CS 70 Discrete Mathematics and Probability Theory
Fall 2021 Ayazifar and 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 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.
- (Remote) 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. 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) $\forall x \in U, W(x) \implies B(x)$.

   Answer: False. This is the converse of $B(x) \implies W(x)$, which is not necessarily true even if $W(x) \implies B(x)$ is true.

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

   Answer: False. This is contradicted if there is a student who does not want to save the world or want a billion dollars by the time they're 30.

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

   Answer: True. For any student for which $S(x) \vee B(x)$ is true, either $S(x)$ is true (in which case $R(x)$ is true) or $B(x)$ is true (in which case $W(x)$ is true), so the implication always holds.

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

   Answer: True. For any student for which $S(x) \wedge B(x)$ is true, both $S(x)$ is true (so $R(x)$ is true) and $B(x)$ is true (so $W(x)$ is true), so the implication always holds.

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

   Answer: True. This is just the contrapositive of $S(x) \implies R(x)$, which holds for every x.

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

   Answer: True, by the same logic as the previous part.

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

   Answer: True. If $2|a$, then the prime factorization of a contains 2, and a^3 contains 2^3 and thus 4 divides a^3. Thus, the contrapositive is true and the statement is true.

3. For an integer a, if $2 \not| a$ then $4 \not| a^3$.

   Answer: True. If $4|a^3$, and note the prime factorization of $a^3 = p_1^3 \cdots p_m^3$ where $a = p_1 \cdots p_m$ and at least one of the p_i must be 2.

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.

   Answer: True. Neither job can participate in a rogue pair since they both have their favorite candidate.

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.

   Answer: False. Consider the preference lists.

$$\begin{array}{ll} A: \ 1,2 & 1: B,A \\ B: \ 1,2 & 2: B,A \end{array}$$

   The pairing $(A,1)$ and $(B,2)$ satisfies the property and B and 1 is a rogue couple.

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

   Answer: False.

$$\begin{array}{ll} A: \ 3,1,2 & 1: \ C,A,B \\ B: \ 1,2,3 & 2: \ A,B,C \\ C: \ 2,3,1 & 3: \ B,C,A \end{array}$$

   The pairing $(A,1),(B,2),(C,3)$ is stable (for each job, they are the least favorite job of the candidate they prefer to their current partner), and nobody is paired with their favorite partner.

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

   Answer: 0. This is really asking if every job can get rejected during a run of the job-proposed algorithm. Consider a 3-job example where the first two jobs ask the first candidate, one is rejected and then asks the same candidate as the third job, who is rejected and then ask the first candidate who then rejects the first job. So everyone got rejected once. Preference list that make that happen are as follows:

$$\begin{array}{ll} A: \ 1,2,3 & 1: \ C,A,B \\ B: \ 1,2,3 & 2: \ A,B,C \\ C: \ 2,1,3 & 3: \ B,C,A \end{array}$$

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

   Answer: $n^2 - n$. There are at most that many unmatched pairs, and any matching that consists of pairs where the entities are each other's least favorite partner has the property that all pairs not in the matching are rogue. One can set up preference lists where everyone's least favorite partners form a matching.

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

   Answer: 1. Euclid's algorithm produces the Fibonacci sequence from F_n to F_1 as arguments during the recursion, i.e. the argument of gcd is $F_n \pmod{F_{n-1}} = F_n - F_{n-1} = F_{n-2}$.

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.)

   Answer: $(-1)^{n-1} F_n \pmod{F_{n-1}}$ which is $(-1)^{n-1} F_{n-2} \pmod{F_{n-1}}$.The iterative version of extended gcd produces a multiplier of (-1) on the second equation in each step of the procedure, i.e.

$$\begin{aligned}
(1)F_n + (0)F_{n-1} &= F_n \\
(0)F_n + (1)F_{n-1} &= F_{n-1} \\
(1)F_n - (1)F_{n-1} &= F_{n-2} \\
(-1)F_n + (2)F_{n-1} &= F_{n-3} \\
(2)F_n - (3)F_{n-1} &= F_{n-4} \\
\vdots &= \vdots \\
(-1)^{n-2}(F_{n-1})F_n + (-1)^{n-1}(F_n)F_{n-1} &= 0
\end{aligned}$$

   Notice that the coefficient of F_{n-1}, one "adds" the coefficients of two previous terms in absolute value, and the signs alternate. The final coefficient of F_{n-1} when

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

   Answer: Base case: For $n = 1$, the LHS is $F_1 = 1$. The RHS is $F_3 - 1 = 2 - 1 = 1$. So the base case holds.

   Inductive hypothesis: $\sum_{i=1}^{n} F_i = F_{n+2} - 1$. We want to show $\sum_{i=1}^{n+1} F_i = F_{n+3} - 1$.

   Inductive step:

$$\sum_{i=1}^{n+1} F_i = \sum_{i=1}^{n} F_i + F_{n+1} = F_{n+2} - 1 + F_{n+1} = F_{n+3} - 1.$$

5. Proofs.

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

   Answer: Proof by contrapositive: We show if $a \leq 700$ and $b \leq 700$ and $c \leq 700$, then $a + b + c \leq 2100$. This follows by just adding the first inequalities.

   Proof by cases: If $a > 700$ or $b > 700$ we're done. Otherwise $c > 2100 - a - b \geq 700$.

   Direct proof: By symmetry, assume wlog $a \geq b \geq c$. Then $2100 < a + b + c \leq 3a$, so $a > 700$.

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.)

   Answer: Given base cases of 30 and 35, let m be the number of cents we wish to make change for. If m is a multiple of 10, we just use $m/10$ dimes. Otherwise, $m = 10k+5$ for some integer $k \geq 2$. In this case, we just use 1 quarter and $k-2$ dimes, whose total value is $25+(k-2)10 = 10k+5$ cents.

   More indirectly one can use proof by induction similarly to lecture to show for all $k \geq 5$, we can make $5k$ cents. The base cases $k = 5,6$ are satisfied by a quarter or three dimes. The inductive step is to inductively make change for $5(k-2)$ cents, and then add a dime to make change for $5k$ cents.

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.

   Answer: Proceed by contradiction. Suppose M_1 is job-preferred to M_2, but M_2 is not candidate-preferred to M_1. Then there exists a candidate C that prefers M_1 over M_2. Let $(J,C) \in M_1$ and let $(J',C) \in M_2$, where C prefers J over J'. Let C' be the candidate matched to J in M_2, so $(J,C') \in M_2$. Since M_1 is job-preferred to M_2, J prefers C over C'. However, this means that (J,C) would be a rogue couple in M_2, contradicting the assumption that M_2 is stable.

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:
   U:

   Answer: $L : 3n/2$, $U : 3n/2$. The number of edges in a graph where vertex v has degree $d(v)$ is $\frac{1}{2}\sum_{v\in V} d(v)$, which is $3n/2$ if every vertex has degree 3.

   (b) For a complete graph on n vertices.
   L:
   U:

   Answer: $L = U : \binom{n}{2} = n(n-1)/2$. There are $\binom{n}{2}$ pairs of vertices, each with an edge between them.

   (c) For a hypercube of dimension n.
   L:
   U:

   Answer: $L = U : n2^{n-1}$. Each vertex has degree n and there are 2^n of them, so the total number of edges is $\frac{1}{2}\sum_{v\in V} d(v) = n2^n/2 = n2^{n-1}$

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

Answer: $L = U : n - c$. One way to see this: Start with the graph with no edges (which has n components), and add the edges in one by one. Since adding the edges doesn't create cycles, each edge we add has endpoints in different components, i.e. reduces the number of components by 1. So we need to add $n - c$ edges to go from n components to c components.

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

Answer: $L = U : n - 1$. The graph is connected so it must have at least $n - 1$ vertices. A graph with average degree d has $nd/2$ edges. Since $d < 2$, this must be strictly less than n, i.e. at most $n - 1$.

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

Answer: $L : n - 1$, $U : 2n - 4$. The lower bound follows because the graph is connected. The upper bound was seen in lecture, but to recount the proof: Since the graph is bipartite, it can't have odd-length cycles, so all cycles have length at least 4. This gives $4f \leq 2e$, and plugging into $e + 2 = v + f$ we get $e + 2 \leq v + e/2$. Solving for e gives $e \leq 2(v - 2) = 2n - 4$.

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

Answer: $L : n - 1$, $U : 3(n - 2)/2$. Partial credit for $5(n - 2)/3$. There can be no cycle of length 5 (graph is bipartite) so the minimum length cycle is of length 6. $6f \leq 2e$ and $e + 2 = v + f$. This yields, $e + 2 \leq v + \frac{1}{3}e$. Solving yields $e \leq \frac{3}{2}(v - 2)$. Use $v = n$.

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:

Answer: $L : N/2$, $U : (N \log N)/2$. The minimum sized cut, cuts the hypercube into 2 pieces. The graph is bipartite so there is a cut that cuts all edges.

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:

Answer: $L : 1, U : d$. There is a degree 1 vertex which can be cut, and take S to include the maximum degree vertex.

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

   L:
   U:

   Answer: $L: 2, U: d+1$. The lower bound is due to an edge existing so one must use at least 2 colors. The upper bound is due to the coloring algorithm of removing a vertex, coloring the remaining graph and when the vertex is put back, its neighbors use d colors, so one of the $d+1$ is available.

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

   L:
   U:

   Answer: $L = U : d$. The edges next to the degree d-vertex need d different colors. In addition, we can color the graph with at most d colors using recursion since the graph is acyclic, i.e. a collection of trees. Delete a leaf vertex, recursively color the rest of the graph using at most d colors, and then add the leaf back. This adds one edge, next to at most $d-1$ other edges, so there is a color we can choose for this edge that maintains the validity of the coloring.

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.
   Answer: True. A graph is nonplanar if it contains K_5.

   (b) What is the largest number of edges that can be removed without disconnecting Big Chungus?
   Answer: 6. Notice that the graph is a tree attached to K_5. As such, we can remove 6 edges from K_5 without disconnecting it.

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.

   Answer: True. There is a two-coloring of each component. Adding an edge may join two vertices of the same color, but one can switch the colors in one component and the coloring will then be valid.

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.)

   Answer: $n/2$. Then, the new vertex will then be connected to a pair of vertices that are adjacent in the cycle since otherwise there would be at least $n/2$ vertices that it was not connected to.

9. Every bipartite planar graph has an Eulerian tour.

   Answer: False. An example is a graph consisting of a single edge.

7. More Short answer: modular arithmetic and polynomials

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

   Answer: $5 \pmod{24}$, since $5 \cdot 5 = 25 = 24 + 1$.

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

   Answer: $a \pmod{35}$. The idea is this is the result of encrypting and decrypting the message a using RSA (which in turn recovers the original message), where $p = 5, q = 7, e = 5, d = 5$.

   More indirectly, one can appeal to FLT to see $a^4 \equiv 1 \mod 5, a^6 \equiv 1 \mod 7$. So $a^{24} \equiv 1 \mod 5$ and $a^{24} \equiv 1 \mod 7$, which by CRT implies $a^{24} \equiv 1 \mod 35$.

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

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

   Answer: True. $x^{-1}(x^1 + \cdots + x^{p-1}) = 1 + \cdots + x^{p-2} = x^{p-1} + x^1 + \cdots + x^{p-2} = k(x) \pmod{p}$ since $x^{p-1} = 1 \pmod{p}$.

   (b) **6 points**

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

   Answer: $x = 1 \pmod{p}$. From the previous part, we have $k(x) = x^{-1}k(x) \pmod{p}$ and $k(x)(x^{-1} - 1) = 0 \pmod{p}$. Thus, unless $x^{-1} = 1 \pmod{p}$, we have $k(x) = 0 \pmod{p}$.

   We gave partial credit to the claim that $\{x, x^2, \ldots, x^{p-1}\}$ has a bijection with $\{1,2,\ldots(p-1)\} \pmod{p}$. This isn't always true (e.g, the powers of 2 are only equivalent to one of 1, 2, 4 $\pmod{7}$), but it is true quite often. When it is true, then we have $k(x) \equiv p(p-1)/2 \pmod{p}$, and since p is odd this is a multiple of p.

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

   Answer: True. We show $m | \frac{mn}{d}$ as follows. Since $d | n$, we have $n = kd$ and $\frac{mn}{d} = km$.

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

   Answer: d. There is a single solution for $y = a/d \pmod{m/d}$ and $y = b/d \pmod{n/d}$, and $x = yd + imn/d \pmod{mn}$ for $i \in \{0,\ldots,d-1\}$ satisfies $x = a \pmod{m}$ and $x = b \pmod{n}$ as $mn/d = 0 \pmod{m}$ and $mn/d = 0 \pmod{n}$. Any $z = 0 \mod m$ and $z = 0 \pmod{n}$ implies that z is a multiple of mn/d, these are the only solutions.

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

   Answer: a. By definition, $nn^{-1} \pmod{m} \equiv 1 \pmod{m}$.

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?

   Answer: 13. This means $r = 3 \pmod{5}$ and $r = 1 \pmod{4}$. Using CRT, we get 13

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

   Answer: 33. CRT gives a unique solution $\pmod{pq}$, so $4 * 5 = 20$ shots after the 13th round 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?

Answer: 67. This is the smallest prime greater than $\max(2^6, 47+1)$. The field should be able to represent the secret and have $47+1$ points.

9. Give a degree 2 polynomial that passes through $(1,1),(2,0)$ and $(3,0)$ over $GF(5)$ (or $\pmod{5}$.)
   Answer: $3(x-2)(x-3)$. Lagrange for point 1, and don't need for points 2 and 3.

10. **6 points**
    Show that $x^{p!} = 1 \pmod{p}$ for $x \not\equiv 0 \pmod{p}$.
    Answer: $x^{p!} = (x^z)^{p-1} = 1 \pmod{p}$ for $z = p!/(p-1)$ for $x \not\equiv 0 \pmod{p}$ by Fermat's Theorem..

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

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

   (a) Evaluate $x^{3!} \pmod{7}$ for $x \neq 0 \pmod{7}$.
   Answer: $1 \pmod{7}$. $x^6 = 1 \pmod{7}$ by Fermat's Theorem.

   (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 $0! = 1$.)
   Answer: $x^2 + 2x + 4$. The terms corresponding to $k \geq 3$ are all powers of x^6, and in turn are equivalent to $1 \pmod{7}$ by the previous part. There are 98 of them, so this is equivalent to $4 + 98 + x^{0!} + x^{1!} + x^{2!}$. This is equivalent to $x^2 + 2x + 4 \pmod{7}$.

   (c) What are the roots of the resulting polynomial? (Maybe useful: $4 = -3 \pmod{7}$.)
   Answer: $1, 4 \pmod{7}$. The polynomial is equivalent to $x^2 + 2x - 3 \pmod{7}$. This can be factored as $(x+3)(x-1)$ whose roots are $-3 = 4 \pmod{7}$ and $1 \pmod{7}$.

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 $x \equiv (-2)^{-1} \pmod{7}$.
   Answer: 10. The inverse of -2 is $3 \pmod{7}$ which is equivalent to $10 \pmod{7}$.

   (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.
   Answer: $10^{-1} \pmod{d}$. $(10a+b) \times (10^{-1} \pmod{d}) = a + 10^{-1}b \pmod{d}$. So $(10a+b)$ is equivalent to $0 \pmod{d}$, i.e. divisible by d, iff $a + 10^{-1}b \pmod{d}$ is divisible by 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 $Q(x)$?
   Answer: $k-1$. Since $P(x)$ can be written as $x^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_1x + a_0$, $Q(x)$ can be written as $a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_1x + a_0$.

   (b) What is the value of $Q(x_i)$?
   Answer: $y_i - x_i^k$, since $Q(x_i) = P(x_i) - x_i^k = y_i - x_i^k$.

(c) Prove that there exists a unique $P(x)$ with leading coefficient 1 that goes through the k points.
Answer: For each i, $P(x_i) = x_i^k + Q(x_i)$ since $Q(x_i) = y_i - x_i^k$. It is unique as $Q(x)$ is uniquely determined by the k points above and any $P(x)$ has this form.

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.
Answer: Not necessarily true - it's possible no corruptions occurred at all, in which case any choice of $E(x)$ is valid, and Bob and Charlie just happened to both choose 1 as a root of $E(x)$.

(b) No corruption occurred on packets 2 and 3.
Answer: True. From Bob's solution, we have $r_i = P(i)$ for all $i \neq 1,2$. From Charlie's solution, we have $r_i = P(i)$ for all $i \neq 1,3$. Putting these together, we have $r_i = P(i)$ for all $i \neq 1$.

(c) No corruption occurred on packets 4 through 7.
Answer: True. For the same reason as the previous part.

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.

Answer: True. The computed error polynomial, $E(x)$, must have roots at the k corrupted points so is uniquely determined. Now $Q(x) = P(x)E(x)$ on $n+k$ points and has degree $k-1$ so must be the same polynomial as $P(x)E(x)$.

8. Counting

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

Answer: m^n. There are m possibilities for each of n choices.

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?

Answer: $m!m^{n-m}$. There are $m!$ ways to put the first m balls into the m bins, and each remaining $n-m$ ball can choose from any of m possibilities.

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 $n \geq 9$.

Answer: $\binom{n}{5}\binom{n-5}{4}(m-2)^{n-9}$. We have $\binom{n}{5}$ different ways to choose the balls 5 in bin 1. Then, there are $\binom{n-5}{4}$ ways to choose 4 of the remaining $n-5$ balls to place in bin 2. Then, for each of the remaining $n-9$ balls we can place it in one of the $m-2$ remaining bins.

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

Answer: $\binom{n+m-1}{m-1}$. n stars for balls, $m-1$ bars for separating into 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?

Answer: $5!2^5$. For each server, Alberto has 2 choices of which meme goes where, for a total of $2^5 = 32$ choices for meme per server. Then, there are 5! different orderings, for a total of $32 \cdot 5! = \boxed{3840}$ different ways to 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.)

   Answer: We use inclusion/exclusion. Let A be the set of ways to place balls such that bin 1 gets at least 6 balls, and B be the set of ways to place balls such that bin 2 gets at least 5 balls. We want to count the size of $A \cup B$ (the number of invalid ways to place balls), and then subtract that from the answer to the previous part (the number of ways to place balls, valid or invalid), to get the total number of valid ways to place balls.

   To count the number of ways in A, in each way we first place 6 balls in bin 1, and then distribute the remaining $n-6$ balls among the m bins. This gives $|A| = \binom{n+m-7}{m-1}$ by stars and bars. By a similar argument, $|B| = \binom{n+m-6}{m-1}$ and $|A \cap B| = \binom{n+m-12}{m-1}$. Putting it all together, we get:

$$\binom{n+m-1}{m-1} - \binom{n+m-7}{m-1} - \binom{n+m-6}{m-1} + \binom{n+m-12}{m-1}.$$

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.

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

   Answer: The left hand size, chooses the TA's from all n people, then chooses the readers from $n-k_1$ remaining people and finally chooses the AI's from $n-k_1-k_2$ remaining people.

   The right hand side sorts all the people on of $n!$ ways, chooses the first k_1 to be TA's and order doesn't matter, and then chooses the next k_2 people to be readers and order doesn't matter, and then chooses the next k_3 people to be AI's where order doesn't matter. Finally, the order doesn't matter on who is left off staff.

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.)

   Answer: First generate a degree 2 polynomial $T(x)$ for the TAs with $T(0) = \text{Secret}$. We can give one point $(x_i, T(x_i))$ to the i'th TA.

   Secondly, create a degree-2 polynomial $P(x)$ with $P(0) = \text{Secret}$. Keep track of the first three points on this polynomial, namely $(1, P(1)), (2, P(2)), (3, P(3))$. Each TA will receive $(1, P(1))$.

   Next, create a degree-1 polynomial $R(x)$ with $R(0) = P(2)$ and give one point $(x_i, R(x_i))$ to each reader.

   We also need a degree-2 polynomial $A(x)$ with $A(0) = P(3)$ and distribute one point to each AI.