CS 70 Discrete Mathematics and Probability Theory
Spring 2022 Rao and Sen

Final Solutions

PRINT Your Name: Oski Bear

SIGN Your Name: $\mathscr{O}\mathscr{S}\mathscr{K}\mathscr{I}$

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

1. **Pledge.**

Berkeley Honor Code: As a member of the UC Berkeley community, I act with honesty, integrity, and respect for others.

In particular, I acknowledge that:

- I alone am taking this exam. Other than with the instructor and GSIs, I will not have any verbal, written, or electronic communication about the exam with anyone else while I am taking the exam or while others are taking the exam.
- I will not have any other browsers open while taking the exam.
- I will not refer to any books, notes, or online sources of information while taking the exam, other than what the instructor has allowed.
- I will not take screenshots, photos, or otherwise make copies of exam questions to share with others.
- I won't work for people from Stanford. [This is optional.]

Signed:______________

2. **Propositions. Other stuff.**

1. $\forall x \exists y\, P(x,y) \equiv \neg \exists x \forall y$ ________

   Answer: $\neg P(x,y)$. If for all x, there exists a y such that the proposition $P(x,y)$ holds, then it is not possible for there to exist an x such that for all y, the proposition does not hold.

2. $P \implies Q \equiv \neg P \vee$ ________

   Answer: Q. This follows from the definition of implication.

3. Consider a non-empty set U, predicates $P(x)$ and $Q(x)$ for any $x \in U$, and predicates $R(x,y)$ and $S(x,y)$ for any $x,y \in U$. Which of the following statements are always true?

   (a) $(\forall x,y \in U, P(x) \implies Q(y)) \equiv (\exists x \in U, P(x)) \implies (\forall x \in U, Q(x))$

   Answer: True. If there exists a $P(x)$ which is true, then $Q(y)$ must be true for every y in both statements. If not, then both statements hold regardless of the predicate $Q(\cdot)$.

   (b) $(\exists x,y \in U, P(x) \implies Q(y)) \equiv (\exists x \in U, P(x)) \implies (\forall x \in U, Q(x))$

   Answer: False. If $P(x)$ holds for one element of U, than $Q(x)$ must hold for at least one x is what the left hand side notes. For the right hand side if $P(x)$ holds for one element of U, $Q(x)$ must hold for all elements of U.

   (c) $(\exists x,y \in U, P(x) \implies Q(y)) \equiv (\exists x \in U, P(x)) \implies (\exists x \in U, Q(x))$

   Answer: False. The LHS is True if $P(x)$ is False for even one element as the statement $P(x) \implies Q(y)$ is vacuously true. But the Right Hand side is False if $Q(y)$ is always False and any $P(x)$ is true.

   (d) $(\forall x,y \in U, R(x,y) \equiv P(x) \wedge Q(y)) \implies (\forall x,y \in U, P(x) \implies R(x,y))$.

   Answer: False. $Q(y)$ could be false and $P(x)$ could be true. Thus, $P(x) \not\Longrightarrow P(x) \wedge Q(y)$.

   (e) $(\forall x,y \in U, S(x,y) \implies R(x,y)) \implies (\forall x,y \in U, \neg S(x,y)) \vee (\exists x,y \in U, R(x,y))$.

   Answer: True. The implication on the left says either $S(x,y)$ is always false or there is some x,y that is true.

4. For any natural numbers a and n both greater than 2, any solution to $x^n = a$ is either an integer or an irrational number.

   Answer: True. If it is rational c/d, then $c^n = ad^n$ and c is a multiple of a. Similarly d is a multiple of a and therefore c/d is not in reduced form. One constructs a contradiction, by noting there is a reduced form.

5. In a stable matching instance where a candidate has the same partner in both the job-optimal matching and candidate-optimal matching, that candidate has only one possible partner in any stable matching.

   Answer: True. If the candidate is paired with someone else in a stable matching S, then the job partner prefers this candidate to their partner in S (since it was paired with the candidate in the job optimal matching) and the candidate prefers the job partner (in the candidate optimal matching) to its partner in S. This is a rogue couple in S, so no such S exists.

6. In a stable matching instance that terminates in 5 days in the job-optimal stable matching algorithm, at most 5 jobs do not get the first partner in their preference list.

   Answer: False. It could be that half the jobs are rejected on the first day in an instance where $n > 12$.

3. To Prove or Disprove, that is the question.

1. (8 points) Prove or disprove: If a positive integer is congruent to 2 mod 3, it is divisible by a prime that is congruent to 2 mod 3.

   Answer: True. Suppose not. Then the prime factorization of our number consists only of primes that are 1 mod 3 or 0 mod 3, and product of those primes will be 0 or 1 mod 3, contradicting the fact that our number is 2 mod 3. Thus, our assumption was incorrect, and there exists a 2 mod 3 prime that divides our number.

2. (10 points) Prove or disprove: For a three digit number n with digits a, b and c in the hundreds, tens and ones place, respectively, $7 \mid n$ if and only if $7 \mid (10a + b - 2c)$. (Hint: $7 \mid m$ if and only if $7 \mid 3m$.)

   Answer:

$$
\begin{aligned}
n = 100a + 10b + c = 70a + 7b + 7c + 3(10a + b - 2c)& \\
&= 70a + 7b + 7c + 3(7k) \\
&= 7(10a + b + c + k)
\end{aligned}
$$

   We used $7 | 10a + b - 2c$ in the second line and the last line shows $7 \mid n$.
   To prove the other way one gets $7k = 100a + 10b + c = 70a + 7b + 7c + 3(10a + b - 2c)$ And there for $3(10a + b - 2c) = 7(k - 10a - b - c)$, which says $10a + b - 2c$ contains a factor of 7.

4. We are the mods! We are the mods! We are! We are! We are the mods!

1. For a prime p, if $a^4 \equiv 10 \pmod p$ and $a^6 \equiv 19 \pmod p$, what is $a^{10} \pmod p$?

   Answer: $190 \pmod p$. $a^{10} \equiv (a^6)(a^4) \equiv 19 \times 10 \equiv 190 \pmod p$.

2. For all integer x and y, $\gcd(x, y) = \gcd(x, x - 5y)$.

   Answer: False. One counterexample is given by $x = 20, y = 2$ (Thank you to Osher Lerner for pointing this out!).

3. If $\gcd(a, b) = 1$, then $a - b$ is not a multiple of a. (Assume a and b are integers such that $a, b \geq 2$.)

   Answer: True. If $a \mid (a - b)$ then $(a - b) = ka$ and $b = (k - 1)a$, in which case $\gcd(a, b) = a$.

4. For a, b with $\gcd(a, b) = 1$, how many solutions are there to $za = b \pmod{ab}$? (A solution is a value for z that satisfies the equation.)

   Answer: 0. For there to be a solution $za - b = i(ab)$ but the right hand side is a multiple of a, where the left hand side is not a multiple of a as b is not a multiple of a. Also a does not have a multiplicative inverse $\pmod{ab}$

5. Let $x = pd$ and $y = qd$ where $d = \gcd(x,y)$ and p,q and d are prime, and $d = ax+by$. Answers below are possibly in terms of x,y,p,q,d,a,b and constants.

   (a) What is the multiplicative inverse of $q \pmod p$?
   Answer: b. Dividing $d = ax+by$ by d yields $1 = ap+bq = bq \pmod p$.

   (b) What is $a^x \pmod p$? (Simplify.)
   Answer: $a^d \pmod p$. $a^{pd} = (a^p)^d = a^d \pmod p$, the second equality is due to $a^p = a \pmod p$ by Fermat for $a \neq 0 \pmod p$ and trivially if $a = 0 \pmod p$.

   (c) What is $a^{(x-d)(y-d)} \pmod{pq}$? (Simplify.)
   Answer: $1 \pmod{pq}$. $a^{(p-1)d(q-1)d} = (a^{(p-1)(q-1)})^{d^2} = 1^{d^2} = 1 \pmod{pq}$, the second equality is due to $a^{(p-1)(q-1)} = 1 \pmod{pq}$ by RSA for $a \neq 0 \pmod{pq}$ and trivially if $a = 0 \pmod{pq}$.

6. Let (N,e) and d be the public and private keys for an RSA scheme where $N = pq$ for primes p and q.

   (a) $x^{ed} = 1 \pmod N$ for all x.
   Answer: False. What is true is $x^{(p-1)(q-1)} = x$ where $N = pq$ and the fact that $ed = k(p-1)(q-1)+1$.

   (b) $ed = 1 \pmod N$.
   Answer: False. $ed = 1 \pmod{(p-1)(q-1)}$

   (c) The encryption of x times the encryption of y is the encryption of xy.
   Answer: True. $x^e y^e = (x+y)^e \pmod N$

   (d) The encryption of x plus the encryption of y is the encryption of $x+y$ for all x,y.
   Answer: False. $x^e + y^e \neq (x+y)^e \pmod N$ in general. E.g., for $x = y = 2$ and $N = 7 \times 11$ and $e = 3$.

5. Polynomials: So much more than omials.

1. How many polynomials of degree 2 over arithmetic modulo 5 have exactly two, not necessarily distinct, roots? You may leave your answer as an expression.
   Answer: 60 or $4(\binom{5}{2}+5)$. There $\binom{5}{2}$ possible roots without multiplicity, and 5 sets of roots with multiplicity. Then one can multiply by 4 values to scale the leading coefficient.

2. Give a polynomial $\pmod 5$ of degree 2 that contains points $(1,0),(2,3),(3,0)$.
   Answer: $2(x-1)(x-3)$. Roots at 1 and 3, and evaluates to 4 at 2.

3. Any polynomial with d roots over arithmetic modulo a prime p has degree at most d.
   Answer: False. $x^2+2x+3 \pmod 5$ has no roots and has degree 2.

4. Any polynomial of degree exactly 2 over arithmetic modulo a prime $p > 2$ has either 0 roots or 2 roots.
   Answer: True. Any linear polynomial has one root as one can set it to zero and solve. If there is 1 root, then factoring gives another.

5. Given a Berlekamp–Welch scheme for a message of size 2 tolerating 1 error and a communication channel where there is at most 1 error.

   (a) What is the degree of the original polynomial, $P(x)$, encoding the message?
   Answer: 1. It encodes two packets.

   (b) Suppose the received message is $R(0) = 0$, $R(1) = 0$, $R(2) = 0$ and $R(3) = 5$ over arithmetic modulo 5. Knowing that there is exactly one error, what is the original polynomial? (Hint: lots of zeros in received message.)
   Answer: $P(x) = 0$. There are three roots for $Q(x) = E(x)P(x)$ which is of degree 2, thus the original polynomial must be trivial.

(c) If the original polynomial is $P(x) = 2x+3 \pmod 5$, and the received message is $R(0) = 3$, $R(1) = 4$, $R(2) = 2$, and $R(3)$ is unknown, what is the error polynomial?
Answer: $x-1$. $P(1) = 0$ not 4 thus the error is at 1.

(d) If the received message is $R(0) = 1$, $R(1) = 3$, and $R(2) = 5$, and $R(3)$ is unknown, what is the original polynomial?
Answer: $2x+1 \pmod 5$. The three points all belong to this polynomial the error is at point 3.

(e) Let $E(x) = x+e$, $Q(x) = ax^2+bx+c$, and $R(0) = 4$. Find the equation relating e,a,b,c for this received message.
Answer: $c = 4e \pmod 5$. It is $a(0)^2 + b(0) + c = 4e \pmod 5$

6. Graphs

1. A cycle cover for a simple graph $G = (V,E)$ is a subset of edges $E' \subseteq E$ where every cycle in G uses an edge in E'. (A cycle must contain at least 3 edges.)

   (a) E is a cycle cover of G.
   Answer: True. Any cycle must contain an edge.

   (b) If G is a tree, the empty set is a cycle cover of G.
   Answer: True. There are no cycles to cover.

   (c) For a connected graph, what is the minimum size of a cycle cover? (Let $m = |E|$ and $n = |V|$.)
   Answer: $m-n+1$.

   (d) (5 points) Argue your answer above is sufficient. (Describe a cycle cover of this size.)
   Answer: Take a tree of the graph that uses $n-1$ edges. Any cycle must use a non-tree edge, thus the set of non-tree edges is a cycle cover.

   (e) (5 points) Argue your answer above is necessary. (Say why fewer edges will not suffice.)
   Answer: If one uses fewer the remaining graph has more edges than a tree and thus must have a cycle and thus there is a cycle that is not covered.

2. An edge coloring of a graph colors the edges so that any two edges incident to a vertex have different colors.

   (a) (6 points) Describe a method to edge color any graph with at most $2d-1$ colors where d is the maximum degree of any vertex.
   Answer: Remove an edge, recursively color the graph, and add back the edge, each adjacent vertex uses at most $d-1$ colors for a total of $2d-2$ and one color is available.

   (b) What is the minimum number of colors to edge color a hypercube of dimension n?
   Answer: n. One can use one color the set of edges corresponding to a dimension as none share an endpoint.

7. Some counting.

1. How many possible strings of red, blue, and purple beads are there of length n?
   Answer: 3^n. First rule of counting.

2. Given an unordered sample of size k out of n objects:

   (a) If the sample is chosen with repetition, how many different possible samples are there?
   Answer: $\binom{k+n-1}{n-1}$. Stars and bars where stars are number of samples, k, and bars are number of objects minus 1.

(b) If the sample is chosen without repetition, how many different possible samples are there?
Answer: $\binom{n}{k}$.

3. Consider the experiment of rolling a die until you see a 6 or until you have rolled 3 times. How many outcomes are there for this experiment? (Examples: (6), (5, 6) are possible outcomes, but (6, 6) is not as the first roll of 6 would have terminated the processes, nor is (5, 5, 5, 6) as it is longer than 3 rolls.)
Answer: 156 or $1+5+5^2\times 6$. There is one outcome of length 1 (a 'six'), 5 outcomes of length 2 (one through 5 and then 'six' and $5^2 \times 6$ outcomes of length 3 (one through 5 twice and than possible one through six.)

4. (10 points) Prove the following identity using a combinatorial argument. **Correct answers that do not use a combinatorial argument will not receive credit.**

$$\sum_{n=k}^{m}\binom{n}{k} = \binom{m+1}{k+1}$$

Answer: The right hand side is the number of $k+1$ sized subsets of $m+1$ objects. Each term in the left hand side corresponds to choosing the object $n+1$ to be the largest and choosing k from the n objects that are smaller than n.

8. Countability

In this problem, we consider that the natural numbers and the rational numbers have total orderings corresponding to their value; for example, $3 < 4$ and $1/3 < 1/2$.

1. For a set A and an ordering, $<$, on the set, let $S_{<x}(A)$ be the set of all subsets S of A, where $y \in S \implies y < x$. That is, $S_{<2}(\mathbb{N}) = \{\varnothing, \{0\}, \{1\}, \{0,1\}\}$, and has cardinality 4.
   (a) $S_{<n}(\mathbb{N})$ is countable for all $n \in \mathbb{N}$.
   Answer: True. Each such set is finite.
   (b) $\bigcup_{n\in\mathbb{N}} S_{<n}(\mathbb{N})$ is countable.
   Answer: True. It is a countable union of countable sets.
   (c) $\bigcup_{q\in\mathbb{Q}} S_{<q}(\mathbb{Q})$ is countable.
   Answer: False. The set of rational numbers less than 1 is countably infinite, and the powerset of a countably infinite set is uncountable.

2. For a set A and an ordering, $<$, the set of ordered partitions of A are the partitions $(S,\ A \setminus S)$ where $\forall x \in S, \forall y \in A \setminus S,\ x < y$. For example, for $A = \{1,2,3\}$, the set of ordered partitions of A is

$$\Big\{(\varnothing,\ \{1,2,3\}),\ (\{1\},\{2,3\}),\ (\{1,2\},\{3\}),\ (\{1,2,3\},\varnothing)\Big\}.$$

   (a) The set of ordered partitions of $\mathbb{N}$ is countable.
   Answer: True. A bijection corresponds to the maximum element in a partition.
   (b) The set of ordered partitions of $\mathbb{Q}$ is countable.
   Answer: False. The set of partitions of rational numbers have a one-to-one mapping from the reals, since each real corresponds to an ordered partition of the rationals.

9. Computability

1. The problem of whether a computer program on input x uses more than M bits of memory is decidable.
Answer: True. Just run the program. If the memory and the program counter repeats prior to more than M mememory locations being used then answer no. This will happen in finite time unless one uses more than M memory locations in which case you answer yes.

2. The problem of whether a computer program on input x executes line n is decidable.

   Answer: False. Given a procedure, **RunsLine**(P,n), one can produce a program **HALT**(P,x) by passing the program: '**Run(**P **on** x**); Print "Hello"** and the line number of the statement **Print "Hello"** to RunsLine and if it says "Yes" we know P halts on x. Thus, **RunsLine** cannot exist as **HALT** does not exist.

10. Probability: Mo' Better Venn.

Recall that a probability space has a sample space Ω and $\mathbb{P}:\Omega\to\mathbb{R}$, where $\mathbb{P}[\omega]\geq 0$ and $\sum_{\omega\in\Omega}\mathbb{P}[\omega]=1$. For an event $A\subset\Omega$, $\overline{A}=\Omega\setminus A$. Consider events $A,B\subseteq\Omega$. In each box, write the expression that correctly completes the corresponding blank.

1. $\mathbb{P}[A\cap B]=1-\mathbb{P}[\overline{A}\cup\overline{B}]-\underline{\quad ? \quad}$.

   Answer: 0. The statement, $\neg(x\in A\wedge x\in B)$ is $x\in\overline{A}\vee x\in\overline{B}$ by Demorgan's Law, thus $Pr[A\cap B]=1-Pr[\overline{A}\cup\overline{B}]$
2. For events $A,B\subset\Omega$ where A and B are independent, $\mathbb{P}[A\cap\overline{B}]=\mathbb{P}[A]\times\underline{\quad ? \quad}$.

   Answer: $1-\mathbb{P}[B]$. It is $\mathbb{P}[\overline{B}]=1-\mathbb{P}[B]$.
3. For event B, and $\omega\in B$, $\mathbb{P}[\omega\mid B]=\mathbb{P}[\omega]\times\underline{\quad ? \quad}$

   Answer: $\frac{1}{\mathbb{P}[B]}$. Conditioning on the event B means you are definitely in B and you must scale up the probabilities of each $\omega\in B$ to add to 1.
4. Given indicator random variables 1_A for event A, and 1_B for B, $\mathbb{E}[1_A\times 1_B]=\mathbb{P}[\underline{\quad ? \quad}]$. Note that $\mathbb{E}[1_A]=\mathbb{P}[A]$. (A set in terms of A and B possibly.)

   Answer: $A\cap B$.
5. $\mathrm{Cov}(1_A,1_B)=\underline{\quad ? \quad}-\mathbb{P}[A]\mathbb{P}[B]$

   Answer: $\mathbb{P}[A\cap B]$. This is $\mathbb{E}[1_A 1_B]$.
6. $\mathrm{Var}(1_A)=\underline{\quad ? \quad}$

   Answer: $\mathbb{P}[A](1-\mathbb{P}[A])$. It is a Bernoulli random variable.
7. $\mathbb{E}[1_A\mid 1_B=0]=\mathbb{P}[A\cap B]\times\underline{\quad ? \quad}$

   Answer: $\frac{\mathbb{P}[A\cap\overline{B}]}{\mathbb{P}[A\cap B]\mathbb{P}[\overline{B}]}$. It is equal to the probability of A and B given $\overline{B}$.
8. $\mathbb{E}[1_A+1_B]=\mathbb{P}[A\cup B]+\underline{\quad ? \quad}$

   Answer: $\mathbb{P}[A\cap B]$. The value is at least 1 in $A\cup B$ and is 2 in $A\cap B$.

11. Heads or Tails

1. Consider two coins, one that lands heads with probability 0.25 and another that lands heads with probability 0.75. We choose one of the two coins with equal probability and flip it twice. Let A be the event that the first toss is a heads, and let B be the event that the second toss is a heads.

   (a) What is $\mathbb{P}[A\mid B]$?

   Answer: $5/8$. $\mathbb{P}[A\mid B]=\frac{\mathbb{P}[A\cap B]}{\mathbb{P}[B]}=\frac{1/2\times 1/16+1/2\times 9/16}{1/2\times 1/4+1/2\times 3/4}=\frac{5}{8}$.

   (b) Let C be the event that the coin with heads probability 0.25 is chosen. What is $\mathbb{P}[C\mid A]$?

   Answer: $1/4$. $\mathbb{P}[C|A]=\frac{\mathbb{P}[A\cap C]}{\mathbb{P}[A]}=\frac{\mathbb{P}[C]\mathbb{P}[A|C]}{\mathbb{P}[C]\mathbb{P}[A|C]+\mathbb{P}[\overline{C}]\mathbb{P}[A|\overline{C}]}=\frac{1/2\times 1/4}{1/2\times 1/4+1/2\times 3/4}=1/4$.

(c) Let 1_A and 1_B be indicator random variables for events A and B, respectively. What is $\text{Corr}(1_A, 1_B)$? (Recall that $\text{Corr}(X,Y) = \text{Cov}(X,Y)/\sqrt{\text{Var}(X)\text{Var}(Y)}$ and $\text{Cov}(X,Y) = \mathbb{E}[XY] - \mathbb{E}[X]\mathbb{E}[Y]$.)
Answer: $\text{Var}(1_A) = \text{Var}(1_B) = 1/4$ since each is a Bernoulli Random variable with probability $1/2$. The correlation coefficient is thus

$$4(\mathbb{E}[1_A 1_B] - \mathbb{E}[1_A]^2) = 4\left(\frac{1}{2}\left(\frac{1}{16} + \frac{9}{16}\right) - \frac{1}{4}\right) = \frac{1}{4}$$

.

2. Consider two independent Bernoulli random variables X and Y with $\mathbb{E}[X] = \mathbb{E}[Y] = 1/2$. What is $\mathbb{P}[X = Y]$?
Answer: 1/2

3. Consider two Bernoulli random variables X and Y with $\mathbb{E}[X] = \mathbb{E}[Y] = 1/2$, such that $\text{Corr}(X,Y) = 0.5$.

(a) What is $\mathbb{E}[XY]$?
Answer: $3/8$. $\text{Var}(X) = \text{Var}(Y) = 1/4$, and $\text{Corr}(X,Y) = \text{Cov}(X,Y)/\sqrt{\text{Var}(X)\text{Var}(Y)}$ thus covariance is $1/8$. And $\mathbb{E}[XY] = \text{Cov}(X,Y) + \mathbb{E}[X]\mathbb{E}[Y] = 3/8$.

(b) What is $\mathbb{P}[X = Y]$?
Answer: $3/4$. $\mathbb{E}[XY] = \mathbb{P}[X = 1, Y = 1] = 3/8$. $\mathbb{P}[X = 1, Y = 0] = 1/2 - 3/8 = 1/8$ and $\mathbb{P}[X = 0, Y = 1] = 1/2 - 1/8 = 3/8$. $\mathbb{P}[X = Y] = \mathbb{P}[X = 1, Y = 1] + \mathbb{P}[X = 0, Y = 0] = 3/4$.

12. Don't Deviate!

Consider $Y = X_1 + \ldots + X_n$, where X_i are independent and identically distributed as follows:

$$X_i = \begin{cases} -1 & \text{with probability } \frac{1}{2} \\ +1 & \text{with probability } \frac{1}{2} \end{cases}$$

1. What is $\mathbb{E}[Y]$?
Answer: 0. Linearity of expectation and $\mathbb{E}[X_i] = 0$.

2. What is $\text{Var}(Y)$?
Answer: n. The average squared distance from 0 is 1 for each X_i and variance adds as they are independent.

3. Using Chebyshev's inequality, give a lower bound on ε such that $\mathbb{P}[|Y| > \varepsilon] \leq 0.05$.
Answer: $\varepsilon \geq \sqrt{20n}$. From Chebyshev, we want $0.05 \geq \frac{\text{Var}(X)}{\varepsilon^2} = \frac{n}{\varepsilon^2}$ and isolate ε.

13. Who doesn't like cake?

1. (10 points) Professor Rao is hosting a party for the CS 70 TAs, but since it is during dead week, not everyone can make it. The number of TAs that attend his party is distributed according to Poisson(λ). Professor Rao plans to split a cake evenly among himself and all of the TAs that arrive. What is the expected proportion of the cake that Professor Rao will receive? (Hint: Recall the Taylor series $e^x = \sum_{i=0}^{\infty} \frac{x^i}{i!}$.)
Answer: Let X be a random variable representing the number of TAs that attend the party, which is Poisson(λ) distributed. If k TAs attend the party, then Professor Rao receives $\frac{1}{k+1}$ of the cake. Thus,

the expected proportion of the cake that Professor Rao receives, by the definition of expectation, is

$$\begin{aligned}\sum_{k=0}^{\infty}\frac{1}{k+1}\mathbb{P}[X=k] &= \sum_{k=0}^{\infty}\frac{1}{k+1}\frac{\lambda^k e^{-\lambda}}{k!}\\ &= \sum_{k=0}^{\infty}\frac{\lambda^k e^{-\lambda}}{(k+1)!}\\ &= \frac{e^{-\lambda}}{\lambda}\sum_{k=0}^{\infty}\frac{\lambda^{k+1}}{(k+1)!}\\ &= \frac{e^{-\lambda}}{\lambda}\left(e^{\lambda}-1\right)\\ &= \frac{1-e^{-\lambda}}{\lambda},\end{aligned}$$

where we use the Taylor expansion to get from the third to fourth line.

2. Qinhong is hosting an end-of-semester party, and needs to cut a cake into slices beforehand. Unfortunately, the more slices he cuts, the smaller each individual slice is, and the less likely it is for people to come to the party! Let X be a random variable representing the number of people who will show up to the party. If Qinhong cuts the cake into n slices, then $\mathbb{E}[X]=\frac{16}{n}$ and $\text{Var}(X)=\frac{256}{n^2}$.
   (a) Qinhong wants there to be enough cake for everyone, so he wants the expected number of people who will arrive to be no greater than the number of slices. Find the smallest value of n such that $\mathbb{E}[X]\le n$.
   Answer: Using $\mathbb{E}[X]=\frac{16}{n}$, we can solve the inequality $\frac{16}{n}\le n$ and get $n\ge 4$.
   (b) Realizing that simply using expected value is not enough to ensure he doesn't run out of cake, Qinhong wants the probability of running out to be no greater than $\frac{1}{9}$. Use Markov's inequality to find the smallest value of n such that $\mathbb{P}[X\ge n]\le\frac{1}{9}$.
   Answer: Markov's inequality gives us $\mathbb{P}[X\ge n]\le\frac{\mathbb{E}[X]}{n}=\frac{16}{n^2}$. Since we want this probability to be at most $\frac{1}{9}$, we set $\frac{16}{n^2}\le\frac{1}{9}$ and solve for n to get $n\ge 12$.
   (c) Unsatisfied with this bound, Qinhong wonders if Chebyshev's inequality can give a better bound. Find the smallest value of n such that $\mathbb{P}[X\ge n]\le\frac{1}{9}$ using Chebyshev's inequality.
   Answer: To use Chebyshev's inequality, we can rewrite the event as $\mathbb{P}[X\ge n]=\mathbb{P}[X-\frac{16}{n}\ge n-\frac{16}{n}]\le\mathbb{P}[|X-\frac{16}{n}|\ge n-\frac{16}{n}]\le\frac{\text{Var}(X)}{(n-\frac{16}{n})^2}$. Plugging in $\text{Var}(X)=\frac{256}{n^2}$ and setting this probability to be at most $\frac{1}{9}$ gives us $\frac{256}{n^2(n-\frac{16}{n})^2}\le\frac{1}{9}$. We can rewrite this inequality as $256\cdot 9\le(n^2-16)^2$, and solving for n gives us $n\ge 8$.
   (d) Now, we will assume that the random variable X can be approximated by an exponential distribution, so $X\sim\text{Exp}(\frac{n}{16})$. Given this information, find the smallest value of n such that $\mathbb{P}[X\ge n]\le\frac{1}{9}$.
   Answer: Using the CDF of the exponential distribution, we can write the exact probability as $\mathbb{P}[X\ge n]=1-\mathbb{P}[X<n]=1-(1-e^{-\frac{n}{16}n})=e^{-n^2/16}$. Setting this probability to be at most $\frac{1}{9}$, we can solve for n in $e^{-n^2/16}\le\frac{1}{9}$ to get $n\ge\sqrt{16\ln 9}$.

14. Probability: small steps.

1. Consider a random variable X, with PDF $f(x)$ and CDF $F(x)$.
   (a) What is $\mathbb{P}[X\in[a,b]]$ in terms of $F(x)$?
   Answer: $F(b)-F(a)$. $\mathbb{P}[X>b]-\mathbb{P}[X>a]$ is the probability of being in between.

(b) What is $\mathbb{P}[X \in [a,b]]$ in terms of $f(x)$?
Answer: $\int_a^b f(x)\,\mathrm{d}x$.

(c) What is $\mathbb{P}[X \le x \mid X > t]$ in terms of $F(x)$? (Look carefully at the event!)
Answer: $(F(x) - F(t))/(1 - F(t))$ for $x > t$ and 0 otherwise.

2. Alice throws darts that land uniformly inside a circular dartboard of radius 1. Bob throws darts that land uniformly inside a circular dartboard of radius 2. Let A be the random variable representing the distance Alice's dart lands from the center of her dartboard, and B be the random variable representing the distance Bob's dart lands from the center of his dartboard. Assume A and B are independent.

(a) What is $F_A(x)$, the CDF of A?
Answer: $F_A(x) = x^2$ for $0 \le x \le 1$ and $F_A(x) = 1$ for $x \ge 1$

(b) What is $f_B(x)$, the PDF of B?
Answer: For $0 \le x \le 2, f(x) = x/2$ and 0 otherwise.

(c) What is the probability Bob beats Alice, $\mathbb{P}[B < A]$? (Hint: if $B < x$ and $A < x$, what is the probability that Bob beats Alice?)
Answer: $1/8$.
For Bob to win $B < 1$ which occurs with probability $1/4$ as it is $1/4$ of the area of the radius 2 dartboard. In this case, the point chosen is uniform over the dartboard of size 1 as is Alice, and thus we have by symmetry the probability that $B < A$ is $1/2 \times 1/4$.
Alternatively, we can do the following:

$$\begin{aligned}\int_0^1 f_B(x)(1 - F_A(x))\,\mathrm{d}x &= \int_0^1 \frac{x}{2}(1 - x^2)\,\mathrm{d}x \\ &= \left(\frac{x^2}{4} - \frac{x^4}{8}\right)\Bigg|_0^1 \\ &= \frac{1}{4} - \frac{1}{8} = \frac{1}{8}\end{aligned}$$

(d) We wish to compute $\mathbb{P}[B < x \mid B < A]$.

i. What is $\mathbb{P}[B < x \cap A < x \cap B < A]$ as a function of x?
Answer: $\frac{x^4}{8}$
$\mathbb{P}[B < x]\mathbb{P}[A < x]\mathbb{P}[B < A \mid B < x, A < x] = \frac{x^2}{4}(x^2)\frac{1}{2} = \frac{x^4}{8}$

ii. What is $\mathbb{P}[B < x \cap A \ge x \cap B < A]$?
Answer: $\frac{x^2}{4}(1 - x^2)$
$\mathbb{P}[B < x \cap A \ge x \cap B < A] = \mathbb{P}[B < x]\mathbb{P}[A \ge x] = \frac{x^2}{4}(1 - x^2)$

iii. What is $\mathbb{P}[B < x \mid B < A]$?
Answer: $2x^2 - x^4$
Add the two answers above and divide by $\mathbb{P}[B < A]$.

15. Estimating Wald(o).

Let $N \sim \text{Poisson}(\lambda)$ and $Y = X_1 + \cdots + X_N$ with i.i.d. $X_i \sim \text{Exp}(\lambda)$.

1. What is $\mathbb{E}[Y]$?
Answer: 1. $\mathbb{E}[\mathbb{E}[Y \mid N]] = \mathbb{E}[N\frac{1}{\lambda}] = \lambda \times \frac{1}{\lambda}$.

2. What is the MMSE of Y given N?

   Answer: $N\frac{1}{\lambda}$.

3. What is the LLSE of Y given N?

   Answer: $N\frac{1}{\lambda}$. Same as above. It is already linear in N.

16. Chaining heads!

You have some biased coins with probability $p = \frac{3}{5}$ of heads.

1. You repeat pairs of coin tosses, until both flips in a pair are heads. How many coin tosses does this take in expectation?

   Answer: The number of pairs of tosses is distributed as Geom$(\frac{9}{25})$, so the expected number of tosses is $\frac{25}{9} \cdot 2 = \frac{50}{9}$.

2. You repeatedly flip the coin until two flips in a row are heads. How many coin tosses does this take in expectation?

   Answer: We set up the hitting time equations

$$\begin{aligned}
\beta(0) &= 1 + \frac{2}{5}\beta(0) + \frac{3}{5}\beta(1) \\
\beta(1) &= 1 + \frac{2}{5}\beta(0) + \frac{3}{5}\beta(2) \\
\beta(2) &= 0
\end{aligned}$$

   Solving yields $\beta(0) = \frac{40}{9}$.

17. Slip, slip, slip away!

(15 points) Leanne begins the following process: at time step 1, she chooses an integer uniformly at random from 0 to n, inclusive. For $t \geq 1$, at time step $t+1$, she chooses an integer uniformly at random from 0 to a_t, inclusive, where a_t is the integer chosen at time step t. Prove that the expected sum of all of the integers Leanne chooses is equal to n.

(Hint: You may find the variable S_m, the expected sum if Leanne starts choosing from 0 to m, useful in your proof. You may also find the following equation helpful: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Finally, induction might be helpful.)

Answer: Let S_m represent the expected sum given that the previous choice was m; we wish to solve for S_n. For each $1 \leq m \leq n$, we get the system of equations

$$S_m = \sum_{i=0}^{m} \frac{1}{m+1}(S_i + i),$$

with $S_0 = 0$.

We now prove the claim via strong induction; we wish to show that $S_i = i$ for all $0 \leq i \leq n$. The base case is

$S_0 = 0$. Now, suppose that $S_i = i$ for all $0 \le i \le m-1$ for some $1 \le m \le n$. Then

$$\begin{aligned} S_m &= \sum_{i=0}^{m} \frac{1}{m+1}(S_i + i) \\ &= \frac{1}{m+1} S_m + \frac{m}{m+1} + \sum_{i=0}^{m-1} \frac{1}{m+1} 2i \\ &= \frac{1}{m+1} S_m + \frac{m}{m+1} + \frac{2}{m+1} \frac{(m-1)m}{2} \\ &= \frac{1}{m+1} S_m + \frac{m^2}{m+1}, \end{aligned}$$

so solving for S_m gives $S_m = m$, as desired. This completes the induction.

18. A single random variable in possession of a well-defined probability function must be in want of a joint distribution.

Elizabeth is visiting Pemberley and wants to explore the 10 rooms, numbered 1 through 10. However, she wants to avoid Mr. Darcy, who is also at Pemberley. Every minute, Elizabeth picks one of the 10 rooms uniformly at random to enter and Darcy, independently of Elizabeth, picks one of the 10 rooms uniformly at random to enter.

1. What is the expected number of minutes that will pass until Elizabeth and Darcy meet each other in the same room?

   Answer: Each minute, Elizabeth will choose a room and the probability that Darcy chooses to enter that same room is $\frac{1}{10}$. Thus, the number of minutes that pass is distributed according to $\text{Geo}\left(\frac{1}{10}\right)$, which has expectation 10.

2. What is the probability that at least 10 minutes will pass before Elizabeth encounters Darcy in the same room as her?

   Answer: We need to compute $\mathbb{P}\left[\text{Geo}\left(\frac{1}{10}\right) \ge 10\right]$. This means that Elizabeth simply needs to avoid Darcy for 10 minutes and afterwards, anything can happen, which happens with probability $\left(\frac{9}{10}\right)^{10}$.

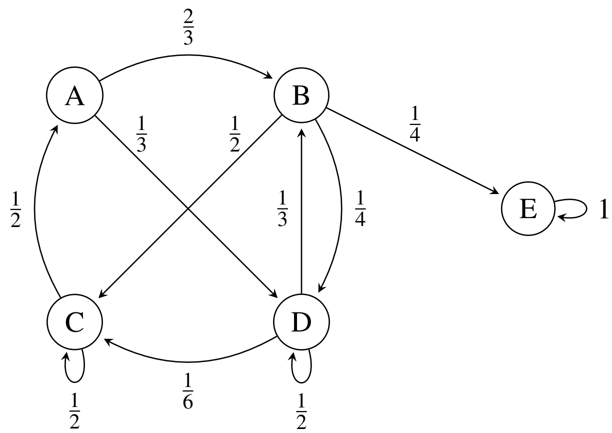
3. Since Darcy owns Pemberley, he knows the estate very well and he has a rough idea of which room Elizabeth is going to. Anxious to redeem himself to her, Darcy changes his strategy: if Elizabeth goes to room number r at some minute, Darcy will choose to enter any room between 1 and r uniformly at random in that same minute. Let E_i be the random variable representing the room Elizabeth enters at the ith minute and D_i represent the room Darcy enters at the ith minute. Derive an expression, possibly involving cases, for the joint distribution $\mathbb{P}[E_i = r_e, D_i = r_d]$ for $r_e, r_d \in \{1,2,3,\dots,10\}$.

   Answer: We have

$$\begin{aligned} \mathbb{P}[E_i = r_e, D_i = r_d] &= \mathbb{P}[E_i = r_e]\mathbb{P}[D_i = r_d \mid E_i = r_e] \\ &= \begin{cases} \left(\frac{1}{10}\right)\left(\frac{1}{r_e}\right) = \frac{1}{10 r_e} & \text{if } r_d \le r_e \\ 0 & \text{if } r_d > r_e \end{cases} \end{aligned}$$

19. Heathcliff, it's me, Cathy!

Catherine and Ellen are locked inside of Wuthering Heights and are trying to escape! Their escape can be modeled as the Markov chain shown below, where at every time step, they transition from one place to another (or they hear servants around and choose to remain in place, represented with self-loops). They begin in Zillah's chamber, represented by **state A**, and if they reach the exit, represented by **state E**, they can successfully escape.



1. (5 points) Catherine and Ellen want to avoid Heathcliff's room, represented by **state C**, during their escape. Set up, **but do not solve**, first step equations for computing the probability that they reach the exit before they reach Heathcliff's room.

   Answer: We set up the first step equations:

$$\begin{aligned}
\alpha(A) &= \frac{2}{3}\alpha(B) + \frac{1}{3}\alpha(D) \\
\alpha(B) &= \frac{1}{2}\alpha(C) + \frac{1}{4}\alpha(D) + \frac{1}{4}\alpha(E) \\
\alpha(C) &= 0 \\
\alpha(D) &= \frac{1}{3}\alpha(B) + \frac{1}{6}\alpha(C) + \frac{1}{2}\alpha(D) \\
\alpha(E) &= 1
\end{aligned}$$

   Solving gives us $\alpha(A) = \frac{4}{15}$.

2. Catherine and Ellen reached the exit before they reached Heathcliff's room and were able to escape! Now, we wish to find the expected amount of time that their escape took. In the following parts, let X_t represent their state at time step t for $t \in \{0, 1, 2, \ldots\}$.

   (a)
$$\mathbb{P}[X_{t+1} = D \mid X_t = B,\ X_{t+1} \neq C] =$$

   Answer: $1/2$. $\frac{\frac{1}{4}}{\frac{1}{4}+\frac{1}{4}} = \frac{1}{2}$

   (b)
$$\mathbb{P}[X_{t+1} = E \mid X_t = B,\ X_{t+1} \neq C] =$$

   Answer: $\frac{\frac{1}{4}}{\frac{1}{4}+\frac{1}{4}} = \frac{1}{2}$

(c) (8 points) Set up, **but do not solve**, hitting time equations for computing the expected amount of time Catherine and Ellen's escape took, given that they successfully avoided Heathcliff's room. 5cm]12cm
Answer: $\beta(B) = 1 + \frac{1}{2}\beta(D) + \frac{1}{2}\beta(E)$

Answer: For completeness, we include a full solution.

Using the condition that C is never visited, we derive new transitions for states B and C:

$$\mathbb{P}[X_{t+1} = D \mid X_t = B, X_{t+1} \neq C] = \frac{\frac{1}{4}}{\frac{1}{4}+\frac{1}{4}} = \frac{1}{2}$$
$$\mathbb{P}[X_{t+1} = E \mid X_t = B, X_{t+1} \neq C] = \frac{\frac{1}{4}}{\frac{1}{4}+\frac{1}{4}} = \frac{1}{2}$$
$$\mathbb{P}[X_{t+1} = B \mid X_t = D, X_{t+1} \neq C] = \frac{\frac{1}{3}}{\frac{1}{3}+\frac{1}{2}} = \frac{2}{5}$$
$$\mathbb{P}[X_{t+1} = D \mid X_t = D, X_{t+1} \neq C] = \frac{\frac{1}{2}}{\frac{1}{3}+\frac{1}{2}} = \frac{3}{5}$$

We now set up the hitting time equations:

$$\beta(A) = 1 + \frac{2}{3}\beta(B) + \frac{1}{3}(D)$$
$$\beta(B) = 1 + \frac{1}{2}\beta(D) + \frac{1}{2}\beta(E)$$
$$\beta(D) = 1 + \frac{2}{5}\beta(B) + \frac{3}{5}\beta(D)$$
$$\beta(E) = 0$$

Solving gives us $\beta(A) = \frac{19}{3}$.