EECS 70 Discrete Mathematics and Probability Theory
Fall 2014 Anant Sahai

Midterm 2

Exam location: 10 Evans, Last name starting with A-B or R-T

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 the person in front of you: _____

Name of the person behind you: _____

Section 0: Pre-exam questions (3 points)

1. **What is your favorite part of 70 so far? (1 pt)**

2. **Describe how you would feel in your dream stress-free vacation. (2 pts)**

Do not turn this page until the proctor tells you to do so. You can work on Section 0 above before time starts.

PRINT your name and student ID: _____

Section 1: Straightforward questions (30 points)

Unless told otherwise, you must show work to get credit. You get one drop: do 5 out of the following 6 questions. (We will grade all 6 and keep only the best 5 scores) However, there will be essentially no partial credit given in this section. Students who get all 6 questions correct will receive some bonus points.

3. Casting Out 9's

Let a number $N = a_0 + a_1 * 10 + a_2 * 10^2 + \cdots + a_k * 10^k$. Prove that $N \equiv a_0 + a_1 + a_2 + \cdots + a_k \pmod 9$.

PRINT your name and student ID: _____

4. Interpolate!

Find the lowest-degree polynomial $P(x)$ that passes through the points $(1,4),(2,3),(5,0)$ in mod 7.

5. RSA Compute

Cindy is sending a message to Tommy with RSA. If she uses the public key $e = 3, N = 55$, what is the value of d that Tommy must use to decrypt the message?

PRINT your name and student ID: _____

6. Packets

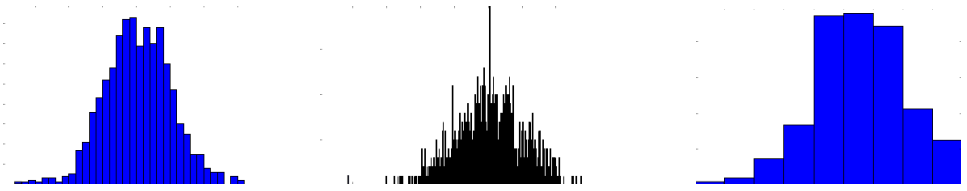
(a) You would like to send a message of length n packets to your friend. You know that at most k errors can occur during transmission. However, you are guaranteed that the first $n-1$ packets you send will arrive uncorrupted. How many packets must you send to guarantee successful transmission of your entire message? Why?

(b) 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? (No proof required)

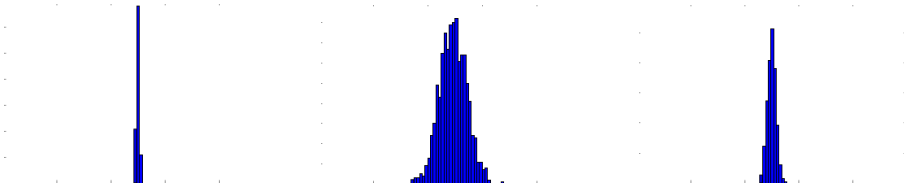
PRINT your name and student ID: _____

7. This Looks Familiar

(a) Excited about his upcoming concert, Justin Bieber decides to toss a large number of fair coins to help him calm his nerves. A trial consists of him flipping k such coins, and an experiment consists of 1000 such trials. He does 3 such experiments, with k being 10, 100, and 10000, respectively. (Justin Bieber can count coins faster than mere mortals.) For each experiment, he plots a histogram of the number of heads in each trial, using a horizontal axis scaled to include all the samples. **Which histogram below corresponds to which value of k?**



(b) Justin Bieber now carries out 3 different experiments with k being 100, 1000, and 10000, respectively. For each experiment, he plots a histogram of the fraction of heads, on a horizontal axis from 0 to 1. **Which histogram below corresponds to which value of k?**

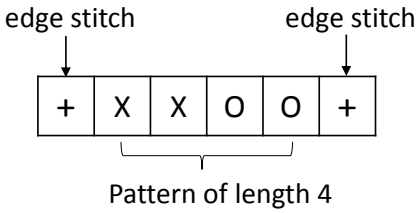


PRINT your name and student ID: _____

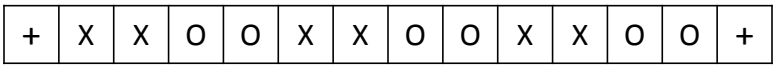
8. Celebrate and Remember Textiles

Mathematics and computing both owe an immense debt to textiles, where many key ideas originated.

Instructions for knitting patterns will tell you to begin by "casting on" the needle some multiple of m plus r, where m is the number of stitches to create one repetition of the pattern and r is the number of stitches needed for the two edges of the piece. For example, in the simple rib stitch pattern below, the repeating pattern is of length $m = 4$, and you need $r = 2$ stitches for the edges.



Thus, to make the final piece wider, you can add as many multiples of the pattern of length 4 as you like; for example, if you want to repeat the pattern 3 times, you need to cast on a total of $3m + r = 3(4) + 2 = 14$ stitches (shown below).



You've decided to knit a 70-themed baby blanket as a gift for your cousin and want to incorporate rows from three different stitch patterns with the following requirements:

- Katie's stitch: Multiple of 7, plus 4
- Anant's lace: Multiple of 4, plus 2
- Gireeja's grid: Multiple of 5, plus 2

You want to be able to switch between knitting these different patterns without changing the number of stitches on the needle, so you must use a number of stitches that simultaneously meets the requirements of all three patterns. **Find the smallest number of stitches you need to cast on in order to incorporate all three patterns in your baby blanket.**

(HINT: There is a tool you learned in class that is perfect for this problem.)

[We know space is limited here, so feel free to use the next page as needed.]

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, demonstrate that it is false.

9. Prime or Composite

If positive integer m does not divide a and $a^{m-1} \not\equiv 1 \bmod m$, then m is composite.

Mark one: TRUE or FALSE.

PRINT your name and student ID: _____

10. Remainder Riddles

There exists a polynomial (over $GF(7)$) $p(x)$ that has a remainder of 3 when divided by $x-1$, a remainder of 1 when divided by $x+1$, and a remainder of $2x+1$ when divided by x^2-1.

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 (65 points)

11. Secret Sharing with Spies (20 points)

An officer stored an important letter in her safe. In case she is killed in battle, she decides to share the password (which is a number) with her troops. However, everyone knows that there are 3 spies among the troops, but no one knows who they are except for the three spies themselves. The 3 spies can coordinate with each other and they will either lie and make people not able to open the safe, or will open the safe themselves if they can. Therefore, the officer would like a scheme to share the password that satisfies the following conditions:

- When M of them get together, they are guaranteed to be able to open the safe even if they have spies among them.
- The 3 spies must not be able to open the safe all by themselves.

Please help the officer to design a scheme to share her password. What is the scheme? What is the smallest M? Show your work and argue why your scheme works and any smaller M couldn't work.

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: _____

12. T/F: A Different Code (25 points)

An n-character message $\vec{a} = (a_0, \ldots, a_{n-1})$, with $a_i \in \text{GF}(p)$, is encoded into a polynomial of degree-d as follows. $P_{\vec{a}}(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_{n-1} x^{d-n+1}$. A codeword of length $n+2k$ is generated by evaluating $P_{\vec{a}}(x)$ as follows. $\vec{c}(\vec{a}) = (P_{\vec{a}}(1), P_{\vec{a}}(2), \ldots, P_{\vec{a}}(n+2k))$. If $p > d > n+2k$ and $k > 0$, then this code has a minimum Hamming distance of $2k+1$.

(Recall that the Hamming distance between two codewords is the number of positions they are different. The minimum distance of a code is the minimum distance between two distinct codewords.)

Mark one: TRUE or FALSE.

If true, prove the statement is true. If false, demonstrate that it is 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: _____

13. Like RSA (20 points)

You want to come up with an RSA-like scheme with $N = pqrs$, where p, q, r, s are distinct primes and the public encrypting function is $x^e \bmod N$.

(a) (5 points) Specify how to choose e.

(b) (15 points) Use the Chinese Remainder Theorem to come up with a decryption procedure that works slightly faster than the usual RSA decryption. Show that your scheme works (*i.e.* you can recover encrypted messages by decrypting them.).

You can assume here that exponentiating smaller numbers to smaller powers mod smaller numbers is significantly faster. So $(ab)^{cd} \bmod ef$ is slower than calculating both $a^c \bmod e$ and $b^d \bmod f$.

(HINT: Your secret key should include p, q, r, s individually.)

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) Oblivious Updates: File Sync (30 points)

Alice and Bob start with identical versions of a file. Assume the original file is n symbols from $GF(p)$, denoted $\vec{m}$. Assume that $2n < p$. Throughout this problem, Alice can send messages (noiselessly) to Bob, but Bob cannot send anything to Alice.

(a) (5 points) Suppose that one of the symbols in Bob's file gets erased. Bob knows which position was erased, but not what it was before it was erased. Alice only knows that one symbol was erased but not which one.

Alice would like to send Bob a short message, such that he can recover the original file $\vec{m}$. But noiseless communication is expensive – can you devise a scheme for Alice to do this, better than re-sending her n-long entire file $\vec{m}$? Argue why this works.

(b) (15 points) Assume that Bob has a correct version of $\vec{m}$. Alice makes a small change to her copy of the file, modifying one of the n symbols. Let this updated file be $\vec{m}'$. Bob later wants to update his copy to match Alice's copy – but Alice has forgotten which symbol she changed!

Once again, Alice would like to send Bob a short message, such that he can recover the updated file $\vec{m}'$. But noiseless communication is expensive – can you devise a scheme for Alice to do this, better than re-sending her n-long entire file $\vec{m}'$? Argue why your scheme works.

(c) (10 points) What if Alice changes $z > 1$ symbols? How would you deal with this case? (The size of the message sent to Bob is allowed to depend on z.) Argue why this works.

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. You can also use this page to report anything suspicious that you might have noticed.]