EECS 70 Discrete Mathematics and Probability Theory
Spring 2014 Anant Sahai

Midterm 2

Exam location: 2050 VLSB, front half: SIDs with second-to-last digit 6 or 8

PRINT your student ID: | | | | | | | | | |

PRINT AND SIGN your name: _____, _____ _____
(last) (first) (signature)

PRINT your Unix account login: cs70-_____

PRINT your discussion section and GSI (the one you attend): _____

Name of the person to your left: _____

Name of the person to your right: _____

Name of someone in front of you: _____

Name of someone behind you: _____

Section 0: Pre-exam questions (3points)

1. **What is your favorite song? (1 pt)**

2. **Describe a sense of accomplishment that you have felt and what prompted it. (2pts)**

Do not turn this page until the proctor tells you to do so.

PRINT your name and student ID: _____

Section 1: Straightforward questions (50 points)

You must show work to get credit. You get two drops: do 5 out of the following 7 questions (we will grade all 7 and keep only the 5 best scores). However, there will be essentially no partial credit given in this section. Students who get all 7 questions correct will receive some bonus points.

3. Interpolate (10 points)

Prof. Sahai decides to share his favorite Pokémon among six of the GSIs, but to keep it a secret unless enough GSIs come together. Each potential favorite Pokémon is given a number (Charizard=0, Wartortle=1, Pidgeot=2, Ninetales=3, Arcanine=4, Scyther=5, Jolteon=6) and the favorite is hidden as the constant term (i.e. as usual, the secret is in $P(0)$) in a polynomial, $P(x)$, of degree $d \leq 4$ using $GF(7)$. You manage to acquire the following five points by attending different GSI office hours: $(1,0),(2,6),(3,0),(4,0),(6,0)$. **Use Lagrange Interpolation to find out the secret** (the Prof's favorite Pokémon).

4. Compute (10 points)

Find 300^{300} mod 35.

PRINT your name and student ID: _____

[Extra page. If you want the work on this page to be graded, make sure you tell us on the problem's main page.]

PRINT your name and student ID: _____

5. Argue (10 points)

In RSA, if Alice wants to send a confidential message to Bob, she uses Bob's public key to encode it. Then Bob uses his private key to decode the message.

Suppose that Bob chose $N = 77$.

And then Bob chose $e = 3$ so his public key is $(3, 77)$.

And then Bob chose $d = 26$ so his private key is $(26, 77)$.

Will this work for encoding and decoding messages? If not, where did Bob <u>first</u> go wrong in the above sequence of steps and what is the consequence of that error. If it does work, then show that it works.

6. Prove (10 points)

Prove the following statement:

If two degree $d \leq n-1$ polynomials $P(x)$ and $Q(x)$ agree at n distinct xs (i.e. For $x_1, x_2, \ldots, x_n$ distinct, $P(x_i) = Q(x_i)$), then they are the same function everywhere else too.

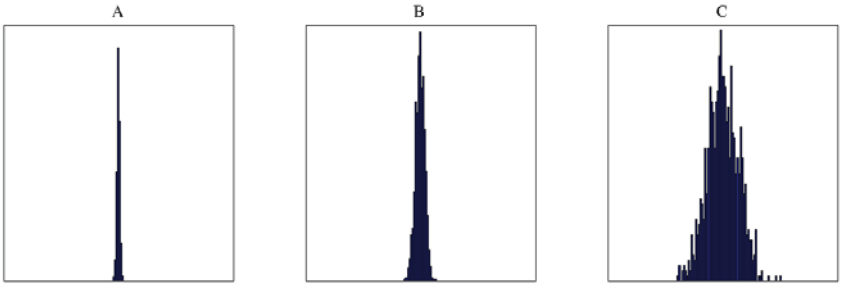
PRINT your name and student ID: _____

[Extra page. If you want the work on this page to be graded, make sure you tell us on the problem's main page.]

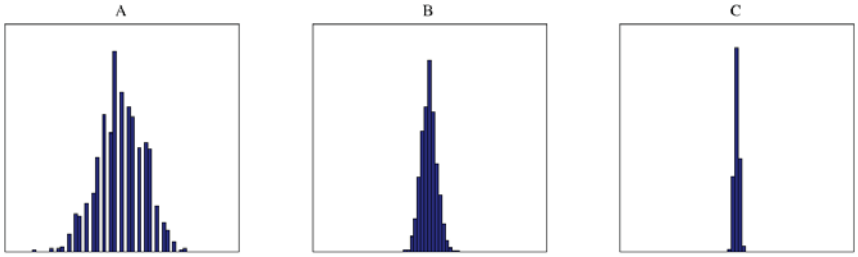
PRINT your name and student ID: _____

7. Recognize (10 points)

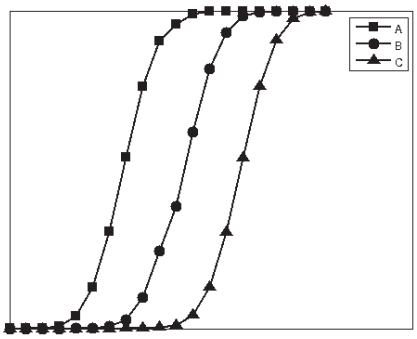
a. I have a large number of biased coins that tend to come up heads 80% of the time, and tails the other 20%. A trial consists of my flipping k such coins, and an experiment consists of 1000 such trials. I do 3 such experiments, with k being 100, 1000, and 10000 respectively. For each experiment, I plot a histogram of the number of heads in each trial, minus $0.8k$. My horizontal axis is the same for all 3 experiments. **Which histogram below corresponds to which value of k?**



b. I do the same experiment as above, but now I plot histograms of the *fraction* of heads (minus 0.8) from each trial. Now **which histogram below corresponds to which value of k?**



c. My friend gives me 3 bags full of biased coins: coins in these bags come up heads 40%, 50%, and 60% of the time respectively. Suppose for each q in $0 \leq q \leq 1$, I record the fraction $f(q)$ of trials in which I get at most q fraction of heads when I flip 100 coins drawn from one of these bags. If I plot q (x axis) vs $f(q)$ (y axis), **which curve below corresponds to which bag?**



PRINT your name and student ID: _____

8. Derive (10 points)

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

9. Solve . . . (10 points)

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:

$A = 0$
$B = 1$
$C = 2$
$D = 3$
$E = 4$
$F = 5$
$G = 6$

PRINT your name and student ID: _____

[Extra page. If you want the work on this page to be graded, make sure you tell us on the problem's main page.]

PRINT your name and student ID: _____

Section 2: True/False (30 points)

For the questions in this section, determine whether the statement is true or false. If true, prove the statement is true. If false, provide a counterexample demonstrating that it is false.

10. Sums (15 points)

Suppose that $n \geq 1$ is a positive integer, $x_1, x_2, \ldots, x_n$ are also nonzero positive integers, and p is a prime. Then

$$(x_1 + x_2 + \cdots + x_n)^p = x_1^p + x_2^p + \cdots + x_n^p \pmod{p}.$$

Mark one: TRUE or FALSE.

PRINT your name and student ID: _____

11. Distance (15 points)

Let $n \geq 1$ be a positive integer. Let $r \geq 1$ be a positive integer. Consider a polynomial based code in which n character messages are encoded into polynomials of degree less than or equal to $n-1$. The codewords are generated by evaluating these polynomials at $n+r$ distinct points (assume the underlying finite field has more than $n+r$ elements).

Then any two codewords corresponding to different messages must differ in at least $r+2$ places.

Mark one: TRUE or FALSE.

PRINT your name and student ID: _____

[Extra page. If you want the work on this page to be graded, make sure you tell us on the problem's main page.]

PRINT your name and student ID: _____

Section 3: Free-form Problems (45 points)

12. You knew this was coming... (20 points)

As you know from homework, we can mod polynomials themselves. For this problem, consider formal polynomials (i.e. a degree at most d formal polynomial is something that can be written $\sum_{i=0}^{d} a_i x^i$) with coefficients in $GF(2)$ (i.e. the a_i are 0 or 1 with usual binary math).

(So, for example, x^2+x is the remainder of poly-long-dividing x^4 by x^3+x+1. Meanwhile, the quotient of the same division is just x. This is because $x^4 = x(x^3+x+1)+(x^2+x)$ when all arithmetic on coefficients is performed mod 2.)

Compute the multiplicative inverse of the formal polynomial $x+1$ in mod x^3+x+1. That is, give a formal polynomial $P(x)$ so that $P(x)(x+1) \bmod (x^3+x+1) = 1$.

(e.g. The multiplicative inverse of x is x^2+1 because $x(x^2+1) \bmod (x^3+x+1) = 1$.)

PRINT your name and student ID: _____

[Extra page. If you want the work on this page to be graded, make sure you tell us on the problem's main page.]

PRINT your name and student ID: _____

13. Magic Command (25 points)

You are a young technomage (one who uses technology to create the impression of magic) who has been asked to help some people on a planet with a fragile new peace treaty. They have a master computer that is connected to a doomsday device capable of blowing up the planet if given the publicly-known command "Magic computer, please blow up the world now." (For the purposes of this problem, feel free to think of this as being a publicly-known magic number like 42).

The problem is that the computer has no security on it. It just accepts plain text commands.

a. (10 pts) You have been asked to add some security to the system to prevent unauthorized use. You can remove the keyboard, add a tamper-proof-decryption module, and force all keyboard input to go through the decryption module before it goes to the computer. But anyone can walk up to the decryption module to study it because it is in the **public** square. **Please show how you would design such a public module that transforms inputs before feeding them into the computer.** This module should effectively make the magic number that blows up the world into something secret.

You can use modulo math operations as you see fit. (You don't have to reprove anything you have seen in lecture or notes.)

b. (15 pts) The people on this planet are divided into two factions: the blues and the golds. Within each color group, there are 4 families. They have agreed on the following behavior:

If at least 2 blue families and at least 2 gold families come together, they should be able to give a valid command to the master computer. In addition, if all the blues agree or all the golds agree, then they should also be able to give a valid command to the master computer. But no other grouping should be able to do it. (e.g. 3 blues and 1 gold *should not* be able to give a command.)

Design a scheme and argue why it works as intended. You can use modulo math operations as you see fit, as well as give pieces of information **secretly** to families. (You don't have to reprove anything you have seen in lecture or notes.)

PRINT your name and student ID: _____

[Extra page. If you want the work on this page to be graded, make sure you tell us on the problem's main page.]

PRINT your name and student ID: _____

14. (Optional) Multiplication (20 points)

Suppose you have invented a machine for doing *mod multiplications* extremely fast.

Given a prime p, your invention takes two equal size lists of numbers from $\{0,1,\ldots,p-1\}$ as inputs and returns the element-wise product of the input lists, mod p. Your machine is fast and can accomodate any size lists, but it is also prone to mistakes. More specifically, you know that at most $\frac{1}{3}$ of the results are wrong. For example, suppose $p = 29$ and we feed the machine the two lists $(1,2,6)$ and $(5,1,2)$ we might get back output $(5,2,11)$ where $11 \neq 6 \times 2$ is a mistake. None of your potential clients is interested in a device which returns false results.

Show that you can augment your machine with Reed-Solomon-like encoding and decoding schemes such that no wrong outputs are ever returned and correct answers are obtained to the m pairs of numbers that you actually want to multiply together. (You will need to ask the machine itself to multiply more than m pairs of numbers to accomplish this.) You can assume you have access to interpolation-based (1-indexed) RS-encoders (parameters like n and k can be adjusted as you would like) as well as Berlekamp-Welch decoders. (Again, internal parameters like n and k can be **independently** adjusted as you would like — in particular, you don't have to use the same n and k that you used for the encoders.)

For concreteness, you can assume that the size of the desired input lists is $m = 6$ and that $p = 127$. (This is a prime number)

(HINT: first explore what happens with $m = 1$ and $m = 2$ to get an idea for what is going on.)

PRINT your name and student ID: _____

[Extra page. If you want the work on this page to be graded, make sure you tell us on the problem's main page.]

PRINT your name and student ID: _____

[Doodle page! Draw us something if you want or give us suggestions or complaints.]