CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 00

1 Administrivia

(a) Make sure you are on the course Ed (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 breakdown of how your grade is calculated, for both the homework and the no-homework option?

(ii) What is the attendance policy for discussions?

(iii) When are homeworks released and when are they due?

(iv) How many "drops" do you get for homeworks? How many mini-vitamins will contribute to your grade?

(v) When is the midterm? When is the final?

(vi) What percentage score is needed to earn full credit on a homework?

Solution:

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

(b) (i) For HW option: Discussion Attendance: 5%, Mini-vitamins: 5%, Homework: 20%, Midterm: 25%, Final: 45%.
For no HW option: Discussion Attendance: 5%, Mini-vitamins: 5%, Midterm: 32%, Final: 58%.

(ii) You will receive 1 attendance point for every discussion, and will need at least 13 points in order to receive full credit for discussion attendance. You are welcome to attend other discussion sections, but your attendance will only be counted for the section you are actually assigned.

(iii) The homework for the current week is released on Gradescope on Sunday. The homework is due on Gradescope the following Saturday at 4:00 PM (grace period until 6:00 PM); the solutions for that homework will be released on Monday, a day after the release of the new homework.

(iv) You can drop the lowest lowest 3 homeworks the entire semester, and the top 13 mini vitamins will count for a grade. However, please save these drops for emergencies. We do not have the bandwidth to make personalized exceptions to this rule.

(v) Midterm Date: 3/6/24 Wednesday 7-9pm, Final Date: 5/10/24 Friday 7-10pm

(vi) 73%.

2 Course Policies

Go to the course website and read the course policies carefully. Leave a followup on Ed 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 Ed or Office Hours.

3 Use of Ed

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

(a) Read the Ed 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.)

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

(c) If you have a question or concern not directly related to the course content, where should you direct it?

Solution:

(a) 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 Ed 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?”

(b) The weekly posts are released every Monday. They’re required reading.

(c) Please send an email to sp24@eecs70.org.

4 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.

5 Propositional Practice

Note 1

In parts (a)-(b), convert the English sentences into propositional logic. In parts (c) - (d), convert the propositions into English. For parts (b) and (d), use the notation $a \mid b$ to denote the statement "a divides b", and use the notation $P(x)$ to denote the statement "x is a prime number".

(a) For every real number k, there is a unique real solution to $x^3 = k$.

(b) If p is a prime number, then for any two natural numbers a and b, if p doesn't divide a and p divides ab, then p divides b.

(c) $(\forall x, y \in \mathbb{R})\,[(xy = 0) \implies ((x = 0) \vee (y = 0))]$

(d) $\neg((\exists y \in \mathbb{N})\,[(\forall x \in \mathbb{N})\,[(x > y) \implies ((y \mid x) \vee P(x))]])$

Solution:

(a) The trickiest part of this problem is the word 'unique'. We can express the existence of a unique solution in propositional logic with two statements connected with an 'and': (1) A solution exists, and (2) Any two solutions have to be the same. Hence, we can rewrite this statement as "For every real number k, there exists a real number x such that $x^3 = k$ and for all reals y and z, if both $y^3 = k$ and $z^3 = k$, then $y = z$." This, in propositional logic, is below:

$$(\forall k \in \mathbb{R})\left[(\exists x \in \mathbb{R})(x^3 = k) \wedge (\forall y, z \in \mathbb{R})(((y^3 = k) \wedge (z^3 = k)) \implies (y = z))\right].$$

(b) This sentence can be written in propositional logic as

$$(\forall p \in \mathbb{N})\,[(P(p)) \implies ((\forall a, b \in \mathbb{N})\,[((p \mid ab) \wedge \neg(p \mid a)) \implies (p \mid b)])].$$

(c) If the product of two real numbers is 0, then one of them must be 0.

(d) There is no natural number that divides every composite number greater than it.

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 01

1 Logical Equivalence?

Note 1

Decide whether each of the following logical equivalences is correct and justify your answer.

(a) $\forall x\ (P(x) \wedge Q(x)) \stackrel{?}{\equiv} \forall x\, P(x) \wedge \forall x\, Q(x)$

(b) $\forall x\ (P(x) \vee Q(x)) \stackrel{?}{\equiv} \forall x\, P(x) \vee \forall x\, Q(x)$

(c) $\exists x\ (P(x) \vee Q(x)) \stackrel{?}{\equiv} \exists x\, P(x) \vee \exists x\, Q(x)$

(d) $\exists x\ (P(x) \wedge Q(x)) \stackrel{?}{\equiv} \exists x\, P(x) \wedge \exists x\, Q(x)$

Solution:

(a) **Correct**.

Assume that the left hand side is true. Then we know for an arbitrary x $P(x) \wedge Q(x)$ is true. This means that both $\forall x P(x)$ and $\forall x Q(x)$. Therefore the right hand side is true. Now for the other direction assume that the right hand side is true. Since for any x $P(x)$ and for any y $Q(y)$ holds, then for an arbitrary x both $P(x)$ and $Q(x)$ must be true. Thus the left hand side is true.

(b) **Incorrect**.

Note that there are many possible counterexamples not described here.

Suppose that the universe (i.e. the values that x can take on) is $\{1,2\}$ and that P and Q are truth functions defined on this universe. If we set $P(1)$ to be true, $Q(1)$ to be false, $P(2)$ to be false and $Q(2)$ to be true, the left-hand side will be true, but the right-hand side will be false. Hence, we can find a universe and truth functions P and Q for which these two expressions have different values, so they must be different.

Another more concrete example is if $P(x) = x < 0$ and $Q(x) = x \geq 0$, where the universe is the real numbers. For any $x \in \mathbb{R}$, exactly one of $P(x)$ or $Q(x)$ is true, but it is not the case that $P(x)$ holds for every x, and it is also not the case that $Q(x)$ holds for every x. Since the LHS and RHS have different values, the two sides are not equivalent.

(c) **Correct**

Assuming that the left hand side is true, we know there exists some x such that one of $P(x)$ and $Q(x)$ is true. Thus $\exists x P(x)$ or $\exists x Q(x)$ and the right hand side is true. To prove the other direction, assume the left hand side is false. Then there does not exists an x for which $P(x) \vee$

$Q(x)$ is true, which means there is no x for which $P(x)$ or $Q(x)$ is true. Therefore the right hand side is false.

(d) **Incorrect**.

Note, there are many possible counterexamples not described here.

Suppose that the universe (i.e. the values that x can take on) is the natural numbers $\mathbb{N}$, and that P and Q are truth functions defined on this universe. Here, suppose we set $P(1)$ to be true and $P(x)$ to be false for all other x, and $Q(2)$ to be true and $Q(x)$ to be false for all other x. (In other words, $P(x) = (x = 1)$ and $Q(x) = (x = 2)$.)

With these definitions, the right hand side would be true, since there exists some value of x that makes $P(x)$ true (namely, $x = 1$), and there exists some value of x that makes $Q(x)$ true (namely, $x = 2$). However, there would be no value of x at which both $P(x)$ and $Q(x)$ would be simultaneously true, so the left hand side would be false. Hence, we can find a universe and truth functions P and Q for which these two expressions have different values, so they must be different.

2 Prove or Disprove

Note 2

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)

(e) The product of a non-zero rational number and an irrational number is irrational.

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. This means that we have

$$\begin{aligned} n^2 + 4n &= (2k+1)^2 + 4(2k+1) \\ &= 4k^2 + 12k + 5 \\ &= 2(2k^2 + 6k + 2) + 1 \end{aligned}$$

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 $\neg(a \leq 11 \vee b \leq 4)$). 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 show a counterexample. Let $n = 7$. Here, $5 \cdot 7^3 = 1715$, but $7! = 5040$. Since $5n^3 < n!$, the claim is false.

A counterexample that is easier to see without much calculation is for a much larger number like $n = 100$; here, $100!$ is clearly more than $5 \cdot 100^3 = 100 \cdot 50 \cdot 25 \cdot 5 \cdot 4 \cdot 2$, since the latter product contains only a subset of the terms in $100!$. □

(e) **Answer**: True.

Proof. We prove the statement by contradiction. Suppose that $ab = c$, where $a \neq 0$ is rational, b is irrational, and c is rational. Since a and b are not zero (because 0 is rational), c is also non-zero. Thus, we can express $a = \frac{p}{q}$ and $c = \frac{r}{s}$, where p, q, r, and s are nonzero integers. Then

$$b = \frac{c}{a} = \frac{rq}{ps},$$

which is the ratio of two nonzero integers, giving that b is rational. This contradicts our initial assumption, so we conclude that the product of a nonzero rational number and an irrational number is irrational. □

3 Twin Primes

Note 2

(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.

4 Airport

Note 3

Suppose that there are $2n+1$ airports, where n is a positive integer. The distances between any two airports are all different. For each airport, exactly one airplane departs from it and is destined for the closest airport. Prove by induction that there is an airport which has no airplanes destined for it.

Solution: We proceed by induction on n. For $n = 1$, let the 3 airports be A, B, C and without loss of generality suppose B, C is the closest pair of airports (which is well defined since all distances are different). Then the airplanes departing from B and C are flying towards each other. Since the airplane from A must fly to somewhere else, no airplanes are destined for airport A.

Now suppose the statement holds for $n = k$, i.e. when there are $2k+1$ airports. For $n = k+1$, i.e. when there are $2k+3$ airports, the airplanes departing from the closest two airports (say X and Y) must be destined for each other's starting airports. Removing these two airports reduce the problem to $2k+1$ airports.

From the inductive hypothesis, we know that among the $2k+1$ airports remaining, there is an airport with no incoming flights which we call airport Z. When we add back the two airports that we removed, there are two scenarios:

- Some of the flights get remapped to X or Y.
- None of the flights get remapped.

In either scenario, we conclude that the airport Z will continue to have no incoming flights when we add back the two airports, and so the statement holds for $n = k+1$. By induction, the claim holds for all $n \geq 1$.

5 A Coin Game

Note 3

Your "friend" Stanley Ford suggests you play the following game with him. You each start with a single stack of n coins. On each of your turns, you select one of your stacks of coins (that has at least two coins) and split it into two stacks, each with at least one coin. Your score for that turn is the product of the sizes of the two resulting stacks (for example, if you split a stack of 5 coins into a stack of 3 coins and a stack of 2 coins, your score would be $3 \cdot 2 = 6$). You continue taking turns until all your stacks have only one coin in them. Stan then plays the same game with his stack of n coins, and whoever ends up with the largest total score over all their turns wins.

Prove that no matter how you choose to split the stacks, your total score will always be $\frac{n(n-1)}{2}$. (This means that you and Stan will end up with the same score no matter what happens, so the game is rather pointless.)

Solution:

We can prove this by strong induction on n.

Base Case: If $n = 1$, you start with a stack of one coin, so the game immediately terminates. Your total score is zero–and indeed, $\frac{n(n-1)}{2} = \frac{1 \cdot 0}{2} = 0$.

Inductive Step: Suppose that if you start with i coins (for i between 1 and n inclusive), your score will be $\frac{i(i-1)}{2}$ no matter what strategy you employ. Now suppose you start with $n+1$ coins. In your first move, you must split your stack into two smaller stacks. Call the sizes of these stacks s_1 and s_2 (so $s_1 + s_2 = n+1$ and $s_1, s_2 \geq 1$). Your end score comes from three sources: the points you get from making this first split, the points you get from future splits involving coins from stack 1, and the points you get from future splits involving coins from stack 2. From the rules of the game, we know you get $s_1 s_2$ points from the first split. From the inductive hypothesis (which we can apply because s_1 and s_2 are between 1 and n), we know that the total number of points you get from future splits of stack 1 is $\frac{s_1(s_1-1)}{2}$ and similarly that the total number of points you get from future splits of stack 2 is $\frac{s_2(s_2-1)}{2}$, regardless of what strategy you employ in splitting them. Thus, the total number of points we score is

$$\begin{aligned} s_1 s_2 + \frac{s_1(s_1-1)}{2} + \frac{s_2(s_2-1)}{2} &= \frac{s_1(s_1-1) + 2s_1 s_2 + s_2(s_2-1)}{2} \\ &= \frac{\big(s_1(s_1-1) + s_1 s_2\big) + \big(s_2(s_2-1) + s_1 s_2\big)}{2} \\ &= \frac{s_1(s_1+s_2-1) + s_2(s_1+s_2-1)}{2} \\ &= \frac{(s_1+s_2)(s_1+s_2-1)}{2} \end{aligned}$$

Since $s_1 + s_2 = n+1$, this works out to $\frac{(n+1)(n+1-1)}{2}$, which is what we wanted to show your total number of points came out to. This completes our proof by induction.

6 Grid Induction

Note 3

Pacman is walking on an infinite 2D grid. He starts at some location $(i, j) \in \mathbb{N}^2$ in the first quadrant, and is constrained to stay in the first quadrant (say, by walls along the x and y axes).

Every second he does one of the following (if possible):

(i) Walk one step down, to $(i, j-1)$.

(ii) Walk one step left, to $(i-1, j)$.

For example, if he is at $(5,0)$, his only option is to walk left 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 in the number of steps he takes? Try to use this to strengthen the inductive hypothesis.)

Solution: On first glance, this problem seems quite tricky, since we'd want to induct on *two* variables (i and j) rather than just one variable (as we've seen most commonly). However, following the hint, if we try out some smaller cases, we can notice that it takes Pacman $i+j$ seconds to reach $(0,0)$ if he starts in position (i, j), regardless 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.

This means that the quantity $i+j$ is something we could instead focus on, rather than the coordinate (i, j). In particular, we can try to induct on $i+j$ (essentially inducting on the amount of time it takes for Pacman to reach $(0,0)$), rather than inducting on i and j separately.

Proof. **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 finite time 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 a finite amount of time 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 a finite amount of time to get to $(0,0)$ no matter what path he takes. Thus, in either case, we have that Pacman will take a finite amount of time (one second for the first move and some additional finite time for the remainder) in order to reach $(0,0)$, proving the claim for $n+1$. □

Note that once we had observed that it seems to take exactly $i+j$ seconds for Pacman to reach $(0,0)$ from (i, j), we could have tried to prove this stronger claim. This is equivalent to the above proof, with the only difference being the more specific length of time used in the inductive hypothesis; all other steps are identical.

One can also prove this statement without this trick inducting on $i+j$. 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.

Proof. **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.

Proof. **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 down, we can immediately apply the inductive hypothesis, since Pacman will be in position (i,n). However, if Pacman moves to the left, 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 left forever: after i such moves, he'll hit the wall on the y-axis and be forced to move down. 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 left, one second making his first move down, 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 $i \in \mathbb{N}$. □

7 (Optional) Calculus Review

In the probability section of this course, you will be expected to compute derivatives, integrals, and double integrals. This question contains a couple examples of the kinds of calculus you will encounter.

(a) Compute the following integral:

$$\int_0^\infty \sin(t)e^{-t}\,\mathrm{d}t\,.$$

(b) Compute the values of $x \in (-2,2)$ that correspond to local maxima and minima of the function

$$f(x) = \int_0^{x^2} t\cos\left(\sqrt{t}\right)\mathrm{d}t\,.$$

Classify which x correspond to local maxima and which to local minima.

(c) Compute the double integral

$$\iint_R 2x + y\,\mathrm{d}A\,,$$

where R is the region bounded by the lines $x = 1$, $y = 0$, and $y = x$.

Solution:

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

$$\begin{aligned} I = \int \sin(t)e^{-t}\,\mathrm{d}t &= uv - \int v\cdot\mathrm{d}u \\ &= -\sin(t)e^{-t} + \int e^{-t}\cos(t)\,\mathrm{d}t \end{aligned}$$

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

$$\begin{aligned} \int e^{-t}\cos(t)\,\mathrm{d}t &= uv - \int v\cdot\mathrm{d}u \\ &= -\cos(t)e^{-t} - \int e^{-t}\cdot\sin(t)\,\mathrm{d}t \\ &= -\cos(t)e^{-t} - I \end{aligned}$$

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:

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

(b) Compute the derivative of the function, and set it equal to 0. Let $y = x^2$. By the Chain Rule and the Fundamental Theorem of Calculus,

$$\begin{aligned}\frac{\mathrm{d}f}{\mathrm{d}x} &= \frac{\mathrm{d}f}{\mathrm{d}y} \cdot \frac{\mathrm{d}y}{\mathrm{d}x} \\ &= y\cos(\sqrt{y}) \cdot 2x \\ &= 2x^3 \cos(|x|) \\ &= 2x^3 \cos(x) = 0\end{aligned}$$

We get that the derivative is 0 only when $x^* = 0$, or when $\cos(x^*) = 0$. On the interval $(-2,2)$, this corresponds to critical points $-\pi/2, 0$, and $\pi/2$.

To classify which correspond to local maxima and which to local minima, we examine how the sign of the derivative changes.

Around $x = \pi/2$, the derivative is positive for $x < \pi/2$ and negative for $x > \pi/2$. The same holds for $x = -\pi/2$. Thus, $x = \pm\pi/2$ correspond to local maxima.

Around $x = 0$, the derivative is negative for $x < 0$ and positive for $x > 0$. Thus, $x = 0$ corresponds to a local minima.

(c) We may set up the integral over the region R as follows:

$$\int_0^1 \int_0^x 2x + y \,\mathrm{d}y \,\mathrm{d}x.$$

Evaluating this integral gives

$$\begin{aligned}\int_0^1 \int_0^x 2x + y \,\mathrm{d}y \,\mathrm{d}x &= \int_0^1 2xy + \frac{y^2}{2}\Big|_0^x \,\mathrm{d}x \\ &= \int_0^1 \frac{5x^2}{2} \,\mathrm{d}x \\ &= \frac{5x^3}{6}\Big|_0^1 \\ &= \frac{5}{6}.\end{aligned}$$

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 02

1 Universal Preference

Note 4

Suppose that preferences in a stable matching instance are universal: all n jobs share the preferences $C_1 > C_2 > \cdots > C_n$ and all candidates share the preferences $J_1 > J_2 > \cdots > J_n$.

(a) What pairing do we get from running the algorithm with jobs proposing? Can you prove this happens for all n?

(b) What pairing do we get from running the algorithm with candidates proposing?

(c) What does this tell us about the number of stable pairings?

Solution:

(a) The pairing results in (C_i, J_i) for each $i \in \{1, 2, ..., n\}$. This result can be proved by induction:

Our base case is when $n = 1$, so the only pairing is (C_1, J_1), and thus the base case is trivially true.

Now assume this is true for some $n \in \mathbb{N}$. On the first day with $n+1$ jobs and $n+1$ candidates, all $n+1$ jobs will propose to C_1. C_1 prefers J_1 the most, and the rest of the jobs will be rejected. This leaves a set of n unpaired jobs and n unpaired candidates who all have the same preferences (after the pairing of (C_1, J_1)). By the process of induction, this means that every i^{th} preferred candidate will be paired with the i^{th} preferred job.

(b) The pairings will again result in (J_i, C_i) for each $i \in \{1, 2, ..., n\}$. This can be proved by induction in the same as above, but replacing "job" with "candidate" and vice-versa.

(c) We know that job-proposing produces a candidate-pessimal stable pairing. We also know that candidate-proposing produces a candidate-optimal stable pairing. We found that candidate-optimal and candidate-pessimal pairings are the same. This means that there is only one stable pairing, since both the best and worst pairings (for candidates) are the same pairings.

2 Pairing Up

Note 4

Prove that for every even $n \geq 2$, there exists an instance of the stable matching problem with n jobs and n candidates such that the instance has at least $2^{n/2}$ distinct stable matchings.

Solution:

To prove that there exists such a stable matching instance for any even $n \geq 2$, it suffices to construct such an instance. But first, we look at the $n = 2$ case to generate some intuition. We can recognize that for the following preferences:

J_1	$C_1 > C_2$
J_2	$C_2 > C_1$

C_1	$J_2 > J_1$
C_2	$J_1 > J_2$

both $S = \{(J_1, C_1), (J_2, C_2)\}$ and $T = \{(C_1, J_2), (C_2, J_1)\}$ are stable pairings.

The $n/2$ in the exponent motivates us to consider pairing the n jobs into $n/2$ groups of 2 and likewise for the candidates. We pair up job $2k-1$ and $2k$ into a pair and candidate $2k-1$ and $2k$ into a pair, for $1 \leq k \leq n/2$.

From here, we recognize that for each pair (J_{2k-1}, J_{2k}) and (C_{2k-1}, C_{2k}), mirroring the preferences above would yield 2 stable matchings from the perspective of just these pairs. If we can extend this perspective to all $n/2$ pairs, this would be a total of $2^{n/2}$ stable matchings.

Our construction thus results in preference lists like follows:

J_1	$C_1 > C_2 > \ldots$
J_2	$C_2 > C_1 > \ldots$
$\vdots$	$\vdots$
J_{2k-1}	$C_{2k-1} > C_{2k} > \ldots$
J_{2k}	$C_{2k} > C_{2k-1} > \ldots$
$\vdots$	$\vdots$
J_{n-1}	$C_{n-1} > C_n > \ldots$
J_n	$C_n > C_{n-1} > \ldots$

C_1	$J_2 > J_1 > \ldots$
C_2	$J_1 > J_2 > \ldots$
$\vdots$	$\vdots$
C_{2k-1}	$J_{2k} > J_{2k-1} > \ldots$
C_{2k}	$J_{2k-1} > J_{2k} > \ldots$
$\vdots$	$\vdots$
C_{n-1}	$J_n > J_{n-1} > \ldots$
C_n	$J_{n-1} > J_n > \ldots$

Each match will have jobs in the kth pair paired to candidates in the kth pair for $1 \leq k \leq n/2$.

A job j in pair k will never form a rogue couple with any candidate c in pair $m \neq k$ since it always prefers the candidates in this pair over all candidates across other pairs. Since each job in pair k can be stably matched to either candidate in pair k, and there are $n/2$ total pairs, the number of stable matchings is $2^{n/2}$.

3 Upper Bound

Note 4

(a) In the notes, we show that the stable matching algorithm terminates in at most n^2 days. Prove the following stronger result: the stable matching algorithm will always terminate in at most $(n-1)^2 + 1 = n^2 - 2n + 2$ days.

(b) Provide a set of preference lists for 4 jobs and 4 candidates that will result in the upper bound from part (a) when running the Propose-and-Reject algorithm. Verify this by running the Propose-and-Reject algorithm on your preference lists.

Solution:

(a) Recall that there is always a candidate who receives only one proposal (on the last day). Other than that candidate, every other candidate can reject up to $n-1$ jobs. Thus, there's a total of $(n-1)^2 = n^2 - 2n + 1$ rejections. Conceptually, in the worst case scenario, there would be exactly one rejection per day; if we were to hand out none, then the algorithm would terminate. On the final day, the candidate who is proposed to only once receives their offer. Thus, the process takes at most $(n-1)^2 + 1 = n^2 - 2n + 2$ days.

(b) As per discussion in the solution to part (a), the main motivation for the construction will be the line "in the worst case scenario, there would be exactly one rejection per day". One such preference list that would result in this as follows, and the execution of the algorithm is presented as well.

Jobs	Preferences
J_1	$C_1 > C_2 > C_3 > C_4$
J_2	$C_2 > C_3 > C_1 > C_4$
J_3	$C_3 > C_1 > C_2 > C_4$
J_4	$C_1 > C_2 > C_3 > C_4$

Candidates	Preferences
C_1	$J_2 > J_1 >$ anything
C_2	$J_3 > J_2 >$ anything
C_3	$J_4 > J_3 >$ anything
C_4	anything

Candidate	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7	Day 8	Day 9	Day 10
C_1	J_1, J_4	J_1	J_1	J_1, J_3	J_1	J_1	J_1, J_2	J_2	J_2	J_2
C_2	J_2	J_2, J_4	J_2	J_2	J_2, J_3	J_3	J_3	J_1, J_3	J_3	J_3
C_3	J_3	J_3	J_3, J_4	J_4	J_4	J_2, J_4	J_4	J_4	J_1, J_4	J_4
C_4										J_1

4 Build-Up Error?

Note 5

What is wrong with the following "proof"? In addition to finding a counterexample, you should explain what is fundamentally wrong with this approach, and why it demonstrates the danger of build-up error.

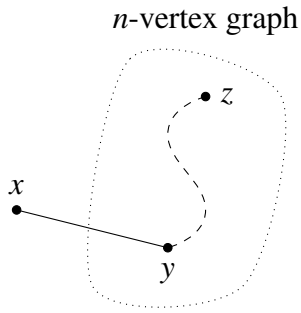
False Claim: If every vertex in an undirected graph has degree at least 1, then the graph is connected.

Proof? We use induction on the number of vertices $n \geq 1$.

Base case: There is only one graph with a single vertex and it has degree 0. Therefore, the base case is vacuously true, since the if-part is false.

Inductive hypothesis: Assume the claim is true for some $n \geq 1$.

Inductive step: We prove the claim is also true for $n+1$. Consider an undirected graph on n vertices in which every vertex has degree at least 1. By the inductive hypothesis, this graph is connected. Now add one more vertex x to obtain a graph on $(n+1)$ vertices, as shown below.



All that remains is to check that there is a path from x to every other vertex z. Since x has degree at least 1, there is an edge from x to some other vertex; call it y. Thus, we can obtain a path from x to z by adjoining the edge $\{x,y\}$ to the path from y to z. This proves the claim for $n+1$. □

Solution:

The mistake is in the argument that *"every $(n+1)$-vertex graph with minimum degree 1 can be obtained from an n-vertex graph with minimum degree 1 by adding 1 more vertex"*. Instead of starting by considering an arbitrary $(n+1)$-vertex graph, this proof only considers an $(n+1)$-vertex graph that you can make by starting with an n-vertex graph with minimum degree 1. As a counterexample, consider a graph on four vertices $V = \{1,2,3,4\}$ with two edges $E = \{\{1,2\},\{3,4\}\}$. Every vertex in this graph has degree 1, but there is no way to build this 4-vertex graph from a 3-vertex graph with minimum degree 1.

More generally, this is an example of *build-up error* in proof by induction. Usually this arises from a faulty assumption that every size $n+1$ graph with some property can be "built up" from a size n graph with the same property. (This assumption is correct for some properties, but incorrect for others, such as the one in the argument above.)

One way to avoid an accidental build-up error is to use a *"shrink down, grow back"* process in the inductive step: start with a size $n+1$ graph, remove a vertex (or edge), apply the inductive hypothesis $P(n)$ to the smaller graph, and then add back the vertex (or edge) and argue that $P(n+1)$ holds.

Let's see what would have happened if we'd tried to prove the claim above by this method. In the inductive step, we must show that $P(n)$ implies $P(n+1)$ for all $n \geq 1$. Consider an $(n+1)$- vertex graph G in which every vertex has degree at least 1. Remove an arbitrary vertex v, leaving an n-vertex graph G' in which every vertex has degree... uh-oh! The reduced graph G' might contain a vertex of degree 0, making the inductive hypothesis $P(n)$ inapplicable! We are stuck—and properly so, since the claim is false!

5 Proofs in Graphs

Note 5

(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 that there existed a city which was reachable from every other city by traveling through at most 2 roads.

[*Hint:* Induction]

(b) Consider a connected graph G with n vertices which has exactly $2m$ vertices of odd degree, where $m > 0$. Prove 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).

[*Hint:* In lecture, we have shown that a connected undirected graph has an Eulerian tour if and only if every vertex has even degree. This fact may be useful in the proof.]

(c) Prove that any graph G is bipartite if and only if it has no tours of odd length.

[*Hint:* In one of the directions, consider the lengths of paths starting from a given vertex.]

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.

Alternate Solution :Alternatively, we can prove this using properties of directed graphs. Let c be the city with the largest in-degree. Note that this graph is essentially a complete graph, where each edge is a directed edge instead of an undirected edge. Therefore, the total in degree sums to $n(n-1)/2$, and so does the total out degree. In addition, the in degree + out degree of any vertex must add up to $n-1$.

Because the total in-degree of all vertices is $n(n-1)/2$, The largest in-degree is $d \geq (n-1)/2$. Let S be the these d cities that can reach c by one edge.

For any other city x, it has to have at least $(n-1)-d$ out-degree (because in-degree $<= d$). Notice that there are n total vertices, two of which are x or c, and d vertices that connect to c through one edge. Thus, there are $n-2-d$ other vertices. Since x has out degree at least $n-1-d > n-2-d$, it must therefore connect to at least one vertex in S by the pigeonhole principle.

Thus, all vertices are either connected to c through 1 or 2 edges.

(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.

(c) To prove the claim, we need to prove two directions: if G is bipartite, it contains no tours of odd length, and if G contains no tours of odd length, it must be bipartite.

Suppose G is bipartite, and let L and R be the two disjoint sets of vertices such that there does not exist any edge between two vertices in L or two vertices in R. Further, suppose there is some tour in G, and we start traversing this tour at $v_0 \in L$.

Since each edge in G connects a vertex in L to a vertex in R, the first edge in the tour connects the start vertex v_0 to a vertex $v_1 \in R$. Similarly, the second edge connects $v_1 \in R$ to $v_2 \in L$. In general, it must be the case that the $2k$th edge connects vertex $v_{2k-1} \in R$ to $v_{2k} \in L$, and the $2k+1$th edge connects vertex $v_{2k} \in L$ to $v_{2k+1} \in R$.

Since only even numbered edges connect to vertices in L, and we started our tour in L, the tour must end with an even number of edges.

For the opposite direction, suppose G contains no tours of odd length. Without loss of generality, let us consider one connected component of G; the following reasoning can be applied to all of the connected components of G.

Let v be an arbitrary vertex in G; we can divide all of the vertices in G into two disjoint sets:

$$R = \{u \mid \text{the shortest path from } u \text{ to } v \text{ is even}\}$$
$$L = \{u \mid \text{the shortest path from } u \text{ to } v \text{ is odd}\}$$

We claim that no two vertices in L are adjacent. For contradiction, suppose there do exist adjacent vertices $u_1, u_2 \in L$. Consider the tour consisting of:

- the shortest path from v to u_1 (odd length)
- the edge (u_1, u_2) (length 1)
- the shortest path from u_2 to v (odd length)

This tour has odd length, and contradicts our assumption that G has no tours of odd length. This means that no two vertices in L are adjacent.

Similarly, we claim that no two vertices in R are adjacent. For contradiction, suppose there do exist adjacent vertices $u_1, u_2 \in R$. Consider the tour consisting of:

- the shortest path from v to u_1 (even length)
- the edge (u_1, u_2) (length 1)
- the shortest path from u_2 to v (even length)

This tour has odd length, and contradicts our assumption that G has no tours of odd length. This means that no two vertices in R are adjacent.

We've just shown that there are no edges between two vertices in L, and no edges between two vertices in R. If there are multiple connected components in G, the same partition can be applied to all of the components. Together, this means that G is bipartite.

6 (Optional) Nothing Can Be Better Than Something

Note 4

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, each job/candidate prefers being unmatched rather than be matched with those below a certain point in their preference list. Let the term "entity" 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/or 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;
- there is no matched job and matched candidate that would both prefer to be matched with each other over their current partners; and
- 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 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, they must remain unmatched in any other stable matching as well. Prove this fact by contradiction.

Solution:

(a) We form an instance of the standard stable matching problem as follows. Following, the hint, we introduce an imaginary mate, r_e, (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, r_e, is owned by the entity, e, we introduce it for.

Each robot, r_e, prefers its owner e, i.e. it puts its owner at the top of its preference list. The rest of its preference list is arbitrary and includes all other owners and the robots of other types of entities. An entity e of a robot, r_e 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 other robots can be placed in arbitrary order in e's list.

For this instance of the stable matching problem which we refer to as the robot instance, I, the propose and reject algorithm will give us a stable matching, M.

To extract the desired partial matching, we simply remove all pairs in M with at least one robot (two robots can match each other). We refer to each entity which is not matched as single. We observe, an entity, e, will never be matched with another entity's robot, $r_{e'}$, because then e and its robot, r_e, would form a rogue couple (r_e prefers e to other owners, and e prefers r_e more than other robots). It remains to show this is a stable matching as specified in the problem as follows:

- there is no matched entity, e, who prefers being unmatched over being with their current partner since the e and r_e would form a rogue couple in M;
- there is no matched/filled job, j, and unmatched candidate, c, that would both prefer to be matched with each other since otherwise j and c would form a rogue couple in M;
- there is no matched job j and matched candidate c that would both prefer to be matched with each other over their current partners since then j and c would form a rogue couple in M;
- similarly, there is no unmatched job, j, and matched candidate, c, that would both prefer to be matched with each other over their current status since j and c would be a rogue couple in M;
- there is no unmatched job, j, and unmatched candidate, c, that would both prefer to be with each other over being unmatched since j and c would be a rogue couple in M.

Thus, the resulting partial matching is stable.

(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. The stable pairing S where j_1 and c_1 are paired 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 they prefer over j_1. (If c_1 were unpaired or paired with a job they do 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.) with the pattern that (c_i, j_i) is in S and (j_i, c_{i-1}) is in T. At some time i, one must encounter j_1 in this process as there are a finite number of jobs. A this point $(j_1 = j_i, c_{i-1})$ is in T, which implies that j_1 is matched in T.

A similar argument can be used for candidates.

This contradicts the assumption that j_1 is unmatched in T. 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.

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 03

1 Short Tree Proofs

Note 5

Let $G = (V, E)$ be an undirected graph with $|V| \geq 1$.

(a) Prove that every connected component in an acyclic graph is a tree.

(b) Suppose G has k connected components. Prove that if G is acyclic, then $|E| = |V| - k$.

(c) Prove that a graph with $|V|$ edges contains a cycle.

Solution:

(a) Every connected component is connected, and acyclic because the graph is acyclic; by definition, this is a tree.

(b) Because each connected component is a tree, each connected component has $|V_i| - 1$ edges. The total number of edges is thus $\sum_i (|V_i| - 1) = |V| - k$.

(c) An acyclic graph has $|V| - k$ edges which cannot equal $|V|$, thus if a graph has $|V|$ edges it has a cycle.

2 Touring Hypercube

Note 5

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.

(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.

3 Planarity and Graph Complements

Note 5

Let $G = (V, E)$ be an undirected graph. We define the complement of G as $\overline{G} = (V, \overline{E})$ where $\overline{E} = \{(i, j) \mid i, j \in V, i \neq j\} - E$; that is, $\overline{G}$ has the same set of vertices as G, but an edge e exists is $\overline{G}$ if and only if it does not exist in G.

(a) Suppose G has v vertices and e edges. How many edges does $\overline{G}$ have?

(b) Prove that for any graph with at least 13 vertices, G being planar implies that $\overline{G}$ is non-planar.

(c) Now consider the converse of the previous part, i.e., for any graph G with at least 13 vertices, if $\overline{G}$ is non-planar, then G is planar. Construct a counterexample to show that the converse does not hold.

Hint: Recall that if a graph contains a copy of K_5, then it is non-planar. Can this fact be used to construct a counterexample?

Solution:

(a) If G has v vertices, then there are a total of $\frac{v(v-1)}{2}$ edges that could possibly exist in the graph. Since e of them appear in G, we know that the remaining $\frac{v(v-1)}{2} - e$ must appear in $\overline{G}$.

(b) Since G is planar, we know that $e \leq 3v-6$. Plugging this in to the answer from the previous part, we have that $\overline{G}$ has at least $\frac{v(v-1)}{2} - (3v-6)$ edges. Since v is at least 13, we have that $\frac{v(v-1)}{2} \geq \frac{v \cdot 12}{2} = 6v$, so $\overline{G}$ has at least $6v - 3v + 6 = 3v + 6$ edges. Since this is strictly more than the $3v-6$ edges allowed in a planar graph, we have that $\overline{G}$ must not be planar.

(c) The converse is not necessarily true. As a counterexample, suppose that G has exactly 13 vertices, of which five are all connected to each other and the remaining ten have no edges incident to them. This means that G is non-planar, since it contains a copy of K_5. However, $\overline{G}$ also contains a copy of K_5 (take any 5 of the 8 vertices that were isolated in G), so $\overline{G}$ is also non-planar. Thus, it is possible for both G and $\overline{G}$ to be non-planar.

4 Modular Practice

Note 6

Solve the following modular arithmetic equations for x and y.

(a) $9x + 5 \equiv 7 \pmod{13}$.

(b) Show that $3x + 12 \equiv 4 \pmod{21}$ does not have a solution.

(c) The system of simultaneous equations $5x + 4y \equiv 0 \pmod{7}$ and $2x + y \equiv 4 \pmod{7}$.

(d) $13^{2023} \equiv x \pmod{12}$.

(e) $7^{62} \equiv x \pmod{11}$.

Solution:

(a) Subtract 5 from both sides to get:

$$9x \equiv 2 \pmod{13}.$$

Now since $\gcd(9, 13) = 1$, 9 has a (unique) inverse mod 13, and since $9 \times 3 = 27 \equiv 1 \pmod{13}$ the inverse is 3. So multiply both sides by $9^{-1} \equiv 3 \pmod{13}$ to get:

$$x \equiv 6 \pmod{13}.$$

(b) Notice that any number $y \equiv 4 \pmod{21}$ can be written as $y = 4 + 21k$ (for some integer k). Evaluating y mod 3, we get $y \equiv 1 \pmod{3}$.

Since the right side of the equation is $1 \pmod{3}$, the left side must be as well. However, $3x + 12$ will never be $1 \pmod{3}$ for any value of x. Thus, there is no possible solution.

(c) First, subtract the first equation from four times the second equation to get:

$$\begin{aligned} 4(2x+y) - (5x+4y) &\equiv 4(4) - 0 \pmod{7} \\ 8x + 4y - 5x - 4y &\equiv 16 \pmod{7} \\ 3x &\equiv 2 \pmod{7} \end{aligned}$$

Multiplying by $3^{-1} \equiv 5 \pmod{7}$, we have $x \equiv 10 \equiv 3 \pmod{7}$.

Plugging this into the second equation, we have

$$2(3) + y \equiv 4 \pmod{7},$$

so the system has the solution $x \equiv 3 \pmod{7}$, $y \equiv 5 \pmod{7}$.

(d) We use the fact that $13 \equiv 1 \pmod{12}$. Thus, we can rewrite the equation as

$$x \equiv 13^{2023} \equiv 1^{2023} \equiv 1 \pmod{12}.$$

(e) One way to solve exponentiation problems is to test values until one identifies a pattern.

$$\begin{aligned} 7^1 &\equiv 7 \pmod{11} \\ 7^2 &\equiv 49 \equiv 5 \pmod{11} \\ 7^3 &= 7 \cdot 7^2 \equiv 7 \cdot 5 \equiv 2 \pmod{11} \\ 7^4 &= 7 \cdot 7^3 \equiv 7 \cdot 2 \equiv 3 \pmod{11} \\ 7^5 &= 7 \cdot 7^4 \equiv 7 \cdot 3 \equiv 10 \equiv -1 \pmod{11} \end{aligned}$$

We theoretically could continue this until we the sequence starts repeating. However, notice that if $7^5 \equiv -1 \implies 7^{10} = (7^5)^2 \equiv (-1)^2 \equiv 1 \pmod{11}$.

Similarly, $7^{60} = (7^{10})^6 \equiv 1^6 \equiv 1 \pmod{11}$. As a final step, we have $7^{62} = 7^2 \cdot 7^{60} \equiv 7^2 \cdot 1 = 49 \equiv 5 \pmod{11}$.

5 Short Answer: Modular Arithmetic

Note 6

(a) What is the multiplicative inverse of $n-1$ modulo n? (Your answer should be an expression that may involve n)

(b) What is the solution to the equation $3x \equiv 6 \pmod{17}$?

(c) Let $R_0 = 0; R_1 = 2; R_n = 4R_{n-1} - 3R_{n-2}$ for $n \geq 2$. Is $R_n \equiv 2 \pmod{3}$ for $n \geq 1$? (True or False)

(d) Given that $(7)(53) - m = 1$, what is the solution to $53x + 3 \equiv 10 \pmod{m}$? (Answer should be an expression that is interpreted $\pmod{m}$, and shouldn't consist of fractions.)

Solution:

(a) The answer is $n-1 \pmod{n}$. We can see this by noting that it is $-1 \pmod{n}$, or more directly, $(n-1)(n-1) \equiv n^2 - 2n + 1 \equiv 1 \pmod{n}$.

(b) The answer is $x \equiv 2 \pmod{17}$. Muliply both sides by 6 (the multiplicative inverse of 3 modulo 17) and reduce.

(c) The statement is true. We can see this by taking the recursive formula modulo 3. This gives us that $R_n \equiv R_{n-1} \pmod{3}$, hence since $R_1 \equiv 2 \pmod{3}$, every R_i must also be 2 modulo 3.

(d) Note that since $7 \cdot 53 - m = 1$, we can take both sides modulo m and find that $7 \cdot 53 \equiv 1 \pmod{m}$, hence 7 is the inverse of 53 modulo m. Thus, we can solve the equation by subtracting by 3 on both sides and multiplying by 7, giving that $x \equiv 49 \pmod{m}$.

6 Wilson's Theorem

Note 6

Wilson's Theorem states the following is true if and only if p is prime:

$$(p-1)! \equiv -1 \pmod{p}.$$

Prove both directions (it holds if AND only if p is prime).

Hint for the if direction: Consider rearranging the terms in $(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$ to pair up terms with their inverses, when possible. What terms are left unpaired?

Hint for the only if direction: If p is composite, then it has some prime factor q. What can we say about $(p-1)! \pmod{q}$?

Solution:

Direction 1: If p is prime, then the statement holds.

For the integers $1, \cdots, p-1$, every number has an inverse. However, it is not possible to pair a number off with its inverse when it is its own inverse. This happens when $x^2 \equiv 1 \pmod{p}$, or when $p \mid x^2 - 1 = (x-1)(x+1)$. Thus, $p \mid x-1$ or $p \mid x+1$, so $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. Thus, the only integers from 1 to $p-1$ inclusive whose inverse is the same as itself are 1 and $p-1$.

We reconsider the product $(p-1)! = 1 \cdot 2 \cdots p-1$. The product consists of 1, $p-1$, and pairs of numbers with their inverse, of which there are $\frac{p-1-2}{2} = \frac{p-3}{2}$. The product of the pairs is 1 (since the product of a number with its inverse is 1), so the product $(p-1)! \equiv 1 \cdot (p-1) \cdot 1 \equiv -1 \pmod{p}$, as desired.

Direction 2: The expression holds *only if* p is prime (contrapositive: if p isn't prime, then it doesn't hold).

We will prove by contradiction that if some number p is composite, then $(p-1)! \not\equiv -1 \pmod{p}$. Suppose for contradiction that $(p-1)! \equiv -1 \pmod{p}$. Note that this means we can write $(p-1)!$ as $p \cdot k - 1$ for some integer k.

Since p isn't prime, it has some prime factor q where $2 \leq q \leq n-2$, and we can write $p = q \cdot r$. Plug this into the expression for $(p-1)!$ above, yielding us $(p-1)! = (q \cdot r)k - 1 = q(rk) - 1 \implies (p-1)! \equiv -1 \pmod{q}$. However, we know q is a term in $(p-1)!$, so $(p-1)! \equiv 0 \pmod{q}$. Since $0 \not\equiv -1 \pmod{q}$, we have reached our contradiction.

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

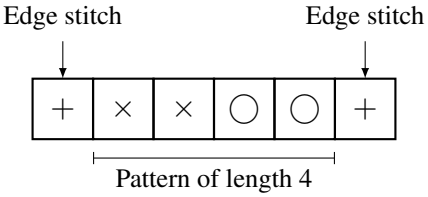
HW 04

1 Celebrate and Remember Textiles

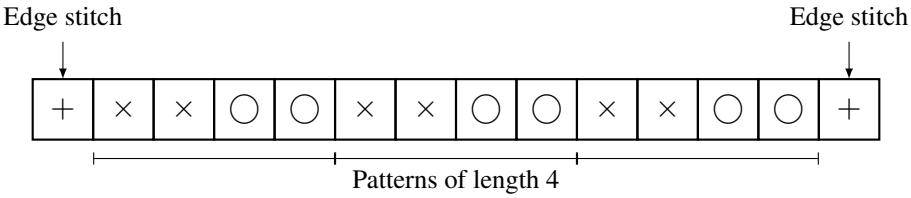
Note 6

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.

2 Euler's Totient Theorem

Note 6
Note 7

Euler's Totient Theorem states that, if n and a are coprime,

$$a^{\phi(n)} \equiv 1 \pmod n$$

where $\phi(n)$ (known as Euler's Totient Function) is the number of positive integers less than or equal to n which are coprime to n (including 1). Note that this theorem generalizes Fermat's Little Theorem, since if n is prime, then $\phi(n) = n - 1$.

(a) Let the numbers less than n which are coprime to n be $m_1, m_2, \ldots, m_{\phi(n)}$. Argue that the set

$$\{am_1, am_2, \ldots, am_{\phi(n)}\}$$

is a permutation of the set

$$\{m_1, m_2, \ldots, m_{\phi(n)}\}.$$

In other words, prove that

$$f : \{m_1, m_2, \ldots, m_{\phi(n)}\} \to \{m_1, m_2, \ldots, m_{\phi(n)}\}$$

is a bijection, where $f(x) \coloneqq ax \pmod{n}$.

(b) Prove Euler's Theorem. (Hint: Recall the FLT proof.)

Solution:

(a) This problem mirrors the proof of Fermat's Little Theorem, except now we work with the set $\{m_1, m_2, \cdots, m_{\phi(n)}\}$.

Since m_i and a are both coprime to n, so is $a \cdot m_i$. Suppose $a \cdot m_i$ shared a common factor with n, and WLOG, assume that it is a prime p. Then, either $p|a$ or $p|m_i$. In either case, p is a common factor between n and one of a or m_i, contradiction.

We now prove that f is injective. Suppose we have $f(x) = f(y)$, so $ax \equiv ay \pmod{n}$. Since a has a multiplicative inverse $\pmod{n}$, we see $x \equiv y \pmod{n}$, thus showing that f is injective.

We continue to show that f is surjective. Take any y that is relatively prime to n. Then, we see that $f(a^{-1}y) \equiv y \pmod{n}$, so therefore, there is an x such that $f(x) = y$. Furthermore, $a^{-1}y \pmod{n}$ is relatively prime to n, since we are multiplying two numbers that are relatively prime to n.

(b) Since both sets have the same elements, just in different orders, multiplying them together gives

$$m_1 \cdot m_2 \cdot \ldots \cdot m_{\phi(n)} \equiv am_1 \cdot am_2 \cdot \ldots \cdot am_{\phi(n)} \pmod{n}$$

and factoring out the a terms,

$$m_1 \cdot m_2 \cdot \ldots \cdot m_{\phi(n)} \equiv a^{\phi(n)} \left(m_1 \cdot m_2 \cdot \ldots \cdot m_{\phi(n)}\right) \pmod{n}.$$

Thus we have $a^{\phi(n)} \equiv 1 \pmod{n}$.

3 Sparsity of Primes

Note 6

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. We want to find n such that $(n+1)$, $(n+2)$, $\ldots$, and $(n+k)$ are all not powers of primes. We can enforce this by saying that $n+1$ through $n+k$ each must have two distinct prime divisors. In your proof, you can choose these prime divisors arbitrarily.

Solution:

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

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

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

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

4 RSA Practice

Note 7

Consider the following RSA scheme and answer the specified questions.

(a) Assume for an RSA scheme we pick 2 primes $p = 5$ and $q = 11$ with encryption key $e = 9$, what is the decryption key d? Calculate the exact value.

(b) If the receiver gets 4, what was the original message?

(c) Encode your answer from part (b) to check its correctness.

Solution:

(a) The private key d is defined as the inverse of $e \pmod{(p-1)(q-1)}$. Thus we need to compute

$9^{-1} \bmod (5-1)(11-1) = 9^{-1} \bmod 40$. Compute $\text{egcd}(40,9)$:

$$\begin{aligned} \text{egcd}(40,9) &= \text{egcd}(9,4) && [4 = 40 \bmod 9 = 40 - 4(9)] \\ &= \text{egcd}(4,1) && [1 = 9 \bmod 4 = 9 - 2(4)]. \\ 1 &= 9 - 2(4). \\ 1 &= 9 - 2(40 - 4(9)) \\ &= 9 - 2(40) + 8(9) = 9(9) - 2(40). \end{aligned}$$

We get $-2(40) + 9(9) = 1$. So the inverse of 9 is 9. So $d = 9$.

(b) 4 is the encoded message. We can decode this with $D(m) \equiv m^d \equiv 4^9 \equiv 14 \pmod{55}$. Thus the original message was 14.

(c) The answer from the second part was 14. To encode the number x we must compute $x^e \bmod N$. Thus, $14^9 \equiv 14 \cdot (14^2)^4 \equiv 14 \cdot (31^2)^2 \equiv 14 \cdot (26^2) \equiv 14 \cdot 16 \equiv 4 \pmod{55}$. This verifies the second part since the encoded message was supposed to be 4.

5 Tweaking RSA

Note 7

You are trying to send a message to your friend, and as usual, Eve is trying to decipher what the message is. However, you get lazy, so you use $N = p$, and p is prime. Similar to the original method, for any message $x \in \{0, 1, \ldots, N-1\}$, $E(x) \equiv x^e \pmod{N}$, and $D(y) \equiv y^d \pmod{N}$.

(a) Show how you choose e and d in the encryption and decryption function, respectively. Prove the correctness property: the message x is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$.

(b) Can Eve now compute d in the decryption function? If so, by what algorithm?

(c) Now you wonder if you can modify the RSA encryption method to work with three primes ($N = pqr$ where p, q, r are all prime). Explain the modifications made to encryption and decryption and include a proof of correctness showing that $D(E(x)) = x$.

Solution:

(a) Choose e such that it is coprime with $p-1$, and choose $d \equiv e^{-1} \pmod{p-1}$.
We want to show x is recovered by $E(x)$ and $D(y)$, such that $D(E(x)) = x$.
In other words, $x^{ed} \equiv x \pmod{p}$ for all $x \in \{0, 1, \ldots, N-1\}$.
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

$$\begin{aligned} x^{ed} &\equiv x^{k(p-1)+1} \pmod{p} \\ &\equiv x^{k(p-1)}x \pmod{p} \\ &\equiv 1^k x \pmod{p} \\ &\equiv x \pmod{p}, \end{aligned}$$

  by using FLT.

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

(b) Since Eve knows $N = p$, and $d \equiv e^{-1} \pmod{p-1}$, now she can compute d using EGCD.

(c) Let e be co-prime with $(p-1)(q-1)(r-1)$. Give the public key: (N, e) and calculate $d = e^{-1} \pmod{(p-1)(q-1)(r-1)}$. People who wish to send me a secret, x, send $y = x^e \pmod{N}$. We decrypt an incoming message, y, by calculating $y^d \pmod{N}$.

Does this work? We prove that $x^{ed} - x \equiv 0 \pmod{N}$, and thus $x^{ed} = x \pmod{N}$.
To prove that $x^{ed} - x \equiv 0 \pmod{N}$, we factor out the x to get
$x \cdot (x^{ed-1} - 1) = x \cdot (x^{k(p-1)(q-1)(r-1)+1-1} - 1)$ because $ed \equiv 1 \pmod{(p-1)(q-1)(r-1)}$.

We now show that $x \cdot (x^{k(p-1)(q-1)(r-1)} - 1)$ is divisible by p, q, and r. Thus, it is divisible by N, and $x^{ed} - x \equiv 0 \pmod{N}$.
To prove that it is divisible by p:

- if x is divisible by p, then the entire thing is divisible by p.
- if x is not divisible by p, then that means we can use FLT on the inside to show that $(x^{p-1})^{k(q-1)(r-1)} - 1 \equiv 1 - 1 \equiv 0 \pmod{p}$. Thus it is divisible by p.

To prove that it is divisible by q:

- if x is divisible by q, then the entire thing is divisible by q.
- if x is not divisible by q, then that means we can use FLT on the inside to show that $(x^{q-1})^{k(p-1)(r-1)} - 1 \equiv 1 - 1 \equiv 0 \pmod{q}$. Thus it is divisible by q.

To prove that it is divisible by r:

- if x is divisible by r, then the entire thing is divisible by r.
- if x is not divisible by r, then that means we can use FLT on the inside to show that $(x^{r-1})^{k(p-1)(q-1)} - 1 \equiv 1 - 1 \equiv 0 \pmod{r}$. Thus it is divisible by r.

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 05

1 Equivalent Polynomials

Note 7
Note 8

This problem is about polynomials with coefficients in GF(p) for some prime $p \in \mathbb{N}$. We say that two such polynomials f and g are *equivalent* if $f(x) \equiv g(x) \pmod{p}$ for every $x \in \text{GF}(p)$.

(a) Show that $f(x) = x^{p-1}$ and $g(x) = 1$ are **not** equivalent polynomials under GF(p).

(b) Use Fermat's Little Theorem to find a polynomial with degree strictly less than 5 that is equivalent to $f(x) = x^5$ over GF(5); then find a polynomial with degree strictly less than 11 that is equivalent to $g(x) = 4x^{70} + 9x^{11} + 3$ over GF(11).

(c) In GF(p), prove that whenever $f(x)$ has degree $\geq p$, it is equivalent to some polynomial $\tilde{f}(x)$ with degree $< p$.

Solution:

(a) For f and g to be equivalent, they must satisfy $f(x) \equiv g(x) \pmod{p}$ for all values of x, including zero. But $f(0) \equiv 0 \pmod{p}$ and $g(0) \equiv 1 \pmod{p}$, so they are not equivalent.

(b) Fermat's Little Theorem says that for any nonzero integer a and any prime number p, $a^{p-1} \equiv 1 \mod p$. We're allowed to multiply through by a, so the theorem is equivalent to saying that $a^p \equiv a \mod p$; note that this is true even when $a = 0$, since in that case we just have $0^p \equiv 0 \pmod{p}$.

The problem asks for a polynomial $\tilde{f}(x)$, different from $f(x)$, with the property that $\tilde{f}(a) \equiv a^5 \mod 5$ for any integer a. Directly using the theorem, $\tilde{f}(x) = x$ will work. We can do something similar with $g(x) = 4x^{70} + 9x^{11} + 3$ modulo 11; since $x^{11} \equiv x \pmod{11}$, we repeatedly substitute x^{11} with x, effectively reducing the exponent by 10. We can only do this as long as the exponent remains greater than or equal to 11, so we end up with $\tilde{g}(x) = 4x^{10} + 9x + 3$.

(c) One proof uses Fermat's Little Theorem. As a warm-up, let $d \geq p$; we'll find a polynomial equivalent to x^d. For any integer, we know

$$\begin{aligned} a^d &= a^{d-p}a^p \\ &\equiv a^{d-p}a \pmod{p} \\ &\equiv a^{d-p+1} \pmod{p}. \end{aligned}$$

In other words x^d is equivalent to the polynomial $x^{d-(p-1)}$. If $d-(p-1) \geq q$, we can show in the same way that x^d is equivalent to $x^{d-2(p-1)}$. Since we subtract $p-1$ every time, the

sequence $d, d-(p-1), d-2(p-1), \ldots$ must eventually be smaller than p. Now if $f(x)$ is any polynomial with degree $\geq p$, we can apply this same trick to every x^k that appears for which $k \geq p$.

Another proof uses Lagrange interpolation. Let $f(x)$ have degree $\geq p$. By Lagrange interpolation, there is a unique polynomial $\tilde{f}(x)$ of degree at most $p-1$ passing through the points $(0, f(0)), (1, f(1)), (2, f(2)), \ldots, (p-1, f(p-1))$, and we know it must be equivalent to $f(x)$ because f also passes through the same p points.

2 Secret Sharing

Note 8

Suppose the Oral Exam questions are created by 2 TAs and 3 Readers. The answers are all encrypted, and we know that:

- Two TAs together should be able to access the answers
- Three Readers together should be able to access the answers
- One TA and one Reader together should also be able to access the answers
- One TA by themself or two Readers by themselves should not be able to access the answers.

Design a Secret Sharing scheme to make this work.

Solution:

Solution 1 We can use a degree 2 polynomial, which is uniquely determined by 3 points. Evaluate the polynomial at 7 points, and distribute a point to each Reader and 2 points to each TA. Then, all possible combinations will have at least 3 points to recover the answer key.

Basically, the point of this problem is to assign different weight to different class of people. If we give one share to everyone, then 2 Readers can also recover the secret and the scheme is broken.

Solution 2 We construct three polynomials, one for each way of recovering the answer key:

- A degree 1 polynomial for recovering with two TAs, evaluated at 2 points. Distribute a point to each TA.
- A degree 2 polynomial for recovering with three readers, evaluated at 3 points. Distribute a point to each Reader.
- A degree 1 polynomial for recovering with one TA + one reader. Evaluate this polynomial at 2 points, and distribute one point to all TAs and one point to all readers.

All combinations can then use the corresponding polynomial to recover the answer key.

3 One Point Interpolation

Note 8

Suppose we have a polynomial $f(x) = x^k + c_{k-1}x^{k-1} + \cdots + c_2x^2 + c_1x + c_0$.

(a) Can we determine $f(x)$ with k points? If so, provide a set of inputs $x_0, x_1, \ldots, x_{k-1}$ such that knowing points $(x_0, f(x_0)), (x_1, f(x_1)), \ldots, (x_{k-1}, f(x_{k-1}))$ allows us to uniquely determine $f(x)$, and show how $f(x)$ can be determined from such points. If not, provide a proof of why this is not possible.

(b) Now, assume each coefficient is an integer satisfying $0 \leq c_i < 100 \quad \forall i \in [0, k-1]$. Can we determine $f(x)$ with one point? If so, provide an input x_* such that knowing the point $(x_*, f(x_*))$ allows us to uniquely determine $f(x)$, and show how $f(x)$ can be determined from this point. If not, provide a proof of why this is not possible.

Solution:

(a) Yes. Since the leading coefficient is 1, we only need to find the k remaining coefficients $c_0, c_1, \ldots, c_{k-1}$ to determine $f(x)$. This can be done with *any* k distinct points.

For example, suppose we know the points $(0, f(0)), (1, f(1)), \ldots, (k-1, f(k-1))$. We can then write the degree $k-1$ polynomial

$$g(x) = c_{k-1}x^{k-1} + \cdots + c_2x^2 + c_1x + c_0 = f(x) - x^k$$

which can be determined via Lagrange interpolation on $(0, f(0)), (1, f(1)-1), (2, f(2)-2^k), \ldots, (k-1, f(k-1)-(k-1)^k)$, uniquely yielding our desired coefficients $c_0, c_1, \ldots, c_{k-1}$.

(b) Yes. We can express each nonnegative two-digit integer $c_i = 10d_{2i+1} + d_{2i}$ for digits $d_i \in [0, 9]$.

Using $x_* = 100$,

$$\begin{aligned} f(100) &= 100^k + c_{k-1}100^{k-1} + \cdots + c_2100^2 + c_1100 + c_0 \\ &= 10^{2k} + (10d_{2k-1} + d_{2k-2})10^{2k-2} + \cdots + (10d_5 + d_4)10^4 + (10d_3 + d_2)10^2 + (10d_1 + d_0) \\ &= 10^{2k} + 10^{2k-1}d_{2k-1} + 10^{2k-2}d_{2k-2} + \cdots + 10^5d_5 + 10^4d_4 + 10^3d_3 + 10^2d_2 + 10d_1 + d_0 \end{aligned}$$

Thus, the rightmost $2k-1$ digits of $f(100)$, from right to left, are $d_0, d_1, \ldots, d_{2k-1}$; we can then determine our desired coefficients $c_i = 10d_{2i+1} + d_{2i}$.

4 Error-Correcting Codes

Note 9

(a) Recall from class the error-correcting code for erasure errors, which protects against up to k lost packets by sending a total of $n+k$ packets (where n is the number of packets in the original message). Often the number of packets lost is not some fixed number k, but rather a *fraction* of the number of packets sent. Suppose we wish to protect against a fraction α of lost packets (where $0 < \alpha < 1$). At least how many packets do we need to send (as a function of n and α)?

(b) Repeat part (a) for the case of general errors.

Solution:

(a) Suppose we send a total of m packets (where m is to be determined). Since at most a fraction α of these are lost, the number of packets received is at least $(1-\alpha)m$. But in order to reconstruct the polynomial used in transmission, we need at least n packets. Hence it is sufficient to have $(1-\alpha)m \geq n$, which can be rearranged to give $m \geq n/(1-\alpha)$.

(b) Suppose we send a total of $m = n+2k$ packets, where k is the number of errors we can guard against. The number of corrupted packets is at most αm, so we need $k \geq \alpha m$. Hence $m \geq n+2\alpha m$. Rearranging gives $m \geq n/(1-2\alpha)$.

Note: Recovery in this case is impossible if $\alpha \geq 1/2$.

5 Alice and Bob

Note 8
Note 9

(a) Alice decides that instead of encoding her message as the values of a polynomial, she will encode her message as the coefficients of a degree 2 polynomial $P(x)$. For her message $[m_1, m_2, m_3]$, she creates the polynomial $P(x) = m_1x^2 + m_2x + m_3$ and sends the five packets $(0,P(0))$, $(1,P(1))$, $(2,P(2))$, $(3,P(3))$, and $(4,P(4))$ to Bob. However, one of the packet y-values (one of the $P(i)$ terms; the second attribute in the pair) is changed by Eve before it reaches Bob. If Bob receives

$$(0,1),(1,3),(2,0),(3,1),(4,0)$$

and knows Alice's encoding scheme and that Eve changed one of the packets, can he recover the original message? If so, find it as well as the x-value of the packet that Eve changed. If he can't, explain why. Work in mod 7. Also, feel free to use a calculator or online systems of equations solver, but make sure it can work under mod 7.

(b) Bob gets tired of decoding degree 2 polynomials. He convinces Alice to encode her messages on a degree 1 polynomial. Alice, just to be safe, continues to send 5 points on her polynomial even though it is only degree 1. She makes sure to choose her message so that it can be encoded on a degree 1 polynomial. However, Eve changes two of the packets. Bob receives $(0,5)$, $(1,7)$, $(2,x)$, $(3,5)$, $(4,0)$. If Alice sent $(0,5)$, $(1,7)$, $(2,9)$, $(3,-2)$, $(4,0)$, for what values of x will Bob not uniquely be able to determine Alice's message? Assume that Bob knows Eve changed two packets. Work in mod 13. Again, feel free to use a calculator or graphing calculator software.

(c) Alice wants to send a length n message to Bob. There are two communication channels available to her: Channel X and Channel Y. Only 6 packets can be sent through channel X. Similarly, Channel Y will only deliver 6 packets, but it will also corrupt (change the value) of one of the delivered packets. Using each of the two channels once, what is the largest message length n such that Bob so that he can always reconstruct the message?

Solution:

(a) We can use Berlekamp and Welch. We have: $Q(x) = P(x)E(x)$. $E(x)$ has degree 1 since we know we have at most 1 error. $Q(x)$ is degree 3 since $P(x)$ is degree 2. We can write a system of linear equations and solve for the coefficients of $Q(x) = ax^3 + bx^2 + cx + d$ and $E(x) = (x - e)$ by writing the equation $Q(i) = r_i \cdot E(i)$ for $0 \leq i \leq 4$, where r_i is the ith received point.

$$\begin{aligned} d &= 1(0-e) \\ a+b+c+d &= 3(1-e) \\ 8a+4b+2c+d &= 0(2-e) \\ 27a+9b+3c+d &= 1(3-e) \\ 64a+16b+4c+d &= 0(4-e) \end{aligned}$$

Since we are working in mod 7, this is equivalent to:

$$\begin{aligned} d &= -e \\ a+b+c+d &= 3-3e \\ a+4b+2c+d &= 0 \\ 6a+2b+3c+d &= 3-e \\ a+2b+4c+d &= 0 \end{aligned}$$

Solving yields:

$$Q(x) = x^3 + 5x^2 + 5x + 4, E(x) = x - 3$$

To find $P(x)$ we divide $Q(x)$ by $E(x)$ and get $P(x) = x^2 + x + 1$. So Alice's message is $m_1 = 1, m_2 = 1, m_3 = 1$. The x-value of the packet Eve changed is 3.

Alternative solution: Since we have 5 points, we have to find a polynomial of degree 2 that goes through 4 of those points. The point that the polynomial does not go through will be the packet that Eve changed. Since 3 points uniquely determine a polynomial of degree 2, we can pick 3 points and check if it goes through a 4th point. (It may be the case that we need to try all sets of 3 points.)

We pick the points $(1,3), (2,0), (4,0)$. Lagrange interpolation can be used to create the polynomial but we can see that for the polynomial that goes through these 3 points, it has 0s at $x = 2$ and $x = 4$. Thus the polynomial is $k(x-2)(x-4) = k(x^2 - 6x + 8) \pmod 7 \equiv k(x^2 + x + 1) \pmod 7$. We find $k \equiv 1$ by plugging in the point $(1,3)$, so our polynomial is $x^2 + x + 1$. We then check to see if this polynomial goes through one of the 2 points that we didn't use. Plugging in 0 for x, we get 1. The packet that Eve changed is the point that our polynomial does not go through which has x-value 3. Alice's original message was $m_1 = 1, m_2 = 1, m_3 = 1$.

(b) Since Bob knows that Eve changed 2 of the points, the 3 remaining points will still be on the degree 1 polynomial that Alice encoded her message on. Thus if Bob can find a degree 1 polynomial that passes through at least 3 of the points that he receives, he will be able to

uniquely recover Eve's message. The only time that Bob cannot uniquely determine Alice's message is if there are 2 polynomials with degree 1 that pass through 3 of the 5 points that he receives. Since we are working with degree 1 polynomials, we can plot the points that Bob receives and then see which values of x will cause 2 sets of 3 points to fall on a line. $(0,5),(1,7),(4,0)$ already fall on a line. If $x = 6$, $(1,7),(2,6),(3,5)$ also falls on a line. If $x = 5$, $(0,5),(2,5),(3,5)$ also falls on a line. If $x = 9$, $(0,5),(2,9),(4,0)$ falls on the original line, so here Bob can decode the message. If $x = 10$, $(2,10),(3,5),(4,0)$ also falls on a line. So if $x = 6,5,10$, Bob will not be able to uniquely determine Alice's message.

(c) Channel X can send 6 packets, so the first 6 characters of the message can be send through Channel X. Channel Y can send 6 packets, but 1 will be corrupted, thus only a message of length 4 can be sent. Thus, a total of $m = 6+4 = 10$ characters can effectively sent.

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 06

1 Unions and Intersections

Note 11

Given:

- X is a countable, non-empty set. For all $i \in X$, A_i is an uncountable set.
- Y is an uncountable set. For all $i \in Y$, B_i is a countable set.

For each of the following, decide if the expression is "Always countable", "Always uncountable", "Sometimes countable, Sometimes uncountable".

For the "Always" cases, prove your claim. For the "Sometimes" case, provide two examples – one where the expression is countable, and one where the expression is uncountable.

(a) $X \cap Y$

(b) $X \cup Y$

(c) $\bigcup_{i \in X} A_i$

(d) $\bigcap_{i \in X} A_i$

(e) $\bigcup_{i \in Y} B_i$

(f) $\bigcap_{i \in Y} B_i$

Solution:

(a) Always countable. $X \cap Y$ is a subset of X, which is countable.

(b) Always uncountable. $X \cup Y$ is a superset of Y, which is uncountable.

(c) Always uncountable. Let x be any element of X. A_x is uncountable. Thus, $\bigcup_{i \in X} A_i$, a superset of A_x, is uncountable.

(d) Sometimes countable, sometimes uncountable.

Countable: When the A_i are disjoint, the intersection is empty, and thus countable. For example, let $X = \mathbb{N}$, let $A_i = \{i\} \times \mathbb{R} = \{(i,x) \mid x \in \mathbb{R}\}$. Then, $\bigcap_{i \in X} A_i = \varnothing$.

Uncountable: When the A_i are identical, the intersection is uncountable. Let $X = \mathbb{N}$, let $A_i = \mathbb{R}$ for all i. $\bigcap_{i \in X} A_i = \mathbb{R}$ is uncountable.

(e) Sometimes countable, sometimes uncountable.

Countable: Make all the B_i identical. For example, let $Y = \mathbb{R}$, and $B_i = \mathbb{N}$. Then, $\bigcup_{i \in Y} B_i = \mathbb{N}$ is countable.

Uncountable: Let $Y = \mathbb{R}$. Let $B_i = \{i\}$. Then, $\bigcup_{i \in Y} B_i = \mathbb{R}$ is uncountable.

(f) Always countable. Let y be any element of Y. B_y is countable. Thus, $\bigcap_{i \in Y} B_i$, a subset of B_y, is also countable.

2 Count It!

Note 11

For each of the following collections, determine and briefly explain whether it is finite, countably infinite (like the natural numbers), or uncountably infinite (like the reals):

(a) The integers which divide 8.

(b) The integers which 8 divides.

(c) The functions from $\mathbb{N}$ to $\mathbb{N}$.

(d) The set of strings over the English alphabet. (Note that the strings may be arbitrarily long, but each string has finite length. Also the strings need not be real English words.)

(e) The set of finite-length strings drawn from a countably infinite alphabet, $\mathscr{A}$.

(f) The set of infinite-length strings over the English alphabet.

Solution:

(a) Finite. They are $\{-8, -4, -2, -1, 1, 2, 4, 8\}$.

(b) Countably infinite. We know that there exists a bijective function $f : \mathbb{N} \to \mathbb{Z}$. Then the function $g(n) = 8f(n)$ is a bijective mapping from $\mathbb{N}$ to integers which 8 divides.

(c) Uncountably infinite. We use Cantor's Diagonalization Proof:

Let $\mathscr{F}$ be the set of all functions from $\mathbb{N}$ to $\mathbb{N}$. We can represent a function $f \in \mathscr{F}$ as an infinite sequence $(f(0), f(1), \cdots)$, where the i-th element is $f(i)$. Suppose towards a contradiction that there is a bijection from $\mathbb{N}$ to $\mathscr{F}$:

$$
\begin{aligned}
0 &\longleftrightarrow (f_0(0), f_0(1), f_0(2), f_0(3), \dots) \\
1 &\longleftrightarrow (f_1(0), f_1(1), f_1(2), f_1(3), \dots) \\
2 &\longleftrightarrow (f_2(0), f_2(1), f_2(2), f_2(3), \dots) \\
3 &\longleftrightarrow (f_3(0), f_3(1), f_3(2), f_3(3), \dots) \\
&\vdots
\end{aligned}
$$

Consider the function $g : \mathbb{N} \to \mathbb{N}$ where $g(i) = f_i(i) + 1$ for all $i \in \mathbb{N}$. We claim that the function g is not in our finite list of functions. Suppose for contradiction that it were, and that it was the n-th function $f_n(\cdot)$ in the list, i.e., $g(\cdot) = f_n(\cdot)$. However, $f_n(\cdot)$ and $g(\cdot)$ differ in the n-th argument, i.e. $f_n(n) \neq g(n)$, because by our construction $g(n) = f_n(n) + 1$. Contradiction!

(d) Countably infinite. The English language has a finite alphabet (52 characters if you count only lower-case and upper-case letters, or more if you count special symbols – either way, the alphabet is finite).

We will now enumerate the strings in such a way that each string appears exactly once in the list. We will use the same trick as used in Lecture note 10 to enumerate the elements of $\{0,1\}^*$ We get our bijection by setting $f(n)$ to be the n-th string in the list. List all strings of length 1 in lexicographic order, and then all strings of length 2 in lexicographic order, and then strings of length 3 in lexicographic order, and so forth. Since at each step, there are only finitely many strings of a particular length ℓ, any string of finite length appears in the list. It is also clear that each string appears exactly once in this list.

(e) Countably infinite. Let $\mathscr{A} = \{a_1, a_2, \dots\}$ denote the alphabet. (We are making use of the fact that the alphabet is countably infinite when we assume there is such an enumeration.) We will provide two solutions:

Alternative 1: We will enumerate all the strings similar to that in part (b), although the enumeration requires a little more finesse. Notice that if we tried to list all strings of length 1, we would be stuck forever, since the alphabet is infinite! On the other hand, if we try to restrict our alphabet and only print out strings containing the first character $a \in \mathscr{A}$, we would also have a similar problem: the list

$$a, aa, aaa, \dots$$

also does not end.

The idea is to restrict *both* the length of the string and the characters we are allowed to use:

(a) List all strings containing only a_1 which are of length at most 1.

(b) List all strings containing only characters in $\{a_1, a_2\}$ which are of length at most 2 and have not been listed before.

(c) List all strings containing only characters in $\{a_1, a_2, a_3\}$ which are of length at most 3 and have not been listed before.

(d) Proceed onwards.

At each step, we have restricted ourselves to a finite alphabet with a finite length, so each step is guaranteed to terminate. To show that the enumeration is complete, consider any string s of length ℓ; since the length is finite, it can contain at most ℓ distinct a_i from the alphabet. Let k denote the largest index of any a_i which appears in s. Then, s will be listed in step $\max(k, \ell)$, so it appears in the enumeration. Further, since we are listing only those strings that have not appeared before, each string appears exactly once in the listing.

Alternative 2: We will encode the strings into ternary strings. Recall that we used a similar trick in Lecture note 10 to show that the set of all polynomials with natural coefficients is countable. Suppose, for example, we have a string: $S = a_5a_2a_7a_4a_6$. Corresponding to each of the characters in this string, we can write its index as a binary string: $(101, 10, 111, 100, 110)$. Now, we can construct a ternary string where "2" is inserted as a separator between each binary string. Thus we map the string S to a ternary string: 101210211121002110. It is clear that this mapping is injective, since the original string S can be uniquely recovered from this ternary string. Thus we have an injective map to $\{0,1,2\}^*$. From Lecture note 10, we know that the set $\{0,1,2\}^*$ is countable, and hence the set of all strings with finite length over $\mathscr{A}$ is countable.

(f) Uncountably infinite. We can use a diagonalization argument. First, for a string s, define $s[i]$ as the i-th character in the string (where the first character is position 0), where $i \in \mathbb{N}$ because the strings are infinite. Now suppose for contradiction that we have an enumeration of strings s_i for all $i \in \mathbb{N}$: then define the string s' as $s'[i] = (\text{the next character in the alphabet after } s_i[i])$, where the character after z loops around back to a. Then s' differs at position i from s_i for all $i \in \mathbb{N}$, so it is not accounted for in the enumeration, which is a contradiction. Thus, the set is uncountable.

Alternative 1: The set of all infinite strings containing only as and bs is a subset of the set we're counting. We can show a bijection from this subset to the real interval $\mathbb{R}[0,1]$, which proves the uncountability of the subset and therefore entire set as well: given a string in $\{a,b\}^*$, replace the as with 0s and bs with 1s and prepend $'0.'$ to the string, which produces a unique binary number in $\mathbb{R}[0,1]$ corresponding to the string.

3 Fixed Points

Note 12

Consider the problem of determining if a program P has any fixed points. Given any program P, a fixed point is an input x such that $P(x)$ outputs x.

(a) Prove that the problem of determining whether a program has a fixed point is uncomputable.

(b) Consider the problem of outputting a fixed point of a program if it has one, and outputting "Null" otherwise. Prove that this problem is uncomputable.

(c) Consider the problem of outputting a fixed point of a program F if the fixed point exists *and* is a natural number, and outputting "Null" otherwise. If an input is a natural number, then it has no leading zero before its most significant bit.

Show that if this problem can be solved, then the problem in part (b) can be solved. What does this say about the computability of this problem? (You may assume that the set of all possible inputs to a program is countable, as is the case on your computer.)

Solution:

(a) We can prove this by reducing from the Halting Problem. Suppose we had some program `FixedPoint(F)` that solved the fixed-point problem. We can define `TestHalt(F, x)` as follows:

```
def TestHalt(F, x):
    def F'(y):
        F(x)
        return y
    return FixedPoint(F_prime)
```

If $F(x)$ halts, we have that $F'(y)$ will always just return y, so every input is a fixed point. On the other hand, if $F(x)$ does not halt, F' won't return anything for any input y, so there can't be any fixed points. Thus, our definition of `TestHalt` must always work, which is a contradiction; this tells us that `FixedPoint` cannot exist.

(b) If this problem is solvable then the problem in part (a) is solvable, as we can output "no" to whether F has a fixed point if the program in part (b) returns "Null" and "yes" otherwise.

(c) The intuition is that there is a bijection between the set of all inputs and $\mathbb{N}$ so we can reduce the problem in part (b) to this problem. In particular, since the set of all inputs is countably infinite, there exists a bijective function g that maps a natural number n to a unique input string $g(n)$. Also, we can extend the definition of g slightly so that $g(\text{"Null"}) = \text{"Null"}$ so that it is still a bijection.

Consider the following program:

```
def FindFixedPoint(F):
    def F'(n):
        if n not in ℕ:
            error
        x = g(n)
        if F(x) = x:
            return n
        else:
            return n+1
    return g(FindFixedPointInN(F'))
```

Since g is a bijection, g^{-1} exists, and if $g(n) = x$, then $n = g^{-1}(x)$. If there is some x such that $F(x) = x$, then $n = g^{-1}(x)$ will be a fixed point for F'. Thus, if F has a fixed point, `FindFixedPointInN`(F') will return some n where $g(n)$ is a fixed point for F.

On the other hand, if $F(x) \neq x$ for every input x, then $F'(n) = n+1 \neq n$ for every n, which means F' will also not have a fixed point. Thus, our program solves the problem in part (b), which is already shown to be uncomputable. This means that this problem is also uncomputable.

4 Unprogrammable Programs

Note 12

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).

Hint: Use P to solve the halting problem, and consider defining two subroutines to pass in to P, where one of the subroutines always loops.

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 boils down 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)`.

5 Counting, Counting, and More Counting

Note 10

The only way to learn counting is to practice, practice, practice, so here is your chance to do so. Although there are many subparts, each subpart is fairly short, so this problem should not take any longer than a normal CS70 homework problem. You do not need to show work, and **Leave your answers as an expression** (rather than trying to evaluate it to get a specific number).

(a) How many 19-digit ternary (0,1,2) bitstrings are there such that no two adjacent digits are equal?

(b) Two identical decks of 52 cards are mixed together, yielding a stack of 104 cards. How many different ways are there to order this stack of 104 cards?

(c) An anagram of ALABAMA is any re-ordering of the letters of ALABAMA, i.e., any string made up of the letters A, L, A, B, A, M, and A, in any order. The anagram does not have to be an English word.

i. How many different anagrams of ALABAMA are there?

ii. How many different anagrams of MONTANA are there?

(d) How many different anagrams of ABCDEF are there if:

i. C is the left neighbor of E

ii. C is on the left of E (and not necessarily E's neighbor)

(e) We have 8 balls, numbered 1 through 8, and 25 bins. How many different ways are there to distribute these 8 balls among the 25 bins? Assume the bins are distinguishable (e.g., numbered 1 through 25).

(f) There are exactly 20 students currently enrolled in a class. How many different ways are there to pair up the 20 students, so that each student is paired with one other student? Solve this in at least 2 different ways. **Your final answer must consist of two different expressions.**

Solution:

(a) There are 3 options for the first digit. For each of the next digits, they only have 2 options because they cannot be equal to the previous digit. Thus, $3 \cdot 2^{18}$

(b) If we consider the 104! rearrangements of 2 identical decks, since each card appears twice, we would have overcounted each distinct rearrangement. Consider any distinct rearrangement of the 2 identical decks of 52 cards and see how many times this appears among the rearrangement of 104 cards where each card is treated as different. For each identical pair (such as the two Ace of spades), there are two ways they could be permuted among each other (since $2! = 2$). This holds for each of the 52 pairs of identical cards. So the number 104! overcounts the actual number of rearrangements of 2 identical decks by a factor of 2^{52}. Hence, the actual number of rearrangements of 2 identical decks is $\frac{104!}{2^{52}}$.

(c) i. ALABAMA: The number of ways of rearranging 7 distinct letters and is 7!. In this 7 letter word, the letter A is repeated 4 times while the other letters appear once. Hence, the number 7! overcounts the number of different anagrams by a factor of 4! (which is the number of ways of permuting the 4 A's among themselves). Aka, we only want $1/4!$ out of the total rearrangements. Hence, there are $\frac{7!}{4!}$ anagrams.

ii. MONTANA: In this 7 letter word, the letter A and N are each repeated 2 times while the other letters appear once. Hence, the number 7! overcounts the number of different anagrams by a factor of $2! \times 2!$ (one factor of 2! for the number of ways of permuting the 2 A's among themselves and another factor of 2! for the number of ways of permuting the 2 N's among themselves). Hence, there are $\frac{7!}{(2!)^2}$ different anagrams.

(d) i. Suppose we consider CE to be a new letter X; with this replacement, the question is just to count the number of rearrangements of 5 distinct letters, which is 5!.

ii. Symmetry: Let A be the set of all the rearranging of ABCDEF with C on the left side of E, and B be the set of all the rearranging of ABCDEF with C on the right side of E. $|A \cup B| = 6!, |A \cap B| = 0$. There is a bijection between A and B by construct a operation of exchange the position of C and E. Thus $|A| = |B| = \frac{6!}{2}$.

(e) Each ball has a choice of which bin it should go to. So each ball has 25 choices and the 8 balls can make their choices separately. Hence, there are 25^8 ways.

(f) **Answer 1:** Let's number the students from 1 to 20. Student 1 has 19 choices for her partner. Let i be the smallest index among students who have not yet been assigned partners. Then no matter what the value of i is (in particular, i could be 2 or 3), student i has 17 choices for her partner. The next smallest indexed student who doesn't have a partner now has 15 choices for her partner. Continuing in this way, the number of pairings is $19 \times 17 \times 15 \times \cdots \times 1 = \prod_{i=1}^{10}(2i-1)$.

Answer 2: Arrange the students numbered 1 to 20 in a line. There are 20! such arrangements. We pair up the students at positions $2i-1$ and $2i$ for i ranging from 1 to 10. You should be able to see that the 20! permutations of the students doesn't miss any possible pairing. However, it counts every different pairing multiple times. Fix any particular pairing of students. In this pairing, the first pair had freedom of 10 positions in any permutation that generated it, the second pair had a freedom of 9 positions in any permutation that generated it, and so on. There is also the freedom for the elements within each pair i.e. in any student pair (x,y), student x could have appeared in position $2i-1$ and student y could have appeared in position $2i$ and also vice versa. This gives 2 ways for each of the 10 pairs. Thus, in total, these freedoms cause $10! \times 2^{10}$ of the 20! permutations to give rise to this particular pairing. This holds for each of the different pairings. Hence, 20! overcounts the number of different pairings by a factor of $10! \times 2^{10}$. Hence, there are $\frac{20!}{10! \cdot 2^{10}}$ pairings.

Answer 3: In the first step, pick a pair of students from the 20 students. There are $\binom{20}{2}$ ways to do this. In the second step, pick a pair of students from the remaining 18 students. There are $\binom{18}{2}$ ways to do this. Keep picking pairs like this, until in the tenth step, you pick a pair of students from the remaining 2 students. There are $\binom{2}{2}$ ways to do this. Multiplying all these,

we get $\binom{20}{2}\binom{18}{2}\ldots\binom{2}{2}$. However, in any particular pairing of 20 students, this pairing could have been generated in 10! ways using the above procedure depending on which pairs in the pairing got picked in the first step, second step, ..., tenth step. Hence, we have to divide the above number by 10! to get the number of different pairings. Thus there are $\binom{20}{2}\binom{18}{2}\cdots\binom{2}{2}/10!$ different pairings of 20 students.

You may want to check for yourself that all three methods are producing the same integer, even though they are expressed very differently.

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 08

1 Probability Warm-Up

Note 13

(a) Suppose that we have a bucket of 30 green balls and 70 orange balls. If we pick 15 balls uniformly out of the bucket, what is the probability of getting exactly k green balls (assuming $0 \leq k \leq 15$) if the sampling is done **with** replacement, i.e. after we take a ball out the bucket we return the ball back to the bucket for the next round?

(b) Same as part (a), but the sampling is **without** replacement, i.e. after we take a ball out the bucket we **do not** return the ball back to the bucket.

(c) If we roll a regular, 6-sided die 5 times. What is the probability that at least one value is observed more than once?

Solution:

(a) Let A be the event of getting exactly k green balls. Then treating all balls as distinguishable, we have a total of 100^{15} possibilities to draw a sequence of 15 balls. In order for this sequence to have exactly k green balls, we need to first assign them one of $\binom{15}{k}$ possible locations within the sequence. Once done so, we have 30^k ways of actually choosing the green balls, and 70^{15-k} possibilities for choosing the orange balls. Thus in total we arrive at

$$\mathbb{P}[A] = \frac{\binom{15}{k} \cdot 30^k \cdot 70^{15-k}}{100^{15}} = \binom{15}{k} \left(\frac{3}{10}\right)^k \left(\frac{7}{10}\right)^{15-k}.$$

(b) Using a similar approach, there are a total of $100 \cdot 99 \cdots 86 = \frac{100!}{(100-15)!} = \frac{100!}{85!}$ ways to grab 15 balls.

We still want k green balls and $15-k$ orange balls, which we can select in

$$\begin{aligned} &\binom{15}{k} \cdot (30 \cdot 29 \cdots (30-(k-1))) \cdot (70 \cdot 69 \cdots (70-(15-k-1))) \\ &= \binom{15}{k} \frac{30!}{(30-k)!} \cdot \frac{70!}{(70-(15-k))!} \end{aligned}$$

ways. Here, we have $\binom{15}{k}$ possible locations for the k green balls, and we use permutations rather than combinations to account for the fact that we are picking balls without replacement.

Since our sample space is uniform, the probability is thus

$$\mathbb{P}[A] = \frac{\binom{15}{k} \frac{30!}{(30-k)!} \cdot \frac{70!}{(70-(15-k))!}}{\frac{100!}{(100-15)!}} = \frac{\binom{15}{k} \frac{30!}{(30-k)!} \cdot \frac{70!}{(55+k)!}}{\frac{100!}{85!}}.$$

Alternative Solution: Instead of considering a probability space where each ball is distinct, we can also consider a probability space where each ball is indistinguishable, and order does not matter. Intuitively, this is equivalent to the previous solution, since the numerator and denominator are accounting for order in the exact same way; considering the same situation without order and with indistinguishable balls is equivalent to dividing both the numerator and denominator by 15! for the number of arrangements of the 15 balls we select.

With this in mind, we note that the size of the sample space is now $\binom{100}{15}$, since we are choosing 15 balls out of a total of 100. To find $|A|$, we need to be able to find out how many ways we can choose k green balls and $15-k$ orange balls. This means that we have $|A| = \binom{30}{k}\binom{70}{15-k}$, since we must select k green balls out of 30 total, and $15-k$ orange balls out of 70 total.

Putting this together, we have

$$\mathbb{P}[A] = \frac{\binom{30}{k}\binom{70}{15-k}}{\binom{100}{15}}.$$

(c) Let B be the event that at least one value is observed more than once. We see that $\mathbb{P}[B] = 1 - \mathbb{P}[\overline{B}]$. So we need to find out the probability that the values of the 5 rolls are distinct. We see that $\mathbb{P}[\overline{B}]$ simply the number of ways to choose 5 numbers (order matters) divided by the sample space (which is 6^5). So

$$\mathbb{P}[\overline{B}] = \frac{6!}{6^5} = \frac{5!}{6^4}.$$

And

$$\mathbb{P}[B] = 1 - \frac{5!}{6^4}.$$

2 Five Up

Note 13

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?

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 probability of observing at least one head?

(f) What is the probability you will observe more heads than tails?

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 probability of observing the outcome HHHTT? What about HHHHT?

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

(i) What is the probability you will observe more heads than tails?

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 have 2 or fewer heads. Denote the new set $\overline{A}$. Then we know that A and $\overline{A}$ have the same size and they together cover the whole sample space. Therefore, $|A| = |\overline{A}|$ and $|A| + |\overline{A}| = 2^5$, 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) To have more heads than tails is to claim that we flip at least 3 heads. 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: $\frac{\binom{5}{3}+\binom{5}{4}+\binom{5}{5}}{2^5} = \frac{1}{2}$

Alternatively, we see that for every sequence with more heads than tails we can create a corresponding sequence with more tails than heads by "flipping" the bits. For example, a sequence HTHHT which has more heads than tails corresponds to a flipped sequence THTTH which has more tails than heads. As a result, for every sequence with more heads there's a sequence with more tails. Thus, the probability of having a sequence with more heads is $1/2$.

(g) By using the same idea of independence we get for HHHTT:

$$\frac{2}{3}\times\frac{2}{3}\times\frac{2}{3}\times\frac{1}{3}\times\frac{1}{3}=\frac{2^3}{3^5}$$

For HHHHT, we get:

$$\frac{2}{3}\times\frac{2}{3}\times\frac{2}{3}\times\frac{2}{3}\times\frac{1}{3}=\frac{2^4}{3^5}$$

(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. Thus for each $3\le i\le 5$, we need to count the total number of outcomes with exactly i heads and multiply it by the probability of achieving any of those outcomes. This yields:

$$\begin{aligned}\mathbb{P}[\geq 3 \text{ Heads}] &= \binom{5}{3}\left(\frac{2}{3}\right)^3\left(\frac{1}{3}\right)^2+\binom{5}{4}\left(\frac{2}{3}\right)^4\left(\frac{1}{3}\right)^1+\binom{5}{5}\left(\frac{2}{3}\right)^5\left(\frac{1}{3}\right)^0\\ &= \binom{5}{3}\left(\frac{2}{3}\right)^3\left(\frac{1}{3}\right)^2+\binom{5}{4}\left(\frac{2}{3}\right)^4\left(\frac{1}{3}\right)+\binom{5}{5}\left(\frac{2}{3}\right)^5.\end{aligned}$$

3 Aces

Note 13
Note 14

Consider a standard 52-card deck of cards:

(a) Find the probability of getting an ace or a red card, when drawing a single card.

(b) Find the probability of getting an ace or a spade, but not both, when drawing a single card.

(c) Find the probability of getting the ace of diamonds when drawing a 5 card hand.

(d) Find the probability of getting exactly 2 aces when drawing a 5 card hand.

(e) Find the probability of getting at least 1 ace when drawing a 5 card hand.

(f) Find the probability of getting at least 1 ace or at least 1 heart when drawing a 5 card hand.

Solution:

(a) Inclusion-Exclusion Principle: $\frac{4}{52}+\frac{26}{52}-\frac{2}{52}=\frac{28}{52}=\frac{7}{13}$.

(b) Inclusion-Exclusion, but we exclude the intersection: $\frac{4}{52}+\frac{13}{52}-2\cdot\frac{1}{52}=\frac{15}{52}$.

(c) Ace of diamonds is fixed, but the other 4 cards in the hand can be any other card: $\frac{\binom{51}{4}}{\binom{52}{5}}$.

(d) Account for the number of ways to draw 2 aces and the number of ways to draw 3 non-aces: $\frac{\binom{4}{2}\cdot\binom{48}{3}}{\binom{52}{5}}$.

(e) Complement to getting no aces: $\mathbb{P}[\text{at least one ace}] = 1 - \mathbb{P}[\text{zero aces}] = 1 - \frac{\binom{48}{5}}{\binom{52}{5}}$.

(f) Complement to getting no aces and no hearts: $\mathbb{P}[\text{at least one ace OR at least one heart}] = 1 - \mathbb{P}[\text{zero aces AND zero hearts}] = 1 - \frac{\binom{36}{5}}{\binom{52}{5}}$. This is because $52 - 13 - 3 = 36$, where 13 is the number of hearts and 3 is the number of non-heart aces.

4 Independent Complements

Note 14

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:

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

(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.)

5 Faulty Lightbulbs

Note 13
Note 14

Box 1 contains 1000 lightbulbs of which 10% are defective. Box 2 contains 2000 lightbulbs of which 5% are defective.

(a) Suppose a box is given to you at random and you randomly select a lightbulb from the box. If that lightbulb is defective, what is the probability you chose Box 1?

(b) Suppose now that a box is given to you at random and you randomly select two light- bulbs from the box. If both lightbulbs are defective, what is the probability that you chose from Box 1?

Solution:

(a) Let:

- D denote the event that the lightbulb we selected is defective.
- B_i denote the event that the lightbulb we selected is from Box i.

We wish to compute $\mathbb{P}[B_1 \mid D]$. Using Bayes' Rule we get:

$$\begin{aligned}\mathbb{P}[B_1 \mid D] &= \frac{\mathbb{P}[D \mid B_1] \cdot \mathbb{P}[B_1]}{\mathbb{P}[B_1] \cdot \mathbb{P}[D \mid B_1] + \mathbb{P}[B_2] \cdot \mathbb{P}[D \mid B_2]} \\ &= \frac{0.1 \cdot 0.5}{0.5 \cdot 0.1 + 0.5 \cdot 0.05} \\ &= \frac{2}{3}\end{aligned}$$

(b) Let:

- D' denote the event that both the lightbulbs we selected are defective.
- B_i denote the event that the lightbulb we selected is from Box i.

We wish to compute $\mathbb{P}[B_1 \mid D']$. Using Bayes' Rule we get:

$$\begin{aligned}
\mathbb{P}[B_1 \mid D'] &= \frac{\mathbb{P}[D' \mid B_1] \cdot \mathbb{P}[B_1]}{\mathbb{P}[B_1] \cdot \mathbb{P}[D' \mid B_1] + \mathbb{P}[B_2] \cdot \mathbb{P}[D' \mid B_2]} \\
&= \frac{\frac{100}{1000} \cdot \frac{99}{999} \cdot 0.5}{0.5 \cdot \frac{100}{1000} \cdot \frac{99}{999} + 0.5 \cdot \frac{100}{2000} \cdot \frac{99}{1999}} \\
&\approx 0.8
\end{aligned}$$

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 09

1 Symmetric Marbles

Note 14

A bag contains 4 red marbles and 4 blue marbles. Rachel and Brooke play a game where they draw four marbles in total, one by one, uniformly at random, without replacement. Rachel wins if there are more red than blue marbles, and Brooke wins if there are more blue than red marbles. If there are an equal number of marbles, the game is tied.

(a) Let A_1 be the event that the first marble is red and let A_2 be the event that the second marble is red. Are A_1 and A_2 independent?

(b) What is the probability that Rachel wins the game?

(c) Given that Rachel wins the game, what is the probability that all of the marbles were red?

Now, suppose the bag contains 8 red marbles and 4 blue marbles. Moreover, if there are an equal number of red and blue marbles among the four drawn, Rachel wins if the third marble is red, and Brooke wins if the third marble is blue. All other rules stay the same.

(d) What is the probability that the third marble is red?

(e) Given that there are k red marbles among the four drawn, where $0 \leq k \leq 4$, what is the probability that the third marble is red? Answer in terms of k.

(f) Given that the third marble is red, what is the probability that Rachel wins the game?

Solution:

(a) They are not independent; removing one red marble lowers the probability of the next marble being red.

(b) Let p be the probability that Rachel wins. Since there are an equal number of red and blue marbles, by symmetry, the probability that Rachel wins and the probability that Brooke wins is the same. Thus, the probability that there is a tie is $1 - p - p = 1 - 2p$.

We now compute the probability that there is a tie. For there to be a tie, two of the four marbles need to be red. There are $\binom{8}{4}$ ways to pick 4 marbles, and $\binom{4}{2}\binom{4}{2}$ to pick 2 red and blue marbles, respectively, giving a probability of

$$\frac{\binom{4}{2}\binom{4}{2}}{\binom{8}{4}} = \frac{36}{70} = \boxed{\frac{18}{35}}.$$

We conclude that $1-2p=\frac{18}{35}$. Solving for p gives $p=\boxed{\frac{17}{70}}$.

(c) Let A be the event that there are 3 red marbles drawn, and let B be the event that there are 4 red marbles drawn. We wish to compute

$$\mathbb{P}[B \mid (A \cup B)] = \frac{\mathbb{P}[B \cap (A \cup B)]}{\mathbb{P}[A \cup B]} = \frac{\mathbb{P}[B]}{\mathbb{P}[A]+\mathbb{P}[B]}.$$

Similar to the calculation in part (b), the probability that there are 3 red marbles drawn is $\frac{\binom{4}{3}\binom{4}{1}}{\binom{8}{4}} = \frac{16}{70}$, and the probability that there are 4 red marbles drawn is $\frac{\binom{4}{4}\binom{4}{0}}{\binom{8}{4}} = \frac{1}{70}$, giving a final answer of $\frac{\frac{1}{70}}{\frac{16}{70}+\frac{1}{70}} = \boxed{\frac{1}{17}}$.

(d) By symmetry, the probability that the third marble is red is the same as the probability that the first marble is red, or the same as any marble being red. One way to see this is to imagine drawing the four marbles in order, then moving the first marble drawn to the third position. This is another way to draw four marbles that yields the same distribution.

There are 8 red marbles, and 12 marbles in total. Thus, the probability that the third marble is red is $\frac{8}{12} = \boxed{\frac{2}{3}}$.

(e) We are given that there are k red marbles among the 4 drawn. By symmetry, each marble has the same probability of being red, so the probability that the third marble is red is $\boxed{\frac{k}{4}}$.

(f) The only way for Rachel to lose the game given that the third marble is red is if all the other marbles are blue. The probability that the third marble is red and all the other marbles are blue is $\frac{4}{12}\cdot\frac{3}{11}\cdot\frac{8}{10}\cdot\frac{2}{9} = \frac{8}{495}$, and the probability that the third marble is red is $\frac{8}{12} = \frac{2}{3}$, so the probability that Rachel loses given that the third marble is red is $\frac{\frac{8}{495}}{\frac{2}{3}} = \frac{4}{165}$, and the probability that Rachel wins given that the third marble is red is $\boxed{\frac{161}{165}}$.

2 Man Speaks Truth

Note 14

Consider a man who speaks the truth with probability $\frac{3}{4}$.

(a) Suppose the man flips a biased coin that comes up heads $1/3$ of the time, and reports that it is heads.

(i) What is the probability that the coin actually landed on heads?

(ii) Unconvinced, you ask him if he just lied to you, to which he replies "no". What is the probability now that the coin actually landed on heads?

(iii) Did the probability go up, go down, or stay the same with this new information? Explain in words why this should be the case.

(b) Suppose the man rolls a fair 6-sided die. When you ask him if the die came up with a 6, he answers "yes".

(i) What is the probability that the die actually came up with a 6?

(ii) Skeptical, you also ask him whether the die came up with a 1, to which he replies "yes". What is the probability now that the die actually came up with a 6?

(iii) Did the probability go up, go down, or stay the same with this new information? Explain in words why this should be the case.

Solution:

(a) (i) Let S_H denote the event the man says heads, H be the event that the coin comes up heads, and T be the event that the coin comes up tails (note that H and T are complements of each other).

We're given that the man says heads (i.e. that S_H occurs), and we want to find the probability that the coin comes up heads. Using Bayes' rule and total probability, we have

$$\mathbb{P}[H \mid S_H] = \frac{\mathbb{P}[S_H \cap H]}{\mathbb{P}[S_H]} = \frac{\mathbb{P}[S_H \mid H]\mathbb{P}[H]}{\mathbb{P}[S_H \mid H]\mathbb{P}[H] + \mathbb{P}[S_H \mid T]\mathbb{P}[T]}.$$

Here, we have $\mathbb{P}[H] = \frac{1}{3}$ and $\mathbb{P}[T] = \frac{2}{3}$. We know that the man tells the truth $\frac{3}{4}$ of the time, so we also have the conditional probabilities $\mathbb{P}[S_H \mid H] = \frac{3}{4}$ (since the man tells the truth here) and $\mathbb{P}[S_H \mid T] = \frac{1}{4}$ (since the man tells a lie here).

Plugging these probabilities in, we have

$$\mathbb{P}[H \mid S_H] = \frac{\frac{3}{4} \cdot \frac{1}{3}}{\frac{3}{4} \cdot \frac{1}{3} + \frac{1}{4} \cdot \frac{2}{3}} = \frac{3}{3+2} = \frac{3}{5}.$$

(ii) Suppose we define the following events:

- H is the event the coin lands heads, and T is the event the coin lands tails.
- S_H is the event the man says heads, and S_T is the event the man says tails.
- S_Y is the event the man says he lied (responded yes to the question), and S_N is the event the man says he told the truth (responded no to the question).

We're given that the man says heads (i.e. that S_H occurs), and that the man said he did not lie (i.e. that S_N occurs); we want to find the probability that the coin comes up heads. Using Bayes' rule with the product rule and total probability, we have

$$\begin{aligned}
\mathbb{P}[H \mid S_N \cap S_H] &= \frac{\mathbb{P}[S_N \cap S_H \cap H]}{\mathbb{P}[S_N \cap S_H]} \\
&= \frac{\mathbb{P}[S_N \cap S_H \cap H]}{\mathbb{P}[S_N \cap S_H \cap H] + \mathbb{P}[S_N \cap S_H \cap T]} \\
&= \frac{\mathbb{P}[S_N \mid S_H \cap H]\mathbb{P}[S_H \mid H]\mathbb{P}[H]}{\mathbb{P}[S_N \mid S_H \cap H]\mathbb{P}[S_H \mid H]\mathbb{P}[H] + \mathbb{P}[S_N \mid S_H \cap T]\mathbb{P}[S_H \mid T]\mathbb{P}[T]}
\end{aligned}$$

Here, we again have $\mathbb{P}[H] = \frac{1}{3}$ and $\mathbb{P}[T] = \frac{2}{3}$. We also have $\mathbb{P}[S_H \mid H] = \frac{3}{4}$ (since the man told the truth here) and $\mathbb{P}[S_H \mid T] = \frac{1}{4}$ (since the man lied here).

Further, we have $\mathbb{P}[S_N \mid S_H \cap H] = \frac{3}{4}$ (the man told the truth here; he did not lie when he said heads, since the coin was actually heads) and we also have $\mathbb{P}[S_N \mid S_H \cap T] = \frac{1}{4}$ (the man lied here; he had lied prior when he said heads, so his reply that he did not lie is *also* a lie).

Plugging these values in, we have

$$\mathbb{P}[H \mid S_N \cap S_H] = \frac{\frac{3}{4} \cdot \frac{3}{4} \cdot \frac{1}{3}}{\frac{3}{4} \cdot \frac{3}{4} \cdot \frac{1}{3} + \frac{1}{4} \cdot \frac{1}{4} \cdot \frac{2}{3}} = \frac{9}{9+2} = \frac{9}{11}.$$

Intuitively, what we're doing here is taking into account the *order* in which the events occur through the product rule. We essentially have three points in time: (1) the man flips the coin, (2) the man states the outcome of the coin, and (3) the man answers whether he lied or not. The outcomes of the last two points in time are fixed, given the context of the problem (we *know* the man stated the coin is heads, and we *know* the man stated he did not lie), so the only thing that can possibly vary is the outcome of the coin (i.e. it can either be heads or tails). This gives the two branches in the denominator, and it is why we only look at one of these branches in the numerator (i.e. when the coin landed heads).

(iii) This probability went up with the new information. Intuitively, this is because the man tells the truth more often than he lies. The fact that he reaffirms that he did not lie means that there's a higher probability that the coin actually did land on heads.

(b) (i) Let R_6 be the event that he rolled a 6, let R_N be the event that he did not roll a 6, and let S_6 be the event that the man says it was a 6.

We're given that the man says it was a 6 (i.e. S_6 occurs), and we want to find the probability that he actually rolled a 6. Using Bayes' rule and total probability, we have

$$\mathbb{P}[R_6 \mid S_6] = \frac{\mathbb{P}[R_6 \cap S_6]}{\mathbb{P}[S_6]} = \frac{\mathbb{P}[S_6 \mid R_6]\mathbb{P}[R_6]}{\mathbb{P}[S_6 \mid R_6]\mathbb{P}[R_6] + \mathbb{P}[S_6 \mid R_N]\mathbb{P}[R_N]}.$$

Here, since the die is fair, we have $\mathbb{P}[R_6] = \frac{1}{6}$ and $\mathbb{P}[R_N] = \frac{5}{6}$. We also have $\mathbb{P}[S_6 \mid R_6] = \frac{3}{4}$ (since the man told the truth here) and $\mathbb{P}[S_6 \mid R_N] = \frac{1}{4}$ (since the man lied here).

Plugging these values in, we have

$$\mathbb{P}[R_6 \mid S_6] = \frac{\frac{3}{4} \cdot \frac{1}{6}}{\frac{3}{4} \cdot \frac{1}{6} + \frac{1}{4} \cdot \frac{5}{6}} = \frac{3}{3+5} = \frac{3}{8}.$$

(ii) Suppose we define the following events:

- R_6 is the event he rolled a 6, R_1 is the event he rolled a 1, and R_N is the event he rolled neither 1 nor 6.
- S_6 is the event he says the die was a 6, S_1 is the event he says the die was a 1.

We're given that the man says the die was a 6 (i.e. S_6 occurred) *and* he says the die was a 1 (i.e. S_1 occurred); we want to find the probability that the die actually was a 6. Using

Bayes' rule and total probability (note that we have a partition of *three* events here), we have

$$\begin{aligned}
&\mathbb{P}[R_6 \mid S_1 \cap S_6] \\
&= \frac{\mathbb{P}[S_1 \cap S_6 \cap R_6]}{\mathbb{P}[S_1 \cap S_6]} \\
&= \frac{\mathbb{P}[S_1 \cap S_6 \cap R_6]}{\mathbb{P}[S_1 \cap S_6 \cap R_1] + \mathbb{P}[S_1 \cap S_6 \cap R_6] + \mathbb{P}[S_1 \cap S_6 \cap R_N]} \\
&= \frac{\mathbb{P}[S_1 \mid S_6 \cap R_6]\mathbb{P}[S_6 \mid R_6]\mathbb{P}[R_6]}{\mathbb{P}[S_1 \mid S_6 \cap R_6]\mathbb{P}[S_6 \mid R_6]\mathbb{P}[R_6] + \mathbb{P}[S_1 \mid S_6 \cap R_1]\mathbb{P}[S_6 \mid R_1]\mathbb{P}[R_1] + \mathbb{P}[S_1 \mid S_6 \cap R_N]\mathbb{P}[S_6 \mid R_N]\mathbb{P}[R_N]}
\end{aligned}$$

Here, since the die is fair, we have $\mathbb{P}[R_1] = \mathbb{P}[R_6] = \frac{1}{6}$, while $\mathbb{P}[R_N] = \frac{4}{6}$.

For each of the three possible events for the outcome of the die, we have the conditional probabilities

- $\mathbb{P}[S_6 \mid R_1] = \frac{1}{4}$, since the man lied
- $\mathbb{P}[S_6 \mid R_6] = \frac{3}{4}$, since the man told the truth
- $\mathbb{P}[S_6 \mid R_N] = \frac{1}{4}$, since the man lied

Notice that if we condition on the event that the die had a specific outcome (ex. conditioned on the event the die rolled a 6), the event that the man says it was a 6 is actually independent of the event the man says it was a 1. Intuitively, this is because we already know the outcome of the die, so the fact the man says it was a 6 doesn't impact the probability he says it is also a 1—it only encapsulates whether the man lied or not.

This means that we also have the following conditional probabilities:

- $\mathbb{P}[S_1 \mid S_6 \cap R_1] = \mathbb{P}[S_1 \mid R_1] = \frac{3}{4}$, since the man told the truth
- $\mathbb{P}[S_1 \mid S_6 \cap R_6] = \mathbb{P}[S_1 \mid R_6] = \frac{1}{4}$, since the man lied
- $\mathbb{P}[S_1 \mid S_6 \cap R_N] = \mathbb{P}[S_1 \mid R_N] = \frac{1}{4}$, since the man lied

Plugging these all in, we have

$$\mathbb{P}[R_6 \mid S_1 \cap S_6] = \frac{\frac{1}{4} \cdot \frac{3}{4} \cdot \frac{1}{6}}{\frac{1}{4} \cdot \frac{3}{4} \cdot \frac{1}{6} + \frac{3}{4} \cdot \frac{1}{4} \cdot \frac{1}{6} + \frac{1}{4} \cdot \frac{1}{4} \cdot \frac{4}{6}} = \frac{3}{3+3+4} = \frac{3}{10}.$$

Similar to the previous part, what we're doing here is essentially taking into account the order in which the events occur. However, here, it's equally valid to condition on S_1 first, and then compute the probability of S_6 (i.e. swapping S_1 and S_6 above), due to their independence conditioned on R_1, R_6, or R_N.

The three points in time we're considering now are (1) the man rolls the die, (2) the man states whether it was a 6, and (3) the man states whether it was a 1. Again, the latter two outcomes are fixed due to the context in the problem, and the first outcome is free to vary. This is why we need three branches in the denominator, one for each of R_1, R_6, and R_N. We also can't just divide it up into two events, since the response to "did the die come up with a 1" depends on whether the die actually landed on 1, and the response to "did the die come up with a 6" depends on whether the die actually landed on 6; it's easiest to consider each case separately.

(iii) The probability went down with the new information. Since it's impossible for the man to have told the truth in both situations (i.e. the die can't possibly have rolled both a 1 and a 6), it must be the case that one of the statements is a lie. This should lower the probability that the first statement is actually true, i.e. that the die actually landed on a 6.

3 Cliques in Random Graphs

Note 13
Note 14

Consider the 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.

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

(b) A k-clique in a 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 E_S be the event that a set S forms a clique. What is the probability of E_S for a particular set S of k vertices?

(c) Suppose that $V_1 = \{v_1, \ldots, v_\ell\}$ and $V_2 = \{w_1, \ldots, w_k\}$ are two arbitrary sets of vertices. What conditions must V_1 and V_2 satisfy in order for E_{V_1} and E_{V_2} to be independent? Prove your answer.

(d) Prove that $\binom{n}{k} \leq n^k$. (You might find this useful in part (e)).

(e) Prove that the probability that the graph contains a k-clique, for $k \geq 4\log_2 n + 1$, is at most $1/n$. *Hint:* Use the union bound.

Solution:

(a) Between every pair of vertices, there is either an edge or there isn't. 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

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

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, so we have

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

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

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

(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

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

4 Combined Head Count

Note 19

Suppose you flip a fair coin twice.

(a) What is the sample space Ω generated from these flips?

(b) Define a random variable X to be the number of heads. What is the distribution of X?

(c) Define a random variable Y to be 1 if you get a heads followed by a tails and 0 otherwise. What is the distribution of Y?

(d) Compute the conditional probabilities $\mathbb{P}[Y = i \mid X = j]$ for all i, j.

(e) Define a third random variable $Z = X + Y$. Use the conditional probabilities you computed in part (d) to find the distribution of Z.

Solution:

(a) $\{(T,T),(H,T),(T,H),(H,H)\}$.

(b)
$$X = \begin{cases} 0 & \text{w.p.} \quad .25 \\ 1 & \text{w.p.} \quad .5 \\ 2 & \text{w.p.} \quad .25 \end{cases}$$

(c)
$$Y = \begin{cases} 0 & \text{w.p.} \quad .75 \\ 1 & \text{w.p.} \quad .25 \end{cases}$$

(d)
- $\mathbb{P}[Y = 0 \mid X = 0]$: Since $X = 0$, we have no heads; therefore, there is no chance that the first coin is heads, so Y must be 0. So $\mathbb{P}[Y = 0 \mid X = 0] = 1$.
- $\mathbb{P}[Y = 1 \mid X = 0] = 0$ as $\mathbb{P}[Y = 1 \mid X = 0] = 1 - \mathbb{P}[Y = 0 \mid X = 0] = 1 - 1 = 0$.
- $\mathbb{P}[Y = 0 \mid X = 1]$: If we have one head, then we have one of two outcomes, (H,T) or (T,H), and since this is a fair coin, both outcomes happen with equal probability. Only (T,H) makes $Y = 0$; thus $\mathbb{P}[Y = 0 \mid X = 1] = \frac{1}{2}$.
- $\mathbb{P}[Y = 1 \mid X = 1] = 0$ as $\mathbb{P}[Y = 1 \mid X = 1] = 1 - \mathbb{P}[Y = 0 \mid X = 1] = 1 - \frac{1}{2} = \frac{1}{2}$.
- $\mathbb{P}[Y = 0 \mid X = 2]$: Since $X = 0$, we have no tails; therefore, there is no chance that the second coin is tails, so Y must be 0. So $\mathbb{P}[Y = 0 \mid X = 2] = 1$.
- $\mathbb{P}[Y = 1 \mid X = 2] = 0$ as $\mathbb{P}[Y = 1 \mid X = 2] = 1 - \mathbb{P}[Y = 0 \mid X = 2] = 1 - 1 = 0$.

(e) Let's determine the values Z can take and the corresponding probabilities:

- $Z = 0$: $\mathbb{P}(Z = 0) = \mathbb{P}(X = 0 \cap Y = 0) = \mathbb{P}(X = 0) \cdot \mathbb{P}(Y = 0 \mid X = 0) = .25 \cdot 1 = .25$
- $Z = 1$:
$$\begin{aligned} \mathbb{P}(Z = 1) &= \mathbb{P}(X = 0 \cap Y = 1) + \mathbb{P}(X = 1 \cap Y = 0) \\ &= \mathbb{P}(X = 0) \cdot \mathbb{P}(Y = 1 \mid X = 0) + \mathbb{P}(X = 1) \cdot \mathbb{P}(Y = 0 \mid X = 1) \qquad (1) \\ &= .25 \cdot 0 + .5 \cdot .5 = .25 \end{aligned}$$
- $Z = 2$:
$$\begin{aligned} \mathbb{P}(Z = 2) &= \mathbb{P}(X = 1 \cap Y = 1) + \mathbb{P}(X = 2 \cap Y = 0) \\ &= \mathbb{P}(X = 1) \cdot \mathbb{P}(Y = 1 \mid X = 1) + \mathbb{P}(X = 2) \cdot \mathbb{P}(Y = 0 \mid X = 2) \qquad (2) \\ &= .5 \cdot 5 + .25 \cdot 1 = .5 \end{aligned}$$
- $Z = 3$: $\mathbb{P}(Z = 3) = \mathbb{P}(X = 2 \cap Y = 1) = \mathbb{P}(X = 2) \cdot \mathbb{P}(Y = 1 \mid X = 2) = .25 \cdot 0 = 0$

$$Z = \begin{cases} 0 & \text{w.p.} \quad .25 \\ 1 & \text{w.p.} \quad .25 \\ 2 & \text{w.p.} \quad .5 \end{cases}$$

5 Max/Min Dice Rolls

Note 15

Yining rolls three fair six-sided dice.

(a) Let X denote the maximum of the three values rolled. What is the distribution of X (that is, $\mathbb{P}[X = x]$ for $x = 1,2,3,4,5,6$)? You can leave your final answer in terms of "x". [*Hint*: Try to first compute $\mathbb{P}[X \leq x]$ for $x = 1,2,3,4,5,6$]. If you want to check your answer, you can solve this problem using counting and make sure it matches with the formula you derived.

(b) Let Y denote the minimum of the three values rolled. What is the distribution of Y?

Solution:

(a) Let X denote the maximum of the three values rolled. We are interested in $\mathbb{P}(X = x)$, where $x = 1,2,3,4,5,6$. First, define X_1, X_2, X_3 to be the values rolled by the first, second, and third dice. These random variables are i.i.d. and uniformly distributed between 1 and 6 inclusive.

Following the hint we first compute $\mathbb{P}[X \leq x]$ for $x = 1,2,3,4,5,6$:

$$\mathbb{P}[X \leq x] = \mathbb{P}[X_1 \leq x]\mathbb{P}[X_2 \leq x]\mathbb{P}[X_3 \leq x] = \left(\frac{x}{6}\right)\left(\frac{x}{6}\right)\left(\frac{x}{6}\right) = \left(\frac{x}{6}\right)^3$$

Then, observing that $\mathbb{P}[X = x] = \mathbb{P}[X \leq x] - \mathbb{P}[X \leq x-1]$:

$$\mathbb{P}(X = x) = \left(\frac{x}{6}\right)^3 - \left(\frac{x-1}{6}\right)^3 = \frac{3x^2 - 3x + 1}{216} = \begin{cases} \frac{1}{216}, & x = 1 \\ \frac{7}{216}, & x = 2 \\ \frac{19}{216}, & x = 3 \\ \frac{37}{216}, & x = 4 \\ \frac{61}{216}, & x = 5 \\ \frac{91}{216}, & x = 6 \end{cases}$$

One can confirm that $\sum_{x=1}^{6} \mathbb{P}[X = x] = 1$.

(b) Similarly to the previous part, we first compute $\mathbb{P}[Y \geq y]$.

$$\mathbb{P}[Y \geq y] = \mathbb{P}[X_1 \geq y]\mathbb{P}[X_2 \geq y]\mathbb{P}[X_3 \geq y] = \left(\frac{6-(y-1)}{6}\right)\left(\frac{6-(y-1)}{6}\right)\left(\frac{6-(y-1)}{6}\right) = \left(\frac{7-y}{6}\right)^3 .$$

Then, observing that $\mathbb{P}[Y = y] = \mathbb{P}[Y \geq y] - \mathbb{P}[Y \geq y+1]$:

$$\mathbb{P}[Y = y] = \left(\frac{7-y}{6}\right)^3 - \left(\frac{6-y}{6}\right)^3 .$$

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 11

1 Fishy Computations

Note 19

Assume for each part that the random variable can be modelled by a Poisson distribution.

(a) Suppose that on average, a fisherman catches 20 salmon per week. What is the probability that he will catch exactly 7 salmon this week?

(b) Suppose that on average, you go to Fisherman's Wharf twice a year. What is the probability that you will go at most once in 2024?

(c) Suppose that in March, on average, there are 5.7 boats that sail in Laguna Beach per day. What is the probability there will be *at least* 3 boats sailing throughout the *next two days* in Laguna?

(d) Denote $X \sim \text{Pois}(\lambda)$. Prove that

$$\mathbb{E}[Xf(X)] = \lambda\,\mathbb{E}[f(X+1)]$$

for any function f.

Solution:

(a) Let X be the number of salmon the fisherman catches per week. $X \sim \text{Poiss}(20 \text{ salmon/week})$, so

$$\mathbb{P}[X = 7 \text{ salmon/week}] = \frac{20^7}{7!}e^{-20} \approx 5.23 \cdot 10^{-4}.$$

(b) Similarly $X \sim \text{Poiss}(2)$, so

$$\mathbb{P}[X \leq 1] = \frac{2^0}{0!}e^{-2} + \frac{2^1}{1!}e^{-2} \approx 0.41.$$

(c) Let X_1 be the number of sailing boats on the next day, and X_2 be the number of sailing boats on the day after next. Now, we can model sailing boats on day i as a Poisson distribution $X_i \sim \text{Poiss}(\lambda = 5.7)$. Let Y be the number of boats that sail in the next two days. We are interested in $Y = X_1 + X_2$. We know that the sum of two independent Poisson random variables is Poisson (from Theorem 19.5 in lecture notes). Thus, we have $Y \sim \text{Poiss}(\lambda = 5.7 + 5.7 = 11.4)$.

$$\begin{aligned}
\mathbb{P}[Y \geq 3] &= 1 - \mathbb{P}[Y < 3] \\
&= 1 - \mathbb{P}[Y = 0 \cup Y = 1 \cup Y = 2] \\
&= 1 - (\mathbb{P}[Y = 0] + \mathbb{P}[Y = 1] + \mathbb{P}[Y = 2]) \\
&= 1 - \left(\frac{11.4^0}{0!}e^{-11.4} + \frac{11.4^1}{1!}e^{-11.4} + \frac{11.4^2}{2!}e^{-11.4}\right) \\
&\approx 0.999.
\end{aligned}$$

(d) We apply the Law of the Unconscious Statistician,

$$\begin{aligned}
\mathbb{E}[Xf(X)] &= \sum_{x=0}^{\infty} xf(x)\mathbb{P}[X=x] \\
&= \sum_{x=0}^{\infty} xf(x)\frac{e^{-\lambda}\lambda^x}{x!} \\
&= \sum_{x=1}^{\infty} xf(x)\frac{e^{-\lambda}\lambda^x}{x!} \\
&= \lambda \sum_{x=1}^{\infty} f(x)\frac{e^{-\lambda}\lambda^{x-1}}{(x-1)!} \\
&= \lambda \sum_{x=0}^{\infty} f(x+1)\frac{e^{-\lambda}\lambda^x}{x!} \\
&= \lambda\,\mathbb{E}[f(X+1)]
\end{aligned}$$

as desired.

2 Such High Expectations

Note 19

Suppose X and Y are independently drawn from a Geometric distribution with parameter p.

(a) Compute $\mathbb{E}[\min(X,Y)]$.

(b) Compute $\mathbb{E}[\max(X,Y)]$.

Solution:

(a) By independence,

$$\mathbb{P}[\min(X,Y) \geq t] = \mathbb{P}[X \geq t]\mathbb{P}[Y \geq t] = (1-p)^{2(t-1)}.$$

By Tail Sum,

$$\mathbb{E}[\min(X,Y)] = \sum_{t=1}^{\infty} \mathbb{P}[\min(X,Y) \geq t] = \sum_{t=1}^{\infty} (1-p)^{2(t-1)} = \frac{1}{1-(1-p)^2}.$$

Alternate Solution: We can see that $\min(X,Y)$ is a geometric distribution by looking at the tail probability from earlier. In particular, we have that $\min(X,Y) \sim \text{Geom}(1-(1-p)^2)$. This means that

$$\mathbb{E}[\min(X,Y)] = \frac{1}{1-(1-p)^2},$$

from the expectation of a geometric distribution.

(b) We see that

$$\begin{aligned}\mathbb{P}[\max(X,Y) \geq t] = 1 - \mathbb{P}[\max(X,Y) < t] &= 1 - \mathbb{P}[X < t]\mathbb{P}[Y < t] \\ &= 1 - (1 - \mathbb{P}[X \geq t])(1 - \mathbb{P}[Y \geq t]) \\ &= 1 - \left(1 - (1-p)^{t-1}\right)\left(1 - (1-p)^{t-1}\right) \\ &= 1 - \left(1 - 2(1-p)^{t-1} + (1-p)^{2(t-1)}\right) \\ &= 2(1-p)^{t-1} - (1-p)^{2(t-1)}.\end{aligned}$$

Using the result from part (a),

$$\begin{aligned}\mathbb{E}[\max(X,Y)] &= \sum_{t=1}^{\infty} \mathbb{P}[\max(X,Y) \geq t] \\ &= \sum_{t=1}^{\infty} 2(1-p)^{t-1} - (1-p)^{2(t-1)} \\ &= \sum_{t=1}^{\infty} 2(1-p)^{t-1} - \sum_{t=1}^{\infty} (1-p)^{2(t-1)} \\ &= \frac{2}{p} - \frac{1}{1-(1-p)^2}.\end{aligned}$$

Alternate Solution: An extremely elegant one-liner with linearity:

$$\mathbb{E}[\max(X,Y)] = \mathbb{E}[X+Y-\min(X,Y)] = \mathbb{E}[X] + \mathbb{E}[Y] - \mathbb{E}[\min(X,Y)] = \frac{2}{p} - \frac{1}{1-(1-p)^2}.$$

3 Diversify Your Hand

Note 15
Note 16

You are dealt 5 cards from a standard 52 card deck. Let X be the number of distinct values in your hand. For instance, the hand (A, A, A, 2, 3) has 3 distinct values.

(a) Calculate $\mathbb{E}[X]$. (Hint: Consider indicator variables X_i representing whether i appears in the hand.)

(b) Calculate $\text{Var}(X)$.

Solution:

(a) Let X_i be the indicator of the ith value appearing in your hand. Then, $X = X_1 + X_2 + \ldots + X_{13}$. (Here we let 13 correspond to K, 12 correspond to Q, and 11 correspond to J.) By linearity of expectation, $\mathbb{E}[X] = \sum_{i=1}^{13} \mathbb{E}[X_i]$.

We can calculate $\mathbb{P}[X_i = 1]$ by taking the complement, $1 - \mathbb{P}[X_i = 0]$, or 1 minus the probability that the card does not appear in your hand. This is $1 - \frac{\binom{48}{5}}{\binom{52}{5}}$.

Then, $\mathbb{E}[X] = 13\mathbb{P}[X_1 = 1] = 13\left(1 - \frac{\binom{48}{5}}{\binom{52}{5}}\right)$.

(b) To calculate variance, since the indicators are not independent, we have to use the formula $\mathbb{E}[X^2] = \sum_{i=j} \mathbb{E}[X_i^2] + \sum_{i \neq j} \mathbb{E}[X_i X_j]$.

First, we have

$$\sum_{i=j} \mathbb{E}[X_i^2] = \sum_{i=j} \mathbb{E}[X_i] = 13\left(1 - \frac{\binom{48}{5}}{\binom{52}{5}}\right).$$

Next, we tackle $\sum_{i \neq j} \mathbb{E}[X_i X_j]$. Note that $\mathbb{E}[X_i X_j] = \mathbb{P}[X_i X_j = 1]$, as $X_i X_j$ is either 0 or 1.

To calculate $\mathbb{P}[X_i X_j = 1]$ (the probability we have both cards in our hand), we note that $\mathbb{P}[X_i X_j = 1] = 1 - \mathbb{P}[X_i = 0] - \mathbb{P}[X_j = 0] + \mathbb{P}[X_i = 0, X_j = 0]$. Then

$$\begin{aligned}
\sum_{i \neq j} \mathbb{E}[X_i X_j] &= 13 \cdot 12 \mathbb{P}[X_i X_j = 1] \\
&= 13 \cdot 12(1 - \mathbb{P}[X_i = 0] - \mathbb{P}[X_j = 0] + \mathbb{P}[X_i = 0, X_j = 0]) \\
&= 156\left(1 - 2\frac{\binom{48}{5}}{\binom{52}{5}} + \frac{\binom{44}{5}}{\binom{52}{5}}\right)
\end{aligned}$$

Putting it all together, we have

$$\begin{aligned}
\mathrm{Var}(X) &= \mathbb{E}[X^2] - \mathbb{E}[X]^2 \\
&= 13\left(1 - \frac{\binom{48}{5}}{\binom{52}{5}}\right) + 156\left(1 - 2\frac{\binom{48}{5}}{\binom{52}{5}} + \frac{\binom{44}{5}}{\binom{52}{5}}\right) - \left(13\left(1 - \frac{\binom{48}{5}}{\binom{52}{5}}\right)\right)^2.
\end{aligned}$$

4 Swaps and Cycles

Note 15

We'll say that a permutation $\pi = (\pi(1), \ldots, \pi(n))$ contains a *swap* if there exist $i, j \in \{1, \ldots, n\}$ so that $\pi(i) = j$ and $\pi(j) = i$, where $i \neq j$.

(a) What is the expected number of swaps in a random permutation?

(b) In the same spirit as above, we'll say that π contains a *k-cycle* if there exist $i_1, \ldots, i_k \in \{1, \ldots, n\}$ with $\pi(i_1) = i_2, \pi(i_2) = i_3, \ldots, \pi(i_k) = i_1$. Compute the expectation of the number of k-cycles.

Solution:

(a) As a warm-up, let's compute the probability that 1 and 2 are swapped. There are $n!$ possible permutations, and $(n-2)!$ of them have $\pi(1) = 2$ and $\pi(2) = 1$. This means

$$\mathbb{P}[(1,2) \text{ are a swap}] = \frac{(n-2)!}{n!} = \frac{1}{n(n-1)}.$$

There was nothing special about 1 and 2 in this calculation, so for any $\{i,j\} \subset \{1,\ldots,n\}$, the probability that i and j are swapped is the same as above. Let's write $I_{i,j}$ for the indicator that i and j are swapped, and N for the total number of swaps, so that

$$\mathbb{E}[N] = \mathbb{E}\left[\sum_{\{i,j\}\subset\{1,\ldots,n\}} I_{i,j}\right] = \sum_{\{i,j\}\subset\{1,\ldots n\}} \mathbb{P}[(i,j) \text{ are swapped}] = \frac{1}{n(n-1)}\binom{n}{2} = \frac{1}{2}.$$

(b) The idea here is quite similar to the above, so we'll be a little less verbose in the exposition. However, as a first aside we need the notion of a *cyclic ordering* of k elements from a set $\{1,\ldots n\}$. We mean by this a labelling of the k beads of a necklace with elements of the set, where we say that labellings of the beads are the same if we can move them along the string to turn one into the other. For example, $(1,2,3,4)$ and $(1,2,4,3)$ are different cyclic orderings, but $(1,2,3,4)$ and $(2,3,4,1)$ are the same. There are

$$\binom{n}{k}\frac{k!}{k} = \frac{n!}{(n-k)!}\frac{1}{k}$$

possible cyclic orderings of length k from a set with n elements, since if we first count all subsets of size k, and then all permutations of each of those subsets, we have overcounted by a factor of k.

Now, let N be a random variable counting the number of k-cycles, and for each cyclic ordering $(i_1,\ldots,i_k)$ of k elements of $\{1,\ldots,n\}$, let $I_{(i_1,\ldots,i_k)}$ be the indicator that $\pi(i_1) = i_2, \pi(i_2) = i_3, \ldots, \pi(i_k) = i_1$. There are $(n-k)!$ permutations in which $(i_1,\ldots,i_k)$ form an k-cycle (since we are free to do whatever we want to the remaining $(n-k)$ elements of $\{1,\ldots,n\}$), so the probability that $(i_1,\ldots,i_k)$ are such a cycle is $\frac{(n-k)!}{n!}$, and

$$\mathbb{E}[N] = \mathbb{E}\left[\sum_{(i_1,\ldots,i_k) \text{ cyclic ordering}} I_{(i_1,\ldots,i_k)}\right] = \frac{n!}{(n-k)!}\frac{1}{k}\frac{(n-k)!}{n!} = \frac{1}{k}.$$

5 Double-Check Your Intuition Again

Note 16

(a) You roll a fair six-sided die and record the result X. You roll the die again and record the result Y.

(i) What is $\text{cov}(X+Y, X-Y)$?

(ii) Prove that $X+Y$ and $X-Y$ are not independent.

For each of the problems below, if you think the answer is "yes" then provide a proof. If you think the answer is "no", then provide a counterexample.

(b) If X is a random variable and $\text{Var}(X) = 0$, then must X be a constant?

(c) If X is a random variable and c is a constant, then is $\text{Var}(cX) = c\,\text{Var}(X)$?

(d) If A and B are random variables with nonzero standard deviations and $\text{Corr}(A,B) = 0$, then are A and B independent?

(e) If X and Y are not necessarily independent random variables, but $\text{Corr}(X,Y) = 0$, and X and Y have nonzero standard deviations, then is $\text{Var}(X+Y) = \text{Var}(X) + \text{Var}(Y)$?

The two subparts below are **optional** and will not be graded but are recommended for practice.

(f) If X and Y are random variables then is $\mathbb{E}[\max(X,Y)\min(X,Y)] = \mathbb{E}[XY]$?

(g) If X and Y are independent random variables with nonzero standard deviations, then is

$$\text{Corr}(\max(X,Y), \min(X,Y)) = \text{Corr}(X,Y)?$$

Solution:

(a) (i) Using bilinearity of covariance, we have

$$\begin{aligned}\text{cov}(X+Y, X-Y) &= \text{cov}(X,X) + \text{cov}(X,Y) - \text{cov}(Y,X) - \text{cov}(Y,Y)\\ &= \text{cov}(X,X) - \text{cov}(Y,Y),\\ &= 0\end{aligned}$$

where we use that $\text{cov}(X,Y) = \text{cov}(Y,X)$ to get the second equality.

(ii) Observe that $\mathbb{P}[X+Y=7, X-Y=0] = 0$ because if $X-Y=0$, then the sum of our two dice rolls must be even. However, both $\mathbb{P}[X+Y=7]$ and $\mathbb{P}[X-Y=0]$ are nonzero, so $\mathbb{P}[X+Y=7, X-Y=0] \neq \mathbb{P}[X+Y=7] \cdot \mathbb{P}[X-Y=0]$.

(b) Yes. If we write $\mu = \mathbb{E}[X]$, then $0 = \text{Var}(X) = \mathbb{E}[(X-\mu)^2]$ so $(X-\mu)^2$ must be identically 0 since perfect squares are non-negative. Thus $X = \mu$.

(c) No. We have $\text{Var}(cX) = \mathbb{E}[(cX - \mathbb{E}[cX])^2] = c^2\,\mathbb{E}[(X-\mathbb{E}[X])^2] = c^2\,\text{Var}(X)$ so if $\text{Var}(X) \neq 0$ and $c \neq 0$ or $c \neq 1$ then $\text{Var}(cX) \neq c\,\text{Var}(X)$. This does prove that $\sigma(cX) = c\sigma(X)$ though.

(d) No. Let $A = X+Y$ and $B = X-Y$ from part (a). Since A and B are not constants then part (b) says they must have nonzero variances which means they also have nonzero standard deviations. Part (a) says that their covariance is 0 which means they are uncorrelated, and that they are not independent.

Recall from lecture that the converse is true though.

(e) Yes. If $\text{Corr}(X,Y) = 0$, then $\text{cov}(X,Y) = 0$. We have $\text{Var}(X+Y) = \text{cov}(X+Y, X+Y) = \text{Var}(X) + \text{Var}(Y) + 2\,\text{cov}(X,Y) = \text{Var}(X) + \text{Var}(Y)$.

(f) Yes. For any values x, y we have $\max(x,y)\min(x,y) = xy$. Thus, $\mathbb{E}[\max(X,Y)\min(X,Y)] = \mathbb{E}[XY]$.

(g) No. You may be tempted to think that because $(\max(x,y),\min(x,y))$ is either (x,y) or (y,x), then $\text{Corr}(\max(X,Y),\min(X,Y)) = \text{Corr}(X,Y)$ because $\text{Corr}(X,Y) = \text{Corr}(Y,X)$. That reasoning is flawed because $(\max(X,Y),\min(X,Y))$ is not always equal to (X,Y) or always equal to (Y,X) and the inconsistency affects the correlation. It is possible for X and Y to be independent while $\max(X,Y)$ and $\min(X,Y)$ are not.

For a concrete example, suppose X is either 0 or 1 with probability $1/2$ each and Y is independently drawn from the same distribution. Then $\text{Corr}(X,Y) = 0$ because X and Y are independent. Even though X never gives information about Y, if you know $\max(X,Y) = 0$ then you know for sure $\min(X,Y) = 0$.

More formally, $\max(X,Y) = 1$ with probability $3/4$ and 0 with probability $1/4$, and $\min(X,Y) = 1$ with probability $1/4$ and 0 with probability $3/4$. This means

$$\mathbb{E}[\max(X,Y)] = 1 \cdot \frac{3}{4} + 0 \cdot \frac{1}{4} = \frac{3}{4}$$

and

$$\mathbb{E}[\min(X,Y)] = 1 \cdot \frac{1}{4} + 0 \cdot \frac{3}{4} = \frac{1}{4}.$$

Thus,

$$\begin{aligned}\text{cov}(\max(X,Y),\min(X,Y)) &= \mathbb{E}[\max(X,Y)\min(X,Y)] - \frac{3}{16} \\ &= \frac{1}{4} - \frac{3}{16} = \frac{1}{16} \neq 0\end{aligned}$$

We conclude that $\text{Corr}(\max(X,Y),\min(X,Y)) \neq 0 = \text{Corr}(X,Y)$.

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 12

1 Tellers

Note 17

Imagine that X is the number of customers that enter a bank at a given hour. To simplify everything, in order to serve n customers you need at least n tellers. One less teller and you won't finish serving all of the customers by the end of the hour. You are the manager of the bank and you need to decide how many tellers there should be in your bank so that you finish serving all of the customers in time. You need to be sure that you finish in time with probability at least 95%.

(a) Assume that from historical data you have found out that $\mathbb{E}[X] = 5$. How many tellers should you have?

(b) Now assume that you have also found out that $\text{Var}(X) = 5$. Now how many tellers do you need?

Solution:

(a) Suppose we have t tellers, meaning that we can serve t customers, i.e., we fail to finish on time if more than t customers show up. So we want to choose t so that

$$\mathbb{P}[X \geq t] \leq 0.05.$$

Using Markov's inequality, we have $\mathbb{P}[X \geq t] \leq \frac{\mathbb{E}[X]}{t}$. Therefore, we want to choose t so that $\frac{\mathbb{E}[X]}{t} = 0.05$. Since $\mathbb{E}[X] = 5$, this requires $t = 100$. Therefore, 99 tellers are needed in this case.

(b) Now that we have access to the variance as well, we can apply Chebyshev's inequality. Note that Markov's inequality is still correct, but Chebyshev's inequality gives us a tigher bound here. As in part (a), aiming for the probability of finishing in time to be least 95% is equivalent to aiming to limit the probability of not finishing (or in other words, taking more time to finish t customers) to 5%. So, we want

$$\mathbb{P}[|X - \mathbb{E}[X]| \geq t] \leq 0.05$$

Using Chebyshev's inequality, we know $\mathbb{P}[|X - \mathbb{E}[X]| \geq t] \leq \frac{\text{Var}(X)}{t^2}$. Plugging in $\mathbb{E}[X] = 5$ and $\text{Var}(X) = 5$, we get $\mathbb{P}[|X - 5| \geq t] \leq \frac{5}{t^2}$. Since we want to limit $\mathbb{P}[|X - 5| \geq t] \leq 0.05$, we get $\frac{5}{t^2} = 0.05$. Thus $t^2 = 100$ and $t = 10$. Now plugging $t = 10$:

$$\mathbb{P}[|X - 5| \geq 10] = \mathbb{P}[X \geq 5 + 10] = \mathbb{P}[X \geq 15] \leq 0.05$$

as wanted. Thus, 14 tellers are needed this time.

2 Polling Numbers

Note 17

Suppose the whole population of California has Democrats, Republicans, and no other parties. You choose N people independently and uniformly at random from the Californian population, and for each person, you record whether they are a Democrat or a Republican. We want to estimate the true percentage of Democrats among the polled Californians to within 1% with 95% confidence. According to Chebyshev's inequality, what is the minimum number of people you need to poll?

Solution: Let $S = \frac{1}{N}\sum_{i=1}^{N} X_i$, where $X_i = 1$ if the i-th person polled is a Democrat and 0 if they are a Republican. We need to be off by more than 1% no more than 5% of the time, which is represented by $\mathbb{P}[|S - \mathbb{E}[S]| \geq 0.01] \leq 0.05$. To do this, we can apply Chebyshev's inequality, which says $\mathbb{P}[|S - \mathbb{E}[S]| \geq 0.01] \leq \frac{\text{Var}(S)}{0.01^2}$. Thus, we would like $\frac{\text{Var}(S)}{0.01^2} \leq 0.05$. We have that $\text{Var}(S) = \frac{1}{N^2}\sum_{i=1}^{N} \text{Var}(X_i)$. Since X_i are all i.i.d. Bernoulli random variables, their variance is at most $\frac{1}{4}$. We have the following: $\frac{\text{Var}(S)}{0.01^2} \leq \frac{\frac{N}{4}}{N^2 \cdot 0.01^2} \leq 0.05$, which we solve to obtain $N \geq 50000$.

3 Tightness of Inequalities

Note 17

(a) Show by example that Markov's inequality is tight; that is, show that given some fixed $k > 0$, there exists a discrete non-negative random variable X such that $\mathbb{P}[X \geq k] = \mathbb{E}[X]/k$.

(b) Show by example that Chebyshev's inequality is tight; that is, show that given some fixed $k \geq 1$, there exists a random variable X such that $\mathbb{P}[|X - \mathbb{E}[X]| \geq k\sigma] = 1/k^2$, where $\sigma^2 = \text{Var}(X)$.

Solution:

(a) In the proof of Markov's Inequality ($\mathbb{P}[X \geq \alpha] \leq \frac{\mathbb{E}[X]}{\alpha}$), the first time we lose equality is at this step:

$$\mathbb{E}[X] = \sum_{a}(a \cdot \mathbb{P}[X = a]) \geq \sum_{a \geq \alpha}(a \cdot \mathbb{P}[X = a])$$

We get an inequality because we drop all $a \cdot \mathbb{P}[X = a]$ terms where $a < \alpha$. Thus, we can only maintain equality if all of these dropped terms were actually 0. This would mean either $a = 0$ or $\mathbb{P}[X = a] = 0$ for $a > 0$, which means X can put probability on 0, but should put no probability on any other value $< \alpha$.

The next time we lose equality in the proof is the step following the one above:

$$\sum_{a \geq \alpha}(a \cdot \mathbb{P}[X = a]) \geq \alpha \cdot \sum_{a \geq \alpha}\mathbb{P}[X = a]$$

We get an inequality because we treat all $a \geq \alpha$ in the summation as just α, so we can pull out the α term. The only way for us to maintain equality is if we never have to substitute α for some larger a. This tells us that X should not put probability on any value $> \alpha$.

Both of these facts drive the intuition behind our example: that X can only take values 0 and α.

Let X be the random variable which is 0 with probability $1-p$ and k with probability p, where $k > 0$. Then, $\mathbb{E}[X] = kp$, and Markov's inequality says

$$\mathbb{P}(X \geq k) \leq \frac{\mathbb{E}[X]}{k} = \frac{kp}{k} = p,$$

which is tight.

(b) The proof of Chebyshev's Inequality ($\mathbb{P}[|X - \mathbb{E}[X]| \geq \alpha] \leq \frac{\text{Var}(X)}{\alpha^2}$) comes from an application of Markov's Inequality to the variable $Y = (X - \mathbb{E}[X])^2$ being $\geq \alpha^2$. The only ways we can lose equality in the proof of Chebyshev's is if we lose equality in the application of Markov! Therefore, we need the variable Y to satisfy the conditions from Part (a) that ensure the application of Markov will be tight. To recap, we would need Y to only take values 0 and α^2. Thus, $(X - \mathbb{E}[X])$ can take on the values $\{-\alpha, 0, \alpha\}$.

Let

$$X = \begin{cases} -a & \text{with probability } k^{-2}/2 \\ a & \text{with probability } k^{-2}/2 \\ 0 & \text{with probability } 1 - k^{-2} \end{cases}$$

for $a > 0$. Note that $\mathbb{E}[X] = 0$ and $\text{Var}(X) = a^2 k^{-2}$, so $k\sigma = a$, so Chebyshev's inequality gives

$$\mathbb{P}(|X - \mathbb{E}[X]| \geq k\sigma) = \mathbb{P}(|X| \geq a) \leq \frac{1}{k^2},$$

which is tight.

4 Max of Uniforms

Note 21

Let $X_1, \ldots X_n$ be independent Uniform$(0,1)$ random variables, and let $X = \max(X_1, \ldots X_n)$. Compute each of the following in terms of n.

(a) What is the cdf of X?

(b) What is the pdf of X?

(c) What is $\mathbb{E}[X]$?

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

Solution:

(a) $\mathbb{P}[X \leq x] = x^n$ since in order for $\max(X_1, \ldots X_n) < x$, we must have $X_i < x$ for all i. Since they are independent, we can multiply together the probabilities of each of them being less than x, which is x itself, as their distributions are uniform.

(b) The pdf is the derivative of the cdf, so we have $f_X(x) = nx^{n-1}$

(c) To find the expectation, we integrate $xf_X(x)$ over all values of x:

$$\begin{aligned}\mathbb{E}[X] &= \int_0^1 x f_X(x) \\ &= \int_0^1 n x^n dx \\ &= \frac{n}{n+1}\end{aligned}$$

(d) First, we calculate $\mathbb{E}[X^2]$, then apply the formula $\text{Var}(X) = \mathbb{E}[X^2] - \mathbb{E}[X]^2$

$$\mathbb{E}[X^2] = \int_0^1 x^2 f_X(x) = \int_0^1 n x^{n+1} dx = \frac{n}{n+2}$$
$$\text{Var}(X) = \mathbb{E}[X^2] - \mathbb{E}[X]^2 = \frac{n}{n+2} - \frac{n^2}{(n+1)^2}$$

5 Darts with Friends

Note 21

Michelle and Alex are playing darts. Being the better player, Michelle's aim follows a uniform distribution over a disk of radius 1 around the center. Alex's aim follows a uniform distribution over a disk of radius 2 around the center.

(a) Let the distance of Michelle's throw from the center be denoted by the random variable X and let the distance of Alex's throw from the center be denoted by the random variable Y.

(i) What's the cumulative distribution function of X?

(ii) What's the cumulative distribution function of Y?

(iii) What's the probability density function of X?

(iv) What's the probability density function of Y?

(b) What's the probability that Michelle's throw is closer to the center than Alex's throw? What's the probability that Alex's throw is closer to the center?

(c) What's the cumulative distribution function of $U = \max(X, Y)$?

Solution:

(a) (i) To get the cumulative distribution function of X, we'll consider the ratio of the area where the distance to the center is less than x, compared to the entire available area. This gives us the following expression:

$$\mathbb{P}[X \leq x] = \frac{\pi x^2}{\pi} = x^2, \qquad x \in [0,1].$$

(ii) Using the same approach as the previous part:

$$\mathbb{P}[Y \le y] = \frac{\pi y^2}{\pi \cdot 4} = \frac{y^2}{4}, \qquad y \in [0,2].$$

(iii) We'll take the derivative of the CDF to get the following:

$$f_X(x) = \frac{\mathrm{d}}{\mathrm{d}x}\mathbb{P}[X \le x] = 2x, \qquad x \in [0,1].$$

(iv) Using the same approach as the previous part:

$$f_Y(y) = \frac{\mathrm{d}}{\mathrm{d}y}\mathbb{P}[Y \le y] = \frac{y}{2}, \qquad y \in [0,2].$$

(b) We'll condition on Alex's outcome and then integrate over all the possibilities to get the marginal $\mathbb{P}[X \le Y]$ as following:

$$\begin{aligned}\mathbb{P}[X \le Y] &= \int_0^2 \mathbb{P}[X \le Y \mid Y = y] f_Y(y)\,\mathrm{d}y = \int_0^1 y^2 \times \frac{y}{2}\,\mathrm{d}y + \int_1^2 1 \times \frac{y}{2}\,\mathrm{d}y \\ &= \frac{1}{8} + \frac{3}{4} = \frac{7}{8}.\end{aligned}$$

Note the range within which $\mathbb{P}[X \le Y] = 1$. This allowed us to separate the integral to simplify our solution. Using this, we can get $\mathbb{P}[Y \le X]$ by the following:

$$\mathbb{P}[Y \le X] = 1 - \mathbb{P}[X \le Y] = \frac{1}{8}$$

A similar approach to the integral above could be used to verify this result:

$$\mathbb{P}[Y \le X] = \int_0^1 \mathbb{P}[Y \le X \mid X = x] f_X(x)\,\mathrm{d}x = \int_0^1 \frac{x^2}{4} 2x\,\mathrm{d}x = \frac{1}{2}\int_0^1 x^3\,\mathrm{d}x = \frac{1}{8}.$$

(c) Getting the CDF of U relies on the insight that for the maximum of two random variables to be smaller than a value, they both need to be smaller than that value. Using this we can get the following result for $u \in [0,1]$:

$$\mathbb{P}[U \le u] = \mathbb{P}[X \le u]\mathbb{P}[Y \le u] = \left(u^2\right)\left(\frac{u^2}{4}\right) = \frac{u^4}{4}.$$

For $u \in [1,2]$ we have $\mathbb{P}[X \le u] = 1$; this makes

$$\mathbb{P}[U \le u] = \mathbb{P}[Y \le u] = \frac{u^2}{4}.$$

For $u > 2$ we have $\mathbb{P}[U \le u] = 1$ since CDFs of both X and Y are 1 in this range.

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 13

1 Uniform Uniform Computation

Note 21

Suppose $X \sim \text{Uniform}[0,1]$ and $Y \sim \text{Uniform}[0,X]$. That is, conditioned on $X = x$, Y has a $\text{Uniform}[0,x]$ distribution.

(a) What is $\mathbb{P}[Y > 1/2]$?

(b) Calculate $\text{Cov}(X,Y)$.

Solution:

(a) First we compute $\mathbb{P}[Y > 1/2 \mid X = x]$. Conditioned on $X = x, Y$ has the $\text{Uniform}[0,x]$ distribution, and the tail probability of the uniform distribution is as follows:

$$\mathbb{P}\left[Y > \frac{1}{2} \middle| X = x\right] = \begin{cases} 0, & x < 1/2 \\ (x - 1/2)/x, & x \geq 1/2 \end{cases}$$

So, integrate over values of $x \geq 1/2$ to find $\mathbb{P}[Y > 1/2]$ (note that the upper limit of integration is $x = 1$ since $X \sim \text{Uniform}[0,1]$).

$$\begin{aligned} \mathbb{P}[Y > 1/2] &= \int_{-\infty}^{\infty} \mathbb{P}\left[Y > \frac{1}{2} \middle| X = x\right] f_X(x)\,dx = \int_{1/2}^{1} \left(1 - \frac{1}{2x}\right) dx \\ &= \left[x - \frac{1}{2}\ln x\right]_{x=1/2}^{x=1} = \frac{1}{2}(1 - \ln 2). \end{aligned}$$

(b) To compute $\mathbb{E}[XY]$, note we integrate over the region defined by the triangle with endpoints $(0,0),(1,0),(1,1)$.

$$\begin{aligned} \mathbb{E}[XY] &= \int_0^1 \int_0^x xy f_{Y|X=x}(y) f_X(x)\,dy\,dx = \int_0^1 \int_0^x xy \frac{1}{x}\,dy\,dx \\ &= \int_0^1 \int_0^x y\,dy\,dx = \int_0^1 \left[\frac{y^2}{2}\right]_0^x dx = \int_0^1 \frac{x^2}{2}\,dx \\ &= \left[\frac{x^3}{6}\right]_0^1 = \frac{1}{6}. \end{aligned}$$

$\mathbb{E}[X] = \frac{1}{2}$ because it is a $\text{Uniform}[0,1]$ random variable. To compute $\mathbb{E}[Y]$, we can integrate y

over the same triangle as before, scaled by the joint pdf.

$$\begin{aligned}\mathbb{E}[Y] &= \int_0^1 \int_0^x y f_{Y|X=x}(y) f_X(x)\,dy\,dx = \int_0^1 \int_0^x y\frac{1}{x}\,dy\,dx \\ &= \int_0^1 \int_0^x \frac{y}{x}\,dy\,dx = \int_0^1 \left[\frac{y^2}{2x}\right]_0^x dx = \int_0^1 \frac{x}{2}\,dx \\ &= \left[\frac{x^2}{4}\right]_0^1 = \frac{1}{4}.\end{aligned}$$

An intuitive but less rigorous way of arriving at $\mathbb{E}[Y]$ is that Y will on average be half of X, and on average X is $\frac{1}{2}$, so Y is on average $\frac{1}{4}$, using the fact we are working with uniform random variables. Therefore the covariance is

$$\text{Cov}(X,Y) = \frac{1}{6} - \left(\frac{1}{2}\right)\left(\frac{1}{4}\right) = \frac{1}{6} - \frac{1}{8} = \frac{1}{24}.$$

2 Moments of the Gaussian

Note 21

For a random variable X, the quantity $\mathbb{E}[X^k]$ for $k \in \mathbb{N}$ is called the *kth moment* of the distribution. In this problem, we will calculate the moments of a standard normal distribution.

(a) Prove the identity

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp\left(-\frac{tx^2}{2}\right) dx = t^{-1/2}$$

for $t > 0$.

Hint: Consider a normal distribution with variance $\frac{1}{t}$ and mean 0.

(b) For the rest of the problem, X is a standard normal distribution (with mean 0 and variance 1). Use part (a) to compute $\mathbb{E}[X^{2k}]$ for $k \in \mathbb{N}$.

Hint: Try differentiating both sides with respect to t, k times. You may use the fact that we can differentiate under the integral without proof.

(c) Compute $\mathbb{E}[X^{2k+1}]$ for $k \in \mathbb{N}$.

Solution:

(a) Note that a normal distribution with mean 0 and variance t^{-1} has the density function

$$f(x) = \frac{\sqrt{t}}{\sqrt{2\pi}} \exp\left(-\frac{tx^2}{2}\right),$$

and since the density must integrate to 1, we see that

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp\left(-\frac{tx^2}{2}\right) dx = t^{-1/2}.$$

(b) Differentiating the identity from (a) k times with respect to t, we obtain a LHS of

$$\begin{aligned}\frac{\mathrm{d}^k}{\mathrm{d}t^k}\left[\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\exp\left(-\frac{tx^2}{2}\right)\mathrm{d}x\right] &= \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\frac{\mathrm{d}^k}{\mathrm{d}t^k}\left[\exp\left(-\frac{tx^2}{2}\right)\right]\mathrm{d}x \\ &= \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}(-1)^k\frac{x^{2k}}{2^k}\exp\left(-\frac{tx^2}{2}\right)\mathrm{d}x \\ &= \frac{1}{\sqrt{2\pi}}\frac{(-1)^k}{2^k}\int_{-\infty}^{\infty}x^{2k}\exp\left(-\frac{tx^2}{2}\right)\mathrm{d}x\end{aligned}$$

Here, we use the fact that everything involving x is a constant with respect to t.

Looking at the RHS, we have

$$\frac{\mathrm{d}^k}{\mathrm{d}t^k}\left[t^{-1/2}\right] = (-1)^k\frac{1\cdot 3\cdots(2k-3)\cdot(2k-1)}{2^k}t^{-(2k+1)/2}$$

Together, this means that

$$\begin{aligned}\frac{1}{\sqrt{2\pi}}\frac{\cancel{(-1)^k}}{\cancel{2^k}}\int_{-\infty}^{\infty}x^{2k}\exp\left(-\frac{tx^2}{2}\right)\mathrm{d}x &= \cancel{(-1)^k}\frac{1\cdot 3\cdots(2k-3)\cdot(2k-1)}{\cancel{2^k}}t^{-(2k+1)/2} \\ \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}x^{2k}\exp\left(-\frac{tx^2}{2}\right)\mathrm{d}x &= (1\cdot 3\cdots(2k-3)\cdot(2k-1))\,t^{-(2k+1)/2}\end{aligned}$$

If we set $t=1$, we get

$$\mathbb{E}[X^{2k}] = \int_{-\infty}^{\infty}x^{2k}\cdot\frac{1}{\sqrt{2\pi}}\exp\left(-\frac{x^2}{2}\right)\mathrm{d}x = \prod_{i=1}^{k}(2i-1).$$

This is sometimes denoted $(2k-1)!!$. Note that we can also write the result as

$$\mathbb{E}[X^{2k}] = (2k-1)!! = \frac{(2k)!}{2\cdot 4\cdots(2k-2)\cdot(2k)} = \frac{(2k)!}{2^k k!}.$$

(c) $\mathbb{E}[X^{2k+1}] = 0$, since the density function is symmetric around 0.

3 Exponential Median

Note 21

(a) Prove that if $X_1, X_2, \ldots, X_n$ are mutually independent exponential random variables with parameters $\lambda_1, \lambda_2, \ldots, \lambda_n$, then $\min(X_1, X_2, \ldots, X_n)$ is exponentially distributed with parameter $\sum_{i=1}^{n}\lambda_i$.

Hint: Recall that the CDF of an exponential random variable with parameter λ is $1-e^{-\lambda t}$.

(b) Given that the minimum of three i.i.d exponential variables with parameter λ is m, what is the probability that the difference between the median and the smallest is at least s? Note that the exponential random variables are mutually independent.

(c) What is the expected value of the median of three i.i.d. exponential variables with parameter λ?

Hint: Part (b) may be useful for this calculation.

Solution:

(a) In order to prove that $X := \min(X_1, ..., X_n)$ is exponentially distributed with parameter $\lambda := \sum_{i=1}^{n} \lambda_i$, we just need to show that the CDF matches. Hence, we would like to find $\mathbb{P}(X \leq t)$, but it turns out to be easier to find $\mathbb{P}(X > t)$ first. This is because in order for X to be larger than t, you need every X_i to be larger than t, so

$$\begin{aligned}\mathbb{P}(X > t) &= \mathbb{P}(X_1 > t \cap ... \cap X_n > t) \\ &= \mathbb{P}(X_1 > t) \cdot ... \cdot \mathbb{P}(X_n > t)\end{aligned}$$

where the second equality comes from the X_is being mutually independent. Now we know that

$$\begin{aligned}\mathbb{P}(X_i > t) &= 1 - \mathbb{P}(X_i \leq t) \\ &= 1 - \left(1 - e^{-\lambda_i t}\right) \\ &= e^{-\lambda_i t}\end{aligned}$$

where the second equality comes from plugging in the CDF of an exponential random variable. Thus, we get that

$$\begin{aligned}\mathbb{P}(X > t) &= e^{-\lambda_1 t} \cdot ... \cdot e^{-\lambda_n t} \\ &= e^{(-\lambda_1 t) + ... + (-\lambda_n t)} \\ &= e^{-(\lambda_1 + ... + \lambda_n)t} \\ &= e^{-\lambda t}\end{aligned}$$

Thus, the CDF of X is $1 - e^{-\lambda t}$, which matches the CDF of an exponential random variable with parameter λ. Since the CDF uniquely determines the distribution, this allows us to conclude that X is indeed exponentially distributed with parameter λ.

(b) Without loss of generality, let X_1 be the minimum of the three random variables. We also know the median is the second smallest of the random variables, so we can think of it as the

minimum of the remaining two random variables. Then:

$$\begin{aligned}
\mathbb{P}(\min(X_2,X_3)-X_1>s) &= \mathbb{P}(\min(X_2,X_3)>m+s \mid X_1>m, X_2>m, X_3>m) \\
&= \frac{\mathbb{P}(\min(X_2,X_3)>m+s, X_1>m)}{\mathbb{P}(X_1>m, X_2>m, X_3>m)} \\
&= \frac{\mathbb{P}(X_2>m+s, X_3>m+s, X_1>m)}{\mathbb{P}(X_1>m, X_2>m, X_3>m)} \\
&= \frac{\mathbb{P}(X_2>m+s)\mathbb{P}(X_3>m+s)\mathbb{P}(X_1>m)}{\mathbb{P}(X_1>m)\mathbb{P}(X_2>m)\mathbb{P}(X_3>m)} \\
&= \frac{(e^{-\lambda(m+s)}e^{-\lambda(m+s)}e^{-\lambda m})}{e^{-3\lambda m}} \\
&= e^{-2\lambda s}
\end{aligned}$$

Intuitively, suppose you knew that the value of the minimum of the three random variables was m. Then asking for the probability that the difference is at least s is exactly asking for the probability that the minimum of the two remaining random variables is at least $s+m$. But you know that they're both at least m (since m is the minimum), so the memoryless property gives us that the distribution of this difference is exactly the same as the distribution of the minimum of two exponential random variables! Then, the distribution is exponential with parameter 2λ, and the probability is $e^{-2\lambda s}$.

(c) By linearity of expectation, the expected value of the median is the expectation of the minimum plus the expected difference between the median and the minimum. From part a, we know that the minimum is exponentially distributed with parameter 3λ, so its expectation is $\frac{1}{3\lambda}$. Then, from part b, that the expectation of the difference is exponentially distributed with parameter 2λ, so its expectation is $\frac{1}{2\lambda}$.

Putting these two together, we have that the expected value of the median is $\frac{1}{3\lambda}+\frac{1}{2\lambda}=\frac{5}{6\lambda}$.

. . . . . .

In case you are not satisfied with the above explanation, then here is a more formal proof of the fact: If $X_{(1)} := \min\{X_1,X_2,X_3\}$ and $X_{(2)}$ is the median of X_1,X_2,X_3, then $X_{(2)}-X_{(1)}$ is exponentially distributed with parameter 2λ.

To prove that $X_{(2)}-X_{(1)}$ is exponentially distributed, we will calculate $\mathbb{P}\{X_{(2)}-X_{(1)}\geq x\}$ and show that it matches the tail probability of an exponential distribution. So, let $x>0$. First, we will use conditioning to write our event $\{X_{(2)}-X_{(1)}\geq x\}$ in terms of our original random variables X_1, X_2, and X_3.

$$\begin{aligned}
\mathbb{P}\{X_{(2)}-X_{(1)}\geq x\} &= 3\mathbb{P}\{X_{(2)}-X_{(1)}\geq x,\ X_{(1)}=X_1\} \qquad \text{(by symmetry)} \\
&= 3\mathbb{P}\{\min(X_2,X_3)-X_1\geq x,\ \min(X_2,X_3)\geq X_1\}
\end{aligned}$$

This almost looks like what we want to apply the memoryless property of the exponential distribution. Our next step is to condition on the value of X_1. Let f denote the density function for the exponential distribution.

$$\begin{aligned}
&= 3\int_0^\infty \mathbb{P}\{\min(X_2,X_3) \geq x + X_1,\ \min(X_2,X_3) \geq X_1 \mid X_1 = x_1\} f(x_1)\,\mathrm{d}x_1 \\
&= 3\int_0^\infty \mathbb{P}\{\min(X_2,X_3) \geq x + x_1,\ \min(X_2,X_3) \geq x_1 \mid X_1 = x_1\} f(x_1)\,\mathrm{d}x_1 \\
&= 3\int_0^\infty \mathbb{P}\{\min(X_2,X_3) \geq x + x_1,\ \min(X_2,X_3) \geq x_1\} f(x_1)\,\mathrm{d}x_1
\end{aligned}$$

Here, we dropped the conditioning because the random variables $\min(X_2,X_3)$ and X_1 are independent. Now, we can apply the memoryless property.

$$\begin{aligned}
&= 3\int_0^\infty \mathbb{P}\{\min(X_2,X_3) \geq x_1\} \\
&\qquad \times \mathbb{P}\{\min(X_2,X_3) \geq x + x_1 \mid \min(X_2,X_3) \geq x_1\} f(x_1)\,\mathrm{d}x_1 \\
&= 3\int_0^\infty \mathbb{P}\{\min(X_2,X_3) \geq x_1\}\mathbb{P}\{\min(X_2,X_3) \geq x\} f(x_1)\,\mathrm{d}x_1 \\
&= 3\mathbb{P}\{\min(X_2,X_3) \geq x\} \int_0^\infty \mathbb{P}\{\min(X_2,X_3) \geq x_1\} f(x_1)\,\mathrm{d}x_1
\end{aligned}$$

Now, we introduce X_1 back into the integral (trust me, this will work out).

$$\begin{aligned}
&= 3\mathbb{P}\{\min(X_2,X_3) \geq x\} \int_0^\infty \mathbb{P}\{\min(X_2,X_3) \geq x_1 \mid X_1 = x_1\} f(x_1)\,\mathrm{d}x_1 \\
&= 3\mathbb{P}\{\min(X_2,X_3) \geq x\} \int_0^\infty \mathbb{P}\{\min(X_2,X_3) \geq X_1 \mid X_1 = x_1\} f(x_1)\,\mathrm{d}x_1 \\
&= 3\mathbb{P}\{\min(X_2,X_3) \geq x\}\mathbb{P}\{\min(X_2,X_3) \geq X_1\} \\
&= \mathbb{P}\{\min(X_2,X_3) \geq x\} \qquad \text{(by symmetry).}
\end{aligned}$$

We have shown that the tail probabilities of $X_{(2)} - X_{(1)}$ matches that of $\min(X_2,X_3)$, that is, $X_{(2)} - X_{(1)}$ has the same distribution as $\min(X_2,X_3)$. Since $\min(X_2,X_3)$ has the exponential distribution with parameter 2λ, then so does $X_{(2)} - X_{(1)}$.

4 Chebyshev's Inequality vs. Central Limit Theorem

Note 17
Note 21

Let n be a positive integer. Let $X_1, X_2, \ldots, X_n$ be i.i.d. random variables with the following distribution:

$$\mathbb{P}[X_i = -1] = \frac{1}{12}; \qquad \mathbb{P}[X_i = 1] = \frac{9}{12}; \qquad \mathbb{P}[X_i = 2] = \frac{2}{12}.$$

(a) Calculate the expectations and variances of X_1, $\sum_{i=1}^n X_i$, $\sum_{i=1}^n (X_i - \mathbb{E}[X_i])$, and

$$Z_n = \frac{\sum_{i=1}^n (X_i - \mathbb{E}[X_i])}{\sqrt{n/2}}.$$

(b) Use Chebyshev's Inequality to find an upper bound b for $\mathbb{P}[|Z_n| \geq 2]$.

(c) Use b from the previous part to bound $\mathbb{P}[Z_n \geq 2]$ and $\mathbb{P}[Z_n \leq -2]$.

(d) As $n \to \infty$, what is the distribution of Z_n?

(e) We know that if $Z \sim \mathcal{N}(0,1)$, then $\mathbb{P}[|Z| \leq 2] = \Phi(2) - \Phi(-2) \approx 0.9545$. As $n \to \infty$, provide approximations for $\mathbb{P}[Z_n \geq 2]$ and $\mathbb{P}[Z_n \leq -2]$.

Solution:

(a) Firstly, let us calculate $\mathbb{E}[X_1]$ and $\text{Var}(X_1)$; we have

$$\mathbb{E}[X_1] = -\frac{1}{12} + \frac{9}{12} + \frac{4}{12} = 1$$
$$\text{Var}(X_1) = \frac{1}{12} \cdot 2^2 + \frac{9}{12} \cdot 0^2 + \frac{2}{12} \cdot 1^2 = \frac{1}{2}.$$

Using linearity of expectation and variance (since $X_1, \ldots, X_n$ are independent), we find that

$$\mathbb{E}\left[\sum_{i=1}^{n} X_i\right] = \sum_{i=1}^{n} \mathbb{E}[X_i] = n$$
$$\text{Var}\left(\sum_{i=1}^{n} X_i\right) = \sum_{i=1}^{n} \text{Var}(X_i) = \frac{n}{2}$$

Again, by linearity of expectation,

$$\mathbb{E}\left[\sum_{i=1}^{n} (X_i - \mathbb{E}[X_i])\right] = \mathbb{E}\left[\sum_{i=1}^{n} X_i - n\right] = n - n = 0.$$

Subtracting a constant does not change the variance, so

$$\text{Var}\left(\sum_{i=1}^{n} (X_i - \mathbb{E}[X_i])\right) = \text{Var}\left(\sum_{i=1}^{n} X_i - n\right) = \frac{n}{2},$$

as before.

Using the scaling properties of the expectation and variance, we finally have

$$\mathbb{E}[Z_n] = \mathbb{E}\left[\frac{\sum_{i=1}^{n}(X_i - \mathbb{E}[X_i])}{\sqrt{n/2}}\right] = \frac{1}{\sqrt{n/2}}\mathbb{E}\left[\sum_{i=1}^{n}(X_i - \mathbb{E}[X_i])\right] = \frac{0}{\sqrt{n/2}} = 0$$
$$\text{Var}(Z_n) = \text{Var}\left(\frac{\sum_{i=1}^{n}(X_i - \mathbb{E}[X_i])}{\sqrt{n/2}}\right) = \frac{1}{n/2}\text{Var}\left(\sum_{i=1}^{n}(X_i - \mathbb{E}[X_i])\right) = \frac{n/2}{n/2} = 1$$

(b) Using Chebyshev's, we have

$$\mathbb{P}[|Z_n| \geq 2] \leq \frac{\text{Var}(Z_n)}{2^2} = \frac{1}{4}$$

since $\mathbb{E}[Z_n] = 0$ and $\text{Var}(Z_n) = 1$ as we computed in the previous part.

(c) $\frac{1}{4}$ for both, since we have

$$\mathbb{P}[Z_n \geq 2] \leq \mathbb{P}[|Z_n| \geq 2]$$
$$\mathbb{P}[Z_n \leq -2] \leq \mathbb{P}[|Z_n| \geq 2]$$

(d) By the Central Limit Theorem, we know that $Z_n \to \mathcal{N}(0,1)$, the standard normal distribution.

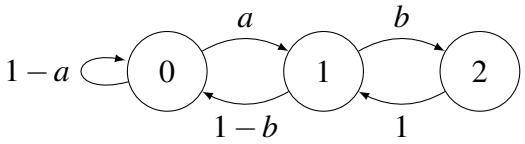
(e) Since $Z_n \to \mathcal{N}(0,1)$, we can approximate $\mathbb{P}[|Z_n| \geq 2] \approx 1 - 0.9545 = 0.0455$. By the symmetry of the normal distribution, $\mathbb{P}[Z_n \geq 2] = \mathbb{P}[Z_n \leq -2] \approx 0.0455/2 = 0.02275$.

It is interesting to note that the CLT provides a much smaller answer than Chebyshev. This is due to the fact that the CLT is applied to a particular kind of random variable, namely the (scaled) sum of a bunch of random variables. Chebyshev's inequality, however, holds for any random variable, and is therefore weaker.

5 Analyze a Markov Chain

Note 22

Consider a Markov chain with the state diagram shown below where $a, b \in (0,1)$.



Here, we let $X(n)$ denote the state at time n.

(a) Show that this Markov chain is aperiodic.

(b) Calculate $\mathbb{P}[X(1) = 1, X(2) = 0, X(3) = 0, X(4) = 1 \mid X(0) = 0]$.

(c) Calculate the invariant distribution.

Solution:

(a) The Markov chain is irreducible because $a, b \in (0,1)$. Also, $P(0,0) > 0$, so that

$$\gcd\{n > 0 \mid P^n(0,0) > 0\} = \gcd\{1, 2, 3, \ldots\} = 1,$$

which shows that the Markov chain is aperiodic.

We can also notice from the definition of aperiodicity that if a Markov chain has a self loop with nonzero probability, it is aperiodic. In particular, a self loop implies that the smallest number of steps we need to take to get from a state back to itself is 1. In this case, since $P(0,0) > 0$, we have a self loop with nonzero probability, which makes the Markov chain aperiodic.

(b) As a result of the Markov property, we know our state at timestep n depends only on timestep $n-1$. Looking at the transition probabilities, we see that the final expression is

$$P(0,1) \times P(1,0) \times P(0,0) \times P(0,1) = a(1-b)(1-a)a.$$

(c) The balance equations are

$$\begin{cases} \pi(0) = (1-a)\pi(0) + (1-b)\pi(1) \\ \pi(1) = a\pi(0) + \pi(2) \end{cases} \implies \begin{cases} a\pi(0) = (1-b)\pi(1) \\ \pi(1) = a\pi(0) + \pi(2) \end{cases}$$
$$\implies \begin{cases} a\pi(0) = (1-b)\pi(1) \\ \pi(1) = a\left(\frac{1-b}{a}\pi(1)\right) + \pi(2) \end{cases}$$
$$\implies \begin{cases} a\pi(0) = (1-b)\pi(1) \\ b\pi(1) = \pi(2) \end{cases}$$

As a side note, these last equations express the equality of the probability of a jump from i to $i+1$ and from $i+1$ to i, for $i=0$ and $i=1$, respectively. These relations are also called the "detailed balance equations".

From these equations we find successively that

$$\pi(1) = \frac{a}{1-b}\pi(0) \qquad \pi(2) = b\pi(1) = \frac{ab}{1-b}\pi(0).$$

The normalization equation is

$$1 = \pi(0) + \pi(1) + \pi(2) = \pi(0)\left(1 + \frac{a}{1-b} + \frac{ab}{1-b}\right)$$
$$1 = \pi(0)\left(\frac{1-b+a+ab}{1-b}\right)$$

so that

$$\pi(0) = \frac{1-b}{1-b+a+ab}.$$

Thus,

$$\pi(0) = \frac{1-b}{1-b+a+ab} \qquad \pi(1) = \frac{a}{1-b+a+ab} \qquad \pi(2) = \frac{ab}{1-b+a+ab}$$

Or in vector form,

$$\pi = \frac{1}{1-b+a+ab}\begin{bmatrix} 1-b & a & ab \end{bmatrix}.$$

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 14

1 Rahil's Dilemma

Note 22

Youngmin and Rahil decided to play a game: A fair coin is flipped until either the last two flips were all heads - then Youngmin wins, or the last three flips were all tails - then Rahil wins. Compute the probability that Rahil wins.

Solution: The corresponding Markov chain is: states are $\mathscr{X} = \{\emptyset, H, HH, T, TT, TTT\}$ and the transition probability matrix is

$$\begin{bmatrix} 0 & 1/2 & 0 & 1/2 & 0 & 0 \\ 0 & 0 & 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & 0 & 1/2 & 0 \\ 0 & 1/2 & 0 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Let $\alpha(i)$ denote the probability of Rahil winning, that is, reaching state TTT before HH. Then, the first-step equations for α are

$$\begin{aligned} \alpha(TTT) &= 1 \\ \alpha(HH) &= 0 \\ \alpha(TT) &= \frac{1}{2}(\alpha(TTT) + \alpha(H)) = \frac{1}{2}(1 + \alpha(H)) \\ \alpha(T) &= \frac{1}{2}(\alpha(TT) + \alpha(H)) \\ \alpha(H) &= \frac{1}{2}(\alpha(T) + \alpha(HH)) = \frac{1}{2}\alpha(T) \\ \alpha(\emptyset) &= \frac{1}{2}(\alpha(T) + \alpha(H)) \end{aligned}$$

Solving these equations, we get

$$\alpha(TT) = \frac{3}{5}$$
$$\alpha(T) = \frac{2}{5}$$
$$\alpha(H) = \frac{1}{5}$$
$$\alpha(\emptyset) = \frac{3}{10}$$

Hence, Rahil wins with probability $\frac{3}{10}$.

2 A Bit of Everything

Suppose that $X_0, X_1, \ldots$ is a Markov chain with finite state space $S = \{1, 2, \ldots, n\}$, where $n > 2$, and transition matrix P. Suppose further that

$$P(1, i) = \frac{1}{n} \quad \text{for all states } i \text{ and}$$
$$P(j, j-1) = 1 \quad \text{for all states } j \neq 1,$$

with $P(i, j) = 0$ everywhere else.

(a) Prove that this Markov chain is irreducible and aperiodic.

(b) Suppose you start at state 1. What is the distribution of T, where T is the number of transitions until you leave state 1 for the first time?

(c) Again starting from state 1, what is the expected number of transitions until you reach state n for the first time?

(d) Again starting from state 1, what is the probability you reach state n before you reach state 2?

(e) Compute the stationary distribution of this Markov chain.

Solution:

(a) For any two states i and j, we can consider the path $(i, i-1, \ldots, 2, 1, j)$, which has nonzero probability of occurring. Thus, this chain is irreducible. To see that it is aperiodic, observe that $d(1) = 1$, as we have self-loop from state 1 to itself.

(b) At any given transition, we leave state 1 with probability with probability $\frac{n-1}{n}$, independently of any previous transition. Thus, the distribution is Geometric, with parameter $\frac{n-1}{n}$.

(c) Suppose that $\beta(i)$ is the expected number of transitions necessary to reach state n for the first time, starting from state i. We have the following first step equations:

$$\begin{aligned}\beta(1) &= 1+\sum_{j=1}^{n}\frac{1}{n}\beta(j),\\ \beta(i) &= 1+\beta(i-1) \quad \text{for } 1<i<n, \text{ and}\\ \beta(n) &= 0.\end{aligned}$$

We can simplify the second recurrence to

$$\beta(i) = i-1+\beta(1) \quad \text{for } 1<i<n.$$

Substituting this simplified recurrence into the first equation, we get that

$$\beta(1) = 1+\frac{1}{n}\sum_{i=1}^{n-1}(i-1+\beta(1)) = 1+\frac{1}{n}\sum_{i=1}^{n-1}(i-1)+\frac{1}{n}\sum_{i=1}^{n-1}\beta(1) = 1+\frac{(n-2)(n-1)}{2n}+\frac{n-1}{n}\beta(1),$$

which we can solve to get that

$$\beta(1) = \boxed{n+\frac{1}{2}(n-1)(n-2)}.$$

(d) Suppose that $\alpha(i)$ is the probability that we reach state n before we reach state 2, starting from state i. One immediate observation we can make is that from any state i in $\{2,\ldots,n-1\}$, we are guaranteed to see state 2 before state n, as we can only take the path $(i,i-1,\ldots,2,1)$. Hence, $\alpha(i)=0$ if $i\in\{2,\ldots,n-1\}$. Moreover, $\alpha(n)=1$, so

$$\alpha(1) = \sum_{i=1}^{n}\frac{1}{n}\alpha(i) = \frac{1}{n}\alpha(1)+\frac{1}{n},$$

hence $\alpha(1) = \boxed{\frac{1}{n-1}}$.

(e) We have the balance equations

$$\begin{aligned}\pi(i) &= \frac{1}{n}\pi(1)+\pi(i+1) \quad \text{if } i\neq n, \text{ and}\\ \pi(n) &= \frac{1}{n}\pi(1).\end{aligned}$$

We can collapse the first recurrence to

$$\pi(i) = \frac{n-i}{n}\pi(1)+\pi(n) = \frac{n-i+1}{n}\pi(1),$$

so we can express each stationary probability in terms of the stationary probability of state 1. We can finish by using the normalization equation:

$$\pi(1)+\pi(2)+\cdots+\pi(n)=1 \implies \frac{1}{n}\pi(1)\sum_{i=1}^{n}n-i+1 = 1.$$

The last sum can be rearranged to be the sum of the integers from 1 up to n, so we get that

$$\pi(1) = \frac{2}{n+1} \implies \pi = \boxed{\frac{2}{n(n+1)}\begin{bmatrix} n & n-1 & \cdots & 1 \end{bmatrix}}.$$

3 Playing Blackjack

Note 22

Suppose you start with \$1, and at each turn, you win \$1 with probability p, or lose \$1 with probability $1-p$. You will continually play games of Blackjack until you either lose all your money, or you have a total of n dollars.

(a) Formulate this problem as a Markov chain.

(b) Let $\alpha(i)$ denote the probability that you end the game with n dollars, given that you started with i dollars.

Notice that for $0 < i < n$, we can write $\alpha(i+1) - \alpha(i) = k(\alpha(i) - \alpha(i-1))$. Find k.

(c) Using part (b), find $\alpha(i)$, where $0 \leq i \leq n$. (You will need to split into two cases: $p = \frac{1}{2}$ or $p \neq \frac{1}{2}$.)

Hint: Try to apply part (b) iteratively, and look at a telescoping sum to write $\alpha(i)$ in terms of $\alpha(1)$. The formula for the sum of a finite geometric series may be helpful when looking at the case where $p \neq \frac{1}{2}$:

$$\sum_{k=0}^{m} a^k = \frac{1-a^{m+1}}{1-a}.$$

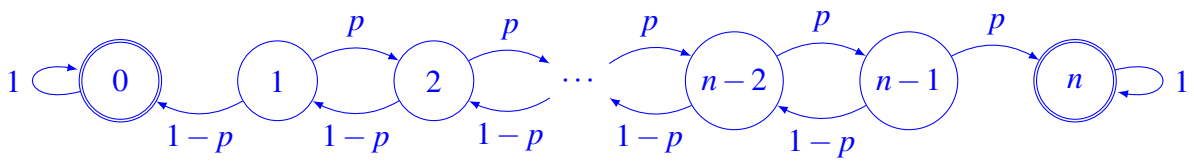
Lastly, it may help to use the value of $\alpha(n)$ to find $\alpha(1)$ for the last few steps of the calculation.

(d) As $n \to \infty$, what happens to the probability of ending the game with n dollars, given that you start with i dollars, with the following values of p?

(i) $p > \frac{1}{2}$
(ii) $p = \frac{1}{2}$
(iii) $p < \frac{1}{2}$

Solution:

(a) We have the following state transition diagram:



In particular, we have $n+1$ states, $\{0,1,2,\ldots,n\}$, where the transition probability from i to $i+1$ is p, and the transition probability from i to $i-1$ is $1-p$. The transition probabilities for $i=0$ and $i=n$ are edge cases, where we stay in place with probability 1.

(b) If we start with i dollars, this means that we start at state i. The next transition can either be to state $i+1$ with probability p, or to state $i-1$ with probability $1-p$. This means that we have

$$\alpha(i) = p\alpha(i+1) + (1-p)\alpha(i-1).$$

Here, a trick is to expand $\alpha(i) = p\alpha(i) + (1-p)\alpha(i)$. Substituting this in, we can rewrite

$$\begin{aligned} p\alpha(i) + (1-p)\alpha(i) &= p\alpha(i+1) + (1-p)\alpha(i-1) \\ (1-p)\left(\alpha(i) - \alpha(i-1)\right) &= p\left(\alpha(i+1) - \alpha(i)\right) \\ \alpha(i+1) - \alpha(i) &= \frac{1-p}{p}\left(\alpha(i) - \alpha(i-1)\right) \end{aligned}$$

(c) Now that we have a relationship between $\alpha(i+1)-\alpha(i)$ and $\alpha(i)-\alpha(i-1)$, notice that we can iteratively apply the recurrence to get

$$\begin{aligned} \alpha(i+1) - \alpha(i) &= \frac{1-p}{p}\left(\alpha(i) - \alpha(i-1)\right) \\ &= \left(\frac{1-p}{p}\right)^2 \left(\alpha(i-1) - \alpha(i-2)\right) \\ &\vdots \\ &= \left(\frac{1-p}{p}\right)^i \left(\alpha(1) - \alpha(0)\right) \\ &= \left(\frac{1-p}{p}\right)^i \alpha(1) \end{aligned}$$

since $\alpha(0) = 0$ (once we lose all our money, we stop and can never reach n).

Further, notice that we have the telescoping sum

$$[\alpha(i) - \alpha(i-1)] + [\alpha(i-1) - \alpha(i-2)] + \cdots + [\alpha(1) - \alpha(0)] = \alpha(i) - \alpha(0) = \alpha(i).$$

This means that we have the summation

$$\begin{aligned} \alpha(i) &= \sum_{k=0}^{i-1} \left(\alpha(k+1) - \alpha(k)\right) \\ &= \sum_{k=0}^{i-1} \left(\frac{1-p}{p}\right)^k \alpha(1) \\ &= \alpha(1) \sum_{k=0}^{i-1} \left(\frac{1-p}{p}\right)^k \\ &= \alpha(1) \cdot \frac{1 - \left(\frac{1-p}{p}\right)^i}{1 - \frac{1-p}{p}} \end{aligned}$$

[Note that if $p = \frac{1}{2}$, the last step is not valid; in fact, since $\frac{1-p}{p} = 1$, this means that $\alpha(i) = i\alpha(1)$. We'll come back to this case later.]

The previous formula applies for all $0 < i \leq n$, so we can let $i = n$ and simplify to find $\alpha(1)$:

$$1 = \alpha(n) = \alpha(1) \cdot \frac{1 - \left(\frac{1-p}{p}\right)^n}{1 - \frac{1-p}{p}}$$

$$\frac{1 - \frac{1-p}{p}}{1 - \left(\frac{1-p}{p}\right)^n} = \alpha(1)$$

Plugging this back in for $\alpha(i)$, we have

$$\alpha(i) = \frac{1 - \frac{1-p}{p}}{1 - \left(\frac{1-p}{p}\right)^n} \cdot \frac{1 - \left(\frac{1-p}{p}\right)^i}{1 - \frac{1-p}{p}} = \frac{1 - \left(\frac{1-p}{p}\right)^i}{1 - \left(\frac{1-p}{p}\right)^n}.$$

Going back to the case where $p = \frac{1}{2}$, we saw that the summation simplifies to $\alpha(i) = i\alpha(1)$. Since $\alpha(n) = 1$, this means that $1 = n\alpha(1)$, or $\alpha(1) = \frac{1}{n}$. This means that we have

$$\alpha(i) = i\alpha(1) = \frac{i}{n}.$$

Together, we have the following formula for any $0 \leq i \leq n$:

$$\alpha(i) = \begin{cases} \frac{1 - \left(\frac{1-p}{p}\right)^i}{1 - \left(\frac{1-p}{p}\right)^n} & p \neq \frac{1}{2} \\ \frac{i}{n} & p = \frac{1}{2} \end{cases}.$$

(d) (i) If $p > \frac{1}{2}$, then $\frac{1-p}{p} < 1$, and as $n \to \infty$, the $\left(\frac{1-p}{p}\right)^n$ term in the denominator vanishes. This means that all we're left with is the numerator, and as such

$$\lim_{n \to \infty} \alpha(i) = 1 - \left(\frac{1-p}{p}\right)^i.$$

(ii) If $p = \frac{1}{2}$, then we know that $\alpha(i) = \frac{i}{n}$. As $n \to \infty$, this fraction goes to 0, and we have

$$\lim_{n \to \infty} \alpha(i) = 0.$$

(iii) If $p < \frac{1}{2}$, then $\frac{1-p}{p} > 1$, and as $n \to \infty$, the $\left(\frac{1-p}{p}\right)^n$ term in the denominator blows up. This means that the denominator tends to $-\infty$, while the numerator remains bounded for any fixed i. This means that the entire fraction tends to 0, i.e,

$$\lim_{n \to \infty} \alpha(i) = 0.$$

Note that this problem shows that, even in the case of a fair game (i.e., $p = \frac{1}{2}$), the probability that a gambler wins \$n before going broke tends to zero as $n \to \infty$. This is one version of the so-called "Gambler's Ruin" problem. Only in the case where $p > \frac{1}{2}$, i.e., when the game is strictly in the gambler's favor, does the gambler come out on top with positive probability.