CS 70 Discrete Mathematics and Probability Theory
Fall 2020 HW 0

1 Administrivia

(a) Make sure you are on the course Piazza (for Q&A) and Gradescope (for submitting homeworks, including this one). Find and familiarize yourself with the course website. What is its homepage's URL?

(b) Read the policies page on the course website.

(i) What is the percentage breakdown of how your grade is calculated (please include both breakdowns)?

(ii) How many discussions do you need to attend to get full credit for discussion attendance?

(iii) Can you attend a section different from the one you signed up for?

(iv) When are the Vitamins due?

Solution:

(a) The course website is located at http://www.eecs70.org/.

(b) (i) Discussion attendance and vitamins are each worth 5% of your grade, homework is worth 20% of your grade, the midterm is worth 30%, and the final is worth 40%.

(ii) You must attend at least 14 discussions out of 27 to get full credit for discussion attendance.

(iii) You are welcome to attend other discussion sections, but your attendance will not be counted for those sections.

(iv) Vitamins are due every Friday at 10:00 PM, with a grace period until 11:59 PM.

2 Course Policies

Go to the course website and read the course policies carefully. Leave a followup in the Homework 0, Question 2 thread on Piazza if you have any questions. Are the following situations violations of course policy? Write "Yes" or "No", and a short explanation for each.

(a) Alice and Bob work on a problem in a study group. They write up a solution together and submit it, noting on their submissions that they wrote up their homework answers together.

(b) Carol goes to a homework party and listens to Dan describe his approach to a problem on the board, taking notes in the process. She writes up her homework submission from her notes, crediting Dan.

(c) Erin comes across a proof that is part of a homework problem while studying course material. She reads it and then, after she has understood it, writes her own solution using the same approach. She submits the homework with a citation to the website.

(d) Frank is having trouble with his homework and asks Grace for help. Grace lets Frank look at her written solution. Frank copies it onto his notebook and uses the copy to write and submit his homework, crediting Grace.

(e) Heidi has completed her homework using LaTeX. Her friend Irene has been working on a homework problem for hours, and asks Heidi for help. Heidi sends Irene her PDF solution, and Irene uses it to write her own solution with a citation to Heidi.

(f) Joe found homework solutions before they were officially released, and every time he got stuck, he looked at the solutions for a hint. He then cited the solutions as part of his submission.

Solution:

(a) Yes, this is a violation of course policy. All solutions must be written entirely by the student submitting the homework. Even if students collaborate, each student must write a unique, individual solution. In this case, both Alice and Bob would be culpable.

(b) No, this is not a violation of course policy. While sharing *written solutions* is not allowed, sharing *approaches* to problems is allowed and encouraged. Because Carol only copied down *notes*, not *Dan's solution*, and properly cited Dan's contribution, this is an actively encouraged form of collaboration.

(c) No, this is not a violation of course policy. Using external sources to help with homework problems, while less encouraged than peer collaboration, is fine as long as (i) the student makes sure to understand the solution; (ii) the student uses understanding to write a new solution, and does not copy from the external source; and (iii) the student credits the external source. However, looking up a homework problem online is a violation of course policies; the correct course of action upon finding homework solutions online is to close the tab.

(d) Yes, this is a violation of course policy, and both Frank and Grace would be culpable. Even though Frank credits Grace, written solutions should never be shared in the first place, and certainly not copied down. This is to ensure that each student learns how to write and present clear and convincing arguments. To be safe, try not to let anybody see your written solutions at any point in the course—restrict your collaboration to *approaches* and *verbal communication*.

(e) Yes, this is a violation of course policy. Once again, a citation does not make up for the fact that written solutions should never be shared, in written or typed form. In this case, both Heidi and Irene would be culpable.

(f) Yes, this is a violation of course policy. Joe should not be reading solutions before they are officially released. Instead, Joe should ask for help when he is stuck through Piazza, Join Me, or an OH appointment.

3 Use of Piazza

Piazza is incredibly useful for Q&A in such a large-scale class. We will use Piazza for all important announcements. You should check it frequently. We also highly encourage you to use Piazza to ask questions and answer questions from your fellow students.

(a) Navigate to the "Index" Piazza post, where you can find links to most resources in the course. Write down the Piazza post number for the Note 1 Thread. (When you see @x on Piazza, where x is a positive integer, then x is the post number of the linked post.)

(b) Read the Piazza Etiquette section of the course policies and explain what is wrong with the following hypothetical student question: "Can someone explain the proof of Theorem XYZ to me?" (Assume Theorem XYZ is a complicated concept.)

(c) When are the weekly posts released? Are they required reading?

Solution:

(a) The post number for the Note 1 Thread is 11.

(b) There are two things wrong with this question. First, this question does not pass the 5-minute test. This concept takes longer than 5 minutes to explain, and therefore is better suited to Office Hours. Second, this question does not hone in on a particular concept with which the student is struggling. Questions on Piazza should be narrow, and should include every step of reasoning that led up to the question. A better question in this case might be: "I understood every step of the proof of Theorem XYZ in Note 2, except for the very last step. I tried to reason it like this, but I didn't see how it yielded the result. Can someone explain where I went wrong?"

(c) The weekly posts are released every Sunday. They're required reading.

4 Timezone

Please fill out the discussion time preference form at `bit.ly/fa20cs70dispref`. What is your magic word?

Solution: Acceptable magic words are "committee dime," "mink agree," "whip separate," "insect mug," or "soda pies."

5 Academic Integrity

Please write or type out the following pledge in print, and sign it.

> I pledge to uphold the university's honor code: to act with honesty, integrity, and respect for others, including their work. By signing, I ensure that all written homework I submit will be in my own words, that I will acknowledge any collaboration or help received, and that I will neither give nor receive help on any examinations.

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 HW 1

1 Calculus Review

(a) Compute a closed-form expression for the value of following summation:

$$\sum_{k=1}^{\infty} \frac{9}{2^k}$$

(b) Use summation notion to write an expression equivalent to the following statement:

The sum of the first n consecutive odd integers, starting from 1

(c) Compute the following integral:

$$\int_0^{\infty} \sin(t)e^{-t}dt$$

(d) Find the maximum value of the following function and determine where it occurs:

$$f(x) = -x \cdot \ln x$$

Solution:

(a) Use the convergence of geometric series with $|r| < 1$.

$$\begin{aligned}\sum_{k=1}^{\infty} \frac{9}{2^k} &= 9 \cdot \sum_{k=1}^{\infty} \frac{1}{2^k} = 9 \cdot (\sum_{k=0}^{\infty} \frac{1}{2^k} - 1) \\ &= 9 \cdot (2-1) = 9\end{aligned}$$

(b) Observe that $2k+1$ is odd for all $k \in \mathbb{Z}$.

$$\sum_{k=0}^{n-1} 2k+1$$

(c) Let $I = \int sin(t)e^{-t}$.
Use integration by parts, with $u = \sin(t)$ and $dv = e^{-t}$.
This means $du = \cos(t)$ and $v = -e^{-t}$.

$$\begin{aligned}I = \int \sin(t)e^{-t}dt &= uv - \int v \cdot du \\ &= -\sin(t)e^{-t} + \int e^{-t}\cos(t)dt\end{aligned}$$

Use integration by parts again on $\int e^{-t}\cos(t)dt$, with $u = \cos(t)$ and $dv = e^{-t}$. This means $du = -\sin(t)$ and $v = -e^{-t}$.

$$\begin{aligned}\int e^{-t}\cos(t)dt &= uv - \int v \cdot du \\ &= -\cos(t)e^{-t} - \int e^{-t}\cdot\sin(t)dt \\ &= -\cos(t)e^{-t} - I\end{aligned}$$

Combining these results:

$$\begin{aligned}I &= -\sin(t)e^{-t} - \cos(t)e^{-t} - I \\ \Rightarrow 2I &= -\sin(t)e^{-t} - \cos(t)e^{-t} \\ \Rightarrow I &= \frac{-\sin(t)e^{-t} - \cos(t)e^{-t}}{2}\end{aligned}$$

Finally, we have:

$$I\Big|_0^\infty = \frac{0-0}{2} - \frac{0-1}{2} = \frac{1}{2}$$

(d) Compute the derivative of the function, and set it equal to 0.

$$\begin{aligned}\frac{df}{dx} &= -1\cdot\ln x + -x\cdot\frac{1}{x} \\ &= -\ln x - 1 = 0 \\ &\Rightarrow x^* = \frac{1}{e}\end{aligned}$$

The optimal value is achieved at $x^* = \frac{1}{e}$, and the corresponding value is $f(x^*) = \frac{1}{e}$.

2 Propositional Practice

In parts (a)-(c), convert the English sentences into propositional logic. In parts (d)-(f), convert the propositions into English. In part (f), let $P(a)$ represent the proposition that a is prime.

(a) There is one and only one real solution to the equation $x^2 = 0$.

(b) Between any two distinct rational numbers, there is another rational number.

(c) If the square of an integer is greater than 4, that integer is greater than 2 or it is less than -2.

(d) $(\forall x \in \mathbb{R})\ (x \in \mathbb{C})$

(e) $(\forall x, y \in \mathbb{Z})(x^2 - y^2 \neq 10)$

(f) $(\forall x \in \mathbb{N})\ [\ (x > 1) \implies (\exists a, b \in \mathbb{N})\ ((a + b = 2x) \wedge P(a) \wedge P(b))\ ]$

Solution:

(a) Let $p(x) = x^2$. The sentence can be read: "There is a solution x to the equation $p(x) = 0$, and any other solution y is equal to x". Or,

$$(\exists x \in \mathbb{R})\left((p(x) = 0) \wedge ((\forall y \in \mathbb{R})(p(y) = 0) \implies (x = y))\right).$$

(b) The sentence can be read "If x and y are distinct rational numbers, then there is a rational number z between x and y." Or,

$$(\forall x, y \in \mathbb{Q})((x \neq y) \implies ((\exists z \in \mathbb{Q})(x < z < y \vee y < z < x))).$$

Equivalently,

$$(\forall x, y \in \mathbb{Q})((x = y) \vee (\exists z \in \mathbb{Q})(x < z < y \vee y < z < x)).$$

Note that $x < z < y$ is mathematical shorthand for $(x < z) \wedge (z < y)$, so the above statement is equivalent to

$$(\forall x, y \in \mathbb{Q})(x = y) \vee ((\exists z \in \mathbb{Q})\left((x < z) \wedge (z < y)\right) \vee \left((y < z) \wedge (z < x)\right)).$$

(c) $(\forall x \in \mathbb{Z})\left((x^2 > 4) \implies ((x > 2) \vee (x < -2))\right)$

(d) All real numbers are complex numbers.

(e) There are no integer solutions to the equation $x^2 - y^2 = 10$.

(f) For any natural number greater than 1, there are some prime numbers a and b such that $2x = a + b$.

In other words: Any even integer larger than 2 can be written as the sum of two primes.

Aside: This statement is known as Goldbach's Conjecture, and it is a famous unsolved problem in number theory (https://xkcd.com/1310/).

3 Tautologies and Contradictions

Classify each statement as being one of the following, where P and Q are arbitrary propositions:

- True for all combinations of P and Q (Tautology)
- False for all combinations of P and Q (Contradiction)
- Neither

Justify your answers with a truth table.

(a) $P \implies (Q \wedge P) \vee (\neg Q \wedge P)$

(b) $(P \vee Q) \vee (P \vee \neg Q)$

(c) $P \wedge (P \implies \neg Q) \wedge (Q)$

(d) $(\neg P \implies Q) \implies (\neg Q \implies P)$

(e) $(\neg P \implies \neg Q) \wedge (P \implies \neg Q) \wedge (Q)$

(f) $(\neg(P \wedge Q)) \wedge (P \vee Q)$

Solution:

(a) **Tautology**

P	Q	$Q \wedge P$	$\neg Q \wedge P$	$P \implies (Q \wedge P) \vee (\neg Q \wedge P)$
T	T	T	F	T
T	F	F	T	T
F	T	F	F	T
F	F	F	F	T

(b) **Tautology**

P	Q	$P \vee Q$	$P \vee \neg Q$	$(P \vee Q) \vee (P \vee \neg Q)$
T	T	T	T	T
T	F	T	T	T
F	T	T	F	T
F	F	F	T	T

(c) **Contradiction**

P	Q	$P \implies \neg Q$	$P \wedge (P \implies Q) \wedge (Q)$
T	T	F	F
T	F	T	F
F	T	T	F
F	F	T	F

(d) **Tautology**

P	Q	$\neg P \implies Q$	$\neg Q \implies P$	$(\neg P \implies Q) \implies (\neg Q \implies P)$
T	T	T	T	T
T	F	T	T	T
F	T	T	T	T
F	F	F	F	T

(e) **Contradiction**

P	Q	$P \implies \neg Q$	$\neg P \implies \neg Q$	$(P \implies \neg Q) \wedge (\neg P \implies \neg Q) \wedge (Q)$
T	T	F	T	F
T	F	T	T	F
F	T	T	F	F
F	F	T	T	F

(f) **Neither**

P	Q	$P \vee Q$	$\neg(P \wedge Q)$	$(P \vee Q) \wedge (\neg(P \wedge Q))$
T	T	T	F	F
T	F	T	T	T
F	T	T	T	T
F	F	F	T	F

4 Prove or Disprove

For each of the following, either prove the statement, or disprove by finding a counterexample.

(a) $(\forall n \in \mathbb{N})$ if n is odd then $n^2 + 4n$ is odd.

(b) $(\forall a, b \in \mathbb{R})$ if $a + b \leq 15$ then $a \leq 11$ or $b \leq 4$.

(c) $(\forall r \in \mathbb{R})$ if r^2 is irrational, then r is irrational.

(d) $(\forall n \in \mathbb{Z}^+)$ $5n^3 > n!$. (Note: $\mathbb{Z}^+$ is the set of positive integers)

Solution:

(a) **Answer**: True.
Proof: We will use a direct proof. Assume n is odd. By the definition of odd numbers, $n = 2k + 1$ for some natural number k. Substituting into the expression $n^2 + 4n$, we get $(2k + 1)^2 + 4 \times (2k + 1)$. Simplifying the expression yields $4k^2 + 12k + 5$. This can be rewritten as $2 \times (2k^2 + 6k + 2) + 1$. Since $2k^2 + 6k + 2$ is a natural number, by the definition of odd numbers, $n^2 + 4n$ is odd.
Alternatively, we could also factor the expression to get $n(n + 4)$. Since n is odd, $n + 4$ is also odd. The product of 2 odd numbers is also an odd number. Hence $n^2 + 4n$ is odd.

(b) **Answer**: True.
Proof: We will use a proof by contraposition. Suppose that $a > 11$ and $b > 4$ (note that this is equivalent to $\neg\big(a \leq 11 \vee b \leq 4\big)$). Since $a > 11$ and $b > 4$, $a + b > 15$ (note that $a + b > 15$ is equivalent to $\neg\big(a + b \leq 15\big)$). Thus, if $a + b \leq 15$, then $a \leq 11$ or $b \leq 4$.

(c) **Answer**: True.
Proof: We will use a proof by contraposition. Assume that r is rational. Since r is rational, it can be written in the form $\frac{a}{b}$ where a and b are integers with $b \neq 0$. Then r^2 can be written as $\frac{a^2}{b^2}$. By the definition of rational numbers, r^2 is a rational number, since both a^2 and b^2 are integers, with $b \neq 0$. By contraposition, if r^2 is irrational, then r is irrational.

(d) **Answer**: False.
Proof: We will use proof by counterexample. Let $n = 7$. $5 \times 7^3 = 1715$. $7! = 5040$. Since $5n^3 < n!$, the claim is false.

5 Twin Primes

(a) Let $p > 3$ be a prime. Prove that p is of the form $3k+1$ or $3k-1$ for some integer k.

(b) *Twin primes* are pairs of prime numbers p and q that have a difference of 2. Use part (a) to prove that 5 is the only prime number that takes part in two different twin prime pairs.

Solution:

(a) First we note that any integer can be written in one of the forms $3k$, $3k+1$, or $3k+2$. (Note that $3k+2$ is equal to $3(k+1)-1$. Since k is arbitary, we can treat these as equivalent forms).

We can now prove the contrapositive: that any integer $m > 3$ of the form $3k$ must be composite. Any such integer is divisible by 3, so this is true right away. Thus our original claim is true as well.

(b) We can check all the primes up to 5 to see that of these, only 5 takes part in two twin prime pairs (3,5 and 5,7). What about primes > 5?

For any prime $m > 5$, we can check if $m+2$ and $m-2$ are both prime. Note that if $m > 5$, then $m+2 > 3$ and $m-2 > 3$ so we can apply part (a) and we can do a proof by cases based on the two forms from part (a).

Case 1: m is of the form $3k+1$. Then $m+2 = 3k+3$, which is divisible by 3. So $m+2$ is not prime.

Case 2: m is of the form $3k-1$. Then $m-2 = 3k-3$, which is divisible by 3. So $m-2$ is not prime.

So in either case, at least one of $m+2$ and $m-2$ is not prime.

6 Social Network

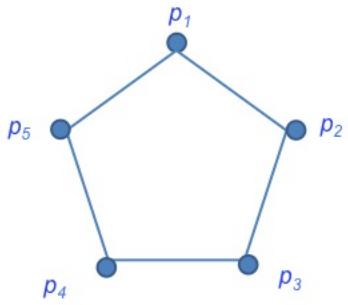
Consider the same setup as Q2 on the vitamin, where there are n people at a party, and every two people are either friends or strangers. Prove or provide a counterexample for the following statements.

(a) For all cases with $n = 5$ people, there exists a group of 3 people that are either all friends or all strangers.

(b) For all cases with $n = 6$ people, there exists a group of 3 people that are either all friends or all strangers.

Solution:

(a) The statement is false. A counterexample is shown below where people are connected if they are friends and unconnected if they are strangers. In this example, at most 2 are friends or strangers.



(b) The statement is true. We proceed with a proof by cases.

For any person p, we could divide the rest of people into 2 groups: the group of p's friends and the group of strangers. By pigeonhole principle, one of the groups must have at least 3 people.

Case 1a: p is friends with at least 3 people, and these friends are all strangers. Then p's friends form a group of at least 3 strangers.

Case 1b: p is friends with at least 3 people, and at least 2 of them are friends with each other. These two, along with p, form a group of 3 friends.

Case 2a: p is strangers with at least 3 people, and these strangers are all friends. Analogous to Case 1a, these strangers form a group of at least 3 friends.

Case 2b: p is strangers with at least 3 people, and at least 2 of them are not friends. Analogous to Case 1b, these 2 strangers form a group of at least strangers.

7 Preserving Set Operations

For a function f, define the image of a set X to be the set $f(X) = \{y \mid y = f(x) \text{ for some } x \in X\}$. Define the inverse image or preimage of a set Y to be the set $f^{-1}(Y) = \{x \mid f(x) \in Y\}$. Prove the following statements, in which A and B are sets. By doing so, you will show that inverse images preserve set operations, but images typically do not.

Hint: For sets X and Y, $X = Y$ if and only if $X \subseteq Y$ and $Y \subseteq X$. To prove that $X \subseteq Y$, it is sufficient to show that $(\forall x)\ ((x \in X) \implies (x \in Y))$.

(a) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

(b) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.

(c) $f^{-1}(A \setminus B) = f^{-1}(A) \setminus f^{-1}(B)$.

(d) $f(A \cup B) = f(A) \cup f(B)$.

(e) $f(A \cap B) \subseteq f(A) \cap f(B)$, and give an example where equality does not hold.

(f) $f(A \setminus B) \supseteq f(A) \setminus f(B)$, and give an example where equality does not hold.

Solution:

In order to prove equality $A = B$, we need to prove that A is a subset of B, $A \subseteq B$ and that B is a subset of A, $B \subseteq A$. To prove that LHS is a subset of RHS we need to prove that if an element is a member of LHS then it is also an element of the RHS.

(a) Suppose x is such that $f(x) \in A \cup B$. Then either $f(x) \in A$, in which case $x \in f^{-1}(A)$, or $f(x) \in B$, in which case $x \in f^{-1}(B)$, so in either case we have $x \in f^{-1}(A) \cup f^{-1}(B)$. This proves that $f^{-1}(A \cup B) \subseteq f^{-1}(A) \cup f^{-1}(B)$.

Now, suppose that $x \in f^{-1}(A) \cup f^{-1}(B)$. Suppose, without loss of generality, that $x \in f^{-1}(A)$. Then $f(x) \in A$, so $f(x) \in A \cup B$, so $x \in f^{-1}(A \cup B)$. The argument for $x \in f^{-1}(B)$ is the same. Hence, $f^{-1}(A) \cup f^{-1}(B) \subseteq f^{-1}(A \cup B)$.

(b) Suppose x is such that $f(x) \in A \cap B$. Then $f(x)$ lies in both A and B, so x lies in both $f^{-1}(A)$ and $f^{-1}(B)$, so $x \in f^{-1}(A) \cap f^{-1}(B)$. So $f^{-1}(A \cap B) \subseteq f^{-1}(A) \cap f^{-1}(B)$.

Now, suppose that $x \in f^{-1}(A) \cap f^{-1}(B)$. Then, x is in both $f^{-1}(A)$ and $f^{-1}(B)$, so $f(x) \in A$ and $f(x) \in B$, so $f(x) \in A \cap B$, so $x \in f^{-1}(A \cap B)$. So $f^{-1}(A) \cap f^{-1}(B) \subseteq f^{-1}(A \cap B)$.

(c) Suppose x is such that $f(x) \in A \setminus B$. Then, $f(x) \in A$ and $f(x) \notin B$, which means that $x \in f^{-1}(A)$ and $x \notin f^{-1}(B)$, which means that $x \in f^{-1}(A) \setminus f^{-1}(B)$. So $f^{-1}(A \setminus B) \subseteq f^{-1}(A) \setminus f^{-1}(B)$.

Now, suppose that $x \in f^{-1}(A) \setminus f^{-1}(B)$. Then, $x \in f^{-1}(A)$ and $x \notin f^{-1}(B)$, so $f(x) \in A$ and $f(x) \notin B$, so $f(x) \in A \setminus B$, so $x \in f^{-1}(A \setminus B)$. So $f^{-1}(A) \setminus f^{-1}(B) \subseteq f^{-1}(A \setminus B)$.

(d) Suppose that $x \in A \cup B$. Then either $x \in A$, in which case $f(x) \in f(A)$, or $x \in B$, in which case $f(x) \in f(B)$. In either case, $f(x) \in f(A) \cup f(B)$, so $f(A \cup B) \subseteq f(A) \cup f(B)$.

Now, suppose that $y \in f(A) \cup f(B)$. Then either $y \in f(A)$ or $y \in f(B)$. In the first case, there is an element $x \in A$ with $f(x) = y$; in the second case, there is an element $x \in B$ with $f(x) = y$. In either case, there is an element $x \in A \cup B$ with $f(x) = y$, which means that $y \in f(A \cup B)$. So $f(A) \cup f(B) \subseteq f(A \cup B)$.

(e) Suppose $x \in A \cap B$. Then, x lies in both A and B, so $f(x)$ lies in both $f(A)$ and $f(B)$, so $f(x) \in f(A) \cap f(B)$. Hence, $f(A \cap B) \subseteq f(A) \cap f(B)$.

Consider when there are elements $a \in A$ and $b \in B$ with $f(a) = f(b)$, but A and B are disjoint. Here, $f(a) = f(b) \in f(A) \cap f(B)$, but $f(A \cap B)$ is empty (since $A \cap B$ is empty).

(f) Suppose $y \in f(A) \setminus f(B)$. Since y is not in $f(B)$, there are no elements in B which map to y. Let x be any element of A that maps to y; by the previous sentence, x cannot lie in B. Hence, $x \in A \setminus B$, so $y \in f(A \setminus B)$. Hence, $f(A) \setminus f(B) \subseteq f(A \setminus B)$.

Consider when $B = \{0\}$ and $A = \{0, 1\}$, with $f(0) = f(1) = 0$. One has $A \setminus B = \{1\}$, so $f(A \setminus B) = \{0\}$. However, $f(A) = f(B) = \{0\}$, so $f(A) \setminus f(B) = \varnothing$.

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 HW 2

1 Induction

Prove the following using induction:

(a) For all natural numbers $n > 2$, $2^n > 2n+1$.

(b) For all positive integers n, $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

(c) For all positive natural numbers n, $\frac{5}{4} \cdot 8^n + 3^{3n-1}$ is divisible by 19.

Solution:

(a) The inequality is true for $n = 3$ because $8 > 7$. Let the inequality be true for $n = k$, such that $2^k > 2k+1$. Then,

$$2^{k+1} = 2 \cdot 2^k > 2 \cdot (2k+1) = 4k+2$$

We know $2k > 1$ because k is a positive integer. Thus:

$$4k+2 = 2k+2k+2 > 2k+1+2 = 2k+3 = 2(k+1)+1$$

We've shown that $2^{k+1} > 2(k+1)+1$, which completes the inductive step.

(b) We can verify that the statement is true for $n = 1$. Assume the statement holds for $n = k$, so that

$$\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}.$$

Then we can write

$$\begin{aligned}
\sum_{i=1}^{k+1} i^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
&= (k+1)\left(\frac{k(2k+1)}{6} + (k+1)\right) \\
&= (k+1)\left(\frac{2k^2+k+6k+6}{6}\right) \\
&= (k+1)\left(\frac{2k^2+7k+6}{6}\right) \\
&= (k+1)\left(\frac{(2k+3)(k+2)}{6}\right) \\
&= \frac{(k+1)(2(k+1)+1)((k+1)+1)}{6},
\end{aligned}$$

as desired. Since we've shown that the statement holds for $n = k+1$, our proof is complete.

(c) For $n = 1$, the statement is "$10+9$ is divisible by 19", which is true. Assume that the statement holds for $n = k$, such that $\frac{5}{4} \cdot 8^k + 3^{3k-1}$ is divisible by 19. Then,

$$\begin{aligned}
\frac{5}{4} \cdot 8^{k+1} + 3^{3(k+1)-1} &= \frac{5}{4} \cdot 8 \cdot 8^k + 3^{3k+2} \\
&= 8 \cdot \frac{5}{4} \cdot 8^k + 3^3 \cdot 3^{3k-1} \\
&= 8 \cdot \frac{5}{4} \cdot 8^k + 8 \cdot 3^{3k-1} + 19 \cdot 3^{3k-1} \\
&= 8 \left(\frac{5}{4} \cdot 8^k + 3^{3k-1} \right) + 19 \cdot 3^{3k-1}
\end{aligned}$$

The first term is divisible by the inductive hypothesis, and the second term is clearly divisible by 19. This completes our proof, as we've shown the statement holds for $k+1$.

2 Negative pacman returns

Pacman has had a bit of a wild night, and wakes up feeling a bit under the weather. He starts at some location $(i, j) \in \mathbb{N}^2$ in the third quadrant, and is constrained walk on the infinite 2D grid and stay in the third quadrant (say, by walls along the negative x and negative y axes). Every second he does one of the following (if possible):

(i) Walk one step up, to $(i, j+1)$.

(ii) Walk one step right, to $(i+1, j)$.

For example, if he is at $(-5,0)$, his only option is to walk right to $(-4,0)$; if Pacman is instead at $(-3,-2)$, he could walk either to $(-2,-2)$ or $(-3,-1)$.

Prove by induction that no matter how he walks, he will always reach $(0,0)$ in finite time. (*Hint*: Try starting Pacman at a few small points like $(-2,-1)$ and looking all the different paths he could take to reach $(0,0)$. Do you notice a pattern?)

Solution:

Following the hint, we notice that it seems as though Pacman takes $i+j$ seconds to reach $(0,0)$ if he starts in position (i, j), regardless of what path he takes. This would imply that he reaches $(0,0)$ in a finite amount of time since $i+j$ is a finite number. Thus, if we can prove this stronger statement, we'll also have proved that Pacman reaches $(0,0)$ in finite time. In order to simplify the induction, we will induct on the quantity $i+j$ rather than inducting on i and j separately.

Base Case: If $i+j = 0$, we know that $i = j = 0$, since i and j must be non-negative. Hence, we have that Pacman is already at position $(0,0)$ and so will take $0 = i+j$ steps to get there.

Inductive Hypothesis: Suppose that if Pacman starts at position $(-i,-j)$ such that $i+j = n$, he will reach $(0,0)$ in n seconds regardless of his path.

Inductive Step: Now suppose Pacman starts at position $(-i,-j)$ such that $i+j=n+1$. If Pacman's first move is to position $(-i+1,-j)$, the sum of his x and y positions will be $-i+1-j=-(i+j)+1=n$. Thus, our inductive hypothesis tells us that it will take him n further seconds to get to $(0,0)$ no matter what path he takes. If Pacman's first move isn't to $(-i+1,+j)$, then it must be to $(i,j-1)$. Again in this case, the inductive hypothesis will tell us that Pacman will use n more moves to get to $(0,0)$ no matter what path he takes. Thus, in either case, we have that Pacman will take a total of $n+1$ seconds (one for the first move and n for the remainder) in order to reach $(0,0)$, proving the claim for $n+1$.

One can also prove this statement without strengthening the inductive hypothesis. The proof isn't quite as elegant, but is included here anyways for reference. We first prove by induction on i that if Pacman starts from position $(-i,0)$, he will reach $(0,0)$ in finite time.

Base Case: If $i=0$, Pacman starts at position $(0,0)$, so he doesn't need any more steps. Thus, it takes Pacman 0 steps to reach the origin, where 0 is a finite number.

Inductive Hypothesis: Suppose that if $i=n$ (that is, if Pacman starts at position $(-n,0)$), he will reach $(0,0)$ in finite time.

Inductive Step: Now say Pacman starts at position $(-n-1,0)$. Since he is on the x-axis, he has only one move: he has to move to $(-n,0)$. From the inductive hypothesis, we know he will only take finite time to get to $(0,0)$ once he's gotten to $(-n,0)$, so he'll only take a finite amount of time plus one second to get there from $(-n-1,0)$. A finite amount of time plus one second is still a finite amount of time, so we've proved the claim for $-i=-n-1$.

We can now use this statement as the base case to prove our original claim by induction on j.

Base Case: If $j=0$, Pacman starts at position $(i,0)$ for some $i\in\mathbb{N}$. We proved above that Pacman must reach $(0,0)$ in finite time starting from here.

Inductive Hypothesis: Suppose that if Pacman starts in position $(-i,-n)$, he'll reach $(0,0)$ in finite time no matter what i is.

Inductive Step: We now consider what happens if Pacman starts from position $(-i,-n-1)$, where i can be any natural number. If Pacman starts by moving up, we can immediately apply the inductive hypothesis, since Pacman will be in position (i,n). However, if Pacman moves to the right, he'll be in position $(-i+1,-n-1)$, so we can't yet apply the inductive hypothesis. But note that Pacman can't keep moving right forever: after i such moves, he'll hit the wall on the y-axis and be forced to move up. Thus, Pacman must make a vertical move after only finitely many horizontal moves–and once he makes that vertical move, he'll be in position $(-k,-n)$ for some $0\leq k\leq i$, so the inductive hypothesis tells us that it will only take him a finite amount of time to reach $(0,0)$ from there. This means that Pacman can only take a finite amount of time moving to the right, one second making his first move up, then a finite amount of additional time after his first vertical move. Since a finite number plus one plus another finite number is still finite, this gives us our desired claim: Pacman must reach $(0,0)$ in finite time if he starts from position $(-i,-n-1)$ for any $i\in\mathbb{N}$.

3 Losing Marbles

Two EECS70 GSIs have inexplicably run out of research topics to pursue, papers to read, or homeworks to create, and so they decide to play an incredibly boring game. (This is EECS after all.)

In the game, there is an urn that contains some number of red marbles (R), green marbles (G), and blue marbles (B). There is also an infinite supply of marbles outside the urn.

When it is a player's turn, the player may either:

(i) Remove one red marble from the urn, and add 3 green marbles.

(ii) Remove two green marbles from the urn, and add 7 blue marbles.

(iii) Remove one blue marble from the urn.

These are the only legal moves. The last player that can make a legal move wins. We play optimally, of course – meaning we always play one of the best possible legal moves.

(a) If the urn contains (R, G, B) red, green, and blue marbles initially, then determine the conditions on R, G, B for the first player to win the game. Prove it. In this case, does it matter what strategy the players use?

Hint: Assign each marble a weight, and argue that at every step, the combined weight will go down by exactly 1.

(b) Prove by induction that, if the urn initially contains a finite number of marbles at the start of the game, then the game will end after a finite number of moves.

Solution:

(a) We assign a weight to each marble such that after each step, the combined weight of all the marbles goes down by exactly 1.

We start with blue marbles and move (3), and so we assign each blue marble to have a weight of 1.

From move (2), we conclude that two green marbles must weigh $7+1$, and so each green marble must weight 4.

From move (1), we conclude that each red marble must weigh $3 \cdot 4 + 1 = 13$.

Therefore the combined weight of the marbles at the very start is $13R + 4G + B$. By construction, this weight will decrease by 1 every step (except when the weight is 0, in which case game over), so whenever $13R + 4G + B$ is odd, the first player will win.

(b) Let Φ_n be the combined weight after taking n moves. We will prove using induction, n moves, the combined weight Φ_n will be $13R + 4G + B - n$.

Proof. Proof by induction over n, the number of legal moves made.

Base case: Let $n = 0$, then $\Phi_0 = 13R + 4G + B - 0$, trivially.

Inductive hypothesis: Assume that for some $k \in \mathbb{N}, \Phi_k = \Phi_0 - k$.

Inductive step: Now consider the $k+1$-th turn. We know that any move will decrease the value of Φ_k by exactly 1, so we conclude that: $\Phi_{k+1} = \Phi_k - 1$. Subbing in our inductive hypothesis, we get $\Phi_{k+1} = (\Phi_0 - k) - 1 = \Phi_0 - (k+1)$, as desired. The claim follows by induction. □

Since R, G, B are all finite, then $13R + 4G + B$ is also finite, and we know from induction that the weight achieves 0 after $13R + 4G + B$ moves. We also know that since R, G, B are all natural numbers, the weight must be non-negative, and equals to 0 if and only if there are no more marbles.

Hence, after a finite number of moves, the game will end.

4 Nothing Can Be Better Than Something

In the stable matching problem, suppose that some jobs and candidates have hard requirements and might not be able to just settle for anything. In other words, in addition to the preference orderings they have, they prefer being unmatched to being matched with some of the lower-ranked entities (in their own preference list). We will use the term entity to refer to a candidate/job. A matching could ultimately have to be partial, i.e., some entities would and should remain unmatched.

Consequently, the notion of stability here should be adjusted a little bit to capture the autonomy of both jobs to unilaterally fire employees and employees to just walk away. A matching is stable if

- there is no matched entity who prefers being unmatched over being with their current partner;
- there is no matched/filled job and unmatched candidate that would both prefer to be matched with each other over their current status;
- similarly, there is no unmatched job and matched candidate that would both prefer to be matched with each other over their current status;
- there is no matched job and matched candidate that would both prefer to be matched with each other over their current partners; and
- there is no unmatched job and unmatched candidate that would both prefer to be with each other over being unmatched.

(a) Prove that a stable pairing still exists in the case where we allow unmatched entities.

(HINT: You can approach this by introducing imaginary/virtual entities that jobs/candidates "match" if they are unmatched. How should you adjust the preference lists of jobs/candidates, including those of the newly introduced imaginary ones for this to work?)

(b) As you saw in the lecture, we may have different stable matchings. But interestingly, if an entity remains unmatched in one stable matching, it/she must remain unmatched in any other stable matching as well. Prove this fact by contradiction.

Solution:

(a) Following the hint, we introduce an imaginary mate (let's call it a robot) for each entity. Note that we introduce one robot for each entity, i.e. there are as many robots as there are candidates+jobs. For simplicity let us say each robot is owned by the entity we introduce it for.

Each robot prefers its owner, i.e. it puts its owner at the top of its preference list. The rest of its preference list can be arbitrary. The owner of a robot puts it in their preference list exactly after the last entity they are willing to match with. i.e. owners like their robots more than entities they are not willing to match, but less than entities they like to match. The ordering of entities who someone does not like to match as well as robots they do not own is irrelevant as long as they all come after their robot.

To illustrate, consider this simple example: there are three jobs $1,2,3$ and three candidates A,B,C. The preference lists for jobs is given below:

Job	Preference List
1	$A > B$
2	$B > A > C$
3	C

The following depicts the preference lists for candidates:

Candidate	Preference List
A	1
B	$3 > 2 > 1$
C	$2 > 3 > 1$

In this example, 1 is willing to match A and B and it likes A better than B, but it'd rather be single than to be with C. On the other side B has a low standard and does not like being single at all. She likes 3 first, then 2, then 1 and if there is no option left she is willing to be forced into singleness. On the other hand, A has pretty high standards. She either matches 1 or remains single.

According to our explanation we should introduce a robot for each entity. Let's name the robot owned by entity X as R_X. So we introduce job robots R_A, R_B, R_C and candidate robots R_1, R_2, R_3. Now we should modify the existing preference lists and also introduce the preference lists for robots.

According to our method, 1's preference list should begin with its original preference list, i.e. $A > B$. Then comes the robot owned by 1, i.e. R_1. The rest of the ordering, which should include C and R_2, R_3 does not matter, and can be arbitrary.

For B, the preference list should begin with $3 > 2 > 1$ and continue with R_B, but the ordering between the remaining robots (R_A and R_C) does not matter.

What about robots' preference lists? They should begin with their owners and the rest does not matter. So for example R_A's list should begin with A, but the rest of the entities/robots (B, C, R_1, R_2, and R_3) can come in any arbitrary order.

So the following is a list of preference lists that adhere to our method. There are arbitrary choices which are shown in bold (everything in bold can be reordered within the bold elements).

Job	Preference List
1	$A > B > R_1 > \mathbf{3} > \mathbf{R_3} > \mathbf{R_2}$
2	$B > A > C > R_2 > \mathbf{R_1} > \mathbf{R_3}$
3	$C > R_3 > \mathbf{R_1} > \mathbf{R_3} > \mathbf{A} > \mathbf{B}$
R_A	$A > \mathbf{B} > \mathbf{C} > \mathbf{R_1} > \mathbf{R_2} > \mathbf{R_3}$
R_B	$B > \mathbf{R_1} > \mathbf{R_2} > \mathbf{R_3} > \mathbf{A} > \mathbf{C}$
R_C	$C > \mathbf{A} > \mathbf{R_2} > \mathbf{B} > \mathbf{R_1} > \mathbf{R_3}$

and the following depicts the preference lists for candidates and job robots:

Candidate	Preference List
A	$1 > R_A > \mathbf{3} > \mathbf{R_B} > \mathbf{2} > \mathbf{R_C}$
B	$3 > 2 > 1 > R_B > \mathbf{R_C} > \mathbf{R_A}$
C	$2 > 3 > 1 > R_C > \mathbf{R_A} > \mathbf{R_B}$
R_1	$1 > \mathbf{R_B} > \mathbf{2} > \mathbf{R_C} > \mathbf{3} > \mathbf{R_A}$
R_2	$2 > \mathbf{R_A} > \mathbf{R_C} > \mathbf{1} > \mathbf{3} > \mathbf{R_B}$
R_3	$3 > \mathbf{2} > \mathbf{1} > \mathbf{R_A} > \mathbf{R_C} > \mathbf{R_B}$

Now let us prove that a stable pairing between robots and owners actually corresponds to a stable pairing (with singleness as an option). This will finish the proof, since we know that in the robots and owners case, the propose and reject algorithm will give us a stable matching.

It is obvious that to extract a pairing without robots, we should simply remove all pairs in which there is at least one robot (two robots can match each other, yes). Then each entity which is not matched is declared to be single. It remains to check that this is a stable matching (in the new, modified sense). Before we do that, notice that an entity will never be matched with another entity's robot, because if that were so it and its robot would form a rogue couple (the robot prefers its owner, and the owner actually prefers their robot more than other robots).

(a) No one who is paired would rather break out of their pairing and be single. This is because if that were so, that entity along with its robot would have formed a rogue couple in the original pairing. Remember, the robot prefers its owner more than anything, so if the owner likes it more than their mate too, they would be a rogue couple.

(b) There is no rogue couple. If a rogue couple j and c existed, they would also be a rogue couple in the pairing which includes robots. If neither j nor c is single, this is fairly obvious. If one or both of them are single, they prefer the other entity over being single, which in the robots scenario means they prefer being with each other over being with their robot(s) which is their actual match.

This shows that each stable pairing in the robots and entities setup gives us a stable pairing in the entities-only setup. It is noteworthy that the reverse direction also works. If there is a stable pairing in the entities-only setup, one can extend it to a pairing for robots and entities setup by first creating pairs of owners who are single and their robots, and then finding an arbitrary stable matching between the unmatched robots (i.e. we exclude everything other than the unmatched robots and find a stable pairing between them). To show why this works, we have to refute the possibility of a rogue pair. There are three cases:

(a) A entity-entity rogue pair. This would also be rogue pair in the entities-only setup. The entities prefer each other over their current matches. If their matches are robots, that translates to them preferring each other over being single in the entities-only setup.

(b) A entity-robot rogue pair. If the entity is matched to their robot, our pair won't be a rogue pair since a entity likes their robot more than any other robot. On the other hand if the entity is matched to another entity, they prefer being with that entity over being single which places that entity higher than any robot. Again this refutes the entity-robot pair being rogue.

(c) A robot-robot rogue pair. If both robots are matched to other robots, then by our construction, this won't be a rogue couple (we explicitly selected a stable matching between left-alone robots). On the other hand, if either robot is matched to a entity, that entity is its owner, and obviously a robot prefers its owner more than anything, including other robots. So again this cannot be a rogue pair.

This completes the proof.

(b) We will perform proof by contradiction. Assume that there exists some job j_1 who is paired with a candidate c_1 in stable pairing S and unpaired in stable pairing T. Note that this means j_1 and c_1 both prefer to be with each other over being single. Since T is a stable pairing and j_1 is unpaired, c_1 must be paired in T with a job j_2 whom she prefers over j_1. (If c_1 were unpaired or paired with a job she does not prefer over j_1, then (j_1, c_1) would be a rogue couple in T, which is a contradiction.)

Since j_2 is paired with c_1 in T, it must be paired in S with some candidate c_2 whom j_2 prefers over c_1. This process continues (c_2 must be paired with some j_3 in T, j_3 must be paired with some c_3 in S, etc.) until all entitys are paired. Indeed, the last candidate c_n needs a partner in T and cannot be single (for the same reasons that c_1, c_2, and all the candidates before her need partners in T who they like better than their partners in S, to maintain stability). At this point, j_1 will be the only unpaired job, but to maintain the stability of T, we require j_1 to be paired in T with c_n. Yet we assumed j_1 was single, so we have reached a contradiction. Therefore,

our assumption must be false, and there cannot exist some job who is paired in a stable pairing S and unpaired in a stable pairing T. A similar argument can be used for candidates.

Since no job or candidate can be paired in one stable pairing and unpaired in another, every job or candidate must be either paired in all stable pairings or unpaired in all stable pairings.

Here is another possible proof:

We know that some job-optimal stable pairing exists. Call this pairing M. We first establish two lemmas.

Lemma 1. If a job is single in job-optimal pairing M, then it is single in all other stable pairings.

Proof. Assume there exists a job that is single in M but not single in some other stable pairing M'. Then M would not be a job-optimal pairing, so this is a contradiction.

Lemma 2. If a candidate is paired in job-optimal pairing M, she is paired in all other stable pairings.

Proof. Assume there exists a candidate that is paired in M but single in some other stable pairing M'. Then M would not be candidate-pessimal, so this is a contradiction.

Let there be k single jobs in M. Let M' be some other stable pairing. Then by Lemma 1, we know single jobs in M' will be greater than or equal to k. We also know that there are $n-k$ paired jobs and candidates in M. Then by Lemma 2, we know that the number of paired candidates in M' will be greater than or equal to $n-k$.

Now, we want to prove that if a job is paired in M, then it is paired in every other stable pairing. We prove this by contradiction. Assume that there exists a job m that is paired in M but is single in some other stable pairing M'. Then there must be strictly greater than k single jobs in M', and thus strictly greater than k single candidates in M'. Since there are strictly greater than k single candidates in M', there must be strictly less than $n-k$ paired candidates in M'. But this contradicts that the number of paired candidates in M' will be greater than or equal to $n-k$.

We also have to prove that if a candidate is single in M, then she must be single every other stable pairing. We again prove this by contradiction. Assume that there exists a candidate w that is single in M and paired in some other stable pairing M'. Then there are strictly greater than $n-k$ paired candidates in M', which means there are strictly greater than $n-k$ paired jobs in M'. This means there must be strictly less than k single jobs in M'. But this contradicts that the number of single jobs in M' will be greater than or equal to k.

Since we have proved both 1) If a job is single in M then it is single in every other stable pairing and 2) If a job is paired in M then it is paired in every other stable pairing (note that the contrapositive of this is if a job is single in any other stable pairing, then this job is single in M), we know that a job is single in M if and only if it is single in every other stable pairing.

Similarly, since we have proved both 1) If a candidate is single in M then she is single in every other stable pairing and 2) If a candidate is paired in M then she is paired in every other stable pairing, we know that a candidate is single in M if and only if she is single in every stable pairing. Thus we have proved that if a entity is single in one stable pairing, it is single in every stable pairing.

5 The Ranking List

Let's study the stable matching problem a little bit quantitavely. Here we define the following notation: on day j, let $P_j(M)$ be the rank of the job that applicant M proposes to (where the first application on her list has rank 1 and the last has rank n). Also, let $R_j(W)$ be the total number of applicants that job W has rejected up through day $j-1$ (i.e. not including the proposals on day j). Answer the following questions using the notation above.

(a) Prove or disprove the following claim: $\sum_M P_j(M) - \sum_W R_j(W)$ is independent of j. If it is true, also give the value of $\sum_M P_j(M) - \sum_W R_j(W)$. The notation, $\sum_M$ and $\sum_W$, simply means that we are summing over all applicants and all jobs.

(b) Prove or disprove the following claim: one of the **applicants or jobs** must be matched to something that is ranked in the top half of their preference list. You may assume that n is even.

Solution:

(a) **True.** On day $j = 1$, each applicant proposes to the first job on her list so $\sum_M P_1(M) = n$, and no job rejected any applicant through day 0, and therefore $\sum_W R_1(W) = 0$. Hence, $\sum_M P_1(M) - \sum_W R_1(W) = n$. In general, each time a job rejects an applicant on day $j-1$, $\sum_W R_j(W)$ increases by exactly 1. Similarly $\sum_M P_j(M)$ increases by exactly 1, since the rejected applicant proposes to the next job on her list on day j. Therefore $\sum_M P_j(M) - \sum_W R_j(W)$ stays constant and is independent of j. □

More formally, we can prove this by induction on j, with $j = 1$ as base case.
Induction Hypothesis: Assume $\sum_M P_j(M) - \sum_W R_j(W) = n$.
Induction Step: The quantity $\sum_W R_{j+1}(W) - \sum_W R_j(W)$ is exactly the number of men rejected by women on day j. But each of the rejected applicants proposes to the next job on their list on day $j+1$, and so this quantity is also equal to $\sum_M P_{j+1}(M) - \sum_M P_j(M)$. Equating the two, we get

$$\sum_W R_{j+1}(W) - \sum_W R_j(W) = \sum_M P_{j+1}(M) - \sum_M P_j(M).$$

Therefore,

$$\sum_M P_{j+1}(M) - \sum_W R_{j+1}(W) = \sum_M P_j(M) - \sum_W R_j(W)$$

and the right hand side is equal to n by the induction hypothesis. □

(b) **True.** Assume that no applicant is matched with a job in the top half of her preference list. Then each applicant must have been rejected at least $n/2$ times, for a total of at least $n^2/2$ rejections. This implies that at least one job must have rejected at least $n/2$ applicants (because if not, then the total number of rejections must be less than $(n/2) \cdot n$, contradiction). But now, by the improvement lemma, this job must be matched with an applicant she likes more than the $n/2$ men she rejected, meaning that the applicant she is matched with is in the top half of her preference list. □

Alternative Proof:

Assume towards contradiction that every applicant and every job is matched to someone who is ranked in the bottom half of their preference list.

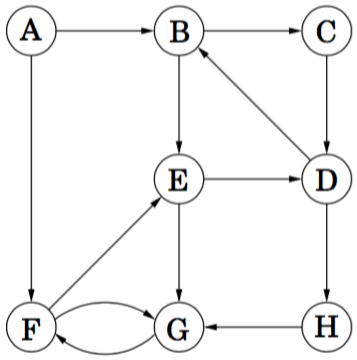
Observe that an applicant M is matched to someone in the top half of her preference list if and only if $P_m(M) \leq n/2$, where m is the last day of the algorithm. Therefore, if M is matched to someone in the bottom half of her preference list, then $P_m(M) > n/2$, i.e., $P_m(M) \geq n/2 + 1$. Summing over the men gives us $\sum_M P_m(M) \geq n^2/2 + n$. By part (a), it follows that $\sum_W R_m(W) = \sum_M P_m(M) - n \geq n^2/2$.

Observe also that if $R_m(W) \geq n/2$, then by the improvement lemma, W must be matched to a job in the top half of her preference list. Therefore, from our assumption that W is matched to someone in the bottom half of her preference list, we get $R_m(W) < n/2$. Summing over the women gives us $\sum_W R_m(W) < n^2/2$. But this contradicts our earlier result above! □

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 HW 3

1 Graph Basics

In the first few parts, you will be answering questions on the following graph G.



(a) What are the vertex and edge sets V and E for graph G?

(b) Which vertex has the highest in-degree? Which vertex has the lowest in-degree? Which vertices have the same in-degree and out-degree?

(c) What are the paths from vertex B to F, assuming no vertex is visited twice? Which one is the shortest path?

(d) Which of the following are cycles in G?

i. $(B,C),(C,D),(D,B)$
ii. $(F,G),(G,F)$
iii. $(A,B),(B,C),(C,D),(D,B)$
iv. $(B,C),(C,D),(D,H),(H,G),(G,F),(F,E),(E,D),(D,B)$

(e) Which of the following are walks in G?

i. (E,G)
ii. $(E,G),(G,F)$
iii. $(F,G),(G,F)$
iv. $(A,B),(B,C),(C,D),(H,G)$
v. $(E,G),(G,F),(F,G),(G,C)$
vi. $(E,D),(D,B),(B,E),(E,D),(D,H),(H,G),(G,F)$

(f) Which of the following are tours in G?

i. (E,G)

ii. $(E,G),(G,F)$

iii. $(F,G),(G,F)$

iv. $(E,D),(D,B),(B,E),(E,D),(D,H),(H,G),(G,F)$

In the following three parts, let's consider a general undirected graph G with n vertices ($n \geq 3$).

(g) True/False: If each vertex of G has degree at most 1, then G does not have a cycle.

(h) True/False: If each vertex of G has degree at least 2, then G has a cycle.

(i) True/False: If each vertex of G has degree at most 2, then G is not connected.

Solution:

(a) A graph is specified as an ordered pair $G = (V,E)$, where V is the vertex set and E is the edge set.

$$V = \{A,B,C,D,E,F,G,H\},$$
$$E = \{(A,B),(A,F),(B,C),(B,E),(C,D),(D,B),(D,H),(E,D),(E,G),(F,E),(F,G),(G,F),(H,G)\}.$$

(b) G has the highest in-degree (3). A has the lowest in-degree (0).

$\{B,C,D,E,F,H\}$ all have the same in-degree and out-degree. H and C has in-degree (out-degree) equal to 1 and the other four have in-degree (out-degree) equal to 2.

(c) There are three paths:
$(B,C),(C,D),(D,H),(H,G),(G,F)$
$(B,E),(E,D),(D,H),(H,G),(G,F)$
$(B,E),(E,G),(G,F)$
The first two have length 5, while the last one has length 3, so the last one is the shortest path.

(d) A cycle is a path that starts and ends at the same point. This means that (iii) is not a cycle, since it starts at A but ends at B. In addition, all the vertices $\{v_1,\ldots,v_n\}$ in the cycle $(v_1,v_2),(v_2,v_3),\ldots,(v_{n-1},v_n)$ should be distinct, so (iv) is not a cycle. The correct answers are (i) and (ii).

(e) A walk consists of any sequence of edges such that the endpoint of each edge is the same as the starting vertex of the next edge in the sequence. Example (iv) does not fit this definition–even though it uses only valid edges, the endpoint of the second to last edge in D, while the start point of the next edge is H. Example (v) also is not a walk, since it tries to walk from G to C as its last step, but there is no such edge. All the rest are walks.

(f) A tour is simply a walk that has the same start and end vertex. Only (iii) satisfies this definition. Note in part (d), we already said that (iii) was a cycle–and indeed, all cycles are also tours.

(g) True. In order for there to be a cycle in G starting and ending at some vertex v, we would need at least two edges incident to v: one to leave v at the start of the cycle, and one to return to v at the end. If every vertex has degree at most 1, no vertex has two or more edges incident on it, so no vertex is capable of acting as the start and end point of a cycle.

(h) True. Consider starting a walk at some vertex v_0, and at each step, walking along a previously untraversed edge, stopping when we first visit some vertex w for the second time. If this process terminates, the part of our walk from the first time we visited w until the second time is a cycle. Thus, it remains only to argue this process always terminates.

Each time we take a step from some vertex v, since we are not stopping, we must have visited that vertex exactly once and not yet left. It follows that we have used at most one edge incident with v (either we started at v, or we took an edge into v). Since v has degree at least 2, there must be another edge leaving v for us to take.

(i) False. For example, a 3-cycle (triangle) is connected and every vertex has degree 2.

2 Binary Trees

You have seen the recursive definition of binary trees from lecture and from previous classes. Here, we define binary trees in graph theoretic terms as follows (**Note:** here we will modify the definition of leaves slightly for consistency).

- A binary tree of height > 0 is a tree where exactly one vertex, called the **root**, has degree 2, and all other vertices have degrees 1 or 3. Each vertex of degree 1 is called a **leaf**. The **height** h is defined as the maximum length of the path between the root and any leaf.
- A binary tree of height 0 is the graph with a single vertex. The vertex is both a leaf and a root.

(a) Let T be a binary tree of height > 0, and let $h(T)$ denote it's height. Let r be the root in T and u and v be it's neighbors. Show that removing r from T will result in two binary trees, L, R with roots u and v respectively. Also, show that $h(T) = \max(h(L), h(R)) + 1$

(b) Using the graph theoretic definition of binary trees, prove that the number of vertices in a binary tree of height h is at most $2^{h+1} - 1$

(c) Prove that all binary trees with n leaves have $2n - 1$ vertices

Solution:

(a) Since r has degree 2, removing it will break T into two connected components, call them L and R. By symmetry, we just need to prove that L is a binary tree. Without loss of generality, suppose $u \in L$. Before removing r, u had degree 1 or 3. If u had degree 1, then after removing r, u is a single vertex, and so is a binary tree of height 0, and also is a root. If u had degree 3, then after removing r, u has degree 2, and all other vertices in L have degree 1 or 3. Thus, L is a binary tree with root u.

To prove that $h(T) = \max(h(L), h(R)) + 1$, we note that because T is a tree, any path from r to a leaf must go through either u or v but not both. Thus the maximum distance from r to any leaf is one plus either the maximum distance from u to any leaf in L (as the path cannot go back through r) or the maximum distance from v to any leaf in R. Formally, if we define $\mathscr{L}(L)$ and $\mathscr{L}(R)$ to be the set of leaves in L and R respectively, and $d(r,l)$ as the length of the path from r to some leaf l, then we have

$$\begin{aligned} h(T) &= \max(1 + \max_{l \in \mathscr{L}(L)} (d(u,l)), 1 + \max_{l \in \mathscr{L}(R)} (d(u,l))) \\ &= 1 + \max(h(L), h(R)) \end{aligned}$$

(b) Induction: **Base Case** a binary tree of height 0 is a singleton and so has $2^1 - 1 = 1$ vertex. **Inductive Hypothesis:** assume for all $k < h$, a binary tree of height k has at most $2^{k+1} - 1$ vertices. **Inductive Step:** By part a, we can remove the root from a binary tree and obtain two binary trees: L, and R of height k and l respectively. Since $h(T) = \max(h(L), h(R)) + 1$, we know that $k, l < h$ so we can apply the inductive hypothesis to L and R. Thus, we have that the number of vertices in T is at most $1 + 2^{k+1} - 1 + 2^{l+1} - 1 \leq 2^h * 2 - 1$.

(c) Induction: **Base Case** if a binary tree has one leaf, it is a singleton and so has $1 = 2 * 1 - 1$ vertices. **Inductive Hypothesis:** assume for all $k < n$, a binary tree with k leaves has $2k - 1$ vertices. **Inductive Step:** For a binary tree, T, with $n > 1$ leaves, remove the root, r and break T into binary trees L and R. Suppose L has a leaves and R has b leaves. Note that all the leaves of T are in L or R, as $n > 1$ implies the root is not a leaf, which means $a + b = n$. By the inductive hypothesis, L has $2a - 1$ vertices, and R has $2b - 1$ vertices, and so the number of vertices in T is $2a - 1 + 2b - 1 + 1 = 2(a + b) - 1 = 2n - 1$.

3 Proofs in Graphs

Please prove or disprove the following claims.

(a) On the axis from San Francisco traffic habits to Los Angeles traffic habits, Old California is more towards San Francisco: that is, civilized. In Old California, all roads were one way streets. Suppose Old California had n cities ($n \geq 2$) such that for every pair of cities X and Y, either X had a road to Y or Y had a road to X. Prove or disprove that there existed a city which was reachable from every other city by traveling through at most 2 roads.

[*Hint:* Induction]

(b) In lecture, we have shown that a connected undirected graph has an Eulerian tour if and only if every vertex has even degree.

Consider a connected graph G with n vertices which has exactly $2m$ vertices of odd degree, where $m > 0$. Prove or disprove that there are m walks that *together* cover all the edges of G (i.e., each edge of G occurs in exactly one of the m walks, and each of the walks should not contain any particular edge more than once).

Solution:

(a) We prove this by induction on the number of cities n.

Base case For $n = 2$, there's always a road from one city to the other.

Inductive Hypothesis When there are k cities, there exists a city c that is reachable from every other city by traveling through at most 2 roads.

Inductive Step Consider the case where there are $k+1$ cities. Remove one of the cities d and all of the roads to and from d. Now there are k cities, and by our inductive hypothesis, there exists some city c which is reachable from every other city by traveling through at most 2 roads. Let A be the set of cities with a road to c, and B be the set of cities two roads away from c. The inductive hypothesis states that the set S of the k cities consists of $S = \{c\} \cup A \cup B$.

Now add back d and all roads to and from d. Between d and every city in S, there must be a road from one to the other. If there is at least one road from d to $\{c\} \cup A$, c would still be reachable from d with at most 2 road traversals. Otherwise, if all roads from $\{c\} \cup A$ point to d, d will be reachable from every city in B with at most 2 road traversals, because every city in B can take one road to go to a city in A, then take one more road to go to d. In either case there exists a city in the new set of $k+1$ cities that is reachable from every other city by traveling at most 2 roads.

(b) We split the $2m$ odd-degree vertices into m pairs, and join each pair with an edge, adding m more edges in total. (Here, we allow for the possibility of multi-edges, that is, pairs of vertices with more than one edge between them.) Notice that now all vertices in this graph are of even degree. Now by Euler's theorem the resulting graph has an Eulerian tour. Removing the m added edges breaks the tour into m walks covering all the edges in the original graph, with each edge belonging to exactly one walk.

4 Planarity

(a) Prove that $K_{3,3}$ is nonplanar.

(b) Consider graphs with the property T: For every three distinct vertices v_1, v_2, v_3 of graph G, there are at least two edges among them. Use a proof by contradiction to show that if G is a graph on ≥ 7 vertices, and G has property T, then G is nonplanar.

Solution:

(a) Assume toward contradiction that $K_{3,3}$ were planar. In $K_{3,3}$, there are $v = 6$ vertices and $e = 9$ edges. If $K_{3,3}$ were planar, from Euler's formula we would have $v - e + f = 2 \Rightarrow f = 5$. On the other hand, each region is bounded by at least four edges, so $4f \leq 2e$, i.e., $20 \leq 18$, which is a contradiction. Thus, $K_{3,3}$ is not planar.

(b) In this problem, we use proof by contradiction. Assume G is planar. Select any five vertices out of the seven. Consider the subgraph formed by these five vertices. They cannot form K_5, since G is planar. So some pair of vertices amongst these five has no edge between them. Label these vertices v_1 and v_2. The remaining five vertices of G besides v_1 and v_2 cannot form K_5 either, so there is a second pair of vertices amongst these new five that has no edge between them. Label these v_3 and v_4. Label the remaining three vertices v_5, v_6 nd v_7. Since v_1v_2 is not an edge, by property T (which states any three vertices must have at least two edges between them)it must be that $\{v_1, v\}$ and $\{v_2, v\}$ are edges, where $v \in \{v_3, v_4, v_5, v_6, v_7\}$. Similarly for v_3, v_4 we have that $\{v_3, v\}$ and $\{v_4, v\}$ are edges, where $v \in \{v_1, v_2, v_5, v_6, v_7\}$. Now consider the subgraph induced by $\{v_1, v_2, v_3, v_5, v_6, v_7\}$. With the three vertices $\{v_1, v_2, v_3\}$ on one side and $\{v_5, v_6, v_7\}$ on the other, we observe that $K_{3,3}$ is a subgraph of this induced graph. This contradicts the fact that G is planar.

The above shows that any graph with 7 vertices and property T is non-planar. Any graph with greater than 7 vertices and property T will also be non-planar because it will contain a subgraph with 7 vertices and property T.

5 Always, Sometimes, or Never

In each part below, you are given some information about the so-called original graph, OG. Using only the information in the current part, say whether OG will always be planar, always be non-planar, or could be either. If you think it is always planar or always non-planar, prove it. If you think it could be either, give a planar example and a non-planar example.

(a) OG can be vertex-colored with 4 colors.

(b) OG requires 7 colors to be vertex-colored.

(c) $e \leq 3v - 6$, where e is the number of edges of OG and v is the number of vertices of OG.

(d) OG is connected, and each vertex in OG has degree at most 2.

(e) Each vertex in OG has degree at most 2.

Solution:

(a) Either planar or non-planar. By the 4-color theorem, any planar graph can provide the planar example. The easiest non-planar example is $K_{3,3}$, which can be 2-colored because it is bipartite.

(Certainly, any graph which can be colored using only 2 colors can also be colored using 4 colors.)

(b) Always non-planar. The 4-color theorem tells us that if a graph is planar, it can be colored using only 4 colors. The contrapositive of this is that if a graph requires more than 4 colors to vertex-color, it must be non-planar. (Using the 5- or 6-color theorem would also work.)

(c) Either planar or non-planar. From the notes, we know that every planar graph follows this formula, so any planar graph is a valid planar example. The easiest non-planar example is again $K_{3,3}$, which has $e = 9$ and $v = 6$, meaning our formula becomes $9 \leq 3(6) - 6 = 12$, which is certainly true.

(d) Always planar. There are two cases to deal with here: either G is a tree, or G is not a tree and so contains at least one cycle. In the former case, we're immediately done, since all trees are planar. In the latter case, consider any cycle in G. We know that every vertex in that cycle is adjacent to the vertex to its left in the cycle and to the vertex to its right in the cycle. But we also know that no vertex can be connected to more than two other vertices, so the cycle isn't connected to anything else. But G is a connected graph, so we must have that G is just a single large cycle. And we can certainly draw a simple cycle on a plane without crossing any edges, so even in this case G is still planar.

(e) Always planar. Each of G's connected components is connected and has no vertex of degree more than 2, so by the previous part, each of them must be planar. Thus, each of G's connected components must be planar, so G itself must be planar.

6 Touring Hypercube

In the lecture, you have seen that if G is a hypercube of dimension n, then

- The vertices of G are the binary strings of length n.
- u and v are connected by an edge if they differ in exactly one bit location.

A *Hamiltonian tour* of a graph is a sequence of vertices $v_0, v_1, \ldots, v_k$ such that:

- Each vertex appears exactly once in the sequence.
- Each pair of consecutive vertices is connected by an edge.
- v_0 and v_k are connected by an edge.

(a) Show that a hypercube has an Eulerian tour if and only if n is even. (*Hint: Euler's theorem*)

(b) Show that every hypercube has a Hamiltonian tour.

Solution:

(a) In the n-dimensional hypercube, every vertex has degree n. If n is odd, then by Euler's Theorem there can be no Eulerian tour. On the other hand, the hypercube is connected: we can get from any one bit-string x to any other y by flipping the bits they differ in one at a time. Therefore, when n is even, since every vertex has even degree and the graph is connected, there is an Eulerian tour.

(b) By induction on n. When $n = 1$, there are two vertices connected by an edge; we can form a Hamiltonian tour by walking from one to the other and then back.

Let $n \geq 1$ and suppose the n-dimensional hypercube has a Hamiltonian tour. Let H be the $n+1$-dimensional hypercube, and let H_b be the n-dimensional subcube consisting of those strings with initial bit b.

By the inductive hypothesis, there is some Hamiltonian tour T on the n-dimensional hypercube. Now consider the following tour in H. Start at an arbitrary vertex x_0 in H_0, and follow the tour T except for the very last step to vertex y_0 (so that the next step would bring us back to x_0). Next take the edge from y_0 to y_1 to enter cube H_1. Next, follow the tour T in H_1 backwards from y_1, except the very last step, to arrive at x_1. Finally, take the step from x_1 to x_0 to complete the tour. By assumption, the tour T visits each vertex in each subcube exactly once, so our complete tour visits each vertex in the whole cube exactly once.

To build some intuition, here are the first few cases:

- $n = 1$: 0, 1
- $n = 2$: 00, 01, 11, 10 [Take the $n = 1$ tour in the 0-subcube (vertices with a 0 in front), move to the 1-subcube (vertices with 1 in front), then take the tour backwards. We know 10 connects to 00 to complete the tour.]
- $n = 3$: 000, 001, 011, 010, 110, 111, 101, 100 [Take the $n = 2$ tour in the 0-subcube, move to the 1-subcube, then take the tour backwards. We know 100 connects to 000 to complete the tour.]

The sequence produced with this method is known as a Gray code.

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 HW 4

1 Fibonacci GCD

The Fibonacci sequence is given by $F_n = F_{n-1} + F_{n-2}$, where $F_0 = 0$ and $F_1 = 1$. Prove that, for all $n \geq 0$, $\gcd(F_n, F_{n-1}) = 1$.

Solution:

Proceed by induction.

Base Case: We have $\gcd(F_1, F_0) = \gcd(1, 0) = 1$, which is true.

Inductive Hypothesis: Assume we have $\gcd(F_k, F_{k-1}) = 1$ for some $k \geq 1$.

Inductive Step: Now we need to show that $\gcd(F_{k+1}, F_k) = 1$ as well.

We can show that:

$$\gcd(F_{k+1}, F_k) = \gcd(F_k + F_{k-1}, F_k) = \gcd(F_k, F_{k-1}) = 1.$$

Note that the second expression comes from the definition of Fibonacci numbers. The last expression comes from Euclid's GCD algorithm, in which $\gcd(x, y) = \gcd(y, x \bmod y)$, since

$$F_k + F_{k-1} \equiv F_{k-1} \pmod{F_k}.$$

Therefore the statement is also true for $n = k + 1$.

By the rule of induction, we can conclude that $\gcd(F_n, F_{n-1}) = 1$ for all $n \geq 1$, where $F_0 = 0$ and $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$.

2 The Last Digit

In each case show your work and justify your answers.

(a) If $9k + 5$ and $2k + 1$ have the same last digit for some natural number k, find the last digit of k.

(b) If $S = \sum_{i=1}^{19} i!$, then find the last digit of S^2.

Solution:

(a) We have

$$\begin{aligned} 9k + 5 &\equiv 2k + 1 \pmod{10}, \\ 7k &\equiv -4 \pmod{10}, \\ 7k &\equiv 6 \pmod{10}. \end{aligned}$$

Now since gcd(7,10)=1, 7 has a (unique) inverse mod 10, and since $7 \times 3 = 21 \equiv 1 \pmod{10}$ the inverse is 3. We multiply both sides of $7k \equiv 6 \pmod{10}$ by 3:

$$k \equiv 18 \equiv 8 \pmod{10}.$$

Hence, the last digit of k is 8.

(b) Note that for $n \geq 5$:

$$n! = \left(\prod_{i=6}^{n} i\right) \times 5! = \left(\prod_{i=6}^{n} i\right) \times 120 \equiv 0 \pmod{10}.$$

So we have:

$$S = \sum_{i=1}^{19} i! = 1! + 2! + 3! + 4! + \sum_{i=5}^{19} i! = 1 + 2 + 6 + 24 + 0 \equiv 3 + 0 \pmod{10}.$$

Then, for S^2:

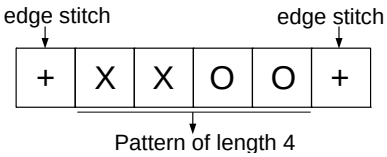
$$S^2 \equiv 9 \pmod{10}.$$

Hence, the last digit of S^2 is 9.

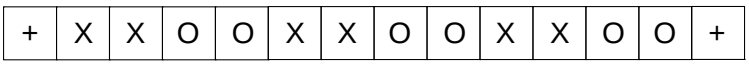
3 Celebrate and Remember Textiles

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:

- Alternating Link: Multiple of 7, plus 4
- Double Broken Rib: Multiple of 4, plus 2
- Swag: 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.**

Solution: Let x be the number of stitches we need to cast on. Using the Chinese Remainder Theorem, we can write the following system of congruences:

$$\begin{aligned} x &\equiv 4 \pmod 7 \\ x &\equiv 2 \pmod 4 \\ x &\equiv 2 \pmod 5. \end{aligned}$$

We have $M = 7 \cdot 4 \cdot 5 = 140$, $r_1 = 4$, $m_1 = 7$, $b_1 = M/m_1 = 4 \cdot 5 = 20$, $r_2 = 3$, $m_2 = 4$, $b_2 = M/m_2 = 7 \cdot 5 = 35$, and $r_3 = 2$, $m_3 = 5$, $b_3 = M/m_3 = 7 \cdot 4 = 28$. We need to solve for the multiplicative inverse of b_i modulo m_i for $i \in \{1,2,3\}$:

$$\begin{aligned} b_1 a_1 &\equiv 1 \pmod{m_1} \\ 20 a_1 &\equiv 1 \pmod 7 \\ 6 a_1 &\equiv 1 \pmod 7 \\ \rightarrow a_1 &= 6, \end{aligned}$$

$$\begin{aligned} b_2 a_2 &\equiv 1 \pmod{m_2} \\ 35 a_2 &\equiv 1 \pmod 4 \\ 3 a_2 &\equiv 1 \pmod 4 \\ \rightarrow a_2 &= 3, \end{aligned}$$

and

$$\begin{aligned} b_3 a_3 &\equiv 1 \pmod{m_3} \\ 28 a_3 &\equiv 1 \pmod 5 \\ 3 a_3 &\equiv 1 \pmod 5 \\ \rightarrow a_3 &= 2. \end{aligned}$$

Therefore,

$$\begin{aligned} x &\equiv 6 \cdot 20 \cdot 4 + 2 \cdot 35 \cdot 3 + 2 \cdot 28 \cdot 2 \pmod{140} \\ &\equiv 102 \pmod{140}, \end{aligned}$$

so the smallest x that satisfies all three congruences is 102. Therefore we should cast on 102 stitches in order to be able to knit all three patterns into the blanket.

4 Sparsity of Primes

A prime power is a number that can be written as p^i for some prime p and some positive integer i. So, $9 = 3^2$ is a prime power, and so is $8 = 2^3$. $42 = 2 \cdot 3 \cdot 7$ is not a prime power.

Prove that for any positive integer k, there exists k consecutive positive integers such that none of them are prime powers.

Hint: this is a Chinese Remainder Theorem problem

Solution:

We want to find x such that $x+1, x+2, x+3, \ldots x+k$ are all not powers of primes. We can enforce this by saying that $x+1$ through $x+k$ each must have two distinct prime divisors. So, select $2k$ primes, $p_1, p_2, \ldots, p_{2k}$, and enforce the constraints

$$\begin{aligned}
x+1 &\equiv 0 \pmod{p_1 p_2} \\
x+2 &\equiv 0 \pmod{p_3 p_4} \\
&\vdots \\
x+i &\equiv 0 \pmod{p_{2i-1} p_{2i}} \\
&\vdots \\
x+k &\equiv 0 \pmod{p_{2k-1} p_{2k}}
\end{aligned}$$

By Chinese Remainder Theorem, we can calculate the value of x so this x must exist, and thus, $x+1$ through $x+k$ are not prime powers.

What's even more interesting here is that we could select any $2k$ primes we want!

5 Fermat's Little Theorem

Fermat's Little Theorem states that for any prime p and any $a \in \{1, 2, \ldots, p-1\}$, we have $a^{p-1} \equiv 1 \pmod{p}$. Without using induction, prove that $\forall n \in \mathbb{N}$, $n^7 - n$ is divisible by 42.

Solution:

Let $n \in \mathbb{N}$. We begin by breaking down 42 into prime factors: $42 = 7 \times 3 \times 2$. Since 7, 3, and 2 are prime, we can apply Fermat's Little Theorem, which says that $a^p \equiv a \pmod{p}$, to get the congruences

$$n^7 \equiv n \pmod{7}, \tag{1}$$
$$n^3 \equiv n \pmod{3}, \quad \text{and} \tag{2}$$
$$n^2 \equiv n \pmod{2}. \tag{3}$$

Now, let's take (2) and multiply it by $n^3 \cdot n$. This gives us

$$n^7 \equiv n^3 \cdot n^3 \cdot n \equiv n \cdot n \cdot n \equiv n^3 \pmod 3,$$

and since by (2), $n^3 \equiv n \pmod 3$, this gives

$$n^7 \equiv n \pmod 3.$$

Similarly, we take (3) and multiply by $n^2 \cdot n^2 \cdot n$ to get

$$n^7 \equiv n^2 \cdot n^2 \cdot n^2 \cdot n \equiv n^4 \pmod 2.$$

Notice that $n^4 \equiv n^2 \cdot n^2 \equiv n \cdot n \equiv n^2 \pmod 2$, and by (3) $n^2 \equiv n \pmod 2$, so we have

$$n^7 \equiv n \pmod 2.$$

Thus,

$$n^7 \equiv n \pmod 7, \tag{4}$$
$$n^7 \equiv n \pmod 3, \quad \text{and} \tag{5}$$
$$n^7 \equiv n \pmod 2. \tag{6}$$

Let $x = n^7 - n$. By the Chinese Remainder Theorem, the system of congruences

$$x \equiv 0 \pmod 7$$
$$x \equiv 0 \pmod 3$$
$$x \equiv 0 \pmod 2$$

has a unique solution modulo $2 \cdot 3 \cdot 7 = 42$, and this unique solution is $x \equiv 0 \pmod{42}$. So, we have that $n^7 - n \equiv 0 \pmod{42}$, which means $n^7 - n$ is divisible by 42.

6 A Taste of RSA

Suppose that p and q are distinct odd primes (i.e. they are primes > 2). Define $N = pq$. Let a be any integer that is relatively prime to N. In other words, $\gcd(a, N) = 1$. Prove that $a^{(p-1)(q-1)+1} \equiv a \pmod N$. It turns out that this equivalence is in fact the basis of RSA, as you will see soon in class.

Solution:

Note: This problem is essentially asking you to prove the correctness of RSA.

We know that a is not a divsible by p and a is not divisible by q since $\gcd(a, pq) = 1$.We subtract a from both sides to get

$$a^{(p-1)(q-1)+1} - a \equiv 0 \pmod{pq}$$
$$a(a^{(p-1)(q-1)} - 1) \equiv 0 \pmod{pq}$$

Since p, q are primes, we just need to show that the left hand side is divisible by both p and q. Since a is not divisible by p, we can use Fermat's Little Theorem to state that $a^{p-1} \equiv 1 \pmod{p}$.

$$a\big((a^{(p-1)})^{q-1} - 1\big) \equiv a(1^{q-1} - 1) \equiv 0 \pmod{p}$$

Thus $a(a^{(p-1)(q-1)} - 1)$ is divisible by p. We can apply the same reasoning to show that the expression is divisible by q. Therefore we have proved our claim that $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$.

Alternative Proof:
Because $\gcd(a, pq) = 1$, we have that a does not divide p and a does not divide q. By Fermat's Little Theorem,

$$a^{(p-1)(q-1)+1} = (a^{(p-1)})^{(q-1)} \cdot a \equiv 1^{q-1} \cdot a \equiv a \pmod{p}.$$

Similarly, by Fermat's Little Theorem, we have

$$a^{(p-1)(q-1)+1} = (a^{(q-1)})^{(p-1)} \cdot a \equiv 1^{p-1} \cdot a \equiv a \pmod{q}.$$

Now, we want to use this information to conclude that $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$. We will first take a detour and show a more general result (you could write this out separately as a lemma if you want).

Consider the system of congruences

$$x \equiv a \pmod{p}$$
$$x \equiv a \pmod{q}.$$

Let's run the CRT symbolically. First off, since p and q are relatively prime, we know there exist integers g, h such that

$$g \cdot p + h \cdot q = 1.$$

We could find these via Euclid's algorithm. By the CRT, the solution to our system of congruences will be

$$x \equiv a \cdot y_1 \cdot q + a \cdot y_2 \cdot p \pmod{pq}.$$

To solve for y_1 and y_2, we must find y_1 such that

$$x_1 \cdot p + y_1 \cdot q = 1$$

and y_2 such that

$$x_2 \cdot q + y_2 \cdot p = 1.$$

This is easy since we already know $g \cdot p + h \cdot q = 1$: the answers are $y_1 = h$ and $y_2 = g$. Finally we can plug in to the solution to get

$$x \equiv a \cdot h \cdot q + a \cdot g \cdot p \equiv a(h \cdot q + g \cdot p) \equiv a \cdot 1 \equiv a \pmod{pq}.$$

Therefore by the CRT we know that the set of solutions that satisfy both $x \equiv a \pmod{p}$ and $x \equiv a \pmod{q}$ is exactly the set of solutions that satisfy $x \equiv a \pmod{pq}$.

So since $a^{(p-1)(q-1)+1} \equiv a \pmod{p}$ and $a^{(p-1)(q-1)+1} \equiv a \pmod{q}$, then by the CRT we know that $a^{(p-1)(q-1)+1}$ satisfies $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$.

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 HW 5

1 RSA with Just One Prime

Given the message $x \in \{0, 1, \ldots, N-1\}$ and $N = pq$, where p and q are prime numbers, conventional RSA encrypts x with $y = E(x) \equiv x^e \pmod{N}$. The decryption is done by $D(y) \equiv y^d \pmod{N}$, where d is the inverse of $e \pmod{(p-1)(q-1)}$.

Alice is trying to send a message to Bob, and as usual, Eve is trying to decipher what the message is. One day, Bob gets lazy and tells Alice that he will now use $N = p$, where p is a 1024-bit prime number, as part of his public key. He tells Alice that it's okay, since Eve will have to try out 2^{1024} combinations to guess x. It is very likely that Eve will not find out the secret message in a reasonable amount of time! In this problem, we will see whether Bob is right or wrong. Assume that Eve has found out about this new setup and that she knows the public key.

Similar to the original method, for any message $x \in \{0, 1, \ldots, N-1\}$, $E(x) \equiv x^e \pmod{p}$, and $D(y) \equiv y^d \pmod{p}$. Choose e such that it is coprime with $p-1$, and choose $d \equiv e^{-1} \pmod{p-1}$.

(a) Prove that the message x is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$.

(b) Can Eve compute d in the decryption function? If so, by what algorithm and approximately how many iterations does it take for it to terminate?

(c) Given part (b), how would Eve recover x and what algorithm would she use? Approximately how many iterations does it take to terminate?

(d) Based on the previous parts, can Eve recover the original message in a reasonable amount of time? Explain.

Solution:

(a) We want to show x is recovered by $E(x)$ and $D(y)$, such that $D(E(x)) = x$. In other words, $x^{ed} \equiv x \pmod{p}$ $\forall x \in \{0, 1, \ldots, N-1\}$.
Proof: By construction of d, we know that $ed \equiv 1 \pmod{p-1}$. This means we can write $ed = k(p-1)+1$, for some integer k, and $x^{ed} = x^{k(p-1)+1}$.

- x is a multiple of p: Then this means $x = 0$, and indeed, $x^{ed} \equiv 0 \pmod{p}$.
- x is not a multiple of p: Then $x^{ed} \equiv x^{k(p-1)+1} \equiv x^{k(p-1)}x \equiv 1^k x \equiv x \pmod{p}$, by using FLT.

And for both cases, we have shown that x is recovered by $E(D(y))$.

(b) Since Eve knows the value of $N = p$, and the fact that $d \equiv e^{-1} \pmod{p-1}$, she can compute d using EGCD. Since EGCD decreases the largest number by at least a factor of two every two iterations, Eve needs at most $2n$ iterations, where n is the number of bits of the larger input. This means at most 2048 iterations.

(c) Since Eve now has d from part 3, and the encrypted message y, she can calculate x directly by using $D(y) = x \equiv y^d \pmod{p}$. She can now use exponentiation by repeated squaring, giving her no more than 1024 iterations.

(d) Assuming each recursive call in EGCD and exponentiation by squaring have reasonable operation time costs, Eve only needs at most 3×1024 iterations, which can easily be done with today's computing power.

2 Squared RSA

(a) Prove the identity $a^{p(p-1)} \equiv 1 \pmod{p^2}$, where a is coprime to p, and p is prime. (Hint: Try to mimic the proof of Fermat's Little Theorem from the notes.)

(b) Now consider the RSA scheme: the public key is $(N = p^2q^2, e)$ for primes p and q, with e relatively prime to $p(p-1)q(q-1)$. The private key is $d = e^{-1} \pmod{p(p-1)q(q-1)}$. Prove that the scheme is correct for x relatively prime to both p and q, i.e. $x^{ed} \equiv x \pmod{N}$. (Hint: Try to mimic the proof of RSA correctness from the notes.)

Solution:

(a) We mimic the proof of Fermat's Little Theorem from the notes.
Let S be the set of all numbers between 1 and $p^2 - 1$ (inclusive) which are relatively prime to p. We can write

$$S = \{1, 2, \ldots, p-1, p+1, \ldots, p^2-1\}$$

Define the set

$$T = \{a, 2a, \ldots, (p-1)a, (p+1)a, \ldots, (p^2-1)a\}$$

We'll show that $S \subseteq T$ and $T \subseteq S$, allowing us to conclude $S = T$:

- $S \subseteq T$: Let $x \in S$. Since $\gcd(a, p) = 1$, the inverse of a exists $\pmod{p^2}$. For ease of notation, we use a^{-1} to denote the quantity $a^{-1} \pmod{p^2}$. We know $\gcd(a^{-1}, p) = 1$, because a^{-1} has an inverse $\pmod{p^2}$ too. Combining this with the fact that $\gcd(x, p) = 1$, we have $\gcd(a^{-1}x, p) = 1$. This tells us $a^{-1}x \in S$, so $a(a^{-1}x) = x \in T$.
- $T \subseteq S$: Let $ax \in T$, where $x \in S$. We know $\gcd(x, p) = 1$ because $x \in S$. Since $\gcd(a, p) = 1$ as well, we know the product xs cannot share any prime factors with p as well, i.e. $\gcd(xs, p) = 1$. This means $xs \in S$ as well, which proves the containment.

We now follow the proof of Fermat's Little Theorem. Since $S = T$, we have:

$$\prod_{s_i \in S} s_i \equiv \prod_{t_i \in T} t_i \pmod{p^2}$$

However, since we defined $T = \{a, 2a, \ldots, (p-1)a, (p+1)a, \ldots, (p^2-1)a\}$:

$$\prod_{t_i \in T} t_i \equiv \prod_{s_i \in S} a s_i \equiv a^{|S|} \prod_{s_i \in S} s_i \pmod{p^2}$$

We can now conclude $(\prod_{s_i \in S} s_i) \equiv a^{|S|} (\prod_{s_i \in S} s_i) \pmod{p^2}$.
Each $s_i \in S$ is coprime to p, so their product $\prod_{s_i \in S} s_i$ is as well. Then, we can multiply both sides of our equivalence with the inverse of $\prod_{s_i \in S} s_i$ to obtain $a^{|S|} \equiv 1 \pmod{p^2}$. Since $|S| = p(p-1)$, we have gotten the desired result.

Alternate Solution: We can use Fermat's Little Theorem, combined with the Binomial Theorem, to get the result. Since $\gcd(a, p) = 1$ and p is prime, $a^{p-1} \equiv 1 \pmod{p}$, so we can write $a^{p-1} = \ell p + 1$ for some integer ℓ. Then,

$$(a^{p-1})^p = (\ell p + 1)^p = \sum_{i=0}^{p} \binom{n}{i} (\ell p)^i = 1 + p \cdot (\ell p) + \binom{p}{2} (\ell p)^2 + \cdots + (\ell p)^p,$$

and since all of the terms other than the first term are divisible by p^2, $a^{p(p-1)} \equiv 1 \pmod{p^2}$.

(b) By the definition of d above, $ed = 1 + kp(p-1)q(q-1)$ for some k. Look at the equation $x^{ed} \equiv x \pmod{N}$ modulo p^2 first:

$$x^{ed} \equiv x^{1+kp(p-1)q(q-1)} \equiv x \cdot (x^{p(p-1)})^{kq(q-1)} \equiv x \pmod{p^2}$$

where we used the identity above. If we look at the equation modulo q^2, we obtain the same result. Hence, $x^{ed} \equiv x \pmod{p^2 q^2}$.

Remark: The first part of the question mirrors the proof of Fermat's Little Theorem. The second and third parts of the question mirror the proof of correctness of RSA.

3 The CRT and Lagrange Interpolation

Let $n_1, \ldots n_k$ be pairwise co-prime, i.e. n_i and n_j are co-prime for all $i \neq j$. The Chinese Remainder Theorem (CRT) tells us that there exist solutions to the following system of congruences:

$$x \equiv a_1 \pmod{n_1} \quad (1)$$
$$x \equiv a_2 \pmod{n_2} \quad (2)$$
$$\vdots \quad (\vdots)$$
$$x \equiv a_k \pmod{n_k} \quad (k)$$

and all solutions are equivalent $\pmod{n_1 n_2 \cdots n_k}$. For this problem, parts (a)-(c) will walk us through a proof of the Chinese Remainder Theorem. We will then use the CRT to revisit Lagrange interpolation.

(a) We start by proving the $k = 2$ case: Prove that we can always find an integer x_1 that solves (1) and (2) with $a_1 = 1, a_2 = 0$. Similarly, prove that we can always find an integer x_2 that solves (1) and (2) with $a_1 = 0, a_2 = 1$.

(b) Use part (a) to prove that we can always find at least one solution to (1) and (2) for any a_1, a_2. Furthermore, prove that all possible solutions are equivalent $\pmod{n_1 n_2}$.

(c) Now we can tackle the case of arbitrary k: Use part (b) to prove that there exists a solution x to (1)-(k) and that this solution is unique $\pmod{n_1 n_2 \cdots n_k}$.

For polynomials $p_1(x)$, $p_2(x)$ and $q(x)$ we say that $p_1(x) \equiv p_2(x) \bmod q(x)$ if $p_1(x) - p_2(x)$ is of the form $q(x) \times m(x)$ for some polynomial $m(x)$.

(d) Define the polynomials $x-a$ and $x-b$ to be co-prime if they have no common divisor of degree 1. Assuming that the CRT still holds when replacing x, a_i and n_i with polynomials (using the definition of co-prime polynomials just given), show that the system of congruences

$$\begin{aligned} p(x) &\equiv y_1 \pmod{(x - x_1)} && (1') \\ p(x) &\equiv y_2 \pmod{(x - x_2)} && (2') \\ &\vdots && (\vdots) \\ p(x) &\equiv y_k \pmod{(x - x_k)} && (k') \end{aligned}$$

has a unique solution $\pmod{(x-x_1)\cdots(x-x_k)}$ whenever the x_i are pairwise distinct. What is the connection to Lagrange interpolation?

Hint: To show that a unique solution exists, you may use the fact that the CRT has a unique solution when certain properties are satisfied.

Solution:

(a) Since $\gcd(n_1, n_2) = 1$, there exist integers k_1, k_2 such that $1 = k_1 n_1 + k_2 n_2$. Setting $x_1 = k_2 n_2 = 1 - k_1 n_1$ and $x_2 = k_1 n_1 = 1 - k_2 n_2$ we obtain the two desired solutions.

(b) Using the x_1 and x_2 we found in Part (a), we show that $a_1 x_1 + a_2 x_2 \pmod{n_1 n_2}$ is a solution to the desired equivalences:

$$\begin{aligned} a_1 x_1 + a_2 x_2 &\equiv a_1 \cdot 1 + a_2 \cdot 0 \equiv a_1 \pmod{n_1} \\ a_1 x_1 + a_2 x_2 &\equiv a_1 \cdot 0 + a_2 \cdot 1 \equiv a_2 \pmod{n_2}. \end{aligned}$$

Such result is also unique. Say that we have two difference solutions $x = c$ and $x = c'$, which both satisfy $x \equiv a_1 \pmod{n_1}$ and $x \equiv a_2 \pmod{n_2}$. This would give us $c \equiv c' \pmod{n_1}$ and $c \equiv c' \pmod{n_2}$, which suggests that $(c - c')$ is divisible by n_1 and n_2. Since n_1 and n_2 are coprime, $gcd(n_1, n_2) = 1$, $(c - c')$ is divisible by $n_1 n_2$. Writing it in modular form gives us $c \equiv c' \pmod{n_1 n_2}$. Therefore, all the result is unique with respect to $\pmod{n_1 n_2}$

(c) We use induction on k. Part (b) handles the base case, $k = 2$. For the inductive hypothesis, assume for $k \leq l$, the system (1)-(k) has a unique solution $a \pmod{n_1 \cdots n_k}$. Now consider $k = l+1$, so we add the equation $x \equiv a_{l+1} \pmod{n_{l+1}}$ to our system, resulting in

$$x \equiv a \pmod{n_1 \cdots n_l}$$
$$x \equiv a_{l+1} \pmod{n_{l+1}}.$$

Since the n_i are pairwise coprime, $n_1 n_2 \cdots n_l$ and n_{l+1} are coprime. Part (b) tells us that there exists a unique solution $a' \pmod{n_1 \cdots n_l n_{l+1}}$. We conclude that a' is the unique solution to (1)-($l+1$), when taken $\pmod{n_1 n_2 \cdots n_l n_{l+1}}$.

(d) We only need to check that $q_i(x) = (x - x_i)$ and $q_j(x) = (x - x_j)$ are coprime whenever $x_i \neq x_j$; that is, that they don't share a common divisor of degree 1. If $d_i(x) = a_i x + b_i$ is a divisor of $q_i(x)$, then $q_i(x) = q'(x)(a_i x + b_i)$ for some polynomial $q'(x)$. But since $q_i(x)$ is of degree 1, $q'(x)$ must be of degree 0 and hence a constant, so $d_i(x)$ must be a constant multiple of $q_i(x)$. Similarly, any degree 1 divisor d_j of $q_j(x)$ must be a constant multiple of $q_j(x)$, and if $x_i \neq x_j$, then none of these multiples overlap, so $q_i(x)$ and $q_j(x)$ are coprime.

From our result in part (d), the congruences (1′)-(k') assert that we are looking for a polynomial $p(x)$ such that $p(x_i) = y_i$. The CRT then establishes the existence of $p(x)$, and that it is unique modulo a degree k polynomial. That is, $p(x)$ is unique if its degree is at most $k-1$. Lagrange interpolation finds $p(x)$.

4 Polynomials in Fields

Define the sequence of polynomials by $P_0(x) = x + 12$, $P_1(x) = x^2 - 5x + 5$ and $P_n(x) = xP_{n-2}(x) - P_{n-1}(x)$.

(For instance, $P_2(x) = 17x - 5$ and $P_3(x) = x^3 - 5x^2 - 12x + 5$.)

(a) Show that $P_n(7) \equiv 0 \pmod{19}$ for every $n \in \mathbb{N}$.

(b) Show that, for every prime q, if $P_{2017}(x) \not\equiv 0 \pmod{q}$, then $P_{2017}(x)$ has at most 2017 roots modulo q.

Solution:

(a) Prove by strong induction. Base cases:

$$P_0(7) \equiv 7 + 12 \equiv 19 \equiv 0 \pmod{19}$$
$$P_1(7) \equiv 7^2 - 5 \cdot 7 + 5 \equiv 49 - 35 + 5 \equiv 19 \equiv 0 \pmod{19}$$

Inductive step: Assume $P_n(7) \equiv 0 \pmod{19}$ for every $n \leq k$. Then

$$\begin{aligned} P_{k+1}(7) &\equiv xP_{k-1}(7) - P_k(7) \pmod{19} \\ &\equiv x \cdot 0 - 0 \pmod{19} \\ &\equiv 0 \pmod{19}. \end{aligned}$$

Hence, we have $P_n(7) \equiv 0 \pmod{19}$ for all naturnal numbers n.

(b) This question asks to prove that, for all prime numbers q, if $P_{2017}(x)$ is a non-zero polynomial $\pmod{q}$, then $P_{2017}(x)$ has at most 2017 roots $\pmod{q}$.

The proof of Property 1 of polynomials (a polynomial of degree d can have at most d roots) still works in the finite field GF(q). Therefore we need only show that P_{2017} has degree at most 2017. We prove that $\deg(P_n) \leq n$ for $n > 1$ by strong induction. Base cases:

$$\begin{aligned}
\deg(P_0) &= \deg(x+12) = 1 \\
\deg(P_1) &= \deg(x^2 - 5x + 5) = 2 \\
\deg(P_2) &= \deg(xP_0(x) - P_1(x)) \leq 2 \\
\deg(P_3) &= \deg(xP_1(x) - P_2(x)) \leq 3
\end{aligned}$$

Assuming degree of $P_n \leq n$ for all $2 \leq n \leq k$, then

$$\begin{aligned}
\deg(P_{k+1}(x)) &\leq \max\{\deg(xP_{k-1}(x)), \deg(P_k(x))\} \\
&= \max\{1 + \deg(P_{k-1}(x)), \deg(P_k(x))\} \\
&\leq \max\{1 + k - 1, k\} \\
&\leq k \\
&\leq k + 1.
\end{aligned}$$

Thus the proof holds for all $n \geq 2, n \in \mathbb{N}$.

5 Secrets in the United Nations

A vault in the United Nations can be opened with a secret combination $s \in \mathbb{Z}$. In only two situations should this vault be opened: (i) all 193 member countries must agree, or (ii) at least 55 countries, plus the U.N. Secretary-General, must agree.

(a) Propose a scheme that gives private information to the Secretary-General and all 193 member countries so that the secret combination s can only be recovered under either one of the two specified conditions.

(b) The General Assembly of the UN decides to add an extra level of security: each of the 193 member countries has a delegation of 12 representatives, all of whom must agree in order for that country to help open the vault. Propose a scheme that adds this new feature. The scheme should give private information to the Secretary-General and to each representative of each country.

Solution:

(a) Create a polynomial of degree 192 and give each country one point. Give the Secretary General $193 - 55 = 138$ points, so that if she collaborates with 55 countries, they will have a total of

192 points and can reconstruct the polynomial. Without the Secretary-General, the polynomial can still be recovered if all 192 countries come together. (We do all our work in GF(p) where $p \geq d+1$).

Alternatively, we could have one scheme for condition (i) and another for (ii). The first condition is the secret-sharing setup we discussed in the notes, so a single polynomial of degree 192 suffices, with each country receiving one point, and evaluation at zero returning the combination s. For the second condition, create a polynomial f of degree 1 with $f(0) = s$, and give $f(1)$ to the Secretary-General. Now create a second polynomial g of degree 54, with $g(0) = f(2)$, and give one point of g to each country. This way any 55 countries can recover $g(0) = f(2)$, and then can consult with the Secretary-General to recover $s = f(0)$ from $f(1)$ and $f(2)$.

(b) We'll layer an *additional* round of secret-sharing onto the scheme from part (a). If t_i is the key given to the ith country, produce a degree-11 polynomial f_i so that $f_i(0) = t_i$, and give one point of f_i to each of the 12 delegates. Do the same for each country (using different f_i each time, of course).

6 Secret Sharing with Spies

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. (The troops only have one chance to open the safe; if they fail the safe will self-destruct.)

Solution:

The key insight is to realize that both polynomial-based secret-sharing and polynomial-based error correction work on the basis of evaluating an underlying polynomial at many points and then trying to recover that polynomial. Hence they can be easily combined.

Suppose the password is s. The officer can construct a polynomial $P(x)$ such that $s = P(0)$ and share $(i, P(i))$ to the i-th person in her troops. Then the problem is: what should the degree of $P(x)$ be and what is the smallest M?

First, the degree of polynomial d should not be less than 3. It is because when $d < 3$, the 3 spies can decide the polynomial $P(x)$ uniquely. Thus, n will be at least 4 symbols.

Let's choose a polynomial $P(x)$ of degree 3 such that $s = P(0)$. We now view the 3 spies as 3 general errors. Then the smallest $M = 10$ since n is at least 4 symbols and we have $k = 3$ general errors, leading us to a "codeword" of $4 + 2 \cdot 3 = 10$ symbols (or people in our case). Even though the 3 spies are among the 10 people and try to lie on their numbers, the 10 people can still be able to correct the $k = 3$ general errors by the Berlekamp-Welch algorithm and find the correct $P(x)$.

Alternative solution:

Another valid approach is making $P(x)$ of degree $M - 1$ and adding 6 public points to deal with 3 general errors from the spies. In other words, in addition to their own point $(i, P(i))$, everyone also knows the values of 6 more points, $(t+1, P(t+1)), (t+2, P(t+2)), \ldots, (t+6, P(t+6))$, where t is the number of the troops. The spies have access to total of $3 + 6 = 9$ points so the degree $M - 1$ must be at least 9 to prevent the spies from opening the safe by themselves. Therefore, the minimum M is 10.

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.

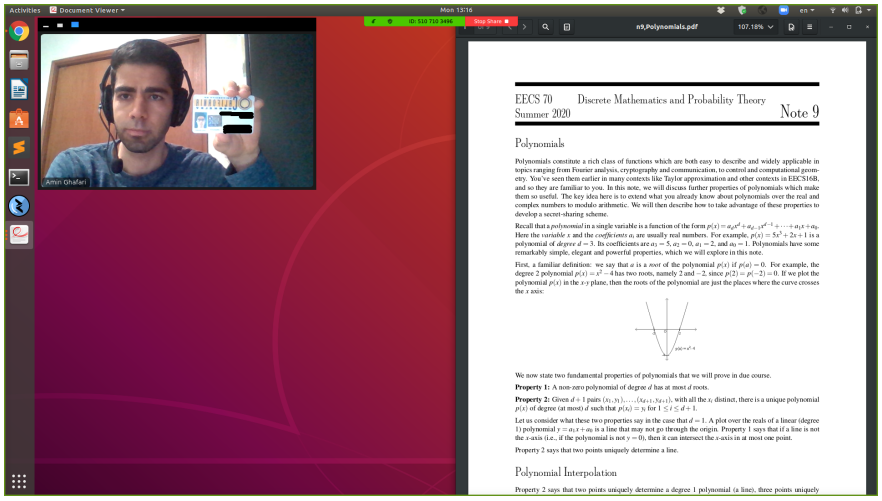


Figure 1: ID card demonstration. Do not actually black out your SID and name.

(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 **??**.

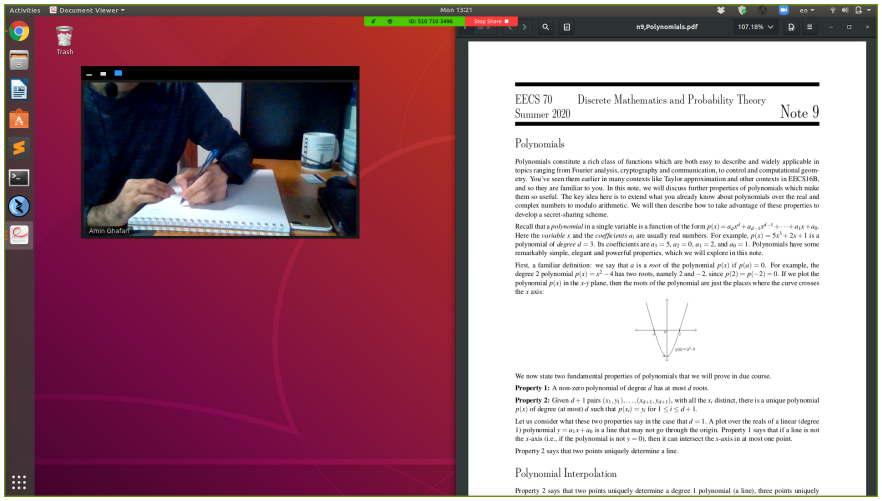


Figure 2: Demonstration of taking your exam. Your setup should look like this while you are taking the exam. The video must be on with your hands visible, alongside your exam pdf or gradescope.

(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:

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

$f(7) = 301$

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 HW 7

1 Strings

How many different strings only contains A, B, C? And how many such strings contains at least one of each characters?

Solution: 3^5 since each position have 3 different choices.

Let E_A be the event that character A doesn't exists in the string, similar for E_B, E_C. Then the total number of bad event is $|E_A + E_B + E_C|$

By the Principle of Inclusion and Exclusion,

$$|E_A+E_B+E_C| = |E_A|+|E_B|+|E_C|-|E_A\cap E_B|-|E_A\cap E_C|-|E_B\cap E_C|+|E_A\cap E_B\cap E_C| = 3*2^5-3*1 = 93$$

, so the total number of valid string is $3^5 - 93 = 150$

2 Palindromes

How many 5-digit palindromes are there? (A palindrome is a number that reads the same way forwards and backwards. For example, 27872 and 48484 are palindromes, but 28389 and 12541 are not.)

Solution:

We construct the number from left-to-right. We have 9 choices for the first digit (since it can't be 0), then 10 choices for the second digit, then 10 choices for the third digit. But now we're out of choices: the fourth digit must match the second, and the last digit must match the first. Therefore, there are $9 \cdot 10 \cdot 10 = 900$ such numbers.

3 Maze in general and Trees too!!!

Given an maze of sidelength n where one starts at $(0,0)$ and goes to (n,n).

(a) How many shortest paths are there that go from $(0,0)$ to (n,n)?

(b) Extending the width by 1, how many shortest paths are there that go from $(0,0)$ to $(n-1,n+1)$.

(c) Now consider shortest paths that meet the conditions which only use to points (x,y) where $y \leq x$. That is, the path cannot cross line $y = x$.

i. Give an expression using part (a) and (b), that counts the number of paths. (Hint: consider what happens after a shortest that crosses $y = x$ at (i,i), that is, the remaining path starting

from $(i, i+1)$ and then continuing to (n,n). If in the remainder of the path, one exchanges the y-direction moves with x-direction moves and vice versa, where does one end up?

ii. A different tack is to derive a recursive formula. We call these paths n-legal paths for a maze of sidelength n, and let F_n be the number of n-legal paths.

Consider a path, and let $i < n$ be the largest value where the path contains (i,i), argue the number of paths is then $F_i * F_{n-i-1}$.

(Hint: if $i = 0$, what are your first and last moves, and where is the remainder of the path allowed to go.)

iii. Give a recursive formula for the number of spanning trees of a complete graph K_n for $n \geq 3$, where each non-root node has degree 3 or 1, and at most 1 node has degree 2?

Two trees are different if and only if either left-subtree is different or right-subtree is different.

(Notice something about your formula and the maze problem. Neat!)

Solution: Let $(x,y) \to (x+1,y)$ be a move 'right' command. And $(x,y) \to (x,y+1)$ be a move 'up' command.

(a) It's $\binom{2n}{n}$ as there are total number of $2n$ moves and n of them are move 'up' command, the rest of them are move 'right' command.

(b) It's $\binom{2n}{n-1}$ as there are $n-1$ move 'right' command.

- The solution is to count the number of pathes that cross $y = x$. Once a path crosses $y = x$, we flip the later protion of the path. Let the invalid path first time crosses $y = x$ at (i,i) and arrives at $(i, i+1)$. Then if we do not flip the path, it will arrive (n,n) takes $n-i$ "go right" command, and $n-1-i$ "go up" command. If we flip these command, it will go to $(i+n-1-i, i+1+n-i) = (n-1, n+1)$. So all invalid pathes maps to a path from $(0,0)$ to $(n-1,n+1)$. Next we argue that all path from $(0,0)$ to $(n-1,n+1)$ maps to a invalid path:

  Pathes from $(0,0)$ to $(n-1,n+1)$ must cross the line $y = x$, let it first cross the line at (i,i) and arrives $(i, i+1)$. Then it takes $n-1-i$ go right command, and $n+1-(i+1)$ go up command. We flip these command, $n-1-i$ go up command, $n+1-i$ go right command, then the path will arrive $(i+n+1-(i+1), i+1+n-1-i) = (n,n)$ and this new path is considered as invalid path since it crosses $y = x$ at point (i,i). So all $(0,0) -> (n-1,n+1)$ pathes can be mapped into a invalid pathes.

  So there is a bijective mapping between invalid pathes and $(0,0) -> (n-1,n+1)$ pathes. The total number is $\binom{2n}{n} - \binom{2n}{n-1}$

- Let F_n be the total number of different ways from $(0,0)$ to (n,n) satisfies the condition above. We know $F_0 = 1$. Let (i,i) be the last point on line $y = x$ that a path touches except for (n,n). Then total number of such path is $F_i * F_{n-1-i}$ where F_i is the total number of pathes from $(0,0)$ to (i,i). Since (i,i) is the last boundry point it touches, so for all later steps, it must not cross the line $y = x-1$, it's equvalient to say the total number of

pathes from $(i+1,i)$ to $(n,n-1)$, it's F_{n-1-i}. F_n is a summation of all these products. $F_n = \sum_{i=0}^{n-1} F_i * F_{n-1-i}$.

- Let T_n be the total number of different trees with n nodes. The number of different trees when the left subtree has size i and right subtree has size $n-i-1$ is $T_i T_{n-i-1}$. If we sum over all possible sizes of left subtrees, we can get the total number of different trees that is structurally different: $T_n = \sum_{i=0}^{n-1} T_i T_{n-i-1}$. And the same counting arguments captures totally different objects! (Maze and trees).

CS 70 Discrete Mathematics and Probability Theory
Fall 2020

HW 8

1 Countability Proof Practice

(a) A disk is a 2D region of the form $\{(x,y) \in \mathbb{R}^2 : (x-x_0)^2 + (y-y_0)^2 \leq r^2\}$, for some $x_0, y_0, r \in \mathbb{R}$, $r > 0$. Say you have a set of disks in $\mathbb{R}^2$ such that none of the disks overlap. Is this set always countable, or potentially uncountable?
(*Hint*: Attempt to relate it to a set that we know is countable, such as $\mathbb{Q} \times \mathbb{Q}$)

(b) A circle is a subset of the plane of the form $\{(x,y) \in \mathbb{R}^2 : (x-x_0)^2 + (y-y_0)^2 = r^2\}$ for some $x_0, y_0, r \in \mathbb{R}$, $r > 0$. Now say you have a set of circles in $\mathbb{R}^2$ such that none of the circles overlap. Is this set always countable, or potentially uncountable?
(*Hint*: The difference between a circle and a disk is that a disk contains all of the points in its interior, whereas a circle does not.)

(c) Is the set containing all increasing functions $f : \mathbb{N} \to \mathbb{N}$ (i.e., if $x \geq y$, then $f(x) \geq f(y)$) countable or uncountable? Prove your answer.

(d) Is the set containing all decreasing functions $f : \mathbb{N} \to \mathbb{N}$ (i.e., if $x \geq y$, then $f(x) \leq f(y)$) countable or uncountable? Prove your answer.

Solution:

(a) Countable. Each disk must contain at least one rational point (an (x,y)-coordinate where $x, y \in \mathbb{Q}$) in its interior, and due to the fact that no two disks overlap, the cardinality of the set of disks can be no larger than the cardinality of $\mathbb{Q} \times \mathbb{Q}$, which we know to be countable.

(b) Possibly uncountable. Consider the circles $C_r = \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = r\}$ for each $r \in \mathbb{R}$. For $r_1 \neq r_2$, C_{r_1} and C_{r_2} do not overlap, and there are uncountably many of these circles (one for each real number).

(c) Suppose that there is a bijection between $\mathbb{N}$ and the set of all increasing functions $\mathbb{N} \to \mathbb{N}$:

$$\begin{aligned} 0 &\mapsto (f_0(0), f_0(1), f_0(2), \ldots) \\ 1 &\mapsto (f_1(0), f_1(1), f_1(2), \ldots) \\ 2 &\mapsto (f_2(0), f_2(1), f_2(2), \ldots) \\ &\vdots \end{aligned}$$

We will use a diagonalization argument to prove that there is a function f which is not in the above list. Define

$$f(n) = 1 + \sum_{i=1}^{n} f_i(n).$$

First, we will show that f is increasing. Indeed, if $m \leq n$, then

$$f(m) = 1 + \sum_{i=1}^{m} f_i(m) \leq 1 + \sum_{i=1}^{n} f_i(m) \leq 1 + \sum_{i=1}^{n} f_i(n) = f(n).$$

The first inequality is because each function is non-negative; the second inequality is because the f_i are increasing.

To show that f is not in the list, note that

$$f(n) = 1 + \sum_{i=1}^{n} f_i(n) \geq 1 + f_n(n) > f_n(n).$$

Since $f(n) > f_n(n)$ for each $n \in \mathbb{N}$, f cannot be any of the functions in the list. Therefore, the set of increasing functions $f : \mathbb{N} \to \mathbb{N}$ is uncountable.

(d) Given any function that begins with $f(0) = n$, consider the number of indices in which the function decreases in output: the set of i such that $f(i) < f(i-1)$. The range of f is a subset of $\mathbb{N}$ so by the well-ordering principle there must be a least element. Call this element a. Then there are only at most $n - a$ transition points. We can set a bijection for any function with $f(0) = n$ to a "word" of indices at which the function decreases. Therefore, the set of decreasing functions $\mathbb{N} \to \mathbb{N}$ has the same cardinality as the set of finite bit strings from a countably infinite alphabet, which is countable. Therefore, the set of all decreasing functions is countable.

2 Hilbert's Hotel

You don't have any summer plans, so you decide to spend a few months working for a magical hotel with a countably infinite number of rooms. The rooms are numbered according to the natural numbers, and all the rooms are currently occupied. Assume that guests don't mind being moved from their current room to a new one, so long as they can get to the new room in a finite amount of time (i.e. guests can't be moved into a room infinitely far from their current one).

(a) A new guest arrives at the hotel. All the current rooms are full, but your manager has told you never to turn away a guest. How could you accommodate the new guest by shuffling other guests around? What if you instead had k guest arrive, for some fixed, positive $k \in \mathbb{Z}$?

(b) Unfortunately, just after you've figured out how to accommodate your first $k+1$ guests, a countably infinite number of guests arrives in town on an infinitely long train. The guests on the train are sitting in seats numbered according to the natural numbers. How could you accommodate all the new guests?

(c) Thanks to a (literally) endless stream of positive TripAdvisor reviews, word of the infinite hotel gets around quickly. Soon enough you find out that a countably infinite number of trains have arrived in town. Each is of infinite length, and carries a countably infinite number of passengers. How would you accommodate all the new passengers?

Solution:

(a) Shift all guests into the room number that is k greater than their current room number. So for a guest in room i move him/her to room $i+k$. Then place the k new guests in the k first rooms in the hotel which will now be unoccupied.

(b) Place all existing guests in room $2i$ where i is their current room number. Place all the new guests in room $2j+1$ where j is their seat number on the train.

(c) **Solution 1**: We first set up a bijection between the newly arriving guests and the set $\mathbb{N} \times \mathbb{N}$. Notice that each guest has an "address": his/her train number i and his/her seat number j. Let this guest be mapped to (i, j). It is clear that this is a bijection.

We know from Lecture Note 10 that the set $\mathbb{N} \times \mathbb{N}$ is countable (via the spiral method) and hence there is a bijection from $\mathbb{N}^2$ to $\mathbb{N}$. Thus the newly arriving guests can be enumerated and considered as if arriving in a single infinite length train with their corresponding seat numbers given by the enumeration. This reduces to the same exact problem as the previous part! Therefore, we can accommodate these guests.

Solution 2: Place all existing guests in room 2^i where i is their current room number. Assign the $(k+2)$th prime, p_{k+2}, to the kth train (e.g. the 0th train will be assigned the 2nd prime, 3). We then place each new guest in room p_{k+2}^{j+1}, where j is the seat number of the new guest on that train.

This works because any power of a prime p will not have any prime factors other than p.

Yes, there will be plenty of empty rooms, but that's okay because every guest will still have somewhere to stay.

3 Finite and Infinite Graphs

The graph material that we learned in lecture still applies if the set of vertices of a graph is infinite. We thus make a distinction between finite and infinite graphs: a graph $G = (V, E)$ is finite if V and E are both finite. Otherwise, the graph is infnite. As examples, consider the graphs

- $G_1 = (V = \mathbb{Z},\ E = \{(i, j) \in \mathbb{Z} \times \mathbb{Z} |\ |i - j| = 1\})$
- $G_2 = (V = \mathbb{Z},\ E = \{(i, j) \in \mathbb{Z} \times \mathbb{Z} |\ i < j\})$
- $G_3 = (V = \mathbb{Z}^2,\ E = \{((i, j), (k, l)) \in \mathbb{Z}^2 \times \mathbb{Z}^2 |\ (i = k \wedge |j - l| = 1) \vee (j = l \wedge |i - k| = 1)\})$

Observe that G_1 is a line of integers, G_2 is a complete graph over all integers, and G_3 is an grid of integers. Prove whether the following sets of graphs are countable or uncountable

(a) The set of all finite graphs $G = (V, E)$, for $V \subseteq \mathbb{N}$

(b) The set of all infinite graphs over a fixed, countably infinite set of vertices (in other words, they all have the same vertex set).

(c) The set of all graphs over a fixed, countably infinite set of vertices, the degree of each vertex is exactly two. For instance, every vertex in G_1 (defined above) has degree 2.

(d) We say that graphs $G = (V,E)$ and $G' = (V',E')$ are isomorphic if the exists some bijection $f : V \to V'$ such that $(u,v) \in V$ iff $(f(u),f(v)) \in V'$. Such a bijection f is called a **graph isomorphism**. Suppose we consider two graphs to be the equivalent if they are isomorphic. The idea is that if we relabel the vertices of a graph, it is still the same graph. Using this definition of "being the same graph", can you conclude that the set of trees over countably infinite vertices is countable?
(*Hint:* Begin by showing that for any graph isomorphism f, and any vertex v, $f(v)$ and v have the same degree)

Solution:

(a) Countable. Let A be the set of graphs we are counting. Let A_k be the set of all graphs $G = (V,E)$, where $V \subseteq \{1,2,\ldots k\}$. A_k is finite because there are only 2^k possible subsets of vertices that is a subset of $\{1,2,...k\}$. For a particular vertex set of size $q \leq k$, there are $\binom{q}{2}$ possible edges over that particular vertex set. Since the number of possible graphs over the vertex set is the power set of all the possible edges to choose from, the number of possible graphs on q vertices is at most $2^{\binom{q}{2}} \leq 2^{k^2}$. There are 2^k ways of choosing a vertex set $V \subseteq \{1,2,\ldots,k\}$, so the number of graphs $|A_k|$ of at most k vertices is bounded at most $2^k \cdot 2^{k^2} = 2^{k^2+k}$. Since each graph's vertex set is a subset of $\mathbb{N}$, the graph must be must be contained in A_k for some k. Thus, $A = \cup_{k=1}^{\infty} A_k$. We can simply enumerate A by enumerating each A_k. Note we are double counting some graphs but for it purpose of showing countability, it's okay.

(b) Uncountable. The set of possible edges in a graph of countably infinite vertices is clearly infinite. The power set of any infinte set is uncountable.

(c) Uncountable.

Recall from lectures that the number of infinite-length binary strings is uncountably infinite. We will construct an injection from this set to the given set of graphs.

First observe that since the number of vertices is countable, we can label them with the positive integers: $V = \{v_i |\ i \in \{1,2,3,\ldots\}\}$. Now consider an infinite binary string $s = b_1b_2b_3\ldots \in \{0,1\}^{\infty}$, where $b_i \in \{0,1\}$ is the ith digit of the string. We can encode the first digit by creating a simple cycle of length $b_1 + 3$ out of vertices $v_1, v_2, \ldots, v_{b_1+2}$ (i.e. we make a chain $v_1 \to v_2 \to \cdots \to v_{b_1+2} \to v_1$). We can also encode b_2 by creating a simple cycle of length $b_2 + 3$ out of the vertices $v_{b_1+3}, v_{b_1+4}, \ldots, v_{b_1+b_2+5}$. Proceeding in this way, we encode the ith digit by making a simple cycle of length $b_i + 3$ out of the vertices $v_{f_s(i)}$ through $v_{f_s(i)+b_i+1}$, where $f_s(i) = 3(i-1) + \sum_{j=1}^{i-1} b_j$. Each vertex in V will be part of exactly one such cycle, and so each vertex will have degree exactly two.

Two see that this is an injection, consider two distinct strings $s = b_1b_2b_3\ldots$ and $s' = b'_1b'_2b'_3\ldots$ that first differ in their ith digit. By construction, the subgraph formed by the first $f_s(i-1)$ vertices will be identical for the each of the graphs. However, the next $b_i + 3$ vertices will be

part of a length-(b_i+3) simple cycle in the graph for s, while the next b'_i+3 vertices will be part of a length-(b'_i+3) simple cycle in the graph for s', with $b'_i+3 \neq b_i+3$. This holds for all $s, s' \in \{0,1\}^\infty$, so we have an injection.

(d) Uncountable. First, to show that if f is a graph isomorphism, then v and $f(v)$ has the same degree, suppose that they do not have the same degree. Then either there is some neighbor, w, of v such that $(f(v), f(w))$ is not in E' or there is some neighbor w', of $f(v)$ such that $(v, f^{-1}(w'))$ is not in E. Either way, f is not an isomorphism.

We will inject the set of infinite bit strings into the set of infinite trees. Specifically, we will construct these trees by adding leaves to the infinite line graph $G = (V,E)$, where $V = \{v_0, v_2, ...\}$ and $E = \{(v_i, v_{i+1}) |\ i \in \mathbb{N}\}$. For each bit string, b, where $b(i)$ is the i^{th} bit of b, construct G_b as follows: First, add 10 leaves to v_0. Then, for each i, if $b(i) = 1$, add a leaf to v_i. We will denote each v_i in G_b as v_i^b. Clearly, the resulting graph is a tree, as adding leaves will never disconnect a graph or create cycles. The graph also has a countable number of vertices because we've only added countably many vertices. To show injection, we first note that any graph isopmorphism must map a vertex to a vertex of the same degree. Now suppose $b \neq b'$ but there is an isomorphism, f, from G_b to $G_{b'}$. By the method of construction each G_b has exactly one vertex of degree ≥ 10. Thus, any isomorphism from the vertex set of G_b to that of $G_{b'}$ must map v_0^b to $v_0^{b'}$. Thus, for each i, it must map v_i^b to $v_i^{b'}$. However, because there is some i where $b(i) \neq b'(i)$, there is some i where where $f(v_i^b)$ and $f(v_i^{b'})$ have different degrees.

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 HW 9

1 Unprogrammable Programs

Prove whether the programs described below can exist or not.

(a) A program $P(F,x,y)$ that returns true if the program F outputs y when given x as input (i.e. $F(x) = y$) and false otherwise.

(b) A program P that takes two programs F and G as arguments, and returns true if F and G halt on the same set of inputs (or false otherwise).

Solution:

(a) P cannot exist, for otherwise we could solve the halting problem:

```
def Halt(F, x):
  def Q(x):
    F(x)
    return 0
  return P(Q, x, 0)
```

`Halt` defines a subroutine `Q` that first simulates F and then returns 0, that is `Q`(x) returns 0 if $F(x)$ halts, and nothing otherwise. Knowing the output of `P`(F,x,0) thus tells us whether F(x) halts or not.

(b) We solve the halting problem once more:

```
def Halt(F, x):
  def Q(y):
    loop
  def R(y):
    If y = x:
      F(x)
    Else:
      loop
  return not P(Q, R)
```

`Q` is a subroutine that loops forever on all inputs. `R` is a subroutine that loops forever on every input except x, and runs $F(x)$ on input x when handed x as an argument. Knowing if `Q` and `R`

halt on the same inputs is thus tantamount to knowing whether F halts on x (since that is the only case in which they could possibly differ). Thus, if $P(Q,R)$ returns "True", then we know they behave the same on all inputs and F must not halt on x, so we return `not P(Q,R)`.

2 Computations on Programs

(a) Is it possible to write a program that takes a natural number n as input, and finds the shortest arithmetic formula which computes n? For the purpose of this question, a formula is a sequence consisting of some valid combination of (decimal) digits, standard binary operators ($+$, $\times$, the "^" operator that raises to a power), and parentheses. We define the length of a formula as the number of characters in the formula. Specifically, each operator, decimal digit, or parentheses counts as one character.

(*Hint:* Think about whether it's possible to enumerate the set of possible arithmetic formulas. How would you know when to stop?)

(b) Now say you wish to write a program that, given a natural number input n, finds another program (e.g. in Java or C) which prints out n. The discovered program should have the minimum execution-time-plus-length of all the programs that print n. Execution time is measured by the number of CPU instructions executed, while "length" is the number of characters in the source code. Can this be done?

(*Hint:* Is it possible to tell whether a program halts on a given input within t steps? What can you say about the execution-time-plus-length of the program if you know that it does not halt within t steps?)

Solution:

(a) Yes it is possible to write such a program.

We already know one way to write a formula for n, which is to just write the number n (with no operators). Let the length of this formula in characters be l. In order to find the *shortest* formula we simply need to search among formulae that have length at most l.

Since there are a finite number of formulas of length at most l, we can write a program that iterates over all of them. For example, if we treat each character as a byte or an 8-bit number, the whole formula becomes a binary integer of length at most $8l$, so we can simply iterate over all binary numbers up to 2^{8l} and for each one check if it is a valid formula.

For each formula that we encounter we can compute its value in finite time (since there are no loop/control structures in formula). Therefore we can check whether it computes n, and then among those that do compute n we find the smallest one.

(b) Yes. Again it is possible to write such a program.

As before, given a number n, there is one program that we know can definitely write n, which is the program that prints the digits of n one by one. Let the length plus running time of this

program be l. We only need to check programs that have a length of at most l and a running time of at most l, since otherwise their running time plus length would be bigger than l.

Similar to the previous part, we can iterate over all programs of length at most l (by treating each one as a large binary integer and checking each one's validity by e.g. compiling it). For each such program, we then run it for at most l steps. If it takes more time, we stop executing it and go to the next program, otherwise in at most l steps we see its output and we can check whether it is equal to n or not.

Now among all programs that have length at most l and execute for at most l steps and print n we find the one that has the shortest length plus execution time.

3 Kolmogorov Complexity

Compressing a bit string x of length n can be interpreted as the task of creating a program of fewer than n bits that returns x. The Kolmogorov complexity of a string $K(x)$ is the length of an optimally-compressed copy of x; that is, $K(x)$ is the length of shortest program that returns x.

(a) Explain why the notion of the "smallest positive integer that cannot be defined in under 280 characters" is paradoxical.

(b) Prove that for any length n, there is at least one string of bits that cannot be compressed to less than n bits.

(c) Say you have a program K that outputs the Kolmogorov complexity of any input string. Under the assumption that you can use such a program K as a subroutine, design another program P that takes an integer n as input, and outputs the length-n binary string with the highest Kolmogorov complexity. If there is more than one string with the highest complexity, output the one that comes first alphabetically.

(d) Let's say you compile the program P you just wrote and get an m bit executable, for some $m \in \mathbb{N}$ (i.e. the program P can be represented in m bits). Prove that the program P (and consequently the program K) cannot exist.

(*Hint*: Consider what happens when P is given a very large input n.)

Solution:

(a) Since there are only a finite number of characters then there are only a finite number of positive integers that can be defined in under 280 characters. Therefore there must be positive integers that are not definable in 280 characters and by the well-ordering principle there is a smallest member of that set. However the statement "the smallest positive integer not definable in under 280 characters" defines the smallest such an integer using only 67 characters (including spaces). Hence, we have a paradox (called the Berry Paradox).

(b) The number of strings of length n is 2^n. The number of strings shorter than length n is $\sum_{i=0}^{n-1} 2^i$. We know that sum is equal to $2^n - 1$ (remember how binary works). Therefore the cardinality of the set of strings shorter than n is smaller than the cardinality of strings of length n. Therefore there must be strings of length n that cannot be compressed to shorter strings.

(c) We write such a program as follows:

```
def P(n):
  complex_string = "0" * n
  for j in range(1, 2 ** n):
    # some fancy Python to convert j into binary
    bit_string = "0:b".format(j)
    # length should now be n characters
    bit_string = (n - len(bit_string)) * "0" + bit_string
    if K(bit_string) > K(complex_string):
      complex_string = bit_string
   return complex_string
```

(d) We know that for every value of n there must be an incompressible string. Such an incompressible string would have a Kolmogorov complexity greater than or equal to its actual length. Therefore our program P must return an incompressible string. However, suppose we choose size n_k such that $n_k \gg m$. Our program $P(n_k)$ will output a string x of length n_k that is not compressible meaning $K(x) \geq n_k$. However we have designed a program that outputs x using fewer bits than n_k. This is a contradiction. Therefore K cannot exist.

4 Five Up

Say you toss a coin five times, and record the outcomes. For the three questions below, you can assume that order matters in the outcome, and that the probability of heads is some p in $0 < p < 1$, but *not* that the coin is fair ($p = 0.5$).

(a) What is the size of the sample space, $|\Omega|$?

(b) How many elements of Ω have exactly three heads?

(c) How many elements of Ω have three or more heads?
(*Hint:* Argue by symmetry.)

For the next three questions, you can assume that the coin is fair (i.e. heads comes up with $p = 0.5$, and tails otherwise).

(d) What is the probability that you will observe the sequence HHHTT? What about HHHHT?

(e) What is the chance of observing at least one head?

(f) What about the chance of observing three or more heads?

For the final three questions, you can instead assume the coin is biased so that it comes up heads with probability $p = \frac{2}{3}$.

(g) What is the chance of observing the outcome HHHTT? What about HHHHT?

(h) What about the chance of at least one head?

(i) What about the chance of ≥ 3 heads?

Solution:

(a) Since for each coin toss, we can have either heads or tails, we have 2^5 total possible outcomes.

(b) Since we know that we have exactly 3 heads, what distinguishes the outcomes is at which point these heads occurred. There are 5 possible places for the heads to occur, and we need to choose 3 of them, giving us the following result: $\binom{5}{3}$.

(c) We can use the same approach from part (b), but since we are asking for 3 or more, we need to consider the cases of exactly 4 heads, and exactly 5 heads as well. This gives us the result as: $\binom{5}{3} + \binom{5}{4} + \binom{5}{5} = 16$.
To see why the number is exactly half of the total number of outcomes, denote the set of outcomes that has 3 or more heads as A. If we flip over every coin in each outcome in set A, we get all the outcomes that has 2 or less head. Denote the new set as A'. Then we know that A and A' have the same size and they together cover the whole sample space. Therefore, $|A| = |A'|$ and $|A| + |A'| = 2^5$, which gives $|A| = 2^5/2$.

(d) Since each coin toss is an independent event, the probability of each of the coin tosses is $\frac{1}{2}$ making the probability of this outcome $\frac{1}{2^5}$. This holds for both cases since both heads and tails have the same probability.

(e) We will use the complementary event, which is the event of getting no heads. The probability of getting no heads is the probability of getting all tails. This event has a probability of $\frac{1}{2^5}$ by a similar argument to the previous part. Since we are asking for the probability of getting at least one heads, our final result is: $1 - \frac{1}{2^5}$.

(f) Since each outcome in this probability space is equally likely, we can divide the number of outcomes where there are 3 or more heads by the total number of outcomes to give us: $\frac{\binom{5}{3}+\binom{5}{4}+\binom{5}{5}}{2^5}$

(g) By using the same idea of independence we get for HHHTT: $\frac{1}{3} \times \frac{1}{3} \times \frac{2}{3} \times \frac{2}{3} \times \frac{2}{3} = \frac{2^3}{3^5}$
For HHHHT, we get:
$\frac{1}{3} \times \frac{2}{3} \times \frac{2}{3} \times \frac{2}{3} \times \frac{2}{3} = \frac{2^4}{3^5}$

(h) Similar to the unbiased case, we will first find the probability of the complement event, which is having no heads. The probability of this is $\frac{1}{3^5}$, which makes our final result $1 - \frac{1}{3^5}$

(i) In this case, since we are working in a nonuniform probability space (getting 4 heads and 3 heads don't have the same probability), we need to separately consider the events with different numbers of heads to find our result. This will get us:

$$\binom{5}{3}\frac{2^3}{3^5}+\binom{5}{4}\frac{2^4}{3^5}+\binom{5}{5}\frac{2^5}{3^5}$$

5 Ball-and-Bin Counting Problems

Say you have 5 bins, and randomly throw 7 balls into them.

1. What is the probability that the first bin has precisely 3 balls in it?
2. What is the probability that the third bin has at least 3 balls in it?
3. What is the probability that at least one of the bins has precisely 3 balls in it?

Solution:

1. First, choose 3 balls out of 7 to put in the first bin. Each of these 3 balls has $Pr = 1/5$ to be in the first bin, and each of the rest $7-3=4$ balls has $Pr = 4/5$ to NOT be in the firts bin. Thus, the answer is

$$\binom{7}{3}\left(\frac{1}{5}\right)^3\left(\frac{4}{5}\right)^4.$$

2. Extend part (a) results into the sum of exactly $3/4/5/6/7$ balls

$$\sum_{k=3}^{7}\binom{7}{k}\left(\frac{1}{5}\right)^k\left(\frac{4}{5}\right)^{7-k}.$$

3. Use inclusion-exclusion. Let A_i be the event that bin i has exactly 3 balls. Then $\sum_{i=1}^{5}\mathbb{P}[A_i] = 5\binom{7}{3}(1/5)^3(4/5)^4$. We have to subtract the events $A_i \cap A_j$, of which there are $\binom{5}{2}$. We have $\mathbb{P}[A_i \cap A_j] = 7!/(3!)^2(1/5)^6(3/5)$.

   The reasoning behind $\frac{7!}{3!3!}$ is because: we want the 7 balls to be split in exactly 3 balls in A_i, 3 balls in A_j, and last ball wherever else. First assume that all 7 balls are lined up, and A_i takes first three balls, A_j takes the next three balls, so you have 7! ways to order all the balls initially. Then, reduce the over-counted parts since the order of the 3 balls in A_i doesn't matter (divide by 3! since there are this many ways to order the 3 balls), and similarly, the order of the 3 balls in A_j doesn't matter either. Thus, you have $\frac{7!}{3!3!}$.

   Therefore our answer is

$$5\binom{7}{3}\left(\frac{1}{5}\right)^3\left(\frac{4}{5}\right)^4-\binom{5}{2}\frac{7!}{3!3!}\left(\frac{1}{5}\right)^6\frac{3}{5}.$$

6 Monty Hall's Revenge

Due to a quirk of the television studio's recruitment process, Monty Hall has ended up drawing all the contestants for his game show from among the ranks of former CS70 students. Unfortunately for Monty, the former students' amazing probability skills have made his cars-and-goats gimmick unprofitable for the studio. Monty decides to up the stakes by asking his contestants to generalise to three new situations with a variable number of doors, goats, and cars:

(a) There are n doors for some $n > 2$. One has a car behind it, and the remaining $n-1$ have goats. As in the ordinary Monty Hall problem, Monty will reveal one door with a goat behind it after you make your first selection. How would switching affect the odds that you select the car?

(Hint: Think about the size of the sample space for the experiment where you *always* switch. How many of those outcomes are favorable?)

(b) Again there are $n > 2$ doors, one with a car and $n-1$ with goats, but this time Monty will reveal $n-2$ doors with goats behind them instead of just one. How does switching affect the odds of winning in this modified scenario?

(c) Finally, imagine there are $k < n-1$ cars and $n-k$ goats behind the $n > 2$ doors. After you make your first pick, Monty will reveal $j < n-k$ doors with goats. What values of j,k maximize the relative improvement in your odds of winning if you choose to switch? (i.e. what j,k maximizes the ratio between your odds of winning when you switch, and your odds of winning when you do not switch?)

Solution:

Throughout the solution, we will refer to W as the event that the contestant wins, and $\mathbb{P}_S(W)$ and $\mathbb{P}_N(W)$ as the probabilities of this event happening if the contestant is (S)witching or (N)ot switching, respectively.

(a) $\mathbb{P}_N(W) = 1/n$ since only one out of n initial choices gets us the car. Under the switching strategy two things can happen: Either the first choice hits the car, and so switching (to any of the remaining $n-2$ doors) will inevitably get us the goat, or our first choice picks a goat, leaving one of the remaining $n-2$ doors with the car. This sequence of choices—first choosing from one of n doors, then switching to one of $n-2$ remaining doors—gives us a sample space of size $n(n-2)$. If we divide the number of favorable outcomes by the total number of outcomes, we get

$$\mathbb{P}_S(W) = \left(\underbrace{1}_{\text{first choice = car}} \cdot \underbrace{0}_{\text{second choice = car}} + \underbrace{(n-1)}_{\text{first choice = goat}} \cdot \underbrace{1}_{\text{second choice = car}} \right) / \underbrace{n(n-2)}_{\text{total \# of choices}}$$
$$= \frac{n-1}{n(n-2)} = \frac{1}{n} \cdot \frac{n-1}{n-2}$$

which is larger than $\mathbb{P}_N(W) = 1/n$ (ever so slightly so the larger n becomes, which demonstrates the intuitive fact that Monty's help gets decreasingly helpful the more doors there are), so switching doors is the better strategy.

(b) $\mathbb{P}_N(W) = 1/n$ remains unchanged. The same approach as in part (a) yields the same numerator as before. For the denominator, we need to figure out the size of the sample space for the experiment where we first pick a door at random, then switch. Again, there are n ways of making the first choice. Once Monty reveals $n-2$ other doors, though, there is only one remaining option for us to switch to. Thus the denominator is much smaller:

$$\begin{aligned}\mathbb{P}_S(W) &= \left(\underbrace{1}_{\text{first choice = car}} \cdot \underbrace{0}_{\text{second choice = car}} + \underbrace{(n-1)}_{\text{first choice = goat}} \cdot \underbrace{1}_{\text{second choice = car}} \right) / \underbrace{n \cdot 1}_{\text{total \# of choices}} \\ &= \frac{n-1}{n} = 1 - \frac{1}{n}\end{aligned}$$

so switching is again the better strategy.

(c) Now $\mathbb{P}_N(W) = k/n$ since k doors hide a car. Reasoning about sample spaces in the same way we did in part (b) gives us a way to compute the denominator of $\mathbb{P}_S(W)$. However, now the numerator (number of favorable outcomes in the case where we switch) changes too:

$$\begin{aligned}\mathbb{P}_S(W) &= \left(\underbrace{k}_{\text{first choice = car}} \cdot \underbrace{k-1}_{\text{second choice = car}} + \underbrace{(n-k)}_{\text{first choice = goat}} \cdot \underbrace{k}_{\text{second choice = car}} \right) / \underbrace{n(n-j-1)}_{\text{total \# of choices}} \\ &= \frac{k(n-1)}{n(n-j-1)} = \frac{k}{n} \cdot \frac{n-1}{n-j-1}.\end{aligned}$$

From here we see that $\mathbb{P}_S(W)/\mathbb{P}_N(W) = \frac{n-1}{n-j-1}$, which is maximal if $j = n-k-1$. In other words, if Monty reveals all but one goat (which he does in the original show where $n = 3, k = 1$ and $j = 1 = n-k-1$), then the contestant can increase their chances of winning by a factor of $\frac{n-1}{k}$ (which is a factor of 2 in the original show). In particular, the largest relative advantage of switching is achieved when $k = 1$.

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 HW 10

1 Independent Complements

Let Ω be a sample space, and let $A, B \subseteq \Omega$ be two independent events.

(a) Prove or disprove: $\overline{A}$ and $\overline{B}$ must be independent.

(b) Prove or disprove: A and $\overline{B}$ must be independent.

(c) Prove or disprove: A and $\overline{A}$ must be independent.

(d) Prove or disprove: It is possible that $A = B$.

Solution:

(a) True. $\overline{A}$ and $\overline{B}$ must be independent:

$$\begin{aligned}
\mathbb{P}[\overline{A} \cap \overline{B}] &= \mathbb{P}[\overline{A \cup B}] && \text{(by De Morgan's law)} \\
&= 1 - \mathbb{P}[A \cup B] && \text{(since } \mathbb{P}[\overline{E}] = 1 - \mathbb{P}[E] \text{ for all } E\text{)} \\
&= 1 - (\mathbb{P}[A] + \mathbb{P}[B] - \mathbb{P}[A \cap B]) && \text{(union of overlapping events)} \\
&= 1 - \mathbb{P}[A] - \mathbb{P}[B] + \mathbb{P}[A]\mathbb{P}[B] && \text{(using our assumption that } A \text{ and } B \text{ are independent)} \\
&= (1 - \mathbb{P}[A])(1 - \mathbb{P}[B]) \\
&= \mathbb{P}[\overline{A}]\mathbb{P}[\overline{B}] && \text{(since } \mathbb{P}[\overline{E}] = 1 - \mathbb{P}[E] \text{ for all } E\text{)}
\end{aligned}$$

(b) True. A and $\overline{B}$ must be independent:

$$\begin{aligned}
\mathbb{P}[A \cap \overline{B}] &= \mathbb{P}[A - (A \cap B)] \\
&= \mathbb{P}[A] - \mathbb{P}[A \cap B] \\
&= \mathbb{P}[A] - \mathbb{P}[A]\mathbb{P}[B] \\
&= \mathbb{P}[A](1 - \mathbb{P}[B]) \\
&= \mathbb{P}[A]\mathbb{P}[\overline{B}]
\end{aligned}$$

(c) False in general. If $0 < \mathbb{P}[A] < 1$, then $\mathbb{P}[A \cap \overline{A}] = \mathbb{P}[\varnothing] = 0$ but $\mathbb{P}[A]\mathbb{P}[\overline{A}] > 0$, so $\mathbb{P}[A \cap \overline{A}] \neq \mathbb{P}[A]\mathbb{P}[\overline{A}]$; therefore A and $\overline{A}$ are not independent in this case.

(d) True. To give one example, if $\mathbb{P}[A] = \mathbb{P}[B] = 0$, then $\mathbb{P}[A \cap B] = 0 = 0 \times 0 = \mathbb{P}[A]\mathbb{P}[B]$, so A and B are independent in this case. (Another example: If $A = B$ and $\mathbb{P}[A] = 1$, then A and B are independent.)

2 Lie Detector

A lie detector is known to be $4/5$ reliable when the person is guilty and $9/10$ reliable when the person is innocent. If a suspect is chosen from a group of suspects of which only $1/100$ have ever committed a crime, and the test indicates that the person is guilty, what is the probability that he is guilty?

Solution:

Let A denote the event that the test indicates that the person is guilty, and B the event that the person is actually guilty. Note that

$$\mathbb{P}[B] = \frac{1}{100}, \quad \mathbb{P}[\overline{B}] = \frac{99}{100}, \quad \mathbb{P}[A \mid B] = \frac{4}{5}, \quad \mathbb{P}[A \mid \overline{B}] = \frac{1}{10}.$$

By Bayes' Rule and the Total Probability Rule the desired probability is

$$\mathbb{P}[B \mid A] = \frac{\mathbb{P}[B]\mathbb{P}[A \mid B]}{\mathbb{P}[A]} = \frac{\mathbb{P}[B]\mathbb{P}[A \mid B]}{\mathbb{P}[B]\mathbb{P}[A \mid B] + \mathbb{P}[\overline{B}]\mathbb{P}[A \mid \overline{B}]} = \frac{(1/100)(4/5)}{(1/100)(4/5) + (99/100)(1/10)} = \frac{8}{107}$$

3 Flipping Coins

Consider the following scenarios, where we apply probability to a game of flipping coins. In the game, we flip one coin each round. The game will not stop until two consecutive heads appear.

(a) What is the probability that the game ends by flipping exactly five coins?

(b) Given that the game ends after flipping the fifth coin, what is the probability that three heads appear in the sequence?

(c) If we change the rule that the game will not stop until three consecutive tails or three consecutive heads appear, what is the probability that the game stops by flipping at most six coins?

Solution:

(a) If the game ends by flipping exactly five coins, we know the flipping results of last three coins must be $\{T,H,H\}$. For the first two coins, the results can be $\{H,T\},\{T,H\}$ or $\{T,T\}$. So the probability equals to $\frac{3}{4} \times \frac{1}{8} = \frac{3}{32}$.

(b) Given the condition that the game ends after flipping the fifth coin, the only possible sequances containing three heads are $\{H,T,T,H,H\}$ and $\{T,H,T,H,H\}$. Let A denote the event that the game ends after flipping the fifth coin, B denote the event that three heads appear when the game ends. Then $\mathbb{P}(A \cap B) = \frac{2}{32}$ and $\mathbb{P}(B|A) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(A)} = \frac{2}{3}$.

(c) We only consider the case that the game ends only because of three consecutive heads appearing. If the game ends in three rounds, the result must be $\{H,H,H\}$ and the probability is $\frac{1}{8}$.

If the game ends in four rounds, the results must be $\{T,H,H,H\}$ and the probability is $\frac{1}{16}$. If the game ends in five rounds, the results must be $\{H,T,H,H,H\}$ or $\{T,T,H,H,H\}$ and the probability is $\frac{1}{16}$. If the game ends in six rounds, the last four coins must be $\{T,H,H,H\}$ and the first two coins cannot be $\{T,T\}$, so the probability is $\frac{3}{4}\times\frac{1}{16}=\frac{3}{64}$. The total probability is

$$\frac{1}{8}+2\times\frac{1}{16}+\frac{3}{64}=\frac{19}{64}$$

. By symmetry, the probability that the game ends in the sixth round because of three consecutive tails is also $\frac{19}{64}$. So the final answer is

$$2\times\frac{19}{64}=\frac{19}{32}$$

.

4 To Be Fair

Suppose you have a biased coin with $\mathbb{P}(\text{heads})\neq 0.5$. How could you use this coin to simulate a fair coin? (*Hint*: Think about pairs of tosses.)

Solution:

Let's think about the experiment of throwing the biased coin twice as hinted towards in the hint: Its sample space is $\Omega=\{\text{HH},\text{TT},\text{HT},\text{TH}\}$ with corresponding probability function $\mathbb{P}(\text{HH})=p^2,\mathbb{P}(\text{TT})=(1-p)^2$ and $\mathbb{P}(\text{HT})=\mathbb{P}(\text{TH})=p(1-p)$. Neither of these probabilities is $1/2$ which is what would be required for simulating a fair coin. However, we can generate new probabilities by looking at conditional probabilities! In particular, knowing that $\mathbb{P}(\text{HT})=\mathbb{P}(\text{TH})$ informs us that $\mathbb{P}(\text{HT}\mid\{\text{HT},\text{TH}\})=\frac{\mathbb{P}(\text{HT})}{\mathbb{P}(\{\text{HT},\text{TH}\})}=\frac{\mathbb{P}(\text{TH})}{\mathbb{P}(\{\text{HT},\text{TH}\})}=\mathbb{P}(\text{TH}\mid\{\text{HT},\text{TH}\})$, and since $\mathbb{P}(\text{HT}\mid\{\text{HT},\text{TH}\})+\mathbb{P}(\text{TH}\mid\{\text{HT},\text{TH}\})=1$, it must be true that

$$\mathbb{P}(\text{HT}\mid\{\text{HT},\text{TH}\})=\mathbb{P}(\text{TH}\mid\{\text{HT},\text{TH}\})=1/2.$$

That is, to simulate a fair coin we can throw the biased coin twice until we observe either HT or TH, since the probability of either showing up first is exactly $1/2$.

5 Identity Theft

A group of n friends go to the gym together, and while they are playing basketball, they leave their bags against the nearby wall. An evildoer comes, takes the student ID cards from the bags, randomly rearranges them, and places them back in the bags, one ID card per bag.

(a) What is the probability that no one receives his or her own ID card back?

Hint: Use the inclusion-exclusion principle.

(b) What is the limit of this proability as $n \to \infty$?

Hint: $e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$.

Solution:

(a) We are looking for the probability of the event that no one receives his or her own ID card back. It is easier to consider the complement of the above event, which is the event that at least one person receives his or her ID card back. Let A_i, $i = 1, \ldots, n$, be the event that the ith friend receives his or her own ID card back, so the event we are considering now is $A_1 \cup \cdots \cup A_n$. We will compute this probability using the generalized inclusion-exclusion formula. Recall that for events a set of n events $B_1, B_2, ..., B_n$ this is

$$\mathbb{P}[\bigcup_{i=1}^{n} B_i] = \sum_{i=1}^{n} \mathbb{P}[B_i] - \sum_{i,j} \mathbb{P}[B_i \cap B_j] + \sum_{i,j,k} \mathbb{P}[B_i \cap B_j \cap B_k] - \ldots \pm \mathbb{P}[\bigcap_{i=1}^{n} B_i] \ .$$

- First, we add $\mathbb{P}(A_1) + \cdots + \mathbb{P}(A_n)$. Here, $\mathbb{P}(A_i)$ is the probability that the ith friend receives his or her own ID card back, which is $1/n$. So, we add $n \cdot (1/n) = 1$.
- Next, we subtract $\sum_{(i,j)} \mathbb{P}(A_i \cap A_j)$, where the sum runs over all $(i, j) \in \{1, \ldots, n\}^2$ with $i < j$. Note that $\mathbb{P}(A_i \cap A_j)$ is the probability that both friend i and friend j receive their own ID cards back, which has probability $(n-2)!/n!$. (To see this, observe that once we have decided that friends i and j will receive their own ID cards back, there are $(n-2)!$ ways to permute the ID cards of the $n-2$ other friends, and there are $n!$ total permutations of the n ID cards.) So, we subtract $\sum_{(i,j)} (n-2)!/n!$, but the summation has $\binom{n}{2}$ terms, so we subtract a total of

$$\binom{n}{2} \frac{(n-2)!}{n!} = \frac{n!}{2!(n-2)!} \cdot \frac{(n-2)!}{n!} = \frac{1}{2!}.$$

- At the kth step of the inclusion-exclusion process, we add $(-1)^{k+1} \sum_{(i_1, \ldots, i_k)} \mathbb{P}(A_{i_1} \cap \cdots \cap A_{i_k})$, where the k-tuples in the summation range over all $(i_1, \ldots, i_k) \in \{1, \ldots, n\}^k$ with $i_1 < \cdots < i_k$. To compute $\mathbb{P}(A_{i_1} \cap \cdots \cap A_{i_k})$, note that we have decided that k friends will receive their own ID cards back, the remaining $n-k$ ID cards can be permuted in $(n-k)!$ ways, and there are $n!$ total permutations, so the probability is $(n-k)!/n!$. The summation has a total of $\binom{n}{k}$ terms, so we add

$$(-1)^{k+1} \binom{n}{k} \frac{(n-k)!}{n!} = (-1)^{k+1} \frac{n!}{k!(n-k)!} \cdot \frac{(n-k)!}{n!} = (-1)^{k+1} \frac{1}{k!}.$$

Now, adding up all of these probabilities together, we have

$$\mathbb{P}(A_1 \cup \cdots \cup A_n) = \frac{1}{1!} - \frac{1}{2!} + \frac{1}{3!} - \cdots + \frac{(-1)^{n+1}}{n!}.$$

Recall that $A_1 \cup \cdots \cup A_n$ is the *complement* of the event we were originally interested in. So,

$$\mathbb{P}(\text{no friends receive their own ID cards back}) = 1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + \frac{(-1)^n}{n!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

(b) Recall the power series for e^x:

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}.$$

Therefore, we have the approximation (which gets better as $n \to \infty$):

$$\mathbb{P}(\text{no friends receive their own ID cards back}) \approx e^{-1} = \frac{1}{e} \approx 0.368.$$

6 Balls and Bins, All Day Every Day

Suppose n balls are thrown into n labeled bins one at a time, where n is a positive *even* integer.

(a) What is the probability that exactly k balls land in the first bin, where k is an integer $0 \leq k \leq n$?

(b) What is the probability p that at least half of the balls land in the first bin? (You may leave your answer as a summation.)

(c) Using the union bound, give a simple upper bound, in terms of p, on the probability that some bin contains at least half of the balls.

(d) What is the probability, in terms of p, that at least half of the balls land in the first bin, or at least half of the balls land in the second bin?

(e) After you throw the balls into the bins, you walk over to the bin which contains the first ball you threw, and you randomly pick a ball from this bin. What is the probability that you pick up the first ball you threw? (Again, leave your answer as a summation.)

Solution:

(a) The probability that a particular ball lands in the first bin is $1/n$. We need exactly k balls to land in the first bin, which occurs with probability $(1/n)^k$, and we need exactly $n-k$ balls to land in a different bin, which occurs with probability $(1-1/n)^{n-k}$, and there are $\binom{n}{k}$ ways to choose which of the k balls land in first bin. Thus, the probability is $\binom{n}{k}(1/n)^k(1-1/n)^{n-k}$.

(b) This is the summation over $k = n/2, \ldots, n$ of the probabilities computed in the first part, i.e., $\sum_{k=n/2}^{n} \binom{n}{k}(1/n)^k(1-1/n)^{n-k}$.

(c) The event that some bin has at least half of the balls is the union of the events A_k, $k = 1, \ldots, n$, where A_k is the event that bin k has at least half of the balls. By the union bound, $\mathbb{P}(\bigcup_{k=1}^{n} A_k) \leq \sum_{k=1}^{n} \mathbb{P}(A_k) = np$.

(d) The probability that the first bin has at least half of the balls is p; similarly, the probability that the second bin has at least half of the balls is also p. There is overlap between these two events, however: the first bin has half of the balls and the second bin has the second half of

the balls. The probability of this event is $\binom{n}{n/2}n^{-n}$: there are n^n total possible configurations for the n balls to land in the bins, but if we require exactly $n/2$ of the balls to land in the first bin and the remaining balls to land in the second bin, there are $\binom{n}{n/2}$ ways to choose which balls land in the first bin. By the principle of inclusion-exclusion, our desired probability is $p+p-\binom{n}{n/2}n^{-n} = 2p-\binom{n}{n/2}n^{-n}$.

(e) Condition on the number of balls in the bin. First we calculate the probability $\mathbb{P}(A_k)$, where A_k is the event that, in addition to the first ball you threw, an additional $k-1$ of the other $n-1$ balls landed in this bin, which by the reasoning in Part (a) has probability

$$\mathbb{P}(A_k) = \binom{n-1}{k-1}(1/n)^{k-1}(1-1/n)^{n-k} \ .$$

If we let B be the event that we pick up the first ball we threw, then

$$\mathbb{P}(B \mid A_k) = 1/k$$

since we are equally likely to pick any of the k balls in the bin. Thus the overall probability we are looking for is, by an application of the law of total probability,

$$\mathbb{P}(B) = \sum_{k=1}^{n}\mathbb{P}(A_k \cap B) = \sum_{k=1}^{n}\mathbb{P}(A_k)\mathbb{P}(B \mid A_k) = \sum_{k=1}^{n}\frac{1}{k}\binom{n-1}{k-1}\left(\frac{1}{n}\right)^{k-1}\left(1-\frac{1}{n}\right)^{n-k}.$$

7 Cliques in Random Graphs

In last week's homework you worked on a graph $G = (V,E)$ on n vertices which is generated by the following random process: for each pair of vertices u and v, we flip a fair coin and place an (undirected) edge between u and v if and only if the coin comes up heads. Now consider:

(a) What is the size of the sample space?

(b) A k-clique in graph is a set S of k vertices which are pairwise adjacent (every pair of vertices is connected by an edge). For example a 3-clique is a triangle. Let's call the event that S forms a clique E_S. What is the probability of E_S for a particular set S of k vertices?

(c) For two sets of vertices $V_1 = \{v_1,\ldots,v_\ell\}$ and $V_2 = \{w_1,\ldots,w_k\}$, are E_{V_1} and E_{V_2} independent?

(d) Prove that $\binom{n}{k} \leq n^k$.

(e) Prove that the probability that the graph contains a k-clique, for $k \geq 4\log n + 1$, is at most $1/n$. (The log is taken base 2). *Hint:* Apply the union bound and part (d).

Solution:

(a) Between every pair of verticles, there is either an edge or not. Since there are two choices for each of the $\binom{n}{2}$ pairs of vertices, the size of the sample space is $2^{\binom{n}{2}}$.

(b) For a fixed set of k vertices to be a k-clique, all of the $\binom{k}{2}$ pairs of those vertices have to be connected by an edge. The probability of this event is $1/2^{\binom{k}{2}}$.

(c) E_{V_1} and E_{V_2} are independent if and only if V_1 and V_2 share at most one vertex: If V_1 and V_2 share at most one vertex, then since edges are added independently of each other, we have

$$\mathbb{P}(E_{V_1} \cap E_{V_2}) = \mathbb{P}(\text{all edges in } V_1 \text{ and all edges in } V_2 \text{ are present}) = \left(\frac{1}{2}\right)^{\binom{|V_1|}{2}} \cdot \left(\frac{1}{2}\right)^{\binom{|V_2|}{2}} = \mathbb{P}(E_{V_1}) \cdot \mathbb{P}(E_{V_2}).$$

Conversely, if V_1 and V_2 share at least two vertices, then their intersection $V_3 = V_1 \cap V_2$ has at least 2 elements, and whence

$$\mathbb{P}(E_{V_1} \cap E_{V_2}) = \left(\frac{1}{2}\right)^{\binom{|V_3|}{2}} \cdot \left(\frac{1}{2}\right)^{\binom{|V_1|}{2}-\binom{|V_3|}{2}} \cdot \left(\frac{1}{2}\right)^{\binom{|V_2|}{2}-\binom{|V_3|}{2}} = \left(\frac{1}{2}\right)^{\binom{|V_1|}{2}+\binom{|V_2|}{2}-\binom{|V_3|}{2}} \neq \mathbb{P}(E_{V_1}) \cdot \mathbb{P}(E_{V_2}).$$

(d) The algebraic solution is an application of the definition of $\binom{n}{k}$:

$$\begin{aligned} \binom{n}{k} = \frac{n!}{(n-k)!k!} &= \frac{n \cdot (n-1) \cdots (n-k+1)}{k!} && (1) \\ &\leq n \cdot (n-1) \cdots (n-k+1) && (2) \\ &\leq n^k && (3) \end{aligned}$$

(e) Let A_S denote the event that S is a k-clique, where $S \subseteq V$ is of size k. Then, the event that the graph contains a k-clique can be described as the union of A_S's over all $S \subseteq V$ of size k. Using the union bound,

$$\mathbb{P}\left[\bigcup_{S \subseteq V, |S|=k} A_S\right] \leq \sum_{S \subseteq V, |S|=k} \mathbb{P}[A_S] = \sum_{S \subseteq V, |S|=k} \frac{1}{2^{\binom{k}{2}}}.$$

Now, since there are $\binom{n}{k}$ ways of choosing a subset $S \subseteq V$ of size k, the right-hand side of the above equality is

$$\frac{\binom{n}{k}}{2^{\binom{k}{2}}} = \frac{\binom{n}{k}}{2^{k(k-1)/2}} \leq \frac{n^k}{\left(2^{(k-1)/2}\right)^k} \leq \frac{n^k}{\left(2^{(4\log n+1-1)/2}\right)^k} = \frac{n^k}{\left(2^{2\log n}\right)^k} = \frac{n^k}{n^{2k}} = \frac{1}{n^k} \leq \frac{1}{n}.$$

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 HW 11

1 Random Variables Warm-Up

Let X and Y be random variables, each taking values in the set $\{0,1,2\}$, with joint distribution

$$\begin{aligned}
&\mathbb{P}[X=0,Y=0]=1/3 && \mathbb{P}[X=0,Y=1]=0 && \mathbb{P}[X=0,Y=2]=1/3\\
&\mathbb{P}[X=1,Y=0]=0 && \mathbb{P}[X=1,Y=1]=1/9 && \mathbb{P}[X=1,Y=2]=0\\
&\mathbb{P}[X=2,Y=0]=1/9 && \mathbb{P}[X=2,Y=1]=1/9 && \mathbb{P}[X=2,Y=2]=0.
\end{aligned}$$

(a) What are the marginal distributions of X and Y?

(b) What are $\mathbb{E}[X]$ and $\mathbb{E}[Y]$?

(c) (optional) What are $\mathrm{Var}(X)$ and $\mathrm{Var}(Y)$?

(d) Let I be the indicator that $X=1$, and J be the indicator that $Y=1$. What are $\mathbb{E}[I]$, $\mathbb{E}[J]$ and $\mathbb{E}[IJ]$?

(e) In general, let I_A and I_B be the indicators for events A and B in a probability space $(\Omega,\mathbb{P})$. What is $\mathbb{E}[I_AI_B]$, in terms of the probability of some event?

Solution:

(a) By the law of total probabilty

$$\mathbb{P}[X=0]=\mathbb{P}[X=0,Y=0]+\mathbb{P}[X=0,Y=1]+\mathbb{P}[X=0,Y=2]=1/3+0+1/3=2/3$$

and similarly

$$\begin{aligned}
\mathbb{P}[X=1]&=0+1/9+0=1/9\\
\mathbb{P}[X=2]&=1/9+1/9+0=2/9.
\end{aligned}$$

As a sanity check, these three numbers are all positive and they add up to $2/3+1/9+2/9=1$ as they should. The same kind of calculation gives

$$\begin{aligned}
\mathbb{P}[Y=0]&=1/3+0+1/9=4/9\\
\mathbb{P}[Y=1]&=0+1/9+1/9=2/9\\
\mathbb{P}[Y=2]&=1/3.
\end{aligned}$$

(b) From the above marginal distributions, we can compute

$$\begin{aligned}
\mathbb{E}[X]&=0\mathbb{P}[X=0]+1\mathbb{P}[X=1]+2\mathbb{P}[X=2]=5/9\\
\mathbb{E}[Y]&=0\mathbb{P}[Y=0]+1\mathbb{P}[Y=1]+2\mathbb{P}[Y=2]=8/9
\end{aligned}$$

(c) Again using our marginal distributions,

$$\mathbb{E}[X^2] = 0\mathbb{P}[X=0] + 1\mathbb{P}[X=1] + 4\mathbb{P}[X=2] = 1$$
$$\mathbb{E}[Y^2] = 0\mathbb{P}[Y=0] + 1\mathbb{P}[Y=1] + 4\mathbb{P}[Y=2] = 14/9$$

and thus

$$\mathrm{Var}(X) = \mathbb{E}[X^2] - \mathbb{E}[X]^2 = 56/81$$
$$\mathrm{Var}(Y) = \mathbb{E}[Y^2] - \mathbb{E}[Y]^2 = 62/81.$$

We didn't ask you to do compute the covariance on the homework, but it is

$$\begin{aligned}
\mathrm{cov}(X,Y) &= \mathbb{E}[XY] - \mathbb{E}[X]\,\mathbb{E}[Y] && (1)\\
&= 0\mathbb{P}[XY=0] + 1\mathbb{P}[XY=1] + 2\mathbb{P}[XY=2] + 4\mathbb{P}[XY=4] - 40/81 && (2)\\
&= 0\cdot 1/3 + 1\cdot 1/9 + 2\cdot 1/9 + 4\cdot 0 - 40/81 && (3)\\
&= -13/81. && (4)
\end{aligned}$$

(d) We know that taking the expectation of an indicator for some event gives the probability of that event, so

$$\mathbb{E}[I] = \mathbb{P}[X=1] = 1/9$$
$$\mathbb{E}[J] = \mathbb{P}[Y=1] = 2/9.$$

The random variable IJ is equal to one if $I=1$ and $J=1$, and is zero otherwise. In other words, it is the indicator for the event that $I=1$ *and* $J=1$:

$$\mathbb{E}[IJ] = \mathbb{P}[I=1, J=1] = 1/9.$$

(e) By what we said in the previous part of the solution, $I_A I_B$ is the indicator for the event $A \cap B$, so

$$\mathbb{E}[I_A I_B] = \mathbb{P}[A \cap B].$$

2 Marginals

(a) Can there exist three random variables X_1, X_2, X_3, each taking values in the set $\{+1,-1\}$, with the property that for every $i \neq j$, the joint distribution of X_i and X_j is given by

$$\mathbb{P}[X_i=1, X_j=-1] = \frac{1}{2} \qquad \mathbb{P}[X_i=-1, X_j=1] = \frac{1}{2} \qquad \mathbb{P}[X_i = X_j] = 0? \tag{5}$$

If so, specify the joint distribution of X_1, X_2, X_3; if not, prove it.

(b) For which natural numbers $n \geq 3$ can there exist random variables $X_1, X_2, \ldots, X_n$, each taking values in the set $\{+1,-1\}$, with the property that for every i and j satisfying $i - j = 1 \pmod{n}$, the joint distribution of X_i and X_j is given by (1)? For any n that work, specify the joint distribution; for those that do not, prove it.

Solution:

(a) No such random variables can exist; let's prove it by contradiction. From the desired joint distribution of X_1 and X_2, we claim that $X_1 = -X_2$ (by which we mean that for every ω in the sample space $X_1(\omega) = -X_2(\omega)$). Similarly, we would need to have $X_2 = -X_3$ and $X_3 = -X_1$. But now

$$X_1 = -X_2 = X_3 = -X_1,$$

a contradiction since $X_1 \in \{+1, -1\}$.

(b) This is only possible if n is even. When $n = 2k+1$, the same argument as above gives us

$$X_1 = -X_2 = X_3 = \cdots = -X_{2k} = X_{2k+1} = -X_1,$$

a contradiction for the same reason as before. However, when $n = 2k$, we can set $X_1, ..., X_{2k}$ to have the joint distribution

$$\mathbb{P}[X_1 = 1, X_2 = -1, \cdots X_{2k} = -1] = 1/2$$
$$\mathbb{P}[X_1 = -1, X_2 = 1, \cdots X_{2k} = 1] = 1/2.$$

3 Testing Model Planes

Amin is testing model airplanes. He starts with n model planes which each independently have probability p of flying successfully each time they are flown, where $0 < p < 1$. Each day, he flies every single plane and keeps the ones that fly successfully (i.e. don't crash), throwing away all other models. He repeats this process for many days, where each "day" consists of Amin flying any remaining model planes and throwing away any that crash. Let X_i be the random variable representing how many model planes remain after i days. Note that $X_0 = n$. Justify your answers for each part.

(a) What is the distribution of X_1? That is, what is $\mathbb{P}[X_1 = k]$?

(b) What is the distribution of X_2? That is, what is $\mathbb{P}[X_2 = k]$? Name the distribution of X_2 and what its parameters are.

(c) Repeat the previous part for X_t for arbitrary $t \geq 1$.

(d) What is the probability that at least one model plane still remains (has not crashed yet) after t days? Do not have any summations in your answer.

(e) Considering only the first day of flights, is the event A_1 that the first and second model planes crash independent from the event B_1 that the second and third model planes crash? Recall that two events A and B are independent if $\mathbb{P}[A \cap B] = \mathbb{P}[A]\mathbb{P}[B]$. Prove your answer using this definition.

(f) Considering only the first day of flights, let A_2 be the event that the first model plane crashes *and* exactly two model planes crash in total. Let B_2 be the event that the second plane crashes on the first day. What must n be equal to in terms of p such that A_2 is independent from B_2? Prove your answer using the definition of independence stated in the previous part.

(g) Are the random variables X_i and X_j, where $i < j$, independent? Recall that two random variables X and Y are independent if $\mathbb{P}[X = k_1 \cap Y = k_2] = \mathbb{P}[X = k_1]\mathbb{P}[Y = k_2]$ for all k_1 and k_2. Prove your answer using this definition.

Solution:

(a) Since Amin is performing n trials (flying a plane), each with an independent probability of "success" (not crashing), we have $X_1 \sim \text{Binom}(n, p)$, or $\mathbb{P}[X = k] = \binom{n}{k} p^k (1-p)^{n-k}$, for $0 \leq k \leq n$.

(b) Each model plane independently has probability p^2 of surviving both days. Whether a model plane survives both days is still independent from whether any other model plane survives both days, so we can say $X_2 \sim \text{Binom}(n, p^2)$, or $\mathbb{P}[X = k] = \binom{n}{k} p^{2k} (1-p^2)^{n-k}$, for $0 \leq k \leq n$.

(c) By extending the previous part we see each model plane has probability p^t of surviving t days, so $X_t \sim \text{Binom}(n, p^t)$, or $\mathbb{P}[X = k] = \binom{n}{k} p^{tk} (1-p^t)^{n-k}$, for $0 \leq k \leq n$.

(d) We consider the complement, the probability that no model planes remain after t days. By the previous part we know this to be $\mathbb{P}[X_t = 0] = \binom{n}{0} p^{t(0)} (1-p^t)^{n-0} = (1-p^t)^n$. So the probability of at least model plane remaining after t days is $1 - (1-p^t)^n$.

(e) No. $\mathbb{P}[A_1 \cap B_1]$ is the probability that the first three model planes crash, which is $(1-p)^3$. But $\mathbb{P}[A_1]\mathbb{P}[B_1] = (1-p)^2(1-p)^2 = (1-p)^4$. So $\mathbb{P}[A_1 \cap B_1] \neq \mathbb{P}[A_1]\mathbb{P}[B_1]$ and A_1 and B_1 are not independent.

(f) $\mathbb{P}[A_1 \cap B_1]$ is the probability that only the first model plane and second model plane crash, which is $(1-p)^2 p^{n-2}$. $\mathbb{P}[A_1]$ is the probability that the first model plane crashes, and exactly one of the remaining $n-1$ model planes crashes, so $\mathbb{P}[A_2] = (1-p) \cdot \binom{n-1}{1}(1-p)p^{n-1-1} = (n-1)(1-p)^2 p^{n-2}$. Trivially, we have $\mathbb{P}[B_2] = 1-p$, so $\mathbb{P}[A_2]\mathbb{P}[B_2] = (n-1)(1-p)^3 p^{n-2}$ which is equal to $\mathbb{P}[A_2 \cap B_2] = (1-p)^2 p^{n-2}$ only when $(n-1)(1-p) = 1$, or when $n = \frac{1}{1-p} + 1$.

(g) No. Let $k_1 = 0$ and $k_2 = 1$. Then $\mathbb{P}[X_i = k_1 \cap X_j = k_2] = 0$ because you can't have 1 plane at the end of day 2 if there are no planes left at the end of day 1. But $\mathbb{P}[X_i = k_1] > 0$ and $\mathbb{P}[X_j = k_2] > 0$ so $\mathbb{P}[X_i = k_1]\mathbb{P}[X_j = k_2] > 0$. Since $\mathbb{P}[X_i = k_1]\mathbb{P}[X_j = k_2] \neq \mathbb{P}[X_i = k_1 \cap X_j = k_2]$, they are not independent.

4 Graph

Consider a random graph (undirected, no multi-edges, no self-loops) on n nodes, where each possible edge exists independently with probability p. Let X be the number of isolated nodes (nodes with degree 0).

(a) What is $\mathrm{E}(X)$? *Consider X to be the sum of the indicators X_i that vertex i is isolated. Why isn't X a binomial random variable?*

(b) (optional) What is $\mathrm{Var}(X)$?

Solution:

(a) Let's first pause and ask ourselves why X is not binomial. If we consider a trial as adding an edge, which happens with probability p, we will have $\frac{n(n-1)}{2}$ trials. If we were interested in the number of edges that the resulting graph has, then it would be binomial. But unfortunately, that is not the random variable we're looking for.

Since we are interested in the number of isolated nodes, we must instead consider a trial creating an isolated node, which happens with probability $(1-p)^{n-1}$. However, now our trials are not independent. For example, given that a node is not isolated, the conditional probability of all nodes connected to that node being isolated becomes 0.

So how can we solve this problem? Let's introduce some indicator variables $X_1, X_2, \ldots, X_n$, where $X_i = 1$ if node i is isolated.
Note that $\mathbb{P}[X_i = 1] = (1-p)^{n-1}$, and thus $\mathbb{E}(X_i) = (1-p)^{n-1}$.
Now, we can rewrite X as

$$X = X_1 + X_2 + \cdots + X_n$$

Using the Linearity of Expectation, we know

$$\begin{aligned}
\mathbb{E}(X) &= \mathbb{E}(X_1 + X_2 + \cdots + X_n) \\
&= \mathbb{E}(X_1) + \mathbb{E}(X_2) + \cdots + \mathbb{E}(X_n) \\
&= (1-p)^{n-1} + (1-p)^{n-1} + \cdots + (1-p)^{n-1} \\
&= n(1-p)^{n-1}
\end{aligned}$$

What happened here? We ended up with the same expectation as a binomial distribution, even though it wasn't binomial. In general, many different distributions can have the same expectation, but can vary greatly. This is one such example. Another is the two following distributions: one that is always $\frac{1}{2}$, and another is a fair coin toss. Both have the same expectation, but are very different.

5 Triangles in Random Graphs

Let's say we make a simple and undirected graph G on n vertices by randomly adding m edges, without replacement. In other words, we choose the first edge uniformly from all $\binom{n}{2}$ possible edges, then the second one uniformly from among the remaining $\binom{n}{2} - 1$ edges, etc. What is the expected number of triangles in G? (A triangle is a triplet of distinct vertices with all three edges present between them.)

Solution:

Let's label our vertices $1, \ldots n$, and first check the probability that vertices $1, 2, 3$ form a triangle. This event is described by a hypergeometric distribution with parameters $\binom{n}{2}$, 3, m: when we make the graph we are drawing the m edges from a bucket of $\binom{n}{2}$ possible edges, 3 of which are the ones connecting vertices 1, 2, and 3. Thus the probability that all three of these edges exist is

$$\mathbb{P}[1, 2, \text{and } 3 \text{ form a triangle}] = \frac{\binom{3}{3}\binom{\binom{n}{2}-3}{m-3}}{\binom{\binom{n}{2}}{m}}$$

In fact, there was nothing special about vertices $1, 2, 3$ in this calculation. The probability that the three edges connecting some triplet of distinct vertices i, j, k is equal to the quantity above. Now, for each subset $\{i, j, k\} \subset \{1, \ldots, n\}$, let $I_{i,j,k}$ be the indicator that these three vertices form a triangle. We then have

$$\begin{aligned}
\mathbb{E}[\#\text{ of triangles}] &= \mathbb{E}\sum_{\{i,j,k\}\subset\{1,\ldots,n\}} I_{i,j,k} \\
&= \sum_{\{i,j,k\}\subset\{1,\ldots,n\}} \mathbb{E}[I_{i,j,k}] && \text{linearity of expectation} \\
&= \sum_{\{i,j,k\}\subset\{1,\ldots,n\}} \mathbb{P}[i,\ j, \text{ and } k \text{ form a triangle}] \\
&= \sum_{\{i,j,k\}\subset\{1,\ldots,n\}} \frac{\binom{3}{3}\binom{\binom{n}{2}-3}{m-3}}{\binom{\binom{n}{2}}{m}} \\
&= \binom{n}{3}\frac{\binom{3}{3}\binom{\binom{n}{2}-3}{m-3}}{\binom{\binom{n}{2}}{m}}
\end{aligned}$$

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 HW 12

1 Graph

Consider a random graph (undirected, no multi-edges, no self-loops) on n nodes, where each possible edge exists independently with probability p. Let X be the number of isolated nodes (nodes with degree 0).

(a) What is $\text{Var}(X)$?

Solution:

(a) Define X_i as the indicator when node i is isolated. Since $Var(X) = E[X^2] - E[X]^2$, and $E[X]$ is $n(1-p)^{n-1}$, it remains to calculate $E[X^2]$.

$$\begin{aligned} E[X^2] &= E[(X_1 + \ldots + X_n)^2] \\ &= E[(\sum_{i=1}^{n} X_i^2) + (\sum_{i \neq j} X_i X_j)]. \\ &= \sum_{i=1}^{n} (1-p)^{n-1} + \sum_{i \neq j} (1-p)^{2n-3} \\ &= n(1-p)^{n-1} + n(n-1)(1-p)^{2n-3} \end{aligned}$$

Putting it all together, $Var(X) = E[X^2] - (E[X])^2 = n(1-p)^{n-1} + n(n-1)(1-p)^{2n-3} - n^2(1-p)^{2n-2}$.

2 Whitening

Let X and Y be two random variables, with $\text{Var}(X) > 0, \text{Var}(Y) > 0$. Show that it is possible to construct $\tilde{X} = aX + bY$ and $\tilde{Y} = cX + dY$, where a, b, c, d are scalars to be chosen subject to the constraint $ad - bc \neq 0$, such that $\text{cov}(\tilde{X}, \tilde{Y}) = 0$.

You may find it unnecessary to transform Y, that is, you only need to solve for a, b to get $\text{cov}(\tilde{X}, Y) = 0$.

Solution:

The covariance between $\tilde{X}$ and $\tilde{Y}$ is given by

$$\text{cov}(\tilde{X}, \tilde{Y}) = ac\,\text{Var}(X) + bd\,\text{Var}(Y) + (ad + bc)\,\text{cov}(X, Y).$$

Our goal is to make this quantity 0. This is an underdetermined equation in a, b, c, d. We can start by choosing $a = d = 1$ and $c = 0$. This simplifies the equation to $b\,\mathrm{Var}(Y) + \mathrm{cov}(X,Y) = 0$, from which we get

$$b = -\frac{\mathrm{cov}(X,Y)}{\mathrm{Var}(Y)}.$$

Hence a suitable transformation is given by

$$\tilde{X} = X - \frac{\mathrm{cov}(X,Y)}{\mathrm{Var}(Y)}Y$$

and $\tilde{Y} = Y$ (note that the condition $ad - bc \neq 0$ is indeed satisfied – this condition was imposed to avoid trivial solutions).

3 Probabilistic Bounds

A random variable X has variance $\mathrm{Var}(X) = 9$ and expectation $\mathbb{E}[X] = 2$. Furthermore, the value of X is never greater than 10. Given this information, provide either a proof or a counterexample for the following statements.

(a) $\mathbb{E}\left[X^2\right] = 13$.

(b) $\mathbb{P}[X = 2] > 0$.

(c) $\mathbb{P}[X \geq 2] = \mathbb{P}[X \leq 2]$.

(d) $\mathbb{P}[X \leq 1] \leq 8/9$.

(e) $\mathbb{P}[X \geq 6] \leq 9/16$.

Solution:

(a) TRUE. Since $9 = \mathrm{Var}(X) = \mathbb{E}[X^2] - \mathbb{E}[X]^2 = \mathbb{E}[X^2] - 2^2$, we have $\mathbb{E}[X^2] = 9 + 4 = 13$.

(b) FALSE. It is not necessary for a random variable to be able to take on its mean as a value. Construct a random variable X that satisfies the conditions in the question but does not take on the value 2. A simple example would be a random variable that takes on 2 values, where $\mathbb{P}[X = a] = \mathbb{P}[X = b] = 1/2$, and $a \neq b$. The expectation must be 2, so we have $a/2 + b/2 = 2$. The variance is 9, so $\mathbb{E}[X^2] = 13$ (from Part (**??**)) and $a^2/2 + b^2/2 = 13$. Solving for a and b, we get $\mathbb{P}[X = -1] = \mathbb{P}[X = 5] = 1/2$ as a counterexample.

(c) FALSE. The median of a random variable is not necessarily the mean, unless it is symmetric. Construct a random variable X that satisfies the conditions in the question but does not have an equal chance of being less than or greater than 2. A simple example would be a random variable that takes on 2 values, where $\mathbb{P}[X = a] = p, \mathbb{P}[X = b] = 1 - p$. Here, we use the same approach as part (b) except with a generic p, since we want $p \neq 1/2$. The expectation must be 2, so we have $pa + (1-p)b = 2$. The variance is 9, so $\mathbb{E}\left[X^2\right] = 13$ and $pa^2 + (1-p)b^2 = 13$.

Solving for a and b, we find the relation $b = 2 \pm 3/\sqrt{x}$, where $x = (1-p)/p$. Then, we can find an example by plugging in values for x so that $a, b \leq 10$ and $p \neq 1/2$. One such counterexample is $\mathbb{P}[X = -7] = 1/10, \mathbb{P}[X = 3] = 9/10$.

(d) TRUE. Let $Y = 10 - X$. Since X is never exceeds 10, Y is a non-negative random variable. By Markov's inequality,

$$\mathbb{P}[10 - X \geq a] = \mathbb{P}[Y \geq a] \leq \frac{\mathbb{E}[Y]}{a} = \frac{\mathbb{E}[10 - X]}{a} = \frac{8}{a}.$$

Setting $a = 9$, we get $\mathbb{P}[X \leq 1] = \mathbb{P}[10 - X \geq 9] \leq 8/9$.

(e) TRUE. Chebyshev's inequality says $\mathbb{P}[|X - \mathbb{E}[X]| \geq a] \leq \text{Var}(X)/a^2$. If we set $a = 4$, we have

$$\mathbb{P}[|X - 2| \geq 4] \leq \frac{9}{16}.$$

Now we observe that $\mathbb{P}[X \geq 6] \leq \mathbb{P}[|X - 2| \geq 4]$, because the event $X \geq 6$ is a subset of the event $|X - 2| \geq 4$.

4 Subset Card Game

Jonathan and Yiming are playing a card game. Jonathan has $k > 2$ cards, and each card has a real number written on it. Jonathan tells Yiming (truthfully), that the sum of the card values is 0, and that the sum of squares of the values on the cards is 1. Specifically, if the card values are $c_1, c_2, \ldots, c_k$, then we have $\sum_{i=1}^{k} c_i = 0$ and $\sum_{i=1}^{k} c_i^2 = 1$. Jonathan and Yiming also agree on a positive target value of α.

The cards are then going to be dealt randomly in the following fashion: for each card in the deck, a fair coin is flipped. If the coin lands heads, then the card goes to Yiming, and if the coin lands tails, the card goes to Jonathan. Note that it is possible for either player to end up with no cards/all the cards.

A player wins the game if the sum of the card values in their hand is at least α, otherwise it is a tie.

(a) Prove that the probability that Yiming wins is at most $\frac{1}{8\alpha^2}$.

(b) Find a deck of k cards and target value α where the probability that Yiming wins is exactly $\frac{1}{8\alpha^2}$.

Solution:

(a) Let I_i be the indicator random variable indicating whether or not card i goes to Yiming. Define $S = \sum_{i=1}^{k} c_i I_i$ as the value of Yiming's hand. Then, we see that $\mathbb{E}[S] = \sum_{i=1}^{k} c_i \cdot \frac{1}{2} = 0$ and

$$\begin{aligned} \text{Var}(S) &= \sum_{i=1}^{k} \text{Var}(c_i I_i) \qquad \text{(due to independence) of } I_i \\ &= \sum_{i=1}^{k} c_i^2 \, \text{Var}(I_i) \end{aligned}$$

We know that I_i is a Bernoulli random variable, so its variance is $\frac{1}{4}$. Thus, we see that $\text{Var}(S) = \frac{1}{4}$.

By Chebyshev, we see that $\mathbb{P}(|S| \geq \alpha) \leq \frac{1}{4\alpha^2}$. Now we need to make a symmetry argument, specifically that for each value of x, $\mathbb{P}(S = x) = \mathbb{P}(S = -x)$. This is true because for each outcome where Yiming gets x, Jonathan gets $-x$, since the sum of the card values is 0. However, we also know that the reverse outcome, where Jonathan gets Yiming's cards and vice versa, has the same probability of happening.

Since the distribution of S is symmetric around 0, we see that $\mathbb{P}(|S| \geq \alpha) = 2\mathbb{P}(S \geq \alpha)$, and plugging into our bound yields $\mathbb{P}(S \geq \alpha) \leq \frac{1}{8\alpha^2}$.

(b) We now need to appeal to the equality case of Chebyshev's inequality. Recall that the derivation of Chebyshev's inequality uses Markov's inequality on the quantity $(S - \mathbb{E}[S])^2$. Let's walk through the proof that $\mathbb{P}(S^2 \geq \alpha^2) \leq \frac{\mathbb{E}[S^2]}{\alpha^2}$ again:

$$\begin{aligned}
\mathbb{E}[S^2] &= \sum_v \mathbb{P}(S^2 = v) \cdot v \\
&= \sum_{0 \leq v < \alpha^2} \mathbb{P}(S^2 = v) \cdot v + \sum_{v \geq \alpha^2} \mathbb{P}(S^2 = v) \cdot v \\
&\geq \sum_{v \geq \alpha^2} \mathbb{P}(S^2 = v) \cdot v \\
&\geq \mathbb{P}(S^2 = \alpha^2) \cdot \alpha^2
\end{aligned}$$

In order for equality to hold, then equality must hold in both the third and fourth steps. We got the third step by saying that v is always at least 0, so we can drop them from the sum. Equality holds if it is not possible for S^2 to be anything strictly between 0 and α^2. We get the fourth line by observing that since $\mathbb{P}(S^2 = v) \cdot v \geq 0$ for all $v > \alpha^2$, we can also drop them from the sum. If we want equality to hold, then these values must also be 0, meaning that S^2 cannot take on values beyond α^2. This means that S^2 is either 0 or α.

If that's the case then the values of the cards can only be $-\alpha, 0$, or α, since it is possible for Yiming to get exactly one card. There also cannot exist two cards with value α, since otherwise Yiming could potentially end up with a hand value of $2\alpha \neq \alpha$. Thus, the deck must be of the form $(\alpha, -\alpha, 0, 0, \ldots, 0)$, and we pick $\alpha = \frac{1}{\sqrt{2}}$ to ensure that the sum of squares must be 1.

5 Just One Tail, Please

Let X be some random variable with finite mean and variance which is not necessarily non-negative. The *extended* version of Markov's Inequality states that for a non-negative function $\phi(x)$ which is monotonically increasing for $x > 0$ and some constant $\alpha > 0$,

$$\mathbb{P}(X \geq \alpha) \leq \frac{\mathbb{E}[\phi(X)]}{\phi(\alpha)}$$

Suppose $\mathbb{E}[X] = 0$, $\text{Var}(X) = \sigma^2 < \infty$, and $\alpha > 0$.

(a) Use the extended version of Markov's Inequality stated above with $\phi(x) = (x+c)^2$, where c is some positive constant, to show that:

$$\mathbb{P}(X \geq \alpha) \leq \frac{\sigma^2 + c^2}{(\alpha + c)^2}$$

(b) Note that the above bound applies for all positive c, so we can choose a value of c to minimize the expression, yielding the best possible bound. Find the value for c which will minimize the RHS expression (you may assume that the expression has a unique minimum). Plug in the minimizing value of c to prove the following bound:

$$\mathbb{P}(X \geq \alpha) \leq \frac{\sigma^2}{\alpha^2 + \sigma^2}.$$

(c) Recall that Chebyshev's inequality provides a two-sided bound. That is, it provides a bound on $\mathbb{P}(|X - \mathbb{E}[X]| \geq \alpha) = \mathbb{P}(X \geq \mathbb{E}[X] + \alpha) + \mathbb{P}(X \leq \mathbb{E}[X] - \alpha)$. If we only wanted to bound the probability of one of the tails, e.g. if we wanted to bound $\mathbb{P}(X \geq \mathbb{E}[X] + \alpha)$, it is tempting to just divide the bound we get from Chebyshev's by two. Why is this not always correct in general? Provide an example of a random variable X (does not have to be zero-mean) and a constant α such that using this method (dividing by two to bound one tail) is not correct, that is, $\mathbb{P}(X \geq \mathbb{E}[X] + \alpha) > \frac{\text{Var}(X)}{2\alpha^2}$ or $\mathbb{P}(X \leq \mathbb{E}[X] - \alpha) > \frac{\text{Var}(X)}{2\alpha^2}$.

Now we see the use of the bound proven in part (b) - it allows us to bound just one tail while still taking variance into account, and does not require us to assume any property of the random variable. Note that the bound is also always guaranteed to be less than 1 (and therefore at least somewhat useful), unlike Markov's and Chebyshev's inequality!

(d) Let's try out our new bound on a simple example. Suppose X is a positively-valued random variable with $\mathbb{E}[X] = 3$ and $\text{Var}(X) = 2$. What bound would Markov's inequality give for $\mathbb{P}[X \geq 5]$? What bound would Chebyshev's inequality give for $\mathbb{P}[X \geq 5]$? What about for the bound we proved in part (b)? (*Note*: Recall that the bound from part (b) only applies for zero-mean random variables.)

Solution:

(a) Note that $\sigma^2 = \text{Var}(X) = \mathbb{E}[X^2] - \mathbb{E}[X]^2 = \mathbb{E}[X^2]$. Using the inequality presented in the problem, we have:

$$\mathbb{P}(X \geq \alpha) \leq \frac{\mathbb{E}[(X+c)^2]}{(\alpha+c)^2} = \frac{\mathbb{E}[X^2 + 2cX + c^2]}{(\alpha+c)^2} = \frac{\mathbb{E}[X^2] + 2c\,\mathbb{E}[X] + c^2}{(\alpha+c)^2} = \frac{\sigma^2 + c^2}{(\alpha+c)^2}$$

(b) We set the derivative with respect to c of the above expression equal to 0, and solve for c.

$$\begin{aligned}
\frac{\mathrm{d}}{\mathrm{d}c}\frac{\sigma^2+c^2}{(\alpha+c)^2} &= 0 \\
\frac{2c(\sigma+c)^2-2(\alpha+c)(\sigma^2+c^2)}{(\alpha+c)^4} &= 0 \\
2c(\sigma+c)^2-2(\alpha+c)(\sigma^2+c^2) &= 0 \\
\alpha c^2+(\alpha^2-\sigma^2)c-\sigma^2\alpha &= 0 \\
c &= \frac{\sigma^2}{\alpha}
\end{aligned}$$

To get the last step we use the quadratic equation and take the positive solution. Plugging in this value for c yields us the desired inequality.

This bound is also known as Cantelli's inequality.

(c) It is possible for one of the tails to contain more probability than the other. One example of a random variable which demonstrates this is X, where $\mathbb{P}(X=0)=0.75$ and $\mathbb{P}(X=10)=0.25$, with $\alpha=7$. Here, $\mathbb{E}[X]=2.5$ and $\mathrm{Var}(X)=100\cdot 0.25\cdot 0.75$, so we have:

$$\mathbb{P}(X\geq \mathbb{E}[X]+7)=0.25>\frac{\mathrm{Var}(X)}{2\cdot 7^2}\approx 0.19$$

(d) Using Markov's: $\mathbb{P}(X\geq 5)\leq \frac{\mathbb{E}[X]}{5}=\frac{3}{5}$

Using Chebyshev's: $\mathbb{P}(X\geq 5)\leq \mathbb{P}(|X-\mathbb{E}[X]|\geq 2)\leq \frac{\mathrm{Var}(X)}{2^2}=\frac{1}{2}$

Using bound shown above (Cantelli's):
Since we have the condition that this bound applies to zero-mean random variables, let us define $Y=X-\mathbb{E}[X]=X-3$. Note that $\mathrm{Var}(Y)=\mathrm{Var}(X)$.

Then we get: $\mathbb{P}(X\geq 5)=\mathbb{P}(Y\geq 2)\leq \frac{\mathrm{Var}(Y)}{2^2+\mathrm{Var}(Y)}=\frac{1}{3}$.

We see that Cantelli's inequality (the bound from part (b)) does better than Chebyshev's, which does better than Markov's (note that having a smaller upper bound is better)! This is a good demonstration on how we might derive better bounds using Markov's inequality, if we know further information about the random variable like its variance.

6 Sum of Poisson Variables

Assume that you were given two independent Poisson random variables X_1, X_2. Assume that the first has mean λ_1 and the second has mean λ_2. Prove that X_1+X_2 is a Poisson random variable with mean $\lambda_1+\lambda_2$.

Hint: Recall the binomial theorem.

$$(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}$$

Solution:

To show that $X_1 + X_2$ is a Poisson random variable with mean $\lambda_1 + \lambda_2$, we have show that

$$\mathbb{P}[(X_1 + X_2) = i] = \frac{(\lambda_1 + \lambda_2)^i}{i!} \mathrm{e}^{-(\lambda_1+\lambda_2)}.$$

We proceed as follows:

$$\begin{aligned}
\mathbb{P}[(X_1 + X_2) = i] &= \sum_{k=0}^{i} \mathbb{P}[X_1 = k, X_2 = (i-k)] = \sum_{k=0}^{i} \frac{\lambda_1^k}{k!} \mathrm{e}^{-\lambda_1} \cdot \frac{\lambda_2^{i-k}}{(i-k)!} \mathrm{e}^{-\lambda_2} \\
&= \mathrm{e}^{-\lambda_1} \mathrm{e}^{-\lambda_2} \sum_{k=0}^{i} \frac{1}{k!(i-k)!} \lambda_1^k \lambda_2^{i-k} = \frac{\mathrm{e}^{-\lambda_1} \mathrm{e}^{-\lambda_2}}{i!} \sum_{k=0}^{i} \frac{i!}{k!(i-k)!} \lambda_1^k \lambda_2^{i-k} \\
&= \frac{\mathrm{e}^{-(\lambda_1+\lambda_2)}}{i!} \sum_{k=0}^{i} \binom{i}{k} \lambda_1^k \lambda_2^{i-k} = \frac{\mathrm{e}^{-(\lambda_1+\lambda_2)}}{i!} (\lambda_1 + \lambda_2)^i
\end{aligned}$$

In the last line, we use the binomial expansion.

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 HW 13

1 Random Cuckoo Hashing

Cuckoo birds are parasitic beasts. They are known for hijacking the nests of other bird species and evicting the eggs already inside. Cuckoo hashing is inspired by this behavior. In cuckoo hashing, when we get a collision, the element that was already there gets evicted and rehashed.

We study a simple (but ineffective, as we'll see) version of cuckoo hashing, where all hashes are random. Let's say we want to hash n pieces of data $d_1, d_2, \ldots, d_n$ into n possible hash buckets labeled $1, \ldots, n$. We hash the $d_1, \ldots, d_n$ in that order. When hashing d_i, we assign it a random bucket chosen uniformly from $1, \ldots, n$. If there is no collision, then we place d_i into that bucket. If there is a collision with some other d_j, we evict d_j and assign it another random bucket uniformly from $1, \ldots, n$. (It is possible that d_j gets assigned back to the bucket it was just evicted from!) We again perform the eviction step if we get another collision. We keep doing this until there is no more collision, and we then introduce the next piece of data, d_{i+1} to the hash table.

(a) What is the probability that there are no collisions over the entire process of hashing $d_1, \ldots, d_n$ to buckets $1, \ldots, n$? What value does the probability tend towards as n grows very large?

(b) Assume we have already hashed $d_1, \ldots, d_{n-1}$, and they each occupy their own bucket. We now introduce d_n into our hash table. What is the expected number of collisions that we'll see while hashing d_n? (*Hint*: What happens when we hash d_n and get a collision, so we evict some other d_i and have to hash d_i? Are we at a situation that we've seen before?)

(c) Generalize the previous part: Assume we have already hashed $d_1, \ldots, d_{k-1}$ successully, where $1 \leq k \leq n$. Let C_k be the number of collisions that we'll see while hashing d_k. What is $\mathbb{E}[C_k]$?

(d) Let C be the total number of collisions over the entire process of hashing $d_1, \ldots, d_n$. What is $\mathbb{E}[C]$? You may leave your answer as a summation.

Solution:

(a) When hashing d_i, there are $(n-i+1)$ empty buckets, as $(i-1)$ of them are already occupied by $d_1, \ldots, d_{i-1}$. If we want no collisions over this entire hashing process, we must choose an empty bucket on the first go for each d_i. This gives:

$$\mathbb{P}[\text{no collisions}] = \frac{n}{n} \cdot \frac{n-1}{n} \cdot \ldots \cdot \frac{1}{n} = \frac{n!}{n^n}$$

To understand what happens as n grows very large, we can upper bound the probability as follows:

$$\mathbb{P}[\text{no collisions}] = \frac{n}{n} \cdot \frac{n-1}{n} \cdot \ldots \cdot \frac{1}{n} \leq 1 \cdot \ldots \cdot 1 \cdot \frac{1}{n} = \frac{1}{n}$$

We are upper bounding each term in the product above by 1, except the very last term, which we leave as $\frac{1}{n}$. When n is large, this upper bound goes to 0, so $\mathbb{P}[\text{no collisions}]$ will also tend to 0.

Another way to obtain the $\frac{n!}{n^n}$ probability is to see that considering the first bucket to which each datum gets hashed is a uniform sample space with size n^n. The number of sample points in our event (no collisions) is the number of ways of assigning each datum a unique bucket to be placed in, i.e. the number of ways to permute the datum within the buckets, or $n!$.

(b) Let C_n be the number of collisions experienced when hashing a single datum into a table with $(n-1)$ buckets already populated. (Note that we don't specify that we hash d_n in particular when defining C.)

First, it is possible that we end with 0 collisions. This happens with probability $\frac{1}{n}$. Otherwise, we get a collision, and we have to evict some other datum d_i. Now, we are back in the original situation; the number of collisions experienced after re-hashing d_i is also C because we are again in the situation of introducing a single datum into a table with $(n-1)$ buckets already populated. However, we do need to count the fact that we already had one collision–the one that evicted d_i. This gives us:

$$\mathbb{E}[C_n] = 0 \cdot \frac{1}{n} + (\mathbb{E}[C_n] + 1) \cdot \frac{n-1}{n}$$

Solving for $\mathbb{E}[C_n]$ above, we get an expected $(n-1)$ collisions.

Remark: It is also perfectly valid to use an infinite sum based solution.

(c) We take a similar approach to the previous part. Let C_k be the number of collisions experienced when hashing a single datum into a table with $(k-1)$.

When we hash d_k we have probability $\frac{n-(k-1)}{n}$ of not getting a collision and finishing the process with 0 collisions. Otherwise, we evict some other datum and are left with the same situation. This gives us:

$$\mathbb{E}[C_k] = 0 \cdot \frac{n-k+1}{n} + (\mathbb{E}[C_k] + 1) \cdot \frac{k-1}{n}$$

Solving for $\mathbb{E}[C_k]$ above, we get an expected $\frac{k-1}{n-k+1}$ collisions.

(d) Let C_k be the random variable denoting number of collisions which occur while hashing the k-th datum, d_k. Let C be the total number of collisions which occur over the entire process. That is, $C = C_1 + C_2 + \cdots + C_n$. Then we have:

$$\mathbb{E}[C] = \mathbb{E}\left[\sum_{k=1}^{n} C_k\right] = \sum_{k=1}^{n} \mathbb{E}[C_k] = \sum_{k=1}^{n} \frac{k-1}{n-k+1} = \sum_{k=0}^{n-1} \frac{k}{n-k}$$

The second step uses linearity of expectation, and the third step makes use of the result from the previous part.

2 Geometric and Poisson

Let $X \sim \text{Geo}(p)$ and $Y \sim \text{Poisson}(\lambda)$ be independent. random variables. Compute $\mathbb{P}(X > Y)$. Your final answer should not have summations.

Solution: We condition on Y so we can use the nice property of geometric random variables that $\mathbb{P}(X > k) = (1-p)^k$, this gives

$$\begin{aligned} P(X > Y) &= \sum_{y=0}^{\infty} P(X > Y | Y = y) \cdot P(Y = y) \\ &= \sum_{y=0}^{\infty} (1-p)^y \cdot \frac{e^{-\lambda}\lambda^y}{y!} \\ &= e^{-\lambda p} e^{\lambda p} \sum_{y=0}^{\infty} \frac{e^{-\lambda}(\lambda(1-p))^y}{y!} \\ &= e^{-\lambda p} \sum_{y=0}^{\infty} \frac{e^{-\lambda(1-p)}(\lambda(1-p))^y}{y!} \\ &= e^{-\lambda p} \end{aligned}$$

To simplify the last summation we observed that the sum could be interpreted as the sum of the probabilities for a Poisson$(\lambda(1-p))$ random variable, which is equal to 1.

3 Exploring the Geometric Distribution

Suppose $X \sim \text{Geometric}(p)$ and $Y \sim \text{Geometric}(q)$ are independent. Find the distribution of $\min\{X, Y\}$ and justify your answer.

Solution:

X is the number of coins we flip until we see a heads from flipping a coin with bias p, and Y is the same as flipping a coin with bias q. Imagine we flip the bias p coin and the bias q coin at the same time. The min of the two random variables represents how many simultaneous flips occur before at least one head is seen.

The probability of not seeing a head at all on any given simultaenous flip is $(1-p)(1-q)$, so the probability that there will be a success on any particular trial is $p+q-pq$. Therefore, $\min\{X, Y\} \sim \text{Geometric}(p+q-pq)$.

We can also solve it algebraically. The probability that $\min\{X, Y\} = k$ for some positive integer k is the probability that the first $k-1$ coin flips for both X and Y were tails, then times the probability that we get heads on the k-th toss. Specifically,

$$((1-p)(1-q))^{k-1} \cdot (p+q-pq)$$

We recognize this as the formula for a geometric random variable with parameter $p+q-pq$.

4 Lunch Meeting

Alice and Bob agree to try to meet for lunch between 12 PM and 1 PM at their favorite sushi restaurant. Being extremely busy, they are unable to specify their arrival times exactly, and can say only that each of them will arrive (independently) at a time that is uniformly distributed within the hour. In order to avoid wasting precious time, if the other person is not there when they arrive they agree to wait exactly fifteen minutes before leaving. What is the probability that they will actually meet for lunch? (hint: Sketch the joint distribution of the arrival times of Alice and Bob. What parts of the distribution corresponds to them meeting for lunch?)

Solution:

Let the random variable A be the time that Alice arrives and the random variable B be the time when Bob arrives. Since A and B are both uniformily distributed, it is helpful to vizualize the distributiion graphically. Consider Figure 1, plotting the space of all outcomes (a,b): The arrival

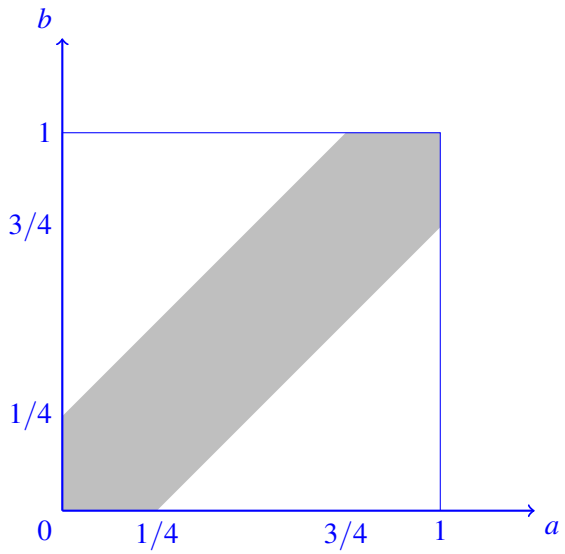


Figure 1: Visualization of joint probability density.

times are uniformily distributed over the box. The shaded region is the set of values (a,b) for which Alice and Bob will actually meet for lunch. Since all points in this square are equally likely, the probably they meet is the ratio of the shaded area to the area of the square. If the area of the square is 1, then the area of the shaded region is

$$1 - 2 \times \left[\frac{1}{2} \times \left(\frac{3}{4}\right)^2\right] = \frac{7}{16},$$

since the area of the white triangle on the upper-left is $(1/2) \cdot (3/4)^2$, and the white triangle on the lower-right has the same area. Therefore, the probability that Alice and Bob actually meet is $7/16$.

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 HW 14

1 Short Answer

(a) Let X be uniform on the interval $[0,2]$, and define $Y = 2X+1$. Find the PDF, CDF, expectation, and variance of Y.

(b) Let X and Y have joint distribution

$$f(x,y) = \begin{cases} cxy + 1/4 & x \in [1,2] \text{ and } y \in [0,2] \\ 0 & \text{else} \end{cases}$$

Find the constant c. Are X and Y independent?

Solution:

(a) Let's begin with the CDF. It will first be useful to recall that

$$F_X(t) = \mathbb{P}(X \le t) = \begin{cases} 0 & t \le 0 \\ \frac{t}{2} & t \in [0,2] \\ 1 & t \ge 1 \end{cases}.$$

Since Y is defined in terms of X, we can compute that

$$\begin{aligned} F_Y[t] = \mathbb{P}(Y \le t) &= \mathbb{P}[2X+1 \le t] \\ &= \mathbb{P}\left[X \le \frac{t-1}{2}\right] \\ &= F_X\left(\frac{t-1}{2}\right) \\ &= \begin{cases} 0 & t \le 1 \\ \frac{t-1}{4} & t \in [1,5] \\ 1 & t \ge 5 \end{cases} \end{aligned}$$

where in the third line we have used the PDF for X. We know that the PDF can be found by taking the derivative of the CDF, so

$$f_Y(t) = \frac{dF_Y(t)}{dt} = \begin{cases} \frac{1}{4} & t \in [1,5] \\ 0 & \text{else} \end{cases}. \tag{1}$$

By linearity of expectation $\mathbb{E}[Y] = \mathbb{E}[2X+1] = 2\,\mathbb{E}[X] + 1 = 3$, and similarly

$$\text{Var}(Y) = \text{Var}(2X+1) = 4\,\text{Var}(X) = 4\frac{4}{12} = \frac{4}{3}$$

(b) To find the correct constant, we use the fact that a PDF must integrate to one. In particular,

$$1 = \int_1^2 \int_0^2 (cxy + 1/4)\, dy\, dx = 3c + 1/2,$$

so $c = 1/6$. In order to check independence, we need to first find the marginal distributions of X and Y:

$$f_X(x) = \int_0^2 f(x,y)\, dy = 1/2 + x/3$$
$$f_Y(y) = \int_1^2 f(x,y)\, dx = 1/4 + y/4.$$

Since $f_X(x) f_Y(y) = 1/8 + y/8 + x/12 + xy/12 \neq 1/4 + xy/6 = f(x,y)$, the random variables are not independent.

2 Continuous Probability Continued

For the following questions, please briefly justify your answers or show your work.

(a) Assume $\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_k$ each hold a fair coin whose two sides show numbers instead of heads and tails, with the numbers on Bob_i's coin being i and $-i$. Each Bob tosses their coin n times and sums up the numbers he sees; let's call this number X_i. For large n, what is the distribution of $(X_1 + \cdots + X_k)/\sqrt{n}$ approximately equal to?

(b) If $X_1, X_2, \ldots$ is a sequence of i.i.d. random variables of mean μ and variance σ^2, what is $\lim_{n\to\infty} \mathbb{P}\left[\sum_{k=1}^n \frac{X_k - \mu}{\sigma n^\alpha} \in [-1,1]\right]$ for $\alpha \in [0,1]$ (your answer may depend on α and Φ, the CDF of a $N(0,1)$ variable)?

Solution:

(a) $\boxed{N\left(0, \sum_{i=1}^k i^2\right)}$.

$(X_1 + \cdots + X_k)/\sqrt{n} = \frac{X_1}{\sqrt{n}} + \cdots + \frac{X_k}{\sqrt{n}}$, and since each $\frac{X_i}{\sqrt{n}}$ converges to $N\left(0, i^2\right)$ by the central limit theorem, their sum must converge to $N\left(0, \sum_{i=1}^k i^2\right)$. Alternatively, if we let X_j^i be the j^{th} coin toss of Bob_i, then $(X_1 + \cdots + X_k)/\sqrt{n} = \frac{1}{\sqrt{n}} \sum_{j=1}^n (X_j^1 + \cdots + X_j^k)$. But the $Y_j = X_j^1 + \ldots X_j^k$ themselves are i.i.d. variables of mean 0 and variance $\sum_{i=1}^k i^2$, and so the central limit theorem again implies a limiting distribution of $N\left(0, \sum_{i=1}^k i^2\right)$ (this constitues an alternative proof of the fact that the sum of Gaussians is also a Gaussian, which we showed in class).

(b) $$\boxed{\lim_{n\to\infty} \mathbb{P}\left[\sum_{k=1}^n \frac{X_k - \mu}{\sigma n^\alpha} \in [-1,1]\right] = \begin{cases} 1, & \text{if } \alpha > \frac{1}{2}, \\ \Phi(1) - \Phi(-1), & \text{if } \alpha = \frac{1}{2}, \\ 0, & \text{if } \alpha < \frac{1}{2} \end{cases}}.$$

For $\alpha > \frac{1}{2}$, the reasoning is exactly as in the law of large numbers: By Chebyshev's inequality, we have $1 - \mathbb{P}\left[\sum_{k=1}^{n} \frac{X_k - \mu}{\sigma n^{\alpha}} \in [-1,1]\right] = \mathbb{P}\left[\sum_{k=1}^{n} \frac{X_k - \mu}{\sigma n^{\alpha}} \notin [-1,1]\right] \leq \frac{1}{n^{2\alpha-1}} \xrightarrow{n\to\infty} 0$. The $\alpha = \frac{1}{2}$ case is a direct consequence of the central limit theorem, while the $\alpha < \frac{1}{2}$ case follows indirectly from it: $\mathbb{P}\left[\sum_{k=1}^{n} \frac{X_k - \mu}{\sigma n^{\alpha}} \in [-1,1]\right] = \mathbb{P}\left[\sum_{k=1}^{n} \frac{X_k - \mu}{\sigma\sqrt{n}} \in \left[-\frac{1}{n^{\frac{1}{2}-\alpha}}, \frac{1}{n^{\frac{1}{2}-\alpha}}\right]\right]$ $\approx \mathbb{P}\left[N(0,1) \in \left[-\frac{1}{n^{\frac{1}{2}-\alpha}}, \frac{1}{n^{\frac{1}{2}-\alpha}}\right]\right] \xrightarrow{n\to\infty} 0$.

3 Exponential Distributions: Lightbulbs

A brand new lightbulb has just been installed in our classroom, and you know the life span of a lightbulb is exponentially distributed with a mean of 50 days.

(a) Suppose an electrician is scheduled to check on the lightbulb in 30 days and replace it if it is broken. What is the probability that the electrician will find the bulb broken?

(b) Suppose the electrician finds the bulb broken and replaces it with a new one. What is the probability that the new bulb will last at least 30 days?

(c) Suppose the electrician finds the bulb in working condition and leaves. What is the probability that the bulb will last at least another 30 days?

Solution:

(a) Let $X \sim \text{Exponential}(1/50)$ be the time until the bulb is broken. For an exponential random variable with parameter λ, the density function is $f_X(x) = \lambda e^{-\lambda x}$ for $x > 0$. So in this case $\lambda = 1/50$. Thus we can integrate the density to find the probability that the lightbulb broke in the first 30 days:

$$\mathbb{P}[X < 30] = \int_0^{30} \left(\frac{1}{50} \cdot e^{-x/50}\right) dx = 1 - e^{-30/50} = 1 - e^{-3/5} \approx 0.451.$$

(b) The new bulb's waiting time Y is i.i.d. with the old bulb's. So the answer is

$$\mathbb{P}[Y > 30] = 1 - \mathbb{P}[Y < 30] = 1 - (1 - e^{-3/5}) = e^{-3/5} \approx 0.549.$$

(c) The bulb is memoryless, so the probability it will last 60 days given that it has lasted 30 days, is just the probability it will last 30 days:

$$\mathbb{P}[X > 60 \mid X > 30] = \mathbb{P}[X - 30 > 30 \mid X > 30] = \mathbb{P}[X > 30] = e^{-3/5} \approx 0.549.$$

4 Useful Uniforms

Let X be a continuous random variable whose image is all of $\mathbb{R}$; that is, $\mathbb{P}[X \in (a,b)] > 0$ for all $a, b \in \mathbb{R}$ and $a \neq b$.

(a) Give an example of a distribution that X could have, and one that it could not.

(b) Show that the CDF F of X is strictly increasing. That is, $F(x+\varepsilon) > F(x)$ for any $\varepsilon > 0$. Argue why this implies that $F : \mathbb{R} \to (0,1)$ must be invertible.

(c) Let U be a uniform random variable on $(0,1)$. What is the distribution of $F^{-1}(U)$?

(d) Your work in part (c) shows that in order to sample X, it is enough to be able to sample U. If X was a discrete random variable instead, taking finitely many values, can we still use U to sample X?

Solution:

(a) Any random variable with density $f(x) > 0$ for all x works as a positive example; e.g. $f(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}$ (corresponding to the normal distribution) or $f(x) = \begin{cases} 1/2, & \text{if } |x| < 1, \\ \frac{1}{4|x|^2}, & \text{if } |x| \geq 1 \end{cases}$.

Any distribution of density f such that $f(x) = 0$ for all $x \in (a,b)$ for some $a, b \in \mathbb{R}, a \neq b$ works as a negative example; e.g. $f(x) = \begin{cases} e^{-x}, & \text{if } x \geq 0, \\ 0, & \text{otherwise} \end{cases}$ (corresponding to an exponential random variable) or $f(x) = \begin{cases} 1, & \text{if } x \in [0,1], \\ 0, & \text{otherwise} \end{cases}$ (corresponding to a uniform variable on $[0,1]$).

(b) $F(x+\varepsilon) = \mathbb{P}[X \leq x+\varepsilon] = \mathbb{P}[X \leq x] + \mathbb{P}[X \in (x, x+\varepsilon]] \geq F(x) + \mathbb{P}[X \in (x, x+\varepsilon)] > F(x)$, where in the very last inequality we used the fact that $\mathbb{P}[X \in (a,b)] > 0$ with $a = x$ and $b = x+\varepsilon$. To show invertibility, we need to show (i) injectivity and (ii) surjectivity. (i): If $x \neq y$, then either $x < y$ or $y < x$ and so either $F(x) < F(y)$ or $F(y) < F(x)$. In either case, $F(x) \neq F(y)$, and so F must be injective. (ii) F is continuous (in fact, differentiable with derivative f), approaching 1 as $x \to \infty$, and approaching 0 as $x \to -\infty$. Therefore, it must assume all values between 0 and 1, and hence is surjective.

(c) $\mathbb{P}\left[F^{-1}(U) \leq x\right] = \mathbb{P}[U \leq F(x)] = F(x)$, where $\{F^{-1}(U) \leq x\} = \{U \leq F(x)\}$ since F is strictly increasing. Thus $F^{-1}(U)$ and X have the very same CDF, which means that $F^{-1}(U)$ and X share the same distribution.

(d) Yes, we can! Assume X took values in a discrete set $\mathscr{A} = \{a_1, a_2, \ldots, a_n\} \subset \mathbb{R}$ with probabilities $\mathbb{P}[X = a_k] = p_k$. Then mimicking the argument from part (c), we can define $G : [0,1] \to \mathscr{A}$

as

$$G(x) = \begin{cases} a_1, & \text{if } x \le p_1, \\ a_2, & \text{if } x \in (p_1, p_1+p_2], \\ a_3, & \text{if } x \in (p_1+p_2, p_1+p_2+p_3], \\ \vdots & \vdots \\ a_{n-1}, & \text{if } x \in (\sum_{k=1}^{n-2} p_k, \sum_{k=1}^{n-1} p_k], \\ a_n, & \text{if } x \in (\sum_{k=1}^{n-1} p_k, 1] \end{cases}$$

(draw a picture of G's graph!), for which we have $\mathbb{P}[G(U) = a_k] = \sum_{j=1}^{k} p_j - \sum_{j=1}^{k-1} p_j = p_k = \mathbb{P}[X = a_k]$. That is, $G(U)$ and X have the same distribution as desired.

5 Uniform Means

To keep the doctor away, Bob goes to the supermarket to buy an apple. Let $X_1, X_2, \ldots, X_n$ be n independent and identically distributed uniform random variables on the interval $[0,1]$ (where n is a positive integer), where X_i is the quality of the ith apple Bob sees.

(a) Let $Y = \min\{X_1, X_2, \ldots, X_n\}$ be the quality of the worst apple Bob will see. Find $\mathbb{E}(Y)$. [*Hint*: Use the tail sum formula, which says the expected value of a nonnegative random variable is $\mathbb{E}(X) = \int_0^\infty \mathbb{P}(X > x)\,dx$. Note that we can use the tail sum formula since $Y \ge 0$.]

(b) Let $Z = \max\{X_1, X_2, \ldots, X_n\}$ be the quality of the best apple Bob will see. Find $\mathbb{E}(Z)$. [*Hint*: Find the CDF.]

Solution:

(a) To calculate $\mathbb{P}(Y > y)$, where $y \in [0,1]$, this means that each X_i is greater than y, for $i = 1, \ldots, n$, so $\mathbb{P}(Y > y) = (1-y)^n$. We then use the tail sum formula:

$$\mathbb{E}(Y) = \int_0^1 \mathbb{P}(Y > y)\,dy = \int_0^1 (1-y)^n\,dy = -\frac{1}{n+1}(1-y)^{n+1}\Big|_0^1 = \frac{1}{n+1}.$$

Alternative Solution 1:
As explained above, $\mathbb{P}[Y \le y] = 1-(1-y)^n$. This gives us the CDF, and if we take its derivative we'll get the probability density function $f(y) = n(1-y)^{n-1}$.

Then

$$\mathbb{E}(Y) = \int_0^1 y \cdot n(1-y)^{n-1}\,dy.$$

Perform a u substitution, where $u = 1-y$ and $du = -dy$. We see:

$$\mathbb{E}(Y) = n \cdot \int_0^1 -(1-u)\cdot u^{n-1}\,du = n \cdot \int_0^1 (u^n - u^{n-1})\,du = n\left[\frac{u^{n+1}}{n+1} - \frac{u^n}{n}\right]_{u=0}^1$$
$$= n\left[\frac{(1-y)^{n+1}}{n+1} - \frac{(1-y)^n}{n}\right]_{y=0}^1 = n\left[0 - \left(\frac{1}{n+1} - \frac{1}{n}\right)\right] = n\left[\frac{1}{n} - \frac{1}{n+1}\right] = \frac{1}{n+1}.$$

Alternative Solution 2:
Consider adding another independent uniform variable X_{n+1}. $\mathbb{P}(X_{n+1} < Y)$ is just the probability that X_{n+1} is the minimum, which is $1/(n+1)$ by symmetry since all the X_i's are identical. It so happens that because X_{n+1} is a uniform variable on [0,1], this probability is equal to $\mathbb{E}(Y)$. Let f_Y denote the PDF of Y.

$$\begin{aligned}
\mathbb{P}(X_{n+1} < Y) &= \int_0^1 \mathbb{P}(X_{n+1} < y \mid Y = y) f_Y(y)\,\mathrm{d}y \\
&= \int_0^1 \mathbb{P}(X_{n+1} < y) f_Y(y)\,\mathrm{d}y && \text{(by independence)} \\
&= \int_0^1 y f_Y(y)\,\mathrm{d}y && \text{(CDF of the uniform distribution)} \\
&= \mathbb{E}(Y).
\end{aligned}$$

Alternative Solution 3:
Since $X_1, \ldots, X_n$ are i.i.d., their values split the interval $[0,1]$ into $n+1$ sections, and we expect these sections to be of equal length because they are uniformly distributed. Therefore, $\mathbb{E}(Y) = 1/(n+1)$, the position of the smallest indicator.

(b) We could use the tail sum formula, but it turns out that the CDF is in a form that makes it easy to take an integral. If $Z \le z$, where $z \in [0,1]$, each X_i must be less than z, which happens with probability z, so $\mathbb{P}[Z \le z] = z^n$. This gives us the CDF, and if we take its derivative we'll get the probability density function $f(z) = nz^{n-1}$. Then

$$\mathbb{E}(Z) = \int_0^1 z \cdot nz^{n-1}\,\mathrm{d}z = \int_0^1 nz^n\,\mathrm{d}z = \left[n \cdot \frac{z^{n+1}}{n+1}\right]_{z=0}^1 = \frac{n}{n+1}.$$

Alternative Solution:
As in the previous part, add another independent uniform random variable X_{n+1}. The probability $\mathbb{P}(X_{n+1} > Z)$ is just the probability that X_{n+1} is the maximum, which is $1/(n+1)$ by symmetry.

$$\begin{aligned}
\mathbb{P}(X_{n+1} > Z) &= \int_0^1 \mathbb{P}(X_{n+1} > z \mid Z = z) f_Z(z)\,\mathrm{d}z = \int_0^1 \mathbb{P}(X_{n+1} > z) f_Z(z)\,\mathrm{d}z \\
&= \int_0^1 (1-z) f_Z(z)\,\mathrm{d}z = \int_0^1 f_Z(z)\,\mathrm{d}z - \int_0^1 z f_Z(z)\,\mathrm{d}z \\
\frac{1}{n+1} &= 1 - \mathbb{E}(Z) \\
\mathbb{E}(Z) &= \frac{n}{n+1}
\end{aligned}$$

Alternative Solution 2:
Since $X_1, \ldots, X_n$ are i.i.d., their values split the interval $[0,1]$ into $n+1$ sections, and we expect these sections to be of equal length because they are uniformly distributed. The expectation of the smallest X_i is $1/(n+1)$, the expectation of the second smallest is $2/(n+1)$, etc. Therefore, $\mathbb{E}(Z) = n/(n+1)$, the position of the largest indicator.

Alternative Solution 3:
Let us define $Y_i = 1 - X_i$. Then, $Z = \max\{X_1, X_2, \ldots, X_n\} = 1 - \min\{Y_1, Y_2, \ldots, Y_n\}$. Observe that, although a function of X_i, the Y_i are also independent and identically distributed uniform random variables over $[0,1]$. Thus, we apply the previous part to find that $\mathbb{E}[\min\{Y_1, Y_2, \ldots, Y_n\}] = 1/n + 1$. As a result,

$$\begin{aligned}\mathbb{E}[Z] &= \mathbb{E}[1 - \min\{Y_1, Y_2, \ldots, Y_n\}] \\ &= 1 = \mathbb{E}[\min\{Y_1, Y_2, \ldots, Y_n\}] \\ &= 1 - \frac{1}{n+1} \\ &= \frac{n}{n+1}\end{aligned}$$

6 Darts but with ML

Suppose Alice and Bob are playing darts on a circular board with radius 1. When Alice throws a dart, the distance of the dart from the center is uniform $[0,1]$. When Bob throws the dart, the location of the dart is uniform over the whole board. Let X be the random variable corresponding to the distance of the player's dart from the center of the board.

(a) What is the pdf of X if Alice throws

(b) What is the pdf of X if Bob throws

(c) Suppose we let Alice throw the dart with probability p, and let Bob throw otherwise. What is the pdf of X (your answer should be in terms of p)?

(d) Using the same premise as in part c, suppose you observe a dart on the board but don't know who threw it. Let x be the dart's distance from the center. We would like to come up with a decision rule to determine whether Alice or Bob is more likely to have thrown the dart given your observation, x. Specifically, if we let A be the event that Alice threw the dart and B be the event that Bob threw, we want to guess A if $\mathbb{P}[A|X \in [x, x+dx]] > \mathbb{P}[B|X \in [x, x+dx]]$ (what do these two probabilities have to sum up to?). For what values of x would we guess A? (your answer should be in terms of p)

Solution:

(a) If Alice threw, then $X \sim U[0,1]$, so it's pdf is $f_{X|A}(x|A) = 1$. Note, the cdf is $\mathbb{P}[X < x|A] = \int_0^x 1 dx = x$, which makes sense because this is exactly the area of a rectangle of length x and height 1.

(b) If Bob throws, then the probability that $X < x$ is equaled to the area of the disc of radius x around the center of the dartboard divided by the area of the dartboard. Thus, we have the cdf

as:

$$\mathbb{P}[X < x|B] = \frac{\pi x^2}{\pi} = x^2$$
$$f_{X|B}(x|B) = \frac{d}{dx}\mathbb{P}[X < x|B] = 2x$$

(c) To find the pdf if X, we can again take the cdf first and take the derivative:

$$\begin{aligned}\mathbb{P}[X < x] &= \mathbb{P}[X < x|A]\mathbb{P}[A] + \mathbb{P}[X < x|B]\mathbb{P}[B] \\ &= px + (1-p)x^2 \\ f_X(x) &= p + 2(1-p)x\end{aligned}$$

(d) Intuitively, we can sketch out the pdfs of both Alice and Bob's throws and we see that Alice is more likely to hit closer to center compared to Bob. Thus it makes sense to say that there is a particular value x^* such that the distance of the dart from the center is less than x^*, then we guess Alice. Otherwise, we guess Bob. Specifically, we can compute with Bayes's rule:

$$\begin{aligned}\mathbb{P}[A|X \in [x, x+dx]] &= \frac{\mathbb{P}[X \in [x, x+dx]|A]\mathbb{P}[A]}{\mathbb{P}[X \in [x, x+dx]]} \\ &= \frac{f_{X|A}(x|A)dx * \mathbb{P}[A]}{f_X(X) * dx} \\ &= \frac{p}{p + 2(1-p)x}\end{aligned}$$

Note that this function is monotonically decreasing in x. In particular, we want to guess Alice if it is more likely that she threw the dart than Bob threw the dart, which means $\mathbb{P}[A|X \in [x, x+dx]] > 1/2$. Thus, we guess Alice if:

$$\begin{aligned}\frac{p}{p + 2(1-p)x} &> \frac{1}{2} \\ 2x(1-p) &< 2p - p \\ x &< \frac{p}{2(1-p)}\end{aligned}$$

Note that if we take $p = 1/2$ and plot out the conditional pdfs of Alice and Bob, we see that Alice's pdf is higher when $x < 1/2$ and Bob's pdf is higher when $x > 1/2$. Incidentally, if we take $p = 1/2$, we see that our decision boundary is exactly 1/2. Thus, the decision boundary corresponds to the point where the two pdfs, after scaling by p and $1-p$, have the same height.

7 Sampling a Gaussian With Uniform

In this question, we will see one way to generate a normal random variable if we have access to a random number generator that outputs numbers between 0 and 1 uniformly at random.

As a general comment, remember that showing two random variables have the same CDF or PDF is sufficient for showing that they have the same distribution.

(a) First, let us see how to generate an exponential random variable with a uniform random variable. Let $U_1 \sim Uniform(0,1)$. Prove that $-\ln U_1 \sim Expo(1)$.

(b) Let $N_1, N_2 \sim \mathcal{N}(0,1)$, where N_1 and N_2 are independent. Prove that $N_1^2 + N_2^2 \sim Expo(1/2)$.

Hint: You may use the fact that over a region R, if we convert to polar coordinates $(x,y) \to (r,\theta)$, then the double integral over the region R will be

$$\iint_R f(x,y)\,dx\,dy = \iint_R f(r\cos\theta, r\sin\theta)\cdot r\,dr\,d\theta.$$

(c) Suppose we have two uniform random variables, U_1 and U_2. How would you transform these two random variables into a normal random variable with mean 0 and variance 1?

Hint: What part (b) tells us is that the point (N_1, N_2) will have a distance from the origin that is distributed as the square root of an exponential distribution. Try to use U_1 to sample the radius, and then use U_2 to sample the angle.

Solution:

(a) The CDF of an exponential $Expo(\lambda)$ distribution is $1 - e^{-\lambda t}$. Let us prove that the $-\ln(U_1)$ also has the same CDF.

We see that

$$\begin{aligned}\mathbb{P}(-\ln(U_1) \le t) &= \mathbb{P}(\ln(U_1) \ge -t)\\ &= \mathbb{P}(U_1 \ge e^{-t})\\ &= 1 - e^{-t}\end{aligned}$$

This shows that $-\ln(U_1)$ has an exponential distribution with $\lambda = 1$.

(b) We compute the CDF of $N_1^2 + N_2^2$. We want the probability that $N_1^2 + N_2^2 \le t$ for some t. This means that we are integrating the joint distribution over a circle of radius $\sqrt{t}$, centered at the origin. We therefore compute the following integral

$$\iint_{(x,y):x^2+y^2\le t} \frac{1}{2\pi} e^{-(x^2+y^2)/2}\,dx\,dy = \int_0^{2\pi}\int_0^{\sqrt{t}} \frac{1}{2\pi} r e^{-r^2/2}\,dr\,d\theta$$

Evaluating this integral yields

$$\int_0^{2\pi} -\frac{e^{-r^2/2}}{2\pi}\bigg|_0^{\sqrt{t}} d\theta = \int_0^{2\pi} \frac{1 - e^{-t/2}}{2\pi}\,d\theta = 1 - e^{-t/2}.$$

This proves that $N_1^2 + N_2^2 \sim Expo(1/2)$.

(c) We will sample the point (N_1, N_2) using uniform random variables U_1 and U_2. We first sample the radius, which we know is an exponential distribution. Therefore, we know that $-2\ln(U_1)$ is an exponential $1/2$ distribution, so $\sqrt{-2\ln(U_1)}$ can be our radius. Since the (N_1, N_2) joint

distribution is rotationally symmetric, we know that we can pick our angle uniformly at random once the radius is determined. Therefore, we let $\theta = 2\pi U_2$.

We will actually arrive at two Gaussians, so we can just take N_1, which will be

$$\boxed{\sqrt{-2\ln(U_1)}\cos(2\pi U_2)}$$

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 HW 15

1 Playing Blackjack

You are playing a game of Blackjack where you start with \$100. You are a particularly risk-loving player who does not believe in leaving the table until you either make \$400, or lose all your money. At each turn you either win \$100 with probability p, or you lose \$100 with probability $1-p$.

(a) Formulate this problem as a Markov chain i.e. define your state space, transition probabilities, and determine your starting state.

(b) Find the probability that you end the game with \$400.

Solution:

(a) Since it is only possible for us to either win or lose \$100, we define the following state space $\chi = \{0, 100, 200, 300, 400\}$. The following are the transition probabilities:

$$\mathbb{P}(0,0) = \mathbb{P}(400,400) = 1$$
$$\mathbb{P}(i, i+100) = p \text{ for } i \in \{100, 200, 300\}$$
$$\mathbb{P}(i, i-100) = 1-p \text{ for } i \in \{100, 200, 300\}$$

(b) We want to find the probability that we are "absorbed" by state 400 before we are absorbed by state 0. We can calculate this probability by leveraging the memoryless property of Markov Chains. Define a_i as the probability of reaching state 400 before 0 starting at state i.

We also know that for $i \in \{100, 200, 300\}$, we have the following relation:

$$a_i = (1-p)a_{i-100} + pa_{i+100} \text{ for } i \in \{100, 200, 300\}$$

We also know that $a_0 = 0$, since if you are at state 0, then there is no chance that you end up at state 400. We also have $a_{400} = 1$ since if we are at state 400, then we have already succeeded in our goal to reach 400.

We have three unknowns $(a_{100}, a_{200}, a_{300})$ and three equations, and we can now solve this

system of equations for a_{100}.

$$a_0 = 0, a_{400} = 1$$
$$\implies a_i = (1-p)a_{i-100} + pa_{i+100} \text{ for } i \in \{100, 200, 300\}$$
$$a_{100} = pa_{200}$$
$$a_{200} = (1-p)a_{100} + pa_{300} \implies a_{200}[1-p(1-p)] = pa_{300}$$
$$\implies a_{200} = \frac{pa_{300}}{1-p(1-p)}$$
$$a_{300} = (1-p)a_{200} + p \implies a_{300} = \frac{(1-p)pa_{300}}{1-p(1-p)} + p$$
$$\implies a_{300} = \frac{p(1-p(1-p))}{1-2p(1-p)}$$
$$\implies a_{200} = \frac{p^2}{1-2p(1-p)}$$
$$\implies a_{100} = \frac{p^3}{1-2p(1-p)}$$

This problem is called Gambler's Ruin, where it is used to show that even if p is decently large, after playing a large number of games without stopping, you will end up at 0 dollars with high probability. Let's look at a nicer way to solve the recurrence relation that gives a somewhat more insightful answer to the problem.

Suppose we have states 0 through N, and you start at state k. You go up a state with probability p and go down with probability $1-p$. You win if you end up at state N, and lose if you end up at state 0.

Again, we can write the recurrence relation as

$$a_i = pa_{i+1} + (1-p)a_{i-1}$$

for $1 \leq i \leq N-1$. We also know that $a_N = 1$ and $a_0 = 0$. We can rewrite the recurrence relation into the following form:

$$(1-p)(a_i - a_{i-1}) = p(a_{i+1} - a_i) \Rightarrow a_{i+1} - a_i = \frac{1-p}{p}(a_i - a_{i-1})$$

Define $w = \frac{1-p}{p}$, which is often called the odds ratio, and define $b_i = a_{i+1} - a_i$. Note that this tells us $a_i = b_0 + b_1 + \cdots + b_{i-1}$. So, the recurrence we have derived is $b_i = w \cdot b_{i-1}$. This tells us that $b_i = w^i b_0$, and

$$a_i = b_0 + \cdots + b_{i-1} = (1 + w + w^2 + \cdots + w^{i-1})b_0$$

What is b_0? We can now use our information that $a_N = 1$, to see that $b_0 = \frac{1}{1+w+w^2+\cdots+w^{N-1}}$. Thus, we finally see that

$$a_i = \frac{1 + w + w^2 + \cdots + w^{i-1}}{1 + w + w^2 + \cdots + w^{N-1}} = \frac{w^i - 1}{w^N - 1}$$

where we used the geometric series formula in the last step: $1 + w + w^2 + \cdots + w^{i-1} = \frac{w^i - 1}{w-1}$. Note that the formula only works if $w \neq 1$.

By the way, if you are interested in how to derive the geometric series, first write it like this:

$$S = 1 + w + w^2 + \cdots + w^{i-1}$$

multiply both sides by w, to get

$$wS = w + w^2 + \cdots + w^i$$

and subtracting these two equations will cancel most of the terms! We get:

$$(w-1)S = w^i - 1$$

solving for S yields $\frac{w^i - 1}{w-1}$.

2 Markov's Coupon Collecting

Courtney is home for Thanksgiving and needs to make some trips to the Traitor Goes grocery store to prepare for the big turkey feast. Each time she goes to the store before the holiday, she receives one of the n different coupons that are being given away. You may recall that we studied how to calculate the expected number of trips to the store needed to collect at least one of each coupon. Using geometric distributions and indicator variables, we determined that expected number of trips to be $n(\ln n + \gamma)$.

Let's re-derive that, this time with a Markov chain model and first-step equations.

(a) Define the states and transition probabilities for each state (explain what states can be transitioned to, and what probabilities those transitions occur with).

(b) Now set up first-step equations and solve for the expected number of grocery store trips Courtney needs to make before Thanksgiving so that she can have at least one of each of the n distinct coupons.

Solution:

(a) We model the coupon collector's problem as a Markov chain with states $X_1, X_2, \ldots, X_n, X_{n+1}$ where X_i represents the state we are at if we have collected $i-1$ of the unique coupons and are seeking the i^{th} coupon. State X_{n+1} represents the terminal state, after we successfully collected all n coupons and don't need to make any more grocery store trips.

If we are at state X_i, we either transition back to X_i with probability $(i-1)/n$, or we collect a new coupon and transition to state X_{i+1} with probability $(n-i+1)/n$. Transitioning to any other state is not possible.

(b) For each state X_i:

$$\begin{aligned}
\beta(X_i) &= 1 + \frac{i-1}{n} \cdot \beta(X_i) + \frac{n-i+1}{n} \cdot \beta(X_{i+1}) \\
\frac{n-i+1}{n} \cdot \beta(X_i) &= 1 + \frac{n-i+1}{n} \cdot \beta(X_{i+1}) \\
\beta(X_i) &= \frac{n}{n-i+1} + \beta(X_{i+1})
\end{aligned}$$

We know that for the terminal state, $\beta(X_{n+1}) = 0$. Then:

$$\begin{aligned}
\beta(X_n) &= n \\
\beta(X_{n-1}) &= n + \frac{n}{2} \\
&\vdots \\
\beta X_1 &= n + \frac{n}{2} + \cdots + \frac{n}{n} \\
&= n \sum_{i=1}^{n} \frac{1}{i} \\
&= n(\ln n + \gamma).
\end{aligned}$$

3 Reflecting Random Walk

Alice starts at vertex 0 and wishes to get to vertex n. When she is at vertex 0 she has a probability of 1 of transitioning to vertex 1. For any other vertex i, there is a probability of $1/2$ of transitioning to $i+1$ and a probability of $1/2$ of transitioning to $i-1$.

(a) What is the expected number of steps Alice takes to reach vertex n? Write down the hitting-time equations, but do not solve them yet.

(b) Solve the hitting-time equations. [*Hint*: Let R_i denote the expected number of steps to reach vertex n starting from vertex i. As a suggestion, try writing R_0 in terms of R_1; then, use this to express R_1 in terms of R_2; and then use this to express R_2 in terms of R_3, and so on. See if you can notice a pattern.]

Solution:

Formulate hitting time equations; the hard part is solving them. R_i represents the expected number of steps to get to vertex n starting from vertex i. In particular, $R_n = 0$ and we are interested in

calculating R_0. We have the equations:

$$\begin{aligned}
R_0 &= 1 + R_1, \\
R_1 &= 1 + \frac{1}{2}R_0 + \frac{1}{2}R_2, \\
&\vdots \\
R_i &= 1 + \frac{1}{2}R_{i-1} + \frac{1}{2}R_{i+1}, \\
&\vdots \\
R_{n-1} &= 1 + \frac{1}{2}R_{n-2} + \frac{1}{2}R_n.
\end{aligned}$$

We can write this in terms of the differences $D_i := R_{i+1} - R_i$. If we take the recurrence relation $R_i = 1 + \frac{1}{2}R_{i-1} + \frac{1}{2}R_{i+1}$, we can rearrange the equation:

$$\begin{aligned}
R_i &= 1 + \frac{1}{2}R_{i-1} + \frac{1}{2}R_{i+1} \\
2R_i &= 2 + R_{i-1} + R_{i+1} \\
R_i - R_{i-1} - 2 &= R_{i+1} - R_i \\
D_{i-1} - 2 &= D_i
\end{aligned}$$

Furthermore, we know that $D_0 := R_1 - R_0 = -1$ from the very first hitting time equation. Since we have shown that D_i decreases by 2 every time, we know that $D_i = -2i - 1$. How do we get back R_i from knowing D_i? Well, we see that

$$R_i = (R_i - R_{i-1}) + (R_{i-1} - R_{i-2}) + \cdots + (R_1 - R_0) + R_0 = D_{i-1} + D_{i-2} + \cdots + D_0 + R_0$$

Therefore, we have $R_i = -1 - 3 - 5 - \cdots - (2i-1) + R_0$. What is the sum of the first i odd integers? Here is how you would derive it. Let $S = 1 + 3 + 5 + \cdots + (2i-1)$. Then, we can also write S backwards, as $S = (2i-1) + (2i-3) + \cdots + 5 + 3 + 1$. Lining up the terms, we see:

$$\begin{aligned}
S &= 1 &&+ 3 &&+ \cdots + (2i-3) + (2i-1) \\
S &= (2i-1) + (2i-3) + \cdots + 3 &&+ 1
\end{aligned}$$

Adding these together gives us $2S = 2i + 2i + 2i + \cdots + 2i = 2i^2$. Solving for S yields $S = i^2$.

Now that we know this fact, we see that $R_i = R_0 - i^2$. Since we know that $R_n = 0$, we see that $R_0 - n^2 = 0$, and thus $R_0 = n^2$.

4 Boba in a Straw

Imagine that Jonathan is drinking milk tea and he has a very short straw: it has enough room to fit two boba (see figure).

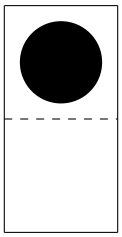


Figure 1: A straw with one boba currently inside. The straw only has enough room to fit two boba.

Here is a formal description of the drinking process: We model the straw as having two "components" (the top component and the bottom component). At any given time, a component can contain nothing, or one boba. As Jonathan drinks from the straw, the following happens every second:

1. The contents of the top component enter Jonathan's mouth.
2. The contents of the bottom component move to the top component.
3. With probability p, a new boba enters the bottom component; otherwise the bottom component is now empty.

Help Jonathan evaluate the consequences of his incessant drinking!

(a) At the very start, the straw starts off completely empty. What is the expected number of seconds that elapse before the straw is completely filled with boba for the first time? [Write down the equations; you do not have to solve them.]

(b) Consider a slight variant of the previous part: now the straw is narrower at the bottom than at the top. This affects the drinking speed: if either (i) a new boba is about to enter the bottom component or (ii) a boba from the bottom component is about to move to the top component, then the action takes two seconds. If both (i) and (ii) are about to happen, then the action takes three seconds. Otherwise, the action takes one second. Under these conditions, answer the previous part again. [Write down the equations; you do not have to solve them.]

(c) Jonathan was annoyed by the straw so he bought a fresh new straw (the straw is no longer narrow at the bottom). What is the long-run average rate of Jonathan's calorie consumption? (Each boba is roughly 10 calories.)

(d) What is the long-run average number of boba which can be found inside the straw? [Maybe you should first think about the long-run distribution of the number of boba.]

Solution:

(a) We model the straw as a four-state Markov chain. The states are $\{(0,0),(0,1),(1,0),(1,1)\}$, where the first component of a state represents whether the top component is empty (0) or full

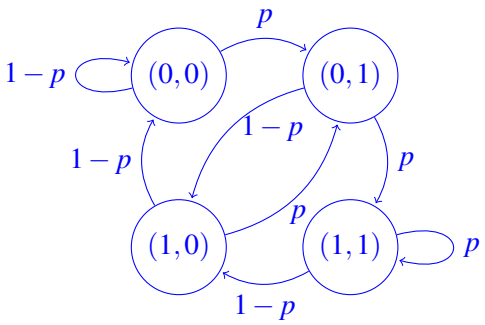


Figure 2: Transition diagram for the Markov chain.

(1); similarly, the second component represents whether the bottom component is empty or full. See Figure **??**.

Now, we set up the hitting time equations. Let T denote the time it takes to reach state $(1,1)$, i.e. $T = \min\{n > 0 : X_n = (1,1)\}$. Let $\mathbb{E}_i[\cdot] = \mathbb{E}[\cdot \mid X_0 = i]$ denote the expectation starting from state i (for convenience of notation). The hitting-time equations are

$$\begin{aligned}
\mathbb{E}_{(0,0)}[T] &= 1 + (1-p)\,\mathbb{E}_{(0,0)}[T] + p\,\mathbb{E}_{(0,1)}[T],\\
\mathbb{E}_{(0,1)}[T] &= 1 + (1-p)\,\mathbb{E}_{(1,0)}[T] + p\,\mathbb{E}_{(1,1)}[T],\\
\mathbb{E}_{(1,0)}[T] &= 1 + (1-p)\,\mathbb{E}_{(0,0)}[T] + p\,\mathbb{E}_{(0,1)}[T],\\
\mathbb{E}_{(1,1)}[T] &= 0.
\end{aligned}$$

The question did not ask you to solve the equations. If you solved the equations anyway and would like to check your work, the hitting time is $\mathbb{E}_{(0,0)}[T] = (1+p)/p^2$.

(b) The new hitting-time equations are

$$\begin{aligned}
\mathbb{E}_{(0,0)}[T] &= (1-p)(1 + \mathbb{E}_{(0,0)}[T]) + p(2 + \mathbb{E}_{(0,1)}[T]),\\
\mathbb{E}_{(0,1)}[T] &= (1-p)(2 + \mathbb{E}_{(1,0)}[T]) + p(3 + \mathbb{E}_{(1,1)}[T]),\\
\mathbb{E}_{(1,0)}[T] &= (1-p)(1 + \mathbb{E}_{(0,0)}[T]) + p(2 + \mathbb{E}_{(0,1)}[T]),\\
\mathbb{E}_{(1,1)}[T] &= 0.
\end{aligned}$$

You did not have to solve the equations, but to get a sense for what the solution is like, solving the equations and plugging in $p = 1/2$ yields (after some tedious algebra) $\mathbb{E}_{(0,0)}[T] = 11$.

(c) This part is actually more straightforward than it might initially seem: the average rate at which Jonathan consumes boba must equal the average rate at which boba enters the straw, which is p per second. Hence, his long-run average calorie consumption rate is $10p$ per second.

(d) We compute the stationary distribution. The balance equations are

$$\begin{aligned}
\pi(0,0) &= (1-p)\pi(0,0) + (1-p)\pi(1,0),\\
\pi(0,1) &= p\pi(0,0) + p\pi(1,0),\\
\pi(1,0) &= (1-p)\pi(0,1) + (1-p)\pi(1,1),\\
\pi(1,1) &= p\pi(0,1) + p\pi(1,1).
\end{aligned}$$

Expressing everything in terms of $\pi(0,0)$, we find

$$\pi(0,1) = \pi(1,0) = \frac{p}{1-p}\pi(0,0),$$
$$\pi(1,1) = \frac{p^2}{(1-p)^2}\pi(0,0).$$

From the normalization condition we have

$$\pi(0,0)\left(1 + \frac{2p}{1-p} + \frac{p^2}{(1-p)^2}\right) = 1,$$

so $\pi(0,0) = (1-p)^2$. Hence, the stationary distribution is

$$\pi(0,0) = (1-p)^2,$$
$$\pi(0,1) = \pi(1,0) = p(1-p),$$
$$\pi(1,1) = p^2.$$

In states $(0,1)$ and $(1,0)$, there is one boba in the straw; in state $(1,1)$, there are two boba in the straw. Therefore, the long-run average number of boba in the straw is

$$\pi(0,1) + \pi(1,0) + 2\pi(1,1) = 2p(1-p) + 2p^2 = 2p.$$

Alternate Solution: The goal of the question was to have you work through the balance equations, but there is a simple solution. Observe that at any given time after at least two seconds have passed, each component has probability p of being filled with boba. Therefore, the number of boba in the straw is like a binomial distribution with 2 independent trials and success probability p, so the average number of boba in the straw is $2p$.