CS 70 Discrete Mathematics and Probability Theory
Summer 2019 James Hulett and Elizabeth Yang Midterm 2

PRINT your name: _____ _____
(First) (Last)

SIGN your name: _____

PRINT your student ID: _____

CIRCLE your exam room: VLSB 2050 Dwinelle 155 Soda 320 Soda 341A Soda 341B

Name of the person sitting to your left: _____

Name of the person sitting to your right: _____

- We will not grade anything outside of the space provided for a problem unless we are clearly told in the space provided for the question to look elsewhere.
- We will not be collecting scratch paper. Write everything you want to be graded on the exam itself.
- Assume independence means *mutual independence* unless otherwise noted.
- You may use binomial coefficients in your answers, unless the question otherwise specifies an answer form (e.g. fraction, decimal).
- Unless otherwise specified, you may use any variables from the problem in your answer.
- You may consult two handwritten double-sided sheets of notes. Apart from that, you may not look at books, notes, etc. Calculators, phones, computers, and other electronics devices are prohibited.
- There are 14 pages (7 sheets) on the exam. Notify a proctor immediately if a page is missing.
- There are 7 questions on this exam, worth a total of 175 points.
- **You may, without proof, use theorems and facts that were proven in the notes, lecture, discussion, or homework.**
- **You have 120 minutes.**

Do not turn this page until your instructor tells you to do so.

1 True/False [3 Points Each, 30 Total]

1 point for True/False marking, 2 points for justification.

For each statement, mark whether it is true or false and give a brief justification (maximum 1 sentence, must fit in box) in the adjacent box.

(a) Working over $GF(7)$, we can use the secret-sharing scheme from class to share a secret among 7 people such that at least 3 of them must come together to recover the secret.

◯ **True**

◯ **False**

(b) If $\mathbb{P}[A \cap B] = \mathbb{P}[A] \times \mathbb{P}[B]$, $\mathbb{P}[A \cap C] = \mathbb{P}[A] \times \mathbb{P}[C]$, and $\mathbb{P}[B \cap C] = \mathbb{P}[B] \times \mathbb{P}[C]$, then $\mathbb{P}[A \cap B \cap C] = \mathbb{P}[A] \times \mathbb{P}[B] \times \mathbb{P}[C]$.

◯ **True**

◯ **False**

(c) If $A \subseteq B$ and B is countable, then A is also countable.

◯ **True**

◯ **False**

(d) If we can reduce A to the Halting Problem, A must be undecidable.

◯ **True**

◯ **False**

(e) Suppose I send $n+2k$ packets in a standard Berlekamp-Welch scheme. If there are $d < k$ corruptions, then the error polynomial $E(x)$ I solve for will only be of degree d rather than degree k.

◯ **True**

◯ **False**

(f) If A is uncountable and B is uncountable, then $A - B$ is countable.

◯ **True**

◯ **False**

(g) The set of recursively enumerable problems is countable.

◯ **True**

◯ **False**

(h) If the error polynomial $E(x)$ from the Berlekamp-Welch scheme has fewer than k distinct roots, then that means fewer than k packets were corrupted.

◯ **True**

◯ **False**

(i) If we want a secret sharing scheme with n participants, and we need at least k of them to unlock the secret, then we can use a polynomial of degree k.

◯ **True**

◯ **False**

(j) Let x_1, x_2, and x_3 be three random numbers drawn with replacement from $\{1,2,...,70\}$. If A is the event that $x_1 = x_2$ and B is the event that $x_2 = x_3$, then A and B are independent of each other.

◯ **True**

◯ **False**

2 Short Answer [3 Points Each, 48 Total]

(a) Suppose I have a deck of 52 cards and I lost 5 cards in the deck because I was careless. I shuffle the deck and take the top card. What is the probability that the card is a spade?

(b) Suppose I roll two 20-sided dice. What is the probability that at least one of the dice is at least 3?

(c) Find the number of non-negative integer solutions to $x_1 + x_2 + x_3 = 30$ where we have that at least one $x_i \leq 5$.

(d) James has 5 pairs of red socks and 10 pairs of blue socks, for a total of 30 socks. If James randomly picks 3 socks, what is the probability that he selected at least two blue socks?

(e) Suppose we want to send n packets, and we know that our channel drops a fraction p of our packets, where $0 < p < 1$. Using the Reed-Solomon encoding from class, how many *total* packets should we send?

(f) How many length-15 bit strings with exactly 5 ones are there such that none of the ones are adjacent to each other? (*Hint: Try to relate these strings to instances of stars and bars.*)

(g) Within a student club of n (distinguishable) members, there are 4 (distinguishable) committees.

(i) We ask each club member to join *exactly* 2 committees. If there are n members, how many ways can these committees be formed?

(ii) We changed the rules so that all members can participate in at most 1 committee, but may also participate in none. We now want all 4 committees to have exactly 3 distinct members. How many ways can we form the committees now? Assume $n \geq 12$.

(h) Suppose Alice wishes to send Bob a length-n message $m_1, m_2, ..., m_n$, using the Berlekamp-Welch algorithm to protect against up to k corruptions. Assume that they are working over $GF(p)$ for some sufficiently large prime p.

(i) Suppose the channel corrupts exactly k packets, meaning that k of the packets Bob receives have a different value from what Alice sent. Given some specific message Alice wants to send, how many possible sequences of $n+2k$ values could Bob receive?

(ii) If the channel randomly chooses k distinct packets to corrupt, what is the probability that none of the k corruptions occurs in the first n packets?

(iii) Suppose the channel only corrupts the first d packets, where $d < k$. How many possible polynomials could Bob get for $E(x)$? That is, how many degree exactly k polynomials $E(x)$ are there such that **(a)** $E(1) = E(2) = ... = E(d) = 0$ and **(b)** the coefficient on the x^k term is 1?

(i) Yaxin downloads a new spam filter for her email. If the filter sees an actual spam email, it sends it to the spam folder with probability 0.8. If the filter sees a non-spam email, it sends it to the spam folder with probability 0.1. For any of Yaxin's incoming email, there is a 0.2 probability it is spam. Given that Yaxin sees a message in her spam folder, what is the probability that it is not actually spam? Give your answer as a simplified fraction.

(j) For this question, you may use factorials and fractions.

(i) How many ways can we rearrange the 9 character string "GOBEARS!!"?

(ii) How many ways can we rearrange the 11 character string "BOOSTANFURD" so that all of the vowels (A, E, I, O, U) appear next to each other?

(k) Each day is sunny with probability $\frac{4}{5}$ and cloudy with probability $\frac{1}{5}$. The weather each day is independent of every other day. On a sunny day, Elizabeth goes to Cheeseboard with probability $\frac{1}{2}$. On a cloudy day she goes with probability $\frac{1}{4}$. What is the probability that she goes to Cheeseboard both next Monday and Tuesday? Leave your answer as a fraction.

(l) A dormitory has $n \geq 4$ students, all of whom like to gossip. One of the students hears a rumor, and tells it to one of the other $n-1$ students picked at random. After that, each student who hears the rumor tells it to another student picked uniformly at random, excluding themselves and the student who just told them the rumor. Let p_r be the probability that the rumor is told at least r times without coming back to a student who has already heard it.

Derive a formula for p_r in terms of r. Assume $3 \leq r \leq n-1$.

3 Astronaut Asli's Anonymous Adventure [2/2/2/2/3/4 Points, 15 Total]

In Seventylandia, 70 officials are voting on whether to let Asli go to space. She needs all officials to vote "yes" in order to go. The officials wish to vote using an *anonymous* secret-sharing scheme, meaning that if Asli doesn't get a unanimous vote, she cannot tell who voted against her.

Working in $GF(71)$, we pick a degree d polynomial $P(x)$ and give official i the point $(i, P(i))$. Asli passes the vote if she can recover $P(x)$.

(a) If official i wants to vote for Asli, what should they do?

(b) If official i does not want to vote for her, what should they do?

(c) What should the degree d be in order to make this scheme work?

(d) Briefly explain why your scheme lets Asli recover $P(x)$ if the vote is unanimously yes.

(e) Briefly explain why Asli cannot recover $P(x)$ if the vote is not unanimously yes.

(f) Briefly explain why this scheme is anonymous.

4 Can You Count It? [5 Points Each, 15 Total]

For each set below, mark whether it is countable or uncountable and prove your claim. One point for the correct bubble, 4 points for the proof.

(a) The set of finite-length strings made of lower-case English letters.

◯ **Countable**

◯ **Uncountable**

(b) The set of pairs of pairs of naturals: $(\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) = \{((n_1, n_2), (n_3, n_4)) \mid n_1, n_2, n_3, n_4 \in \mathbb{N}\}$.

◯ **Countable**

◯ **Uncountable**

(c) The set of functions from $\mathbb{N}$ to $\mathbb{N}$ such that $f(n) \neq n$ for all n.

◯ **Countable**

◯ **Uncountable**

5 Recursive Enumerability Is In Scope. [5/3/3/5/3/3/3 Points, 25 Total]

For parts asking you to fill in the description of a program, you can either write pseudocode or describe what the program is doing in English.

A "halting converter" for a problem *A* is a program `C` that takes an instance of *A* as input and:

- If the correct answer for `x` is true, `C(x)` outputs a pair `(P,y)` such that `P(y)` halts.
- If the correct answer for `x` is false, `C(x)` outputs a pair `(P,y)` such that `P(y)` loops forever.

(a) We first prove that if *A* has a halting converter, *A* is recognizable.

(i) Suppose we have a program `C` that is a halting converter for *A*. Fill in the description of `R` such that it is a recognizer for *A*.

`R(x):`

(ii) Prove that if the correct answer for `x` is true, `R(x)` will return true in finite time.

(iii) Prove that if the correct answer for `x` is false, `R(x)` will return false or loop forever.

(b) We next prove the converse: if A is recognizable, A has a halting converter.

(i) Suppose we have a recognizer `R` for A. Fill in the description of `P` such that, for an instance `x` of the problem A, `P(x)` halts if and only if the correct answer for `x` is true.

```
def P(x):
```

(ii) Prove that if the correct answer for `x` is true, `P(x)` halts.

(iii) Prove that if the correct answer for `x` is false, `P(x)` loops forever.

(iv) Fill in the description of `C` below such that it is a halting converter for A. You may use the program `P` from part (i), even if you did not complete that part.

```
def C(x):
```

6 Can You Count It? 2: Electric Boogaloo [3/5/3/3/4 Points, 18 Total]

(a) I have a group of n people. I want to choose some of them to be on a basketball team and some to be on a soccer team such that no one is on both teams and the sizes of the two teams add up to p.

(i) If I know I want k players on the basketball team, how many ways can I pick the two teams? Place your response in the box. No justification required.

(ii) Let A_k be the answer you obtained above. Fill in the box such that the below identity holds, and **provide a combinatorial proof** for the identity. *You may not cite any results from lecture for this part–anything you use must be reproven.* Your answer can be in terms of p only.

$$\sum_{k=0}^{p} A_k = \binom{n}{p} \times$$

(b) Now, let's count quaternary digit strings, i.e. strings of numbers where each digit can only be $0, 1, 2$, or 3. For example, 01312 is a quaternary string with 5 digits.

(i) How many n digit quaternary digit strings are there? Place your answer in the box.

(ii) How many n digit quaternary digit strings contain exactly k 3's? Place your answer in the box.

(iii) Let Q be the answer obtained from Part (i), and T_k be the answer from Part (ii). In the box, write an expression for Q that is only in terms of T_k. **Provide a brief explanation for your answer.**

7 Streaming Services Battle (Every Day I'm Shufflin') [4 Each, 24 Total]

Write answers in the box. Any correct answer will receive full credit. However, partial credit may be awarded if sufficient work is shown.

(a) Given a playlist, the shuffle feature on Apple Music will play songs as a series of independent *shuffle cycles*. In each shuffle cycle, all songs in the list will be reordered, with each ordering equally likely. For instance, for a playlist of four songs a, b, c, d, one possible sequence of plays could be

$$a\ b\ c\ d \mid b\ d\ c\ a \mid d\ a\ c\ b \mid \ldots$$

where we use $\mid$ to separate the shuffle cycles.

Suppose I have an Apple Music playlist with **exactly two songs**, a and b. I have this playlist on shuffle while I'm away, so when I return, I could be at any position within a shuffle cycle with equal probability. When I return, a is playing.

(i) What is the probability that the next song is b?

(ii) The next song played happened to be b. What is the probability that when I returned (i.e. when a was playing), it was the start of a shuffle cycle?

(b) Spotify's shuffle feature works a little differently. It instead selects any copy of any song from the playlist uniformly at random to play each time. I have a Spotify playlist with 5 copies of song a, 3 copies of song b, and 2 copies of song c (10 copies total).

(i) I shuffle my Spotify playlist for 6 song plays. If I *ignore their play order*, how many different sets of 6 plays could I have gotten? Give your answer as an integer.

(ii) What is the probability that across the 6 songs played on my Spotify shuffle, I get song a twice, song b twice, and song c twice? (*You may leave your answer unsimplified.*)

(c) YouTube Music's (YTM) shuffle functionality is somewhere in between Apple Music's and Spotify's. Specifically, given a playlist of n songs, YTM will still play songs as a series of *independent* length-n shuffle cycles. However, each YTM cycle will behave like Apple Music's shuffle feature (from part (a)) with probability p, and behave like Spotify's shuffle feature (from part (b)) with probability $1-p$.

I have a playlist with **exactly two songs** (one copy of each), a and b. I return when a (YTM) shuffle cycle is about to begin. (*Note: Each of the following answers may be in terms of p.*)

(i) What is the probability that the first song I hear is a and the second is b?

(ii) What is the probability that the second song I hear is b given that the first is a?