CS 70 Discrete Mathematics and Probability Theory
Fall 2020 HW 06

1 Exam Policy and Practice

Please read the all the documents (Policy, Key Changes, and Reminders) of the Exam Policy carefully before proceeding. This question is designed to familiarize you with some of the things you will have to do during the exam.

(a) After reading through the Exam Policy carefully, please answer the following questions.

(i) Given you experience no disruptions during the exam, how many total minutes do you have for scanning and submission?

(ii) Are you required to record locally during the exam? How much space should you have available on your computer for a local recording?

(iii) How should you contact the course staff for an emergency situation during the exam?

(b) Please configure your Zoom link.

(i) You should use the same Zoom link to join the meeting for the midterm as the Zoom link that you send to us. This can easily be done by submitting your Personal Meeting Room link and setting your Personal Meeting ID as your default on all devices you will be using for the final.

(ii) Ensure anyone can join your Zoom link and that there is no waiting room for your Zoom meeting.

(iii) Please the following Google Form with your Zoom link that you plan to use.

(c) You will now conduct a Zoom recording. Please read all instructions beforehand. You will use this recording to submit the mock midterm on gradescope, and should use the remaining time of the recording to work through a practice exam or other study material to simulate the actual circumstances of the final exam. It is advised to complete the LaTex Rehearsal beforehand, to familiarize yourself with typing LaTex answers.

(i) Start the Zoom call for the link you provided above. Turn on your microphone and recording device (webcam, phone camera). Turn off your speaker. Share your entire desktop (not just a particular window).

(ii) Start recording via Zoom. You may record locally or on the cloud.

(iii) Hold your CalID next to your face and record yourself saying your name into the webcam. Both your face and your entire CalID should be visible in the video. We should be able to read your name and SID. This step should take **at least** 3 seconds. See figure **??**. *If*

you do not have a CalID for some reason, please hold up some document which has an image of you and proves your identity, such as a driver's license.

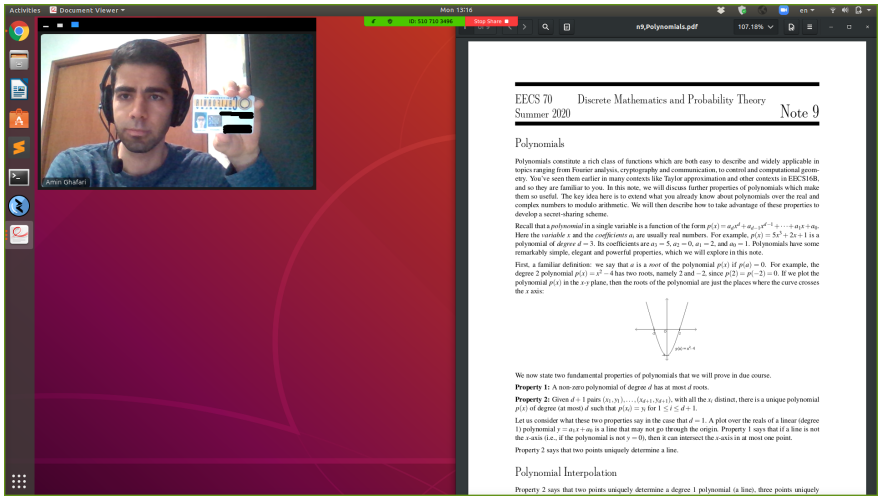

Figure 1: ID card demonstration. Do not actually black out your SID and name.

(iv) Position your recording device in such a way that we can see your workspace and your hands as best as possible. We suggest using your phone to record your hands, but if you are not, then it should be visible in the recording, face down. See figure **??**.

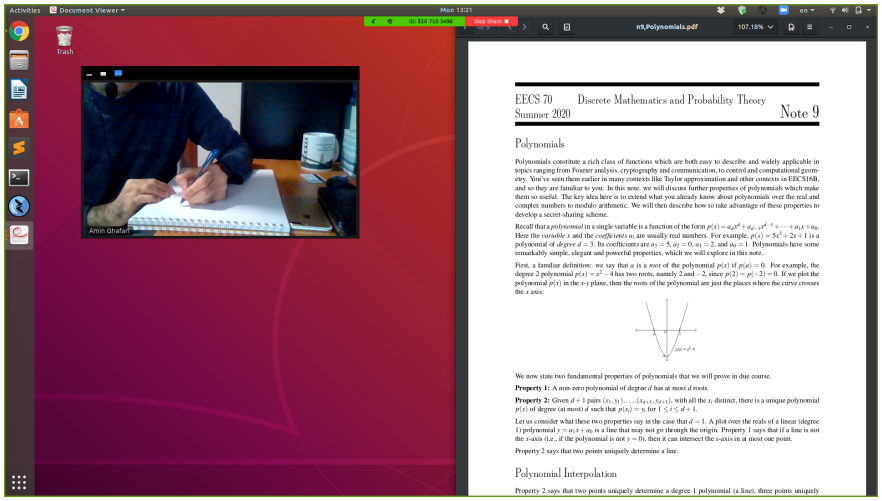

Figure 2: Demonstration of taking your exam. Your setup should look like this while you are taking the exam. The video must be on with your hands visible, alongside your exam pdf or gradescope.

(v) Your microphone should be on at all times. We should be able to see the time on your desktop at all times.

(vi) Record for two hours.

(vii) There are two mock midterm assignments on gradescope. You will see similar assignments on the day of the actual midterm. The one with (Short Answer) will be similar to Vitamins, where you will enter your answers in the gradescope assignment. The other (Written), will be full solution questions, and you will need to scan in your answers.

(viii) Complete and submit to the two mock midterm assignments. This includes both the short answers online, as well as scanning and submitting the written portion of the assignment.

(ix) For the remaining time, you should work through a practice final exam or other study material for the course. The more realistic it is to actually taking a final, the better practice it will be for you on the final.

(x) After two hours, stop the recording. Check your recording to confirm that it contains your video of your hands as well as your desktop throughout its duration. Upload your video to Google drive and submit the link to the video using this Google Form. You must make sure that the link sharing permissions are set so that we may view the video. Write down the magic words from the Google Form. DO NOT use this form for the actual exam, refer to the link in the policies during the actual midterm.

Link for policy:
https://docs.google.com/document/d/1-r3KrjQ46lX-OOiwx6lsoqAeSW0bDdM2oIw0xlKhLi0/edit?usp=sharing

Form to submit Zoom link:
https://forms.gle/2HDJtQijTzQdutgX8

Form to submit 2 hour video link:
https://forms.gle/XTJLhhbhqBNnKkxN9

Solution:

(a) (i) You have a total of 45 minutes for scanning and submission if you experience no disruption. If you experience x minutes of disruption during the exam, you may work for $\min(x, 15)$ minutes past the end of the exam.

(ii) You are not required to record locally; you may do a Zoom cloud recording. You should have 5 GB available on your computer if you are doing a local recording.

(iii) You should contact the course staff by making a private post on Piazza. However, you should not be looking at Piazza during the exam other than to make a private post in the case of an emergency.

(b) Ensure your Zoom link is joinable and that the Zoom link in the form is the correct link which you will be using for the exam.

(c) The possible magic word is "signature".

2 Message is too noisy

In this problem, we are going to discuss the decoding procedure even when the codeword is corrupted more than they could be. For all parts, work in mod 17.

(a) Encode the message $(0,1,4)$ into a polynomial, where $P(0)=0, P(1)=1, P(2)=4$, what is P?

(b) Suppose you send the message $(P(0),P(1),P(2),P(3),P(4))$ to the receiver and last packet is corrupted to 0. Run the decoding process and calulate the Q,E as defined in the lecture. You should also confirm that $Q(x)/E(x)=P(x)$.

(c) After corrupting the 4-th packet to 6 and 5-th packet to 8, decode again, by computing $Q,E,Q(x)/E(x)$, and outputting the first 3 packets. Explain why the decoded message is not the original message, but rather $(1,1,4)$.

(d) Define the Hamming distance between two messages to be the number of packets that differ. For example, the distance between $(0,1,2,3,4)$ and $(0,1,1,4,4)$ is 2 since they differ at the third and forth position.

Let $RS[5,3]$ be all Reed-Solomon codewords with codeword length 5, message length 3. Show that the Hamming distance between any two codewords in $RS[5,3]$ is at least 3. Also show that the codeword $(1,1,3,7,13)$ (which the decoder finds) has the smallest Hamming distance from the non-codeword $(1,1,4,7,13)$ compared to all other codeword in $RS[5,3]$.

(e) We generalize $RS[m,n]$ to be all Reed-Solomon codewords with length m, message length n. (Note: min Hamming distance between any pair of valid codewords is $m-n+1$). Let C' be the corrupted codeword, $msg = Decode(C')$, $E = Encode(msg)$. $Hamming(x,y)$ is the hamming distance between x and y. Show

$$Hamming(C',E) = \min_{E' \in RS[m,n]} (Hamming(C',E'))$$

Hint: if there are too many corruptions, clearly it will decode to a wrong message.

Solution:

(a) $P(x)=x^2$

(b) Codeword $(0,1,4,9,16)$. The decoder solves the following equations:

$$Q(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3, E(x) = b_0 + x$$

$$Q(0) = 0E(0), Q(1) = 1E(1), Q(2) = 4E(2), Q(3) = 9E(3), Q(4) = 16E(4)$$

$Q(x) = x^3 - 4x, E(x) = x - 1$, so $P(x) = x^2$ is the encoder polynomial for message.

(c) We changed 2 positions, but we only have 2 checkbits. RS codes ensures $2k$ checkbits can correct k errors. So with 2 check bits, only 1 error can be corrected. In this sub-question, we have 2 errors, which leads to incorrect decoding. ($Q(x) = 2x^2 - 2x, E(x) = x - 1, P(x) = 2x$)

(d) If there exists two codewords (a,b,c,d,e) and (a',b',c',d',e') with hamming distance at most 2, without loss of generality, we assuming $a=a', b \neq b', c=c', d=d', e \neq e'$. Since $RS[5,3,3]$ can correct up to 1 error, so the corrupted codeword (a,b,c,d',e) is ambiguous.

If we encode (a,b,c) into (a,b,c,d,e) and transmit it to the receiver, during the transmitting d gets corrupted into d'. We expect the decoder to output (a,b,c,d,e) on the receiver side.

If we encode (a,b',c) into (a,b',c,d,e') and transmit it to the receiver, during the transmitting e' gets corrupted into e. We expect the decoder to output (a,b',c,d,e') on the receiver side.

In both case, the decoder gets input (a,b,c,d',e). It's not possible for decoder to output two different messages given the same input.

(e) Let p be the maximum error that $RS[n,k]$ can correct. Then $p \geq Hamming(C',E)$.

If there exists another codeword E'' that has smaller hamming distance, then it's ambiguous for the decoder to decode. The decoder should decode to E'' and E at the same time based on what the original message and error is.

3 Linearity

Prove that Reed Solomon codes are *linear*; that is, the element-wise sum of two Reed Solomon codewords is also a Reed Solomon codeword. To do this, use the coefficient encoding rather than interpolation encoding: If you have a message of length n and you want to send m packets, create a degree $n-1$ polynomial $p(x)$ where your message $(c_0, c_1, \ldots, c_{n-1})$ are the coefficients of $p(x)$, and the codeword is the evaluation of $p(x)$ at $\{0, 1, \ldots, m-1\}$. (Assume we are working on $GF(p)$ for large enough p.)

Solution: Take two different messages a and b (each of length n) and construct polynomials $p(x)$ and $q(x)$ (each of degree $n-1$) respectively. Then generate the codewords corresponding to each, say P and Q (each of length m). Add the two codewords to form a new one, R and note that the i^{th} element of R corresponds to $p(i)+q(i)$. The polynomial $p(x)+q(x)$ corresponds to the generating polynomial for the message $a + b$.

4 Multiplicative

Recall $RS[m,n]$ to be all Reed-Solomon codewords with length m, message length n. Given two codewords $a,b \in RS[m,n]$. Let $c = a * b$ be the element-wise product of a and b. Show that $c \in RS[m, 2n-1]$. (Assume we are working over $GF(p)$, where p is large enough)

Solution: Take two different messages a and b (each of length n) and construct polynomials $p(x)$ and $q(x)$ (each of degree $n-1$) respectively. Then generate the codewords corresponding to each, P and Q (each of length $32n$). Multiply the two codewords to form a new one, R and notice that the i^{th} element of R corresponds to $p(i) * q(i)$. Let $f(x) = p(x) * q(x)$. The polynomial $f(x)$ corresponds to the generating polynomial for the message $(f(0), f(1), f(2), ..., f(2n-1))$.

5 Maze

(a) Given a 4×4 grid, how many different paths from $(0,0)$ to $(4,4)$ satisfy the following condition:

- You can only go from (x,y) to either $(x+1,y)$ or $(x,y+1)$

(b) Given a 4×4 grid, how many different paths from $(0,0)$ to $(4,4)$ satisfy the following condition:

- You can only go from (x,y) to either $(x+1,y)$ or $(x,y+1)$
- You cannot go to points (x,y) where $y>x$, in other word, you cannot cross line $y=x$

(c) How many sequences of 4 pairs of parentheses are mismatched? An example of a matched sequence of paretheses is ()()()(), while a mismatched sequence is))))((((.

Solution:

(a) $\binom{4+4}{4}$. If you want to go from $(0,0)$ to $(4,4)$, you must take 8 steps. In each of these step, it's either go up or go right. And the total number of go up command is exactly 4, the total number of go right command is exactly 4 in order to go to $(4,4)$. So you choose 4 positions out of 8 to take "go up" command, and rest of them are "go right" command. The total number of possible compositions are $\binom{8}{4}$.

(b) The solution is the same as writting numbers on the grid. Let $F(x,y)$ be the total number of moves from $(0,0)$ to (x,y) we have $\forall y>x, F(x,y)=0$ and $\forall x\leq y, y>0, F(x,y)=F(x-1,y)+F(x,y-1)$. And for boundry points $F(x,0)=1$. Then we can fill the table to calculate $F(4,4)$. We have $F(4,4)=14$.

(c) Interpret the left parenthesis as go right in the maze and a right parenthesis as go up in the maze. This is exactly asking how many different pathes that cross the line $y=x$, so it's $\binom{8}{4}-F(4,4)=56$

6 Good Game

Player will send 'GG' (Good Game) to the winner after each defeat in a 1v1 competitive game. Maru is a skilled Terran player in the Game. And he is 27 pts behind Player Sierral. Suppose Sierral has finished all of his games and Maru has 10 games to go. If Maru wins the i-th game, he will get i pts.

(a) What's the maximum number of GGs that Maru can send and have a higher points than Sierral?

(b) How many different ways that Maru can defeat Sierral (earns more than 27 pts)?

Solution:

(a) Maru only needs to win the last 4 games, where he gets $10+9+8+7=34$ pts, so he can lose at most 6 games, and a maximum of 6 GGs can be sent.

(b) Maru needs to win 28 pts, so for every winning configuration with x pts, there is a corresponding losing configuration with pts $55-x$, where $55-x\leq 27, x\geq 28$. So there are $\frac{1}{2}2^{10}$ different ways to win.

7 Counting Functions

(a) Compute $g(n)$, the number of ways to divide $\{1,2,3,...,n\}$ into 2 non-empty groups.

(b) Compute $f(n)$, the number of ways to divide $\{1,2,3,...,n\}$ into 3 non-empty groups. (Hint: our calculation involves a recursive formula, and included g)

(c) How many surjective functions $h : \{1,2,3,...,7\} \to \{1,2,3\}$? You may leave your answer in terms of f and g for partial credit, but also compute the actual number.

Solution:

(a) Answer is $\frac{2^n}{2} - 1$, there are total 2^n ways to divide n numbers into 2 labeled sets. So $\frac{2^n}{2} - 1$ is the number of ways to divide n numbers into 2 unlabeled non-empty sets, where -1 removes the emptyset case.

(b) To count the number of divisions, let $f(x)$ be the number of ways that divide a set of size x into 3 non-empty groups. We have

$f(x) = f(x-1) * 3 + g(x-1)$

For element x, it can join one of the three non-empty divisions formed by $x-1$ elements, which gives $3 * f(x-1)$ different possibilities. Or x itself creates a new group, and the first $x-1$ elements forms exactly 2 non-empty groups.

(c) It's asking how many ways to divide $\{1,2,3,4,5,6,7\}$ into 3 labeled non-empty sets. So it's $f(7) * 3! = 1806$, where we multiply by 3! because order matters.

We calculate $f(7)$ following the recursive definition:

$f(3) = 1, f(4) = 3 * f(3) + 2^2 - 1 = 6, f(5) = f(4) * 3 + 2^3 - 1 = 3 * 6 + 7 = 25, f(6) = 3 * f(5) + 2^4 - 1 = 3 * 25 + 15 = 90, f(7) = 3 * f(6) + 2^5 - 1 = 3 * 90 + 31 = 301$

$f(7) = 301$