CS 70 Discrete Mathematics and Probability Theory
Fall 2020 Rao

Midterm Solutions

PRINT Your Name: Oski Bear

SIGN Your Name: *OSKI*

Do not turn this page until your instructor tells you to do so.

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. $\neg(P \implies Q) \equiv (P \wedge \neg Q)$
   Answer: True. $\neg(P \implies Q) \equiv \neg(\neg P \vee Q) \equiv (P \wedge \neg Q)$.
2. $\forall x \in S, (Q(x) \vee P(x)) \equiv (\forall x \in S, Q(x)) \vee (\forall x \in S, P(x))$
   Answer: False. Consider S to be the naturals and $P(x)$ to be x is even and $Q(x)$ to be x is odd. It is not true that either every natural number is odd, or that every natural number is even.
   For the following two parts, assume $Q(x,y)$ and $P(x)$ are predicates over the domain of x, y.
3. $(\exists x, \forall y, Q(x,y) \wedge P(x)) \implies \exists x, P(x)$
   Answer: True. There is an x where both $Q(x,y)$ and $P(x)$ are true, so there is an x where $P(x)$ is true.
4. $(\exists x, \forall y, Q(x,y) \vee P(x)) \implies \exists x, P(x)$
   Answer: False. $P(x)$ could always be false, and $Q(x,y)$ could always be true.
5. $P(0) \wedge (\forall n \in \mathbb{N}\ P(n) \implies P(n+1)) \implies \neg(\exists n \in \mathbb{N} \neg P(n))$
   Answer: True. This is the principle of induction except that the right hand side is a negation of the negation of $\forall n \in \mathbb{N},\ P(n)$.
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.)
   Answer: (a) and (c). English Ivy from Oregon, if being shipped to California, would break the rule. The Aloe Vera being received in California, if shipped from elsewhere, would also break the rule. Since the Rubber Tree was shipped from California, it could go anywhere and not break the rule. Since Lili recieved the Bamboo plant in Seattle, any origin would not break the rule.

7. If n and m have the same prime factorizations, then they are the same number.
   Answer: True. They multiply out to the same thing.
8. If $xy = n$ and $uv = n$, with $x < y$ and $u < v$, then $x = u$ and $y = v$.
   Answer: False. For example, $x = 2$, $y = 15$ and $u = 6$ and $v = 5$. Really this is a question about prime factorization: in this case, $2 \cdot 3 \cdot 5$ is the prime factorization of 30.
9. If $d|x$ and $d|x+2y$ then $d|y$.
   Answer: False. $d = 2, x = 2$ and $y = 1$.

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.
   Answer: False. It produces one, many instances have more than one pairing.
2. Any job has a unique pessimal candidate.
   Answer: True. By definition, the instance has no ties among those in their preference lists, and 'pessimal' is defined to be the worst candidate in any stable matching.
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.
   Answer: True. The job optimality of the propose-and-reject implies that there is no "better" stable pairing for any job. Thus, if a job is rejected there can be no stable pairing between the job and the corresponding candidate.
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.
   Answer: True. Say (j'', c') is a rogue couple, but the improvement lemma holds for c', and j'' would have asked c' prior to whomever they end up with, therefore c' would not have rejected them other than c.
5. There is **no** stable pairing where every job is paired with its least preferred candidate.
   Answer: False. Make an instance where each candidate has a different job that is first in its preference list, and each job has the corresponding candidate last in its preference list. The pairing where the candidates gets their first job is now stable, as there are no rogue pairs.

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

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

1. Any tree is bipartite.
   Answer: True. Color a vertex red. The repeatedly and alternatively color the uncolored neighbors blue and red. When vertices are being colored, they neighbor a vertex of a different color or uncolored. If the endpoints of an edge are colored in the same step, the graph would contain a cycle. A tree does not contain a cycle.
2. Any graph $G = (V, E)$ with $|E| \geq |V|$ is connected.
   Answer: False. Two disjoint cycles is not connected.

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

   Answer: False. Any bipartite graph is two colorable and can have abitrary degree.

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.)

   Answer: False. A cycle of length 3 cannot be edge colored since every pair of edges share a common vertex.

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.

   Answer: C and D. Can't be even since "if you enter you can leave", so both endpoints have odd degree. The sum of two odds is even. There is no reason that the degrees must be the same: e.g., one could be degree 1 and the other could be degree 3 if the walk consists of an edge and then a cycle back to one of the edges endpoints.

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

   Answer: $k+1$. For $k=0$, this must be a tree plus an edge as there is only one cycle. Inductively assume that there are k components. And for $k+1$ one, removing an edge that is not in the cycle increases the number of components by one.

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.)

   Answer: False. If the average degree is 2, than the number of edges is $|V|$ which implies it is not a tree and has a cycle if connected, or one of its connected components has a cycle.

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*.

   Answer: False. Each arc contributes one to the total outdegree and one to the total indegree.

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.)

   Answer: $(3v-6)/2$. We have that every face has length ≥ 6, so $6f \leq 2e$, or $f \leq e/3$. Plugging into Euler's formula: $v+f=e+2$, we obtain $v+e/3 \geq e+2$ and simplifying we obtain $e \leq (3v-6)/2$.

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

   Answer: 3. From the previous part, the sum of degrees is $2e$ which is at most $(3v-6)$ and therefore there is a vertex of degree at most 2. One can remove and inductively color the remaining graph.

This works since emoving an vertex of degree at most 2 in the graph is always possible from the previous part and does not create any cycles, thus 3 colors is sufficent using induction. The base case of 3 vertices can clearly be colored with 3 colors.

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

1. What is $2^{11} \pmod{11}$?
   Answer: 2. $2^{10} = 1 \pmod{11}$ is $1 \pmod{11}$ by FLT.
2. What is $2^{25} \pmod{33}$?
   Answer: 32. $2^{20} = 1 \pmod{33}$ since $2^{(11-1)(3-2)} = 1 \pmod{33}$ by FLT plus CRT.
3. $ab \equiv 0 \pmod{N}$ implies that $a \equiv 0 \pmod{N}$ or $b \equiv 0 \pmod{N}$.
   Answer: False. Consider $N = 6$, and $a = 2$ and $b = 3$.
4. For primes p and q, find all values of $x \in \{1, \ldots, pq-1\}$, where $x | (a^{k(p-1)(q-1)+1} - a)$?
   Answer: p and q. This is from the fact that RSA decodes, so the expression is $0 \pmod{pq}$ and is thus divisible by p and q. In fact, the proof of RSA proves that it is divisible by p and q using Fermat's little theorem and then applies CRT.
5. If $a \neq 1 \pmod{N}$ and $a^{k(N-1)} \neq 1 \pmod{N}$ then N is not prime.
   Answer: True. Fermat's theorem implies for primes that $a^{N-1} = 1 \pmod{N}$ and therefore that $a^{k(N-1)} = 1 \pmod{N}$, and thus N cannot be prime.
   False. The above was intended to say $a \neq 0 \pmod{N}$. We gave everyone credit for this one.
6. How many solutions are there to $ax = b \pmod{n}$, if $gcd(a,n) = d$ and $gcd(b,n) = d$?
   Answer: d. Notice that $ax/d = b/d \pmod{n/d}$ has one solution since $gcd(a/d, n/d) = 1$, or $ax/d = b/d + k(n/d)$, and if $x' = x + j(n/d)$ yields an equation $ax'/d + b/d + k'(n/d)$ with $k' = k + (aj/d)$ which is an integer since $d|a$. Now multiply through shows that $ax = b \pmod{n}$ for both x and x'. Now there are d multiples of n/d that keep x' in the range $\{0, \ldots, n-1\}$ (including 0.)
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., $(q^{-1} \pmod{p})$.)
   Answer: $aq(q^{-1} \pmod{p})$. CRT. That is, $q(q^{-1} \pmod{p}) = 0 \pmod{q}$ as there is a multiple of p and $q(q^{-1} \pmod{p}) = 1 \pmod{p}$ by definition of inverse.
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?
   Answer: pq. There is only one solution $\pmod{pq}$ to such equations according to the CRT.

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 $gcd(a,b) = 1$.)
   Answer: $(p-1)(q-1)$. pq minus the numbers divisible by p and the numbers divisible by q and except 0 is subtracted twice: $pq - p - q + 1 = (p-1)(q-1)$.
2. For a with $gcd(a, pq) = 1$, and $T = \{ax \pmod{pq} | x \in S\}$, what is the size of T?
   Answer: $(p-1)(q-1)$. The function $f(x) = ax \pmod{pq}$ is a bijection from S and T is exactly the set of numbers that are relatively prime to pq.

3. What is $a^{|T|} \pmod{pq}$?
   Answer: 1. Since $f(x) = ax \pmod{pq}$, we have that the set S is the same set as the set of equivalence classes $\pmod{pq}$ that are relatively prime to pq. Multiplying the elments together gives a factor of $a^{|S|}$ on one side and then one can multiply by the multiplicative inverses to remove all other factors as they are relatively prime to 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.)
   Answer: 8. Any degree 7 polynomials that share 8 points agree.
2. If a non-zero polynomial has d roots it must have at least degree _____.
   Answer: d. As the roots can be factored out.
3. How many roots does the polynomial, $x^2 - 2 \pmod{5}$ have?
   Answer: 0. By enumeration: $(1)^2 - 2 = -1 \pmod{5}$ and so on.
4. If a polynomial has d roots it's degree is at most d.
   Answer: False. See the previous answer.
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 $P(x)$?
   Answer: $d-2$.
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 $Q(x)$?
   Answer: $r+2$.

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.
   Answer: $p \geq \max(2^b, n+1)$. The modulus needs to be large enough so that one can represent the secret s and should be large enough to have $n+1$ different points on which to evaluate the polynomial.
2. One wishes to communicate a message of n packets with b bits each and wants to tolerate k erasures?
   Answer: $p \geq \max(2^b, n+k)$. The modulus needs to be large enough so that one can represent each packet and should be large enough to have $n+k$ different points on which to evaluate the polynomial.
3. One wishes to communicate a message of n packets with b bits each and wants to tolerate k corruptions?
   Answer: $p \geq \max(2^b, n+2k)$. The modulus needs to be large enough so that one can represent each packet and should be large enough to have $n+k$ different points on which to evaluate the polynomial.

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. $\binom{n}{k}$
   Answer: B and C. This is from class for A, and it also counts B as $\binom{n}{k} = \binom{n}{n-k}$.
2. $\binom{n}{n-k}$.
   Answer: B and C. This is from class for A, and it also counts B as $\binom{n}{k} = \binom{n}{n-k}$.
3. $\binom{n-1}{k-1}$.
   Answer: E. Here again, we want k numbers but each group has to have at least 1, so we can just have $n-k$ stars and then add 1 to the value we get for each group of stars that are separated by bars.
4. $\binom{n+k-1}{k-1}$.
   Answer: D. n stars separated by $k-1$ bars yields k groups of stars whose sizes add up to n. The expression comes from choosing $k-1$ places to put bars.
5. 2^n
   Answer: A. Each of n elements can be in the set of not.

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.)
   Answer: 1. $x = a^{(-1)}b \pmod p$ is a root, and there is at most 1.
2. What is the number of degree d polynomials?
   Answer: $(p-1)p^d$. One needs to choose a non-zero first coefficient, and then one can choose arbitrary coefficients for the remaining ones.
3. What is the number of exactly degree d polynomials with d distinct roots?
   Answer: $(p-1)\binom{p}{d}$. There are $\binom{p}{d}$ ways to choose the roots and one can multiply the expression by an arbitrary non-zero leading coefficient.
4. What is the number of exactly degree d polynomials with d roots (allowing for multiplicity)?
   Answer: $(p-1)\binom{d+p-1}{d}$. We have p possible roots and the total number of roots is d, so it is p numbers that add up to d.

.

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.

   Answer: By definition of divides $x = id$, $y + kx = jd$. Thus, $y = jd - k(id) = d(j - ik)$ and since $(j - ik)$ is an integer due to the closure of integer multiplication and addition $d|y$.

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

   Answer: Proof by Contraposition. If n is even, then $n = 2k$ and $n^2 - 6n + 5 = 4k^2 - 24k + 5 = 2(2k^2 - 12k + 2) + 1$ and is therefore 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 $2^{a+b} = 2^a 2^b$.)

   Answer: For $n = 1$, the statement is "$21 + 4$ is divisible by 25", which is true. Assume that the statement holds for $n = k$, such that $3(7^n) + 2(5n - 3)$ is divisible by 25. Then,

$$\begin{aligned} 3 \cdot 7^{k+1} + 2^{5(k+1)-3} &= 3 \cdot 7 \cdot 7^k + 2^{5k-3+5} \\ &= 7 \cdot 3 \cdot 7^k + 2^5 \cdot 2^{5k-3} \\ &= 7 \cdot 3 \cdot 7^k + 32 \cdot 2^{5k-3} \\ &= 7 \cdot 3 \cdot 7^k + 7 \cdot 2^{5k-3} + 25 \cdot 3^{3k-1} \\ &= 7\left(3 \cdot 7^{k-1} + 2^{5k-3}\right) + 25 \cdot 2^{5n-3} \end{aligned}$$

   The first term is divisible by the inductive hypothesis, and the second term is clearly divisible by 19. This completes our proof, as we've shown the statement holds for $k + 1$.

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

Answer: To show $g(X)\Delta g(Y) \subseteq g(X\Delta Y)$. Let $y \in g(X)\Delta g(Y)$. If $y \in g(X) - g(Y)$, then there exists $x \in X$ with $y = g(x)$ and for all $x \in Y$ and $y \neq g(x)$, thus $x \in X - Y$. Similarly, if $y \in g(Y) - g(X)$ we have $x \in Y - X$.

The intended question was $g(X)\Delta g(Y) \subseteq g(X\Delta Y)$ not the strict inequality shown above.

Those who recognized the strict issue were awarded partial points as that case is poorly phrased. The correct thing to show strictness is to give an example for X, Y and $g(\cdot)$ where the inequality is strict.

Such an example is $X = \{1,2\}$, $Y = \{2,3\}$, $g(1) = g(3) =$ 'A', and $g(3) =$ 'B'. Here, $g(X)\Delta g(Y) = \phi$ where $g(X\Delta Y) = \{$'A'$\}$.

Alternatively, one can show the inequality is not-strict, by letting having $g(\cdot) =$ 'A' (i.e., a constant function) on all values in which case both $g(X)\Delta g(Y) = g(X\Delta Y) = \phi$.

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.)

   Answer:

   Traverse the cycle, color the edges with $i \pmod 2$ where i is the ith step in the traveral. The colors of edges incident to an intermediate vertex are different since $i \neq i+1 \pmod 2$. When one returns to the original vertex, the color of the incoming arc is $k = 0 \pmod 2$ where k is length of the cycle and the equality, where the first edge had color $1 \pmod 2$, and so these edges are differently colored as well.

   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 $|U| = |V|$.

   Answer: The total number of edges incident to the set U is $|U|d$ since every vertex in U has degree d. Moreover, each edge in E is incident to a vertex in U. Thus, $|U|d = |E|$. Similarly $|V|d = |E|$. The two statements imply that $|U|d = |V|d$ or 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 $k = 1$.)

   Answer: We will do this by induction on k.

   Each connected component can be traversed using an Eulerian Tour.

Begin from an arbitrary vertex $u \in U$ and traverse the tour and place alternative edges into two groups; the odd edges go to group 1 and the even go to group 2.

Notice that group 1 edges leave vertices in U, and group 2 edges enter vertices in U in this traversal. This is flipped for V.

Form two graphs from the two sets of edges. Each graph has degree 2^{k-1} as each vertex since one always enters and leaves each vertex the same number of times in an Eulerian Tour, the two sets induce the same degree on each vertex in U (and similarly in V.)

One can than recursively color the edges in the two graphs with 2^{k-1} colors each, which yields a $2(2^{k-1}) = 2^k$ colors.

The base case is a degree 2 graph, where each connected component is a simple cycle of even length (due to it being bipartite), and it follows from the previous part that this can be 2-colored.