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?
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.
   (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.

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 $P(x)^2 - P(x) + 1 \equiv 0 \mod p$.

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 $P(0)$?

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

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?

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

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

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?

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

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

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

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

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).

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

   (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?

7. Prove with a combinatorial argument:

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

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.

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

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

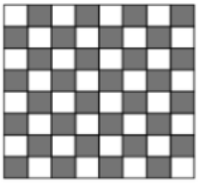
2. **Diagon Alley**
   Show that the halting problem reduces to the contradiction found in Cantor's diagonal argument.

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?

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?
   (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?
   (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 $0 < Pr[B] < 1$.
   (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 $0 < Pr[B] < 1$.
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?
   (b) What is the probability no bin contains two marbles of the same color?
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.



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
   (b) Find the probability of answering the two questions correctly
   (c) Find the probability of answering at least one question correctly
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)
   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)
   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?
   4. What is the chance that you are hired as a Tutor exactly 3 times in 5 semesters?
   5. What is your chance of being a TA at least once in your first 3 semesters?

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.

(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.

(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.

(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.

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?

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

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