MIDTERM 2 REVIEW

COMPUTER SCIENCE MENTORS 70

October 23, 2016

1 FLT and RSA

1. **Becoming Alice**
Alice wants to send Bob a message $m = 5$ using his public key $(n = 26, e = 11)$. What ciphertext $E(m)$ will Alice send? How will Bob decode it?

Solution:

$$\begin{aligned}
5^1 &\equiv 5 \mod 26 \\
5^2 &\equiv 25 \mod 26 \\
&\equiv -1 \mod 26 \\
5^4 &\equiv (-1)^2 \mod 26 \\
&\equiv 1 \mod 26 \\
5^8 &\equiv 1 \mod 26 \\
5^{11} &\equiv 5^8 * 5^2 * 5^1 \mod 26 \\
&\equiv 1 * -1 * 5 \mod 26 \\
&\equiv -5 \mod 26 \\
&\equiv 21 \mod 26
\end{aligned} \tag{1}$$

So our encoded message is $C = 21$. To find d, we need to factor N into its two prime factors, P and Q which are 2 and 13, and then find: $e-1 \mod (p-1)(q-1)$, so find $11 - 1 \mod 12; d = 11$ $C^d \mod N = 21^{11} \mod 26 = 5$

2. **Cracking RSA**
Suppose Bob's RSA public key is (e, n), where e is the encryption key, and $n = pq$ is

the product of two primes. Alice has just sent a secret message $c = m^e \mod n$ to Bob using Bobs public key.

(a) Explain how Bob can decrypt the message he has received.

Solution: $c^d \mod n = m^{ed} \mod n = m$

(b) Now suppose that by eavesdropping on their conversation you managed to overhear the ciphertext c. Moreover, when crafting his public key Bob foolishly chose primes that were too small, so that by continuously running a fast factoring algorithm on one of Berkeleys supercomputing clusters for two weeks, you eventually manage to factor n, and recover p and q. Given e, p, q, and c, explain how you can now efficiently recover plaintext m of Alice's message to Bob.

Solution: Compute $d' = e - 1 \mod (p-1)(q-1)$ Now you can compute $c^{d'} = m^{ed'} = m$ Note that all operations can be computed by the extended GCD algorithm which is polynomial time, and the exponentiation, also polynomial time.

2 Polynomials

1. **Perfect Polynomial Proof Practice**
Suppose p is a prime number, $P(x)$ is a polynomial with degree d, and $0 < d < \frac{p}{2}$. Prove that there are less than $2d+1$ distinct values of x such that $P(x)^2 - P(x) + 1 \equiv 0 \mod p$.

Solution: Suppose for a contradiction that there are at least $2d+1$ distinct values of x such that $P(x)^2 P(x) + 1 \equiv 0 \mod p$. Then for each of those x-values, we have $P(x)^2 + 1 \equiv P(x) \mod p$. 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.

There is one case in which $P(x)$ and $P(x)^2+1$ have the same degree, if $P(x) = a$ for some constant a. Does the equality hold $\mod p$ for this case? We have $a^2 a + 1 = 0 \mod p$. This equation has no real solutions, let alone integer solutions $\mod p$! Therefore, we can state with confidence that no such $P(x)$ can exist.

2. **Spot the Error**

Assume that $d = 1$, and we are told that

$$\begin{aligned} P(1) &= 2 \\ P(2) &= 3 \\ P(3) &= 2 \\ P(4) &= 0 \\ p &= 5 \end{aligned} \tag{2}$$

but we know there is exactly one incorrect point.

(a) What is $P(0)$?

Solution: This is a line. Try deleting each and seeing whether a line fits the other three points. The line is $P(x) = x + 1$, since

$$\begin{aligned} P(1) &= 1 + 1 = 2 \\ P(2) &= 2 + 1 = 3 \\ P(4) &= 4 + 1 = 0 \end{aligned} \tag{3}$$

(b) What is the error locator polynomial for Berlekamp-Welsh Algorithm for this situation?

Solution: $E(x) = x - 3$

3. **Majority Rules**

Consider the following variant of the secret sharing problem.

(a) We wish to share a secret among twenty-one people, divided into three groups of seven.

(b) A subset of the twenty-one people can recover the secret if and only if it contains majorities (4 or more out of 7) of at least two of the groups.

How would you modify the standard secret sharing scheme to achieve this condition?

Solution: 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. Any two of these points is enough to recover S. Now we need to make $f(i)$ is only known to group i a majority of group i is present. We hand out each $f(i)$ as a new secret within each group. For each group i, we

have a polynomial g_i of degree 3 such that $g_i(0) = f(i)$ (the standard secret sharing scheme). Then, we hand out $g_i(1), g_i(2), \ldots, g_i(7)$ to each of the seven group members. Now, if any four members of a group get together, they can pool their values of g_i to obtain $g_i(0) = f(i)$, which is their groups secret. They can then share with another group (who also must have at least four people) to recover the original secret

4. **The Polynomials Are Alright**
Prove the following theorem in two different ways:
For every prime p, every polynomial over $GF(p)$, even polynomials with degree $\geq p$, is equivalent to a polynomial of degree at most $p-1$. (Two polynomials f, g over $GF(p)$ are said to be equivalent iff $f(x) = g(x) \forall x \in GF(p)$.)

   (a) Show how the theorem follows from Fermat's Little Theorem

   Solution: From FLT, we know that for all x, $x^p = x \mod p$. Therefore, any x^a where $a \geq p$ will be equivalent to x^n for some $n \in 0, 1, \ldots, p-1$, and will have a degree at most $p-1$.

   (b) Now prove the theorem using properties of polynomials.

   Solution: Since a polynomial of degree d is described completely by $d+1$ points, we cannot specify a polynomial of degree $\geq p$, because $p = 0$ over $GF(p)$, so $F(p) = F(0)$ for any polynomial F. So we can only specify at most p unique points. As a result, every polynomial is equivalent to a polynomial of degree at most $p-1$.

3 Counting/Combinatorics

1. **Midterm Madness**
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?

Solution:

$$\binom{3}{2} * \binom{5}{3} * \binom{5}{3}$$

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

2. **Counting Cards**
   How many five card hands have at least one card from each suit?

   Solution: 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: $\binom{4}{1}$ Then get two cards from that suit: $\binom{13}{2}$ Finally select a card from each of the other suits: $\binom{13}{1}$

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

3. **Looking at Letters**
   How many letters are in the word MISSISSIPPI?

   Solution: There are 11 letters in MISSISSIPPI

4. **Total Triangles**
   How many triangles does a complete graph with n nodes have?

   Solution: $\binom{n}{3}$

5. **Interesting Integers**
   How many different even integers ≥ 4000 and < 7000 have four different digits?

   Solution: There are 3 choices for the thousands digit: 4, 5, 6 (cant 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 cant 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: $4 * 8 * 7 * 2 + 5 * 8 * 7 * 1$

6. **Fun with Jane**
   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.

(a) How many different ways can Jane wear her rings? (note that Janes rings may be plain, but she can tell her fingers apart).

Solution: If she wears all 5 then there are $\binom{12}{7}$ 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 $\binom{5+7}{7}$. If she changes how many she wears (0 to 5), then there are $\binom{7+0}{7} + \binom{7+1}{7} + \ldots + \binom{7+5}{7}$ ways.

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

Solution: f she wears all of her rings then the answer is $\binom{8}{5}$ (she is choosing 5 fingers to place each ring on) If she wears 0, 1, 2, 3, 4, or 5 rings, then there are $\binom{8}{0} + \binom{8}{1} + \ldots + \binom{8}{5}$ ways.

(c) 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?

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

7. Prove with a combinatorial argument:

$$1 + 2 + \ldots + n = \frac{n * (n+1)}{2}$$

Solution: If we note

$$\frac{n * (n+1)}{2} = \binom{n+1}{2}$$

that , 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 $n1$ 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 $1 + 2 + \ldots + n$.

4 Self Reference

1. **Equality for Every Fun**
   Two functions f, g are equal by the following definition:

$$f, g : X \to Y \text{ and } f = g \iff \forall x \in X f(x) = g(x)$$

   (a) I want to define equality on the set of real, finite length, polynomial functions. Can I do this? Justify your answer.

   Solution: This is possible. Since the polynomial representation of a function is unique and there are a finite number of coefficients, we can simply check the equality of the coefficients.

   (b) I want to define equality on the set of single argument Python functions. Can I do this? Justify your answer.

   Solution: This is not possible. Functions in Python represent general programs. Consider one function that immediately outputs 0 for all inputs, and another that outputs 0 if another program terminates on the input, and 1 if it does not terminate on the input. By the halting problem, we cannot know what the second program outputs, and so we cannot know if the two are equal on all inputs.

   (c) What is, if anything, the difference between these two problems?

Solution: Python programs allow self reference, polynomials do not.

2. **Diagon Alley**
Show that the halting problem reduces to the contradiction found in Cantor's diagonal argument.

Solution: We know the set of computer programs to be countable (they are finite length bit strings stored in memory). This allows us to enumerate all possible arguments to the TestHalt function (remember that the cartesian product of two countable sets is also countable by the spiral argument). We write this as a table with values representing whether TestHalt halts with the given inputs. Our constructed program Turing, which halts whenever TestHalt of P applied to itself does not, must be in this enumeration. However, by its definition, it must have the opposite behavior on P as TestHalt on (P, P), inverting the diagonal of the table. This shows us that Turing cannot be in the table, and so TestHalt is not a valid program.

3. **Floating Outside of Reality**
Assume we have a computer with a finite number of infinite-precision floating point numbers, show, given a fixed starting state of the computer, that there exist real numbers we cannot calculate. How many such numbers are there?

Solution: Remember that the set of all programs is countable, since, in order to write them, they must be formed from a finite length sequence in some alphabet. Since the starting state of the computer is fixed, and each program maps the starting state to the final state of the computer, there is a countably infinite number of states we can reach. In order to have every real number be computable, we would have to have an uncountable infinity of states. Therefore it is impossible to calculate every real number.
There must be an uncountable infinity of these numbers, since, as we have already reasoned, there is a countable infinity of calculable reals, so the set difference between the reals and the calculable reals must be uncountable (the union of the countable calculable reals and the incalculable reals must be uncountable, the union of two countable sets is countable).

5 Probability

1. **What Are the Chances**

(a) Two disjoint events A and B with $Pr[A] > 0$ and $Pr[B] > 0$ cannot be independent. True or False?

Solution: True. $Pr[A \cap B] = 0$ which does not equal $Pr[A]Pr[B]$ if $Pr[A], Pr[B] > 0$. Therefore the disjoint events cannot be independent.

(b) There is a bag with 50 red and 50 blue balls. You pick four balls, without replacement. Given that the first ball is red, what is the probability that the fourth ball is also red?

Solution: $Pr[\text{4th ball is red}] = Pr[\text{2nd ball is red}] = 49/99$

(c) Let $\Omega = \{1, 2, 3, 4, 5, 6\}$ be a uniform probability space. Find two independent events A and B with $0 < Pr[A] < 1$ and $0 < Pr[B] < 1$.

Solution: $A = \{2, 3, 4\}, B = \{1, 4\}$.
$Pr[A] = \frac{3}{6}, Pr[B] = \frac{2}{6}, Pr[A \cap B] = \frac{1}{6}$.

(d) **Challenge:** Let $\Omega = \{1, 2, \ldots, n\}$ be a uniform probability space. Assume that n is not a prime number. Find two independent events A and B with $0 < Pr[A] < 1$ and $0 < Pr[B] < 1$.

Solution: Since n is not prime, we know $n = ab$ for some a, b. Lets try what we did in 3, but generalize it. If $Pr[A] = \frac{a}{n}$ and $Pr[B] = \frac{b}{n}$. Then we want $Pr[A \cap B] = \frac{a*b}{n*n} = \frac{1}{n}$. So we want 1 overlapping point. Let $A = \{1, \ldots, a\}$ and $B = \{a, \ldots, a + b - 1\}$. $|A| = a$, $|B| = b$, $|A \cap B| = 1$, as desired.

2. **Losing My Marbles** We have n bins and r red marbles, g green marbles, and b blue marbles. We randomly throw the $r + g + b$ marbles into the n bins.

(a) What is the probability no bin contains two (or more) marbles?

Solution: Let $k = r + g + b$

$$\frac{\binom{n}{k} * k!}{n^k}$$

(b) What is the probability no bin contains two marbles of the same color?

Solution: Let $k = r + g + b$

$$\frac{\binom{n}{r} * r!}{n^r} * \frac{\binom{n}{g} * g!}{n^g} * \frac{\binom{n}{b} * b!}{n^b}$$

3. **Rook at This**
Given the chessboard below, imagine we place 7 rooks on random squares. What is the probability that all of these rooks are safe from each other? (No need to simplify!)

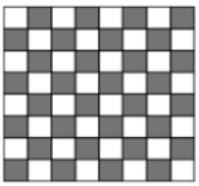
Note: If a rook is placed at square (i, j), no pieces in column j or row i are safe.

Solution: Consider the process of placing each rook on the board. When we place rook 1, we eliminate an entire row and an entire column, so we have effectively restricted the chessboard to a (disjoint) 7x7 board. Each time we add a piece, we lose a row/column. So after the 7th piece is placed, we have just a 1x1 board left.

We can count the ways to set up such a scenario using the multiplication rule:

$$N = 8^2 * 7^2 * 6^2 \ldots * 2^2$$

The total number of ways we could have placed 7 pieces on a 64 square board is $D = \binom{64}{7} * 7!$ (since the order in which we place the rooks matters based on our process above). Our final answer is then $\frac{N}{D}$



6 Conditional

1. **Probably Passing** A multiple choice quiz has 3 questions, each with 5 equally probably answer choices.
   (a) Find the probability of answering the first question correctly

Solution:

$$Pr[getting 1 question right] = \frac{1}{5} = 0.2$$

(b) Find the probability of answering the two questions correctly

Solution:

$$Pr[\text{getting 1 question right}] * Pr[\text{getting 1 question right}]$$
$$= \frac{1}{5} * \frac{1}{5} = 0.2 * 0.2 = 0.04$$

(c) Find the probability of answering at least one question correctly

Solution:

$$1 - (Pr[\text{getting 1 question wrong}])^3$$
$$= 1 - (\frac{4}{5} * \frac{4}{5} * \frac{4}{5}) = 0.488$$

2. **Teach for the Stars**

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.

1. 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)

Solution:

$$0.8 * 0.5 + 0.1 * 0.6 = 0.46$$

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.

2. What is the chance that you stay a Lab Assistant for all 7 semesters after taking the class? (dont need to get the exact number)

Solution:

$$0.8 * 0.3^6 = \text{about 4 in a million}$$

Student hired as LA after taking the class then keeps getting rehired as an LA

3. 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?

Solution:

$$\frac{0.8 * 0.5 * 0.6^5}{0.8}$$

Lab Assistant for the first semester and Tutor for the rest / Lab Assistant for the first semester

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

Solution:

$$0.8 * 0.3 * 0.5 * 0.6 * 0.6 +$$

$$0.8 * 0.5 * 0.6 * 0.6 * 0.4 +$$

$$0.5 * 0.6 * 0.6 * 0.4$$

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

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

Solution: We have 1 - the chance that you arent a TA given that you werent 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

$$1 - (0.8 * 0.3 * 0.8) + 1 - (0.8 * 0.5 * 0.6) + 1 - (0.1 * 0.6 * 0.6) = 0.532$$

7 Infinity and Countability

1. **Countability Warmup**

(a) Consider the set of all pairs of rational numbers:

$$T_1 = (x, y)|\text{ x,y rationals}$$

Is T_1 finite, countably infinite, or uncountably infinite? Explain.

Solution: Countably infinite. Can use same proof that NxN is countably infinite. (Cantor pairing)

(b) Consider the set of pairs where

$$T_2 = (x, y)|x \text{ is a natural number, } y \text{ is a real number}$$

Is T_2 finite, countably infinite, or uncountably infinite? Explain.

Solution: Uncountably infinite. Use Cantor's Diagonalization on the second element.

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

Solution: Finite. Can count each one. How many are there?

(d) Consider the set of triples where

$$T_4 = (x, y, z)|x, y, z \text{ are rational numbers}$$

Is T_4 finite, countably infinite, or uncountably infinite? Explain.

Solution: Countably infinite. From 1, know that (x, y) is countably infinite. Use Cantor pairing to show $((x, y), z) \equiv (x, y, z)$ is countably infinite.

Countability Cooldown

Consider the set of lists of length k, for positive integer k, where

$$T_5 = (x_1, \ldots, x_k)|x_i \in S_i \text{ such that } S_i \neq \emptyset.$$

(a) If any of S are uncountably infinite, what is the cardinality of T_5?

Solution: T_5 is uncountably infinite.

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

Solution: T_5 is finite.

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

Solution: T_5 is countably infinite.