CS 70 Discrete Mathematics and Probability Theory
Fall 2020 Rao Midterm

Remote Proctoring Instructions.

- On questions 1-11: You need only give the answers on the **"Midterm (Short Answers)" gradescope assignment** within the 2 hour time period of the exam. (No justification is required.)
- On questions 12-14, the answers will be written on separate sheets of paper for each part. You will need to scan **seven sheets** of paper to a separate **gradescope assignment called Midterm (PDF and long answers.)**. Each part can only use one page; the solutions use much less, so one page per part is a **hard limit.**
- **Be sure to download the PDF from the Midterm (PDF and long answers) gradescope assignment.**
- Both gradescope assignments will be available at 8:00 PM and the PDF for the **entire exam including short answers** will be available on the "Midterm(PDF and long answers)" assignment.
- There will be no clarifications. If a problem part has an error, we will remove it from 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 individual emergencies, email fa20@eecs70.org or please use the disruption form at: http://bit.ly/70disruption.

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. Also points (pts) are indicated in each problem heading in the pdf. **So do really scan over the exam a bit.**
- The question statement is your friend. Reading it carefully is a tool to get you 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, 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 11 short answer questions in addition to the 7 pages for the proof questions or** 18 pages in total.

Please do not email in this 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 part 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 "{ }": "$$6 ^{G * H}$$" 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 acknowlege 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: 2 points/part unless otherwise stated.

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

   ◯ True

   ◯ False

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

   ◯ True

   ◯ False

   For the following two parts, assume $Q(x,y)$ and $P(x)$ are predicates over the domain of x, y.

3. $(\exists x, \forall y, Q(x,y) \wedge P(x)) \implies \exists x, P(x)$

   ◯ True

   ◯ False

4. $(\exists x, \forall y, Q(x,y) \vee P(x)) \implies \exists x, P(x)$

   ◯ True

   ◯ False

5. $P(0) \wedge (\forall n \in \mathbb{N}\ P(n) \implies P(n+1)) \implies \neg(\exists n \in \mathbb{N} \neg P(n))$

   ◯ True

   ◯ False

6. **More Cards to Flip? (4 points.)** Your friend states that "All plants that are shipped to a Californian address must have originated in California". Staying indoors with windows closed all day, you are suddenly intrigued by this rule.

   Which of the following would you do to test (falsify) your friend's statement?

   (a) Find the destination of Megan's English Ivy plant, being shipped from Oregon
   (b) Find the destination of Tyler's Rubber Tree plant, being shipped from California
   (c) Find the origin of Albert's Aloe Vera plant, who received it in California
   (d) Find the origin of Lili's Bamboo Palm plant, who received it in Seattle

   (Answer may include more than one.)

   ☐

7. If n and m have the same prime factorizations, then they are the same number.

   ◯ True

   ◯ False

8. If $xy = n$ and $uv = n$, with $x < y$ and $u < v$, then $x = u$ and $y = v$.

◯ True

◯ False

9. If $d|x$ and $d|x+2y$ then $d|y$.

◯ True

◯ False

3. Stable Matchings. 2 points/part.

Stable Matching: In the following consider a stable matching instance with n candidates and n jobs each with complete preference lists.

1. The only stable pairing in any instance is produced by the job propose and candidate reject algorithm.

   ◯ True

   ◯ False

2. Any job has a unique pessimal candidate.

   ◯ True

   ◯ False

3. If a candidate rejects a job in the job propose and reject algorithm, there is *no* stable pairing where that candidate and job are paired.

   ◯ True

   ◯ False

4. Consider any stable matching instance, and a run of the job propose and candidate reject algorithm, where exactly one candidate, c, misbehaves. In particular, rejects some job j falsely (that is rejects a job j for a job j' that c prefers less). In this scenario, c is the only candidate that can be in a rogue couple in the final pairing.

   ◯ True

   ◯ False

5. There is **no** stable pairing where every job is paired with its least preferred candidate.

   ◯ True

   ◯ False

4. Graphs. 2 points/part unless otherwise indicated.

All graphs are simple in this problem, unless otherwise stated.

1. Any tree is bipartite.

   ◯ True

   ◯ False

2. Any graph $G = (V, E)$ with $|E| \geq |V|$ is connected.

   ◯ True

   ◯ False

3. Every graph that is vertex-colorable with d colors has max degree $d - 1$.

   ◯ True

   ◯ False

4. Any cycle can be edge colored with 2 colors. (Recall edge coloring is a coloring of edges so that any pair of edges incident to the same vertex have different colors.)

   ◯ True

   ◯ False

5. (4 points) For a graph G, consider a walk which contains any edge at most once and contains all the edges incident to each of its two distinct endpoints, u and v. Recall that a walk is a sequence of edges where successive edges share an endpoint, thus this walk does not reuse edges but does use all the edges incident to u and v.

   If the endpoints, u and v, are different:

   (A) Their degrees must be the same.
   (B) Each must have even degree.
   (C) Each must have odd degree.
   (D) The sum of the degrees of the two vertices is even.

   Answer all that are true.

   ☐

6. Any graph with v vertices and $v - k$ edges for $k \geq 0$ and has exactly one cycle has _____ connected components.

   ☐

7. There is a **simple** graph with average degree of exactly 2 that has no cycles. (Recall that simple means there is at most one edge between any pair of nodes.)

   ◯ True

   ◯ False

8. There is a directed graph, where the sum of the outdegrees *over all vertices* is greater than the sum of indegrees *over all vertices*.

◯ True

◯ False

5. Planar graphs. 3 points/part.

Consider a connected planar graph with $v \geq 3$ vertices, and where every cycle has length at least 6.

1. Give an upper bound on the number of edges, e in terms of the number of vertices, v. (Recall, for example, that any for any planar graph $e \leq 3v - 6$. Your upper bound should be as tight as possible.)

2. How many colors is always sufficient to vertex colored such a graph?

6. Modular Arithmetic:short answer. 2 points per part.

1. What is $2^{11} \pmod{11}$?

2. What is $2^{25} \pmod{33}$?

3. $ab \equiv 0 \pmod{N}$ implies that $a \equiv 0 \pmod{N}$ or $b \equiv 0 \pmod{N}$.

   ◯ True

   ◯ False

4. For primes p and q, find all values of $x \in \{1, \ldots, pq-1\}$, where $x | (a^{k(p-1)(q-1)+1} - a)$?

5. If $a \neq 1 \pmod{N}$ and $a^{k(N-1)} \neq 1 \pmod{N}$ then N is not prime.

   ◯ True

   ◯ False

6. How many solutions are there to $ax = b \pmod{n}$, if $gcd(a,n) = d$ and $gcd(b,n) = d$?

7. Find $x \in \{0, \ldots, pq-1\}$ where $x = a \pmod{p}$ and $x = 0 \pmod{q}$ where p and q are prime? (Answer expression that may involve a, p, q, $\pmod{q}$, $\pmod{p}$ and inverses, e.g., $(q^{-1} \pmod{p})$.)

8. For $x, y \in \mathbb{Z}$ for $x \neq y$, what is the minimum value of $|x-y|$ if $x = y = a \pmod{p}$ and $x = y = b \pmod{q}$ for primes p and q?

7. Another Proof. 3 points/part.

Another proof for RSA can be done as follows.

1. Let S be the set of numbers $\{0,\ldots,pq-1\}$ relatively prime to pq. What is $|S|$? (Recall, a and b are relatively prime if $gcd(a,b)=1$.)

2. For a with $gcd(a,pq)=1$, and $T=\{ax \pmod{pq} | x \in S\}$, what is the size of T?

3. What is $a^{|T|} \pmod{pq}$?

8. Polynomials: Background. 2 points/part.

When we count roots, we mean with multiplicity unless otherwise stated. That is, $Q(x) = (x-2)^2$ has two roots. Polynomials are over a field unless otherwise specified.

1. If two polynomials of degree 7 in share _____ points then they must be the same (working $\pmod{17}$.) (Answer is the smallest integer that makes the statement true.)

2. If a non-zero polynomial has d roots it must have at least degree _____.

3. How many roots does the polynomial, $x^2 - 2 \pmod{5}$ have?

4. If a polynomial has d roots it's degree is at most d.

   ◯ True

   ◯ False

5. Given a polynomial $Q(x) = P(x)(x-2)(x-4)$, and d is the degree of $Q(x)$, what is the degree of $P(x)$?

6. Given a polynomial $Q(x) = P(x)(x-2)(x-4)$, and if $P(x)$ has r roots, what is the number of roots for $Q(x)$?

9. Polynomials: applications. 2 points/part.

Recall for secret sharing and error tolerance to erasures and corruptions that one works over arithmetic modulo a prime p. In each of the following situations, how big should p be? (That is, fill in the blank for $p \geq \_\_\_$.)

1. One wishes to share a secret with b-bits among n people where any k can reconstruct the secret.

2. One wishes to communicate a message of n packets with b bits each and wants to tolerate k erasures?

3. One wishes to communicate a message of n packets with b bits each and wants to tolerate k corruptions?

10. Counting: Basics. 2 points/part.

Let $S = \{1, \ldots, n\}$.

(A) All subsets of S.

(B) The number of subsets of S of size k.

(C) The number of subsets of S of size $n-k$.

(D) The number of ways for k non-negative integers that add up to n.

(E) The number of ways for k positive integers that add up do n.

For each of the expressions, indicate the letter of the option above that it coresponds to.

Provide all answers that match.

1. $\binom{n}{k}$

2. $\binom{n}{n-k}$.

3. $\binom{n-1}{k-1}$.

4. $\binom{n+k-1}{k-1}$.

5. 2^n

11. Counting and Polynomials. 2 points/part.

Counting and Polynomials. Assume all polynomials are over $\pmod p$ where p is a prime and $p > d$.

Again, when we count roots, we mean with multiplicity unless otherwise stated. That is, $Q(x) = (x-2)^2$ has two roots.

1. What is the number of roots of a degree 1 polynomial $\pmod p$? (A degree one polynomial is $ax+b$, where a is non-zero.)

2. What is the number of degree d polynomials?

3. What is the number of exactly degree d polynomials with d distinct roots?

4. What is the number of exactly degree d polynomials with d roots (allowing for multiplicity)?

.

The Remainder of the Exam is written, and you should be scanning 7 pages for you answers.

12. Quick(ish) Proofs. 3pts/3pts/5pts.

You must write your answer for each subproblem on a separate clearly labelled page.

1. Prove: If $d|x$ and $d|y+kx$ then $d|y$ for any integer k.

2. Prove: If n^2-6n+5 is even, then n is odd.

3. Prove by induction: For all positive natural numbers $n \geq 1$ and that $3(7^n)+2^{(5n-3)}$ is divisible by 25. (It may be useful to see that $2^5 = 32 = 25+7$ and that $2^{a+b} = 2^a 2^b$.)

13. Set Operations. 5 points.

For a function g, define the image of a set X to be the set $g(X) = \{y \mid y = g(x) \text{ for some } x \in X\}$.

Hint: For sets X and Y, $X = Y$ if and only if $X \subseteq Y$ and $Y \subseteq X$. To prove that $X \subseteq Y$, it is sufficient to show that $(\forall x)\ ((x \in X) \implies (x \in Y))$.

Let $X \Delta Y = (X - Y) \cup (Y - X)$, where $X - Y = \{x | x \in X and x \notin Y\}$.

Prove $g(X) \Delta g(Y) \subset g(X \Delta Y)$

14. Edge Coloring when there is no Hotel California. 4 pts/4pts/5pts.

Please write your answer for each part on a separate page for scanning.

1. Show that an even length cycle can be edge colored with 2 colors. (Recall edge coloring is a coloring of edges so that any pair of edges incident to the same vertex have different colors.)

   Recall that a bipartite graph $G = (U \cup V, E)$ where $E \subset U \times V$, i.e., there are two sets U and V and every edge consists of a vertex from U and a vertex from V. It is useful to recall (without proof) that any cycle in a bipartite graph has even length.

   For the following two parts, we consider a bipartite graph, $G = (U \cup V, E)$ where every vertex has degree $d = 2^k$.

2. Show that $|U| = |V|$.

3. Show that the graph can be edge colored with $d = 2^k$ colors. (Hint: a previous part has something to do with $k = 1$.)