^d \pmod N$), for an RSA public key (N, e), how do you recover m? (Answer is expression involving y, N, e.)

7. Modular Arithmetic: Something new.

Define the order of a modulo p to be the smallest positive integer n such that $a^n \equiv 1 \pmod{p}$. Assume p is prime for this problem.

1. Compute the order of 2 modulo 7.

2. Let d be the order of a modulo p, and suppose that $a^n \equiv 1 \pmod{p}$. Compute the value of $n \pmod{d}$. (State a value between 0 and $d-1$.)

3. If d is the order of a modulo p, then

   (a) $d|p$

   (b) $d|(p-1)$

4. At most how many integers in the range $\{0,1,2,\dots,p-1\}$ have order 3 modulo p? (Hint: Consider the polynomial X^3-1. Note that $X=1$ is a solution but 1 has order 1 modulo p.)

8. Polynomials.

All the polynomials are over a field $GF(p)$ for a prime $p > d$ where d is the degree of the polynomial unless otherwise specified.

1. Given three points $P(1) = 1$, $P(2) = 0$, $P(3) = 0$, what is the polynomial $P(x)$ modulo 5. (Hint: this is a $\Delta_1(x)$ in Lagrange interpolation.)

2. If $P(x)$ is a polynomial modulo 5 of degree (at most) 1, and $P(0) = 1$ and $P(1) = 2$, what is $P(x)$?

3. Factor $x^3 + 4 \pmod 5$ as completely as possible. (Hint: what's the relationship between roots and factors?)

4. Every polynomial of degree exactly 1 has exactly 1 root.

   ○ True

   ○ False

5. If a polynomial of degree exactly d has at least $d - 1$ roots, it has exactly d roots.

   ○ True

   ○ False

6. How many packets do you need to send to recover your original message if the length of your message is 5;

   (a) When the channel has a max of 3 erasure errors?

   (b) When the channel has a max of 3 general errors?

(c) When the channel has a max of 2 erasure errors and 2 general errors?

7. Given n points, what is the maximum value of d such that there is at most one degree d polynomial that passes through at least $n-k$ of the given points?

8. Consider a degree 1 polynomial $P(x) = p_1 x + p_0$, and receiving four points $R(0), R(1), R(2), R(3)$ on $P(x)$ with possibly one error. (Recall that $Q(x) = P(x)E(x)$ for an error polynomial $E(x)$ in the Welch-Berlekamp scheme.)

   (a) If the error polynomial $E(x)$ is $x-e$ and $Q(x) = q_2 x^2 + q_1 x + q_0$, what is q_1 in terms of p_0, p_1 and e?

   (b) Working modulo 5, given that $E(x) = x-1$ and $Q(x) = 2x^2 - x - 1$, what is $P(x)$?

9. Counting

1. How many anagrams of the word “SUSPICIOUS” are there?

2. How many anagrams of the word "SUSPICIOUS" are there such that the letter P comes before the letter C, and the letter C comes before the letter O? For example, "PSUSICIOUS" is a valid anagram, but "SISPUCIOUS" is not.

3. How many *strictly* increasing sequences of n integers from 1 to n are there?

4. How many strictly increasing sequences of $n-1$ numbers chosen from 1 to n are there?

5. How many sequences of n numbers from 1 to n are there where removing one number gives a strictly increasing sequence?

6. GME’s stock price is currently \$5000 and angry Melvin Capital investors want to drive the price down. However, due to market restrictions, Melvin Capital’s ability to influence GME stock price at any time is limited two possible techniques:

   - technique A: halving the price.
     For example technique A on the price \$1000 drives the price to \$500.
   - technique B: multiplying the price by $1/5$
     For example technique B on the price \$1000 drives the price to \$200.

   (a) How many different sequences of techniques are there for Melvin Capital to drive the price down to *exactly* \$5?

(b) New technology enables Melvin Capital to perform one additional type of technique:

- technique C: multiplying the price by $1/4$

With this additional technique, how many different sequences of techniques are there for Melvin Capital to drive the price down to *exactly* \$5?

□

7. The Count is back and he has to choose a new 7-digit phone number. Again, we wants it to have the property that the digits are non-increasing. How many phone numbers are there?

□

8. Consider connected graphs with n labeled vertices such that the degree of each vertex is less than 4. How many such graphs have an Eulerian tour?

□

10. Countability

1. Infinite ternary strings.

○ Countable

○ Uncountable

2. The set of irrational numbers in $(0,1)$.

○ Countable

○ Uncountable

3. Constant functions $f : \mathbb{N} \to \mathbb{N}$, where $f(x) = c$ for $c \in \mathbb{N}$

○ Countable

○ Uncountable

4. A countable union of countable sets.

○ Countable

○ Uncountable

5. All finite subsets of $\mathbb{N}$.

○ Countable

○ Uncountable

11. Proof: Induction.

Show that for all positive integers n, $3^{2^n} - 1$ is divisible by 2^{n+2}. (It might be useful to recall: $(a^2 - b^2) = (a-b)(a+b)$.)

12. **Proof: Graphs.**

Show that a connected graph of maximum degree $d \geq 2$ can be vertex colored with d colors as long as there is at least one vertex, v, whose degree $< d$.

13. Modular Arithmetic.

For this problem, let $p \equiv 3 \pmod 4$ and p is prime.

1. Show that $(p-1)/2$ is odd.

2. Show there is no integer a such that $a^2 \equiv -1 \pmod p$. (Hint: Use Fermat's Little Theorem and the previous part.)

14. Combinatorial Proof.

Prove the following combinatorial identity for $n \geq 2k$.

$$k(n-2k+1)\binom{n}{k}\binom{n-k}{k-1} = 2k(2k-1)\binom{n}{2k}\binom{2k-2}{k-1}$$

(Hint: Here's a story. Count the number of ways to create two groups of size k out of n people where exactly one person to be in both groups, and designate one person not in a group as the leader.)