CSM 70 Discrete Mathematics and Probability Theory

Spring 2016

Midterm 2 Review

I. Mod/Bijections/FLT/RSA

1. **Finding Bijections**

   Which of the following functions are bijections from $\mathbf{Z}_8$ to $\mathbf{Z}_8$

   a. f(x) = 3x Yes
   b. f(x) = 3x-2 Yes
   c. f(x) = 4x No

2. **Mapping Mods**

   Why can't we have a surjection from $\mathbf{Z}_8$ to $\mathbf{Z}_{16}$? Why can't we have an injection from $\mathbf{Z}_8$ to $\mathbf{Z}_4$?

   By definition, in a surjection, every element in Y must be mapped onto. Because every x value can only map to 1 y value, only 8 of the 16 Y values (at most) can have a value mapped to it, so not all 16 can have an item mapped to it.

   In the opposite way, in an injection, every element in X must map to a distinct value in Y, but because there are 8 in X and 4 in Y, values must collide, such that at least one value of Y has multiple X's mapping to it, so X's cannot map to distinct value sin Y

3. **Mod Math**

   What is 3^{453} mod 11? What principle/theorem do you use to solve this?

   a. 3^{453} mod 11 = $3^{450} * 3^3$ mod 11 = $(3^{10})^{45} * 3^3$ mod 11 = $1^{10} * 3^3$ mod 11 = 1 * 27 mod 11 = 5 mod 11. Use Fermat's Little Theorem to solve this.

4. **Really Secret Algebra**

   Alex is sending a message to Bob with RSA. If he uses the public key e = 7,N = 33, what is the value of d that Bob must use to decrypt the message?

   N = pq. Factors of 33 are 1, 3, 11, 33. This means p = 3, q = 11 (could be vice versa, but this does not matter). N' = (p-1)(q-1) = 2 * 10 = 20

   d = e^-1 (mod N') = 7' (mod 20) = 3
   d =3

5. **Three is Prime**

   If p and p^2+2 are prime, prove that p must be 3.

   If p is a prime other than 3, then $p \equiv 1$ mod 3 or $p \equiv 2$ mod 3. But either way $p^2 \equiv 1$ mod 3, which means that $p^2+2 \equiv 0$ mod 3, which means p^2+2 is not prime. But if p=3, then $p^2+2=11$, which is prime.

6. **Wilson's World**

   Prove Wilson's Theorem using Fermat's Little Theorem: Let p be a prime integer. Then $(p - 1)! \equiv -1 \pmod{p}$.

   Consider $p(x) = x^p - 1$.

By Fermat's little theorem, $p(x) = 0$ for every nonzero x in mod p.
Therefore, $p(x) = (x-1)(x-2)...(x-(p-1))$.
$p(0) = 0^p - 1 = -1$
$p(0) = (0-1)(0-2)...(0-(p-1)) \equiv (-1)^{p-1} (p-1)!$
So, $-1 \equiv (-1)^{p-1} (p-1)! \equiv (p-1)! \pmod{p}$.

7. **Bijective Magic**

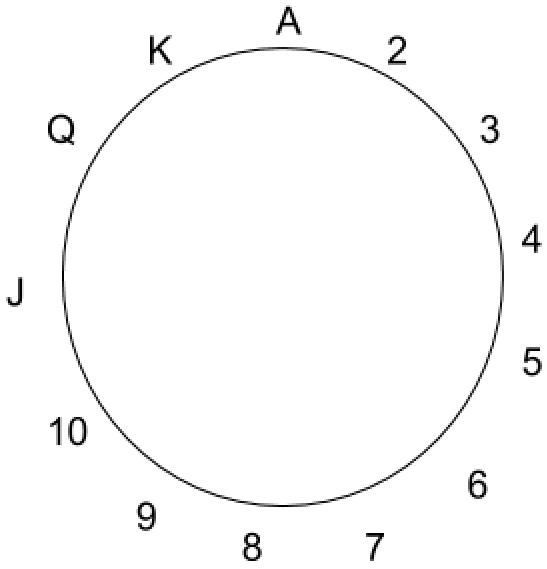
Let's learn a new card trick. You can perform this trick with an assistant, who asks a member of the audience to choose five cards while you face the other way. The assistant then places four of those cards face up on the table and one of them face down. You make a grand entrance and looking at the four cards on the table, correctly guess the one that is face down. How'd you do it?

There are two things you need to guess correctly: the suit and the denomination.
Let's start with the suit.

a. Say the five suits were H, D, H, S, C. Your assistant will place H, D, S, C on the table (in that order) and will place the other H face down. If the chosen cards were D, S, C, C, H your assistant will place C, D, S, H on the table (in that order) and will place the other C face down. Do you see the pattern? What mathematical principle is at play here? Write a strategy you and your assistant can use so that you will always know the suit of the hidden card.

Pigeonhole Principle. You choose 5 cards but there are only 4 suits. There must be a suit that is chosen twice. Hide one of the cards in the duplicate suit and place the other card in the suit on the left side.

Now we need to figure out how to guess the denomination.
Arrange the denominations in a circle.



We define smaller clockwise distance between denominations X and Y as the smallest of the following distances: from X to Y in the clockwise direction or Y to X in the clockwise direction.

b. What is the smaller clockwise distance between 8 and J? Between 3 and K?

3 for both

c. What are all of the possible smaller clockwise distances? In other words, if I choose X and Y arbitrarily, what could the smaller clockwise distance be?

1, 2, 3, 4, 5, 6

How can the assistant use this information to help you guess the hidden card? The assistant has two cards in the same suit. For now assume that the assistant has a secret way of telling you what the smaller clockwise distance between them is.

d. What card should the assistant hide and what card should they place face up on the table?

The assistant should always place the card where you start the smaller clockwise distance. In other words, since you know how many places past the face up card to go, you can figure out which card is face down. For example, if the two cards were K and 2, the assistant will hide the 2 and place the K face up.

Now we need to somehow encode the smaller clockwise distance. Recall that the assistant places four cards face up. The one of the left tells us the suit and where to start counting. There are three other cards that the assistant can use to let you know what the smaller clockwise distance is.

e. How can the assistant use the suits and denominations of the other three cards to encode the information from part c?

We need to encode 1, 2, 3, 4, 5, 6 and we can use three cards to do this. Agree with your partner on an ordering of the suits (C, D, H, S) and denominations (2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K, A).

Of the three cards you can arrange them according to denomination. If there are two or more of the same denomination, use the suit ordering to determine which has a higher ordering. So now you have the three cards in the following order: Smallest (S), Middle (M), Largest (L). How can we arrange SML to encode 1, 2, 3, 4, 5, 6?

There are 6 possible ways to permute SML. Have each of these permutations correspond to one of the smallest clockwise distances.

II. Error Correcting Polynomials

1. Call Me On My Solomon Reed Phone

Alice wants to send Bob a message of length 2 in GF(7)over a noisy channel. She knows that at most 1 character will get corrupted when she sends her message. So, she pads her message with 2 extra characters before sending it. (Using standard interpolation-based 0-indexed Reed Solomon codes.)

This is what Bob receives: A A E G

What was Alice trying to tell him?

Note: Here, assume that letters correspond to numbers as follows:A=0, B=1, C=2, D=3, E=4, F=5, G=6

The four points are (0,0), (1,0), (2,4), (3,6).

Let $Q(x) = ax^2+bx+c$, and $E(x) = x - e$.

This gives the four equations:

$c = 0\,(0 - e) \Rightarrow c = 0$

$a + b = 0\,(1 - e) \Rightarrow b = -a$

$4a - 2a = 4(2 - e) \Rightarrow 2a = 8 - 4e$
$9a - 3a = 6(3 - e) \Rightarrow 6a = 18 - 6e$
You get a=2, b=-2 and e=1. This gives $Q(x) = 2x^2 - 2x$ and $E(x) = (x-1)$. The actual polynomial is $P(x) = 2x$, plugging in x=1, we get that the message was AC

2. **Can't Read This**
Consider the alphabet A = 0, B = 1, C = 2, D = 3, E = 4. Suppose a message of length 3 is sent using the erasure error correction scheme over GF(5), with no more than one erasure. If you receive the following packets, what was the original message? The points are 1-indexed.
(a) C _ A A
$P(1) = 2, P(2) = ?, P(3) = 0, P(4) = 0;$
$\Delta_1 = (x-3)(x-4)/(-2*-3)$
$P(2) = 2(2-3)(2-4) = 4$
Message: CEAA.
(b) _ A C C
$P(1) = ?, P(2) = 0, P(3) = 2, P(4) = 2$
$\Delta_3=(x-2)(x-4)/(4)$
$\Delta_4=(x-2)(x-3)/(2)$
$P(1) = 2(4)(1-2)(1-4) + 2(3)(1-2)(1-3) = 1$
Message: BACC.
(c) C E _ C
$P(1) = 2, P(2) = 4, P(3) = ?, P(4) = 2$
$\Delta_1=(x-2)(x-4)/(3)$
$\Delta_2=(x-1)(x-4)/(3)$
$\Delta_4=(x-1)(x-2)/(1)$
$P(3) = 2(3)(3-2)(3-4) + 4(3)(3-1)(3-4) + 2(3-1)(3-2) = 4$
Pol: $4x^2 + 3$. Message: CEEC.

3. **100% Successful Decoding Guaranteed**
You would like to send a message of length n over a channel. You know that at most k packets may be dropped along the way, and of the packets that are not dropped, at most j may be corrupted. How many packets should you send to guarantee successful decoding? Why?
n+k +2 j packets.
Considering the worst case, where k packets are dropped and j packets are corrupted, we will need k more packets to protect from the erasure errors, and then 2 j more packets to protect from the general errors. Any other edge case must be upper bounded by this number (for example, if 0 packets dropped and j packets corrupted, then we need n+2 j total packets).

4. **Noise Channels**
You would like to send a message of length n > 0 over a lossy channel that drops (erases) packets. If up to a fraction 1/4 of the total number of packets you send get erased, how many extra packets do you need to send (as a function of n)?
floor(¼*n)

5. **Secret Polynomials**

The code to open your secret club's treasure chest is 15. Your club has 4 other members, named John, Paul, George and Ringo. What information can you give each of them so that any 3 of them can discover that the secret is 15, but if only 2 of them share their information, they cannot discover the secret? Fill in the boxes below.

Choose P(x) to be a polynomial of degree at most 2 such that P(0) = 15. We can work modulo 17, or any other prime number bigger than 15. We should choose $P(x) = 15+a_1x +a_2x^2$, where a_1 and a_2, are random numbers between 0 and 16. To make calculations easier, we'll choose 0 for every random number, so P(x) = 15. Tell all of them: "P(x) is a polynomial of degree at most 2 . The secret is P(0)." Tell John: P(1) ≡ 15 (mod 17). Tell Paul: P(2) ≡ 15 (mod 17) . Tell George: P(3) ≡ 15 (mod 17) . Tell Ringo: P(4) ≡ 15 (mod 17) .

6. Consider the following variant of the secret sharing problem. We wish to share a secret among twenty-one people, divided into three groups of seven, so that the following condition is satisfied. A subset of the twenty-one people can recover the secret if and only if it contains majorities (at least four out of seven) of at least two of the groups. How would you modify the standard secret sharing scheme to achieve this condition?

Answer: First, we have the secret s as the constant term in a degree-1 polynomial f(x) = ax + s over GF(p), where p > 7. We hand out f(1), f(2), and f(3) to each of the three groups. However, we will hand them out as a secret to be shared among each of the seven people within the groups (so each point of f given out becomes another secret, hence the hierarchical part of the scheme). For each group i, we have a polynomial g_i of degree 3 such that $g_i(0) = f(i)$. Then, we hand out $g_i(1)$, $g_i(2)$, . . . , $g_i(7)$ to each of the seven group members. Now, if any four members of a group get together, they can recover their group's secret, which they can share with another group (who also must have at least four people) to recover the original secret

7. **Polynomial Problem**

Suppose p is a prime number, P(x) is a polynomial with degree d, and $0 < d < p/2$. Prove that there are less than 2d +1 distinct values of x such that $P(x)^2 −P(x) +1 \equiv 0 \pmod p$.

Solution: Suppose for a contradiction that there are at least 2d + 1 distinct values of x such that $P(x)^2 − P(x) +1 \equiv 0 \pmod p$.

Then for each of those x-values, we have $P(x)^2 +1 \equiv P(x) \pmod p$. So P(x) and $P(x)^2 +1$ are two polynomials of degree at most 2d that match at 2d + 1 points: so they are the same polynomial. But this is impossible, since they have different degrees.

8. **Code Breaker**

You are spiteful for having to study over Spring Break, and so you want to cut off secret communications between your course staff. For each message, what percentage of a message being sent would you have to corrupt to make that message unrecoverable no matter how many extra packets are sent?

50% or more.

The packets that survive are: (n + 2k) - (n + 2k)*P, or (n + 2k) * (1 - P) where P is the percentage lost. Normally we try to solve for k so that (n + 2k) - (n + 2k)*P = n. If you try to solve this for P ≥ .5 then you will find there is no solution

III. Countability

In determining the cardinality of a set, recall that it must be finite, countably infinite, or uncountably infinite. To prove that something is countably infinite, we seek to find a bijection from the set to the naturals. We can do the same thing by finding that the set is infinite and that there exists some way to order them so we can say that some element is first, second, and so on. To prove that a set is uncountably infinite, it is usually a good strategy to use Cantor's diagonalization which is described in note 10, the basic idea of which is that if we assume that there is an ordering, then we can construct another element of the set using the elements in the ordering where the constructed element is not in the ordering.

1. Consider the set of all pairs of rational numbers: $T_1 = \{(x, y) \mid x,y \text{ rationals}\}$
   Is T_1 finite, countably infinite, or uncountably infinite? Explain.

   T_1 is countably infinite.
   Recall that the rationals are countably infinite by the spiral from the notes (note 10). In order to prove that T_1 is countably infinite, we seek to prove that there is a bijection from T_1 to the naturals. Since, the rationals are each countably infinite, we lay out x and y along perpendicular axes. Each point in the first quadrant represents a pair that is in the set T. We can use the cantor pairing function (https://en.wikipedia.org/wiki/Pairing_function#Cantor_pairing_function the relevant part is really just the picture) (note that you may have not heard of this function specifically and it's just an example of a bijection NxN → N). Thus, the bijective function Cantor(Spiral(x), Spiral(y)) is a bijective function from QxQ → N. (where Spiral is the bijective function described in the notes that maps a rational number to the naturals).

2. Consider the set of pairs where $T_2 = \{(x,y) \mid x \text{ is a natural number, } y \text{ is a real number}\}$
   Is T_2 finite, countably infinite, or uncountably infinite? Explain.

   T_2 is uncountably infinite.

   Recall that the real numbers are uncountably infinite by way of cantor's diagonalization from note 10. There are 3 different classifications: T_2 is finite, countably infinite, uncountably infinite.

   We proceed by way of proof by contradiction (this is basically a reformulation of cantor's diagonalization from note 10). Let us assume that T_2 is countably infinite. This means that we can write out an ordering of the pairs that is infinitely long. Let us take the i^{th} digit of the second element (y) in the pair of the i^{th} element of the ordering and construct a real number that has 1 at the i^{th} digit unless the i^{th} digit was 1, then we set it as 2. This number paired with any natural number does not exist as a pair within the ordering by construction, which is a contradiction because it must be an element of the set, yet it is not in the ordering of the set that we said we had. Thus, our assumption must be false, and the set must not be countably infinite.

   T_2 is not finite because T_2 finite $\Rightarrow$ some 'largest' element exists. There is no such largest element because we can always add 1 to a natural or real number.

Thus it must be uncountably infinite.

3. Consider the set of pairs where $T_3 = \{(x,y) \mid x,y$ are bit strings of length $k\}$
Is T_3 finite, countably infinite, or uncountably infinite? Explain.

T_3 is finite. There are 2^k different bit strings of length k from which we can choose x and y, so there are $(2^k)*(2^k) = 4^k$ elements in T_3.

4. Consider the set of triples where $T_4 = \{ (x,y,z) \mid x,y,x$ are rational numbers$\}$
Is T_4 finite, countably infinite, or uncountably infinite? Explain.

T_4 is countably infinite. First, use the bijective function for problem 1. Then we just need to find a mapping from (n, z) where n within Naturals and Z within rationals to the naturals. Since the rationals are countably infinite, we can order them along the vertical axis, and the first two elements along the horizontal axis using the ordering found in problem 1 and we can use cantor's pairing function again to get: f: QxQxQ → N, f = Cantor(Cantor(Spiral(x), Spiral(y)), Spiral(z)). So f is a bijective function from QxQxQ to N, which proves that it is countably infinite.

5. Consider the set of lists of length k, for positive integer k, where $T_5 = \{(x_1, ..., x_k) \mid x_i \in S_i$ such that $S_i \neq \varnothing \}$
If any of S are uncountably infinite, what is the cardinality of T_5?

Uncountably infinite.
It's not finite.
If T_5 was countably infinite, then we could use the ordering that we find to order the elements of the uncountably infinite set S_j (by ordering them according to when they occur in the ordering that we find), which we cannot do.
Thus T_5 is not finite nor countably infinite, so it must be uncountably infinite.
Cantor's diagonalization might be applicable here as an alternative, but since we don't know what the sets S are specifically, it's hard to construct some other element based on elements that we have seen. Cantor's diagonalization could be used in a very straightforward manner if the question specifically mentioned one of S being the reals.

If all of S are finite, is T_5 finite, countably infinite, or uncountably infinite?

Finite.
The size of T_5 is $\Pi_i |S_i|$ because in the list of length k, for each element we can choose any element of the set from which we draw that element. (note that this question did not ask for the exact size of T_5). If k = 2 and S_1 and S_2 are both {0, 1}, then T_5 is {(0, 0), (0, 1), (1, 0), (1, 1)}, and $|T_5|$ would be 4.

If none of S are uncountably infinite and at least one is infinite, what is the cardinality of T_5?

Countably infinite. (note that the question does not ask you to prove this, but just determine which one) In order to prove this, we would like to find some way to order the elements of T_5. Or we can find a bijection $T_5 \to N$. (but those are basically doing the same thing)

(We should use induction because the base case would probably be very simple, and proving the inductive step using the inductive hypothesis should be fairly straightforward. Using contradiction alone probably doesn't make sense since assuming that it is uncountably infinite doesn't really help us make any further points. It doesn't look like there is a straightforward direct proof that I can think of. We might be able to use contraposition, but I think that would end up forcing us to induct anyways.)

We proceed by induction on k (the number elements in the list).

Base case: For k = 1:

If at least one of S is infinite but none are uncountably infinite that means that S_1 must be countably infinite. The size of the set of lists of length one where the element is drawn from a countably infinite set is also countably infinite because we can order the lists by the same ordering that S_1 can be ordered by. (so if S_1 is N, then are ordering is just [0], [1], [2], … since N can be ordered as 0, 1, 2, …)

Inductive hypothesis:

Assume for arbitrary k = j, j>=1:

The cardinality of T_5 for k = j is countably infinite.

Inductive step: (here we could have chosen to reorder the list so that the first j always contains at least one countably infinite set, but we would have to justify doing that)

Then for k = j+1,

i) for 1<= i <= j S_i is a finite set,

Then S_{j+1} must be countably infinite and we can create a bijection by mapping every combination of the first j elements of the list with the first of S_{j+1} and then those combinations with the second of S_{j+1} and so on.

ii) at least one of S_i for 1<=i<=j is countably infinite

Then by the inductive hypothesis, we can order the first j elements in some way because it is countably infinite. So if,

a) S_{j+1} is finite, we can just order them in some way and pair every combination to the first j in order.

b) S_{j+1} is finite, then we can lay out the lists of length j according to the ordering that they must have along the horizontal axis and the ordering of S_{j+1} according to the ordering that it must have, and use cantor's pairing function to find the pair of the list of length j and the element from S_{j+1} is also countably infinite (the pair of list length j and another element is the same as just appending another element and having a list of length j+1).

Thus we have found that there exists a bijection $T_5 \to N$ for all k, so T_5 must be countably infinite.

A conclusion from this problem that you may find interesting is that if all S are countably infinite, then T_5 is also countably infinite means that NxN… is countably infinite (and so is QxQ… and ZxZ…).

IV. Counting

1. A professor designed his final exam as follows: There will be three sections in the exam. Each section has five questions. Students have to pick any two sections to answer, in any order. Within each section, they must choose any three questions. In how many possible ways can a student choose which questions to answer?

   3 CHOOSE 2 * 5 CHOOSE 3 * 5 CHOOSE 3

   Choose which two sections to do, then choose which 3 problems to do for each of the two sections chosen.

2. A committee of five people is to be chosen from a club that has ten scientists and eight engineers. How many ways can the committee be formed if it has to contain at least two scientists and at least one engineer?

   $$\binom{10}{2}\binom{8}{3}+\binom{10}{3}\binom{8}{2}+\binom{10}{4}\binom{8}{1}$$

3. How many five card hands have at least one card from each suit?

   $$\binom{4}{1}\binom{13}{2}\binom{13}{1}\binom{13}{1}\binom{13}{1}$$

   Hand will be of this form: A B C D A where A, B, C, D are the suits.

   First decide which suit will be repeated: 4 CHOOSE 1

   Then get two cards from that suit: 13 CHOOSE 2

   Finally select a card from each of the other suits: 13 CHOOSE 1

4. You’ve been hired by the local phone company. They’re concerned, because all the local taxi companies have started demanding phone numbers made up of exactly 2 different digits. (For instance, “555-5556” and “811-1881” are acceptable, but “111-1111” and “123-4567” are not.) Your job is to help the phone company figure out how long they’ve got before they run out of acceptable phone numbers. How many 7-digit numbers are there that contain exactly 2 different digits?

   10 CHOOSE 2 $\times (2^7 - 2) = 5670$

   First select two numbers you will have in your phone number: 10 CHOOSE 2

   Once you have your numbers, determine how many permutations of them are possible.

   There are 7 positions, 2 options for each position: 2^7

   But if your numbers are X and Y, this would include XXXXXXX and YYYYYYY. So subtract 2.

5. How many triangles does a complete graph with n nodes have?

   n CHOOSE 3

6. How many different sequences of the numbers {0,1,2} of length 10 do not contain any of the subsequences 12, 23, or 31? 3222132111 is such a sequence.

   $3 * 2^9$

   There are 3 options for the first digit, and then 2 options for each subsequent digit.

7. A decimal number is called “increasing” if each digit is nonzero and is greater than the previous one (e.g. 24589 is one). How many 5 digit increasing numbers are there?

   9 CHOOSE 5

   You can arrange any 5 digit sequence from 9 CHOOSE 5 into increasing order.

8. How many license plates with 3 digits followed by 3 letters do not contain both the number 0 and the letter O?

Assuming all decimal digits and letters are permitted, there are a total of $10^3 *26^3$ possible license plates. There are $(10^3 - 9^3)$ strings of decimal digits that contain the number 0 and $26^3 -25^3$ strings of 3 letters that contain the letter O, so there are $(10^3 -9^3)*(26^3 -25^3)$ license plates that can formed from these strings. Thus there $10^3 *26^3 - (10^3 -9^3)*(26^3 -25^3) = 17{,}047{,}279$ license plates that do not contain both the number 0 and the letter O.

9. How many different even integers ≥ 4000 and < 7000 have four different digits?

   There are 3 choices for the thousands digit: 4, 5, 6 (can't have 7)

   Split this into two cases: even (4, 6) and odd(5)

   If the thousands digit is even, then there are only 4 options for the ones digit (we can't repeat the one we used for the thousands). Then there are 8*7 options for the other digits. So we have 4*8*7*2 even integers from 4000 to 7000 that start with 4 or 6 and have different digits.

   If the thousands is odd there are still 5 options for the ones digit. Everything else is the same.

   So we get a total of: 4*8*7*2 + 5*8*7*1

10. A deck of forty cards consists of four 1's, four 2's, …, and four 10's. One matching pair of cards is removed from the deck. Two cards are now drawn at random from the deck. What is the probability they form a pair?

    There are 38 CHOOSE 2 = 703 ways to draw 2 cards from the deck once the pair is removed. This will be the denominator.

    Now we need to count the number of ways we could draw a pair.

    Either we select the two cards that are the same denomination as the removed pair was (there is only 1 way to do this) or we select one of the 9 other denominations (there is 9* 4 CHOOSE 2=54 ways to do this).

    So the final result is: 55/703.

11. Ten points are marked on a circle. How many distinct convex polygons can be drawn using some (or all) of the ten points as vertices?

    Any subset of three or more points will be a polygon. We need to find out how many subsets there are with 3 or more points.

    There are 2^{10} total subsets of the 10 points (each point is either in the subset or not, think of this as a binary string)

    We need to exclude the ones that have 0, 1, 2 elements.

    10 CHOOSE 0 have no elements

    10 CHOOSE 1 have 1 element

    10 CHOOSE 2 have 2 elements.

    Therefore our final answer will be $2^{10} - 1 - 10 - 45 = 968$

12. Plain Jane has 5 identical narrow rings that she likes to wear. She can wear them on any of her 8 fingers (but not her thumbs), and they are narrow enough that she can fit all 5 on one finger if she chooses to. How many different ways can Jane wear her rings? (note that Jane's rings may be plain, but she can tell her fingers apart).

    If she wears all 5 then there are 12 CHOOSE 7 ways for her to wear the rings. Think of this as stars and bars. Let the stars be the rings, and the bars be the partition between fingers. There are 5 stars (5 rings) and 7 bars (7 spaces between 8 fingers). So we get 5+7 CHOOSE 7.

    If she changes how many she wears (0 to 5), then there are (7+0 CHOOSE 7) + (7+1 CHOOSE 7) + … + (7+5 CHOOSE 7) ways.

    If she puts at most one ring on each finger, how many ways are there for her to wear her rings?

If she wears all of her rings then the answer is 8 CHOOSE 5 (she is choosing 5 fingers to place each ring on)

If she wears 0, 1, 2, 3, 4, or 5 rings, then there are (8 CHOOSE 0) + (8 CHOOSE 1) + … + (8 CHOOSE 5) ways.

Suppose Jane is tired of being plain and paints her rings five different colors so she can tell them apart. How does this change your answers above?

Multiply all previous answers by 5! (now we can differentiate between the rings).

V. **Halting**

Undecidability Here we use reductions to prove that certain problems are undecidable.

1. The totality problem is defined as follows: A program F is said to be total if F(x) is defined for all x. Assume there exists a procedure TOTAL that takes an input program P and outputs 'Yes' if P halts on all inputs and 'No' otherwise. Argue that this means we could solve the halting problem.

We can decide whether P halts on input x by constructing another program Q that ignores its own input and always emulates P on input x. Note that Q halts on all inputs if and only if P halts on input x. We now use TOTAL to decide whether Q halts on all inputs, and in doing so we also decide whether P halts on input x.

2. What does this mean about our assumption that TOTAL exists? Is the totality problem decidable?

This means that our assumption was wrong, because we know that the halting problem is undecidable (proof in the lecture notes). I.e. the totality problem is also undecidable.

3. The equivalence problem is defined as follows: Given two programs P and Q, do they compute the same function? (is P(x) = Q(x) for all x?). Prove that the equivalence problem is undecidable by reducing the totality problem to it. In other words, show that you can solve the totality problem using the equivalence problem.

We show that if the equivalence problem is decidable, then the totality problem is decidable as well. To decide whether P is total, we construct another program P 0 which emulates P except that it ignores any output by P and always prints YES. Also, let Q be the program that just prints YES and halts. Complete the reduction by noting that 1. If P is total, P 0 and Q are equivalent because P 0 (x) = Q(x) = YES for all x. 2. If P is not total, P 0 and Q are not equivalent because there exists some x for which P 0 (x) is undefined, but Q(x) = YES. Since the totality problem is undecidable, the equivalence problem must also be undecidable.

Making Midterms Might Make You Mad

Fahad is making questions for a CS70 midterm, and Fahad makes a question that is hard with probability 0.7. The head GSI, Katya, of the class looks at all of Fahad's questions and only gives it to students if she believes it to be an easy question. Katya believes a hard question is easy with probability 0.5 and an easy question is hard with probability 0.3. What's the probability that a hard question actually appears to the students?

We are trying to find the probability that a hard question appears to the students,that is, a hard question appears given that the GSI thinks it is easy

P(It's hard | GSI Says it's easy) = P(GSI says it's easy | It's hard)P(It'shard) / P(GSI says it's easy) by Bayes Rule.

P(GSI says it's easy) = P(GSI says it's easy | It's hard)P(It's hard) + P(GSI says it's easy | It's easy)P(It's easy) by the law of Total Probability.

Hence, overall, when we plug in numbers, we get

(.5)(.7) / ((.5)(.7) + (.3)(.7))

= (.35) / (.56)

VI. Probability

1. Probably 61A

You want to teach 61A! You will apply for some position every semester after taking the class. Once you have first finished the class, you have an 80% chance to be hired as a Lab Assistant, a 10% chance of being hired as a Tutor, and a 10% chance of being hired as a TA. Once you have been a Lab Assistant, you have a 30% chance of being rehired as a Lab Assistant, a 50% chance of being hired as a Tutor, and a 20% chance of being hired as a TA. Once you have been a Tutor, you have a 60% chance of being rehired as a Tutor, and a 40% chance of being hired as a TA. TAs are guaranteed to stay TAs forever when they are hired.

a. What is the chance of being a Tutor on your second semester after finishing the class? (So you were either a Lab Assistant or a Tutor for one semester already)

0.8 * 0.5 + .1 * .6 = .46

Chance of being a Tutor given you have been a Lab Assistant + chance of being a Tutor given you were hired as a Tutor on the first semester.

b. What is the chance that you stay a Lab Assistant for all 7 semesters after taking the class?

.8 * 0.3^6 = about 4 in a million

c. Given you were hired as a Lab Assistant the first semester after taking the class, what is the chance that you stay a Tutor for all 6 remaining semesters?

(.8 * .5 * .6^5)/.8 Lab Assistant for the first semester and Tutor for the rest / Lab Assistant for the first semester

d. What is the chance that you are hired as a Tutor exactly 3 times in 5 semesters?

.8 * .3 * .5 * .6 * .6 +
.8 * .5 * .6 * .6 * .4 +
.5 * .6 * .6 * .4

Since you cannot be demoted, there are only 3 ways to be a Tutor exactly 3 times: LLTTT, LTTT TA, and TTT TA TA

e. What is your chance of being a TA at least once in your first 3 semesters?

We have 1 - the chance that you aren't a TA given that you weren't a TA in the second semester, which is the probability of being a lab assistant twice + lab assistant + tutor, or a tutor twice, which is

1- (.8*.3*.8) + 1 - (.8*.5*.6) + 1 - (.1*.6*.6) = .532

2. Independent Dice

Consider rolling 2 normal 6-sided dice. Let A be the event that the first die comes up as an odd number. Let B be the event that the second die comes up as an odd number. Let C be the event that the sum of the dice values is odd. Intuitively, are A,B,C pairwise independent? That is, are any pair of these events independent? What are the probabilities of each event? Of each pair?

They are all pairwise independent. Knowing the first die coming up odd tells us nothing about the outcome of the second die, and since we don't know anything about the second die, the sum of the values could also be anything (even or odd). A symmetric case holds for the second die. Additionally, knowing the sum of the values being odd doesn't give any information on what each individual die could yield. This can be verified mathematically:

P(A) = 1/2

P(B) = 1/2

P(C) = 1/2 This may not be obvious at first. This is true due to the symmetry of each die (each die has an equivalent number of even faces and odd faces). You can also convince yourself of this probability by writing out the 36-entry chart.

Now for the intersections:

P(A∩B) = 1/4

P(B ∩C) = 1/4

P(A∩C) = 1/4 (completely symmetric to P(B ∩C))

These 3 intersection probabilities may not be very obvious. It is easiest to see this from the chart—simply count the number of entries that match the query (e.g. for P(B ∩C), count the number of entries out of 36 that have the second die showing an odd number and the summation being odd).

Note that for each joint probability, it is equivalent to the product of the individual probabilities. For example, P(A∩B) = P(A)P(B).

For a more air-tight mathematical proof of independence, we would have to repeat this for the complement events, as well.

3. **Mutually Independent Dice**

Continuing from Part 2, are the events A,B,C mutually independent? In other words, is each one independent from the other two? What is the probability of all 3 of them happening together?

They are not mutually independent.

Recall that mutual independence means that P(A ∩ B ∩ C) = P(A)P(B)P(C). This is not true in this case. In this case, once we know the results of any two of the events, we immediately know the result of the third. For example, if we know both A and B happened (i.e. both dice turned up odd), then they must sum to an even number, so C cannot happen. Similarly, if we know A and C happened, then it must be that B cannot have happened. Mathematically, P(A∩B ∩C) = 0, because they can never happen together. Clearly, this is not equal to the product of their individual probabilities

VII. Combinatorial Proofs

Use a combinatorial argument to prove the following identities.

1. $\binom{n}{k}\binom{k}{j} = \binom{n}{j}\binom{n-j}{k-j}$

Either side represents the number of ways to choose a committee of k people, and a subcommittee of j people, from a group of n. On the left side, we first choose the k people for the committee, and then choose j people for the subcommittee from those k. On the right side, we first choose the j people for the subcommittee, and then choose the remaining $k - j$ required committee members from the $n - j$ people who we haven't yet chosen.

2. $$1+2+\cdots+n=\frac{n(n+1)}{2}$$

If we note that $\frac{n(n+1)}{2}=\binom{n+1}{2}$, then we probably want to be selecting two things from a set of size $n + 1$. Both committees and bit strings can be made to work; we will use bit strings.

Let us count the number of bit strings of length $n + 1$ with exactly 2 ones. One way is to choose the two positions for the 1s, out of the $n + 1$ possible positions. There are $\binom{n+1}{2}=\frac{n(n+1)}{2}$ ways to do this. This gives the right hand side.

For the left hand side, count the strings by the location of the first 1 (reading from left to right). If the first 1 is in the first position, then there are n choices for the second 1. If the first 1 is is second position, there are n − 1 positions for the second 1, and so on till we get to the case where the first 1 is in position n, in which case the second 1 must be in the last position, so we have only one choice. This gives $n + (n - 1) + \ldots + 1$, which is the same as $1 + 2 + \ldots + n$.

(credit: http://www.d.umn.edu/~jgreene/discrete/Combinatorial_proofs.pdf)

3. Hockey Stick (from Worksheet 8)

   a. Prove the Hockey Stick Theorem:

$$\sum_{t=k}^{n}\binom{t}{k} = \binom{n+1}{k+1}$$ where n, t are natural numbers and $n > t$

Use a combinatorial argument!

Proof 1: Consider the problem of splitting $n - k$ items into $k + 2$ groups. The right-hand side counts this, by Stars and Bars: $(n - k) + (k + 2) - 1 = n + 1$, and $(k + 2) - 1 = k + 1$. Now, suppose we have chosen x of the items to be in the first group, where x can be anything from 0 to $n - k$. We now have to split the remaining n - k - x items—which can be anything from 0 to n - k—into the k + 1 remaining groups. Letting $t = n - x$, we can do this in $\binom{t}{k}$ ways, because $(n - k - x) + (k + 1) - 1 = n - x = t$ and $(k + 1) - 1 = k$. Because $t = n - x$ ranges from k to n, this is the left-hand side.

Proof 2: Consider the problem of selecting a committee of k + 1 people out of n + 1 people total. Clearly this can be done in $\binom{n+1}{k+1}$ ways, which is the right-hand side.

Now, number the people from 1 to n + 1, and suppose we choose the committee in this order. We split the problem into cases based on the *first* person in the committee, which could be person #1, person #2, and so on, up to person #n-k+1 (if the last k + 1 people are the ones chosen). Assume person #i is the first. Then, to complete the committee, we need to choose the remaining k committee members from the $n + 1 - i$ people who come after this person. This can be anything from k (when $i = n - k + 1$) to n (when i = 1), so these choices are counted by the left-hand side.

(credit: http://www.artofproblemsolving.com/wiki/index.php/Combinatorial_identity)

b. Let S be the set {1, 2, 3, … 2015}. Look at all 1000 element subsets of S. Find the average of all smallest elements of the subsets.

Because we know there are $\binom{2015}{1000}$ of these subsets, we can find the sum of their smallest elements and divide. To find the sum, we consider the number of subsets with each possible smallest element. There are $\binom{2014}{999}$ 1000-element subsets of S with smallest element 1, because the 999 remaining elements can be any other numbers. There are $\binom{2013}{999}$ 1000-element subsets with smallest element 2, because the remaining elements must be 3 or larger. This continues, with the largest possible smallest element being 1016, and $\binom{999}{999}$ such subsets.

Thus, the sum of smallest elements is the following:

$$\begin{aligned}
&\binom{2014}{999}\cdot 1+\binom{2013}{999}\cdot 2+\cdots+\binom{999}{999}\cdot 1016\\
&=\binom{2014}{999}+\binom{2013}{999}+\cdots+\binom{999}{999}\\
&\qquad+\binom{2013}{999}+\cdots+\binom{999}{999}\\
&\qquad\qquad+\\
&\qquad\qquad\ddots\\
&\qquad\qquad+\binom{999}{999}\\
&=\binom{2015}{1000}+\binom{2014}{1000}+\cdots+\binom{1000}{1000}\\
&=\binom{2016}{1001}
\end{aligned}$$

(We used the Hockey Stick Theorem twice.)

Finally, then, the average is

$$\frac{\binom{2016}{1001}}{\binom{2015}{1000}}=\frac{2016}{1000}=\frac{288}{143}$$

VIII. Random Var./Distributions/Expectations/Collisions

1. The Life of Die

Consider a single roll of two dice, one red and one blue.

(a) Let R be the value of the red die. What is the distribution of R? What is the expectation of R?

R: {1, 2, 3, 4, 5, 6} -> [0, 1]

R returns a probability of a roll of the red die having a certain numerical value.

Distribution of R = {(1, ⅙), (2, ⅙), …, (6, ⅙)} where (x, y) means x is the dice value and y is the probability of that value.

E[R] = 1*⅙ + 2*⅙ + … + 6*⅙ = 21/6

(b) Let S be the sum of the numbers on the two dice. What is the distribution of M? What is the expectation of M?

S = R + B, s.t. B = R

S returns the probability of the sum of the red and blue die equating a given value.

Distribution o f S = {(2, 1/36), (3, 2/36), (4, 3/36), … (6, 5/36), (7, 6/36) (8, 5/36) … (12, 1/36)} = {(s, Pr(S = s)) | s ϵ {2, 3, …, 12}}

For any (x, y), y = Pr[x] = (# of positive non-zero integer solutions to r + b = x s.t. $1 \leq r, b \leq 6$) / (# total number of roll permutations)

Ex[S] = 2*(1/36) + 3*(2/36)} + 4 * (3/36) + … 12 * (1/36)
= 14*(1/36) + 14*(2/36) + … + 14*(6/36) + 7*(6/36)
= (14/36)*(1 + 2 + … + 5) + 42/36
= (14/36)*15 + 42/36
= 252/36 = 7

This makes sense because the distribution is symmetric about the center of mass, average, of the distribution.

(c) Let M be the maximum of the numbers on the two dice. What is the distribution of M? What is the expectation of M?

M = max(R, B)

Distribution of M = {(1, 1/36), (2, 3/36), (3, 5/36), (4, 7/36), (5, 9/36), (6, 11/36)}

The probabilities of the max can be found by a counting argument; every pair of dice rolls are equally probable, so count the possible pairs with a max value of interest.

E[M] = 1*Pr[M = 1] + 2*Pr[M = 2] + 3*Pr[M = 3] + … + 6*Pr[M = 6]
= 161/36 = 4.472

2. Hashbrown tables

Let there by a hashtable of size N. If k items are hashed, what is the expected number of collisions?

Define a random variable $X = X_1 + X_2 + \ldots + X_N$
where X_i = { 1 if there is more than one item hashed at location i, 0 otherwise}

Determine the distribution and expectation of X_i

Let L be the event that at most 1 ball lands in a given bin.

Pr[L] = prob of 0 balls + prob of 1 ball = $N!/N^k(N-k)! + k*(N!/N^k(N-k+1)!)$

X_i : {(0, Pr[L]), (1, 1 - Pr[L]}

$E[X_i] = 0 + 1 - Pr[L]$

Note $X_i = X_j$ for all $i \neq j$, $E[X_i] = E[X_j]$. By linearity of expectation,

$E[X] = E[X_1 + X_2 + \ldots + X_N]$
$= E[X_1] + E[X_2] + \ldots + E[X_N]$
$= N * E[X_i]$
$= N * (1 - Pr[L])$