I worked alone without getting any help.

1 Administrivia

(a) http://www.eecs70.org

(b) Homework: 10%
Midterm 1: 25%
Midterm 2: 25%
Final: 40%

2 Course Policies

(a) Yes. As said in Course Policies, "you must always write up the solutions on your own," but Alice and Bob wrote up a solution together.

(b) No. As long as Dan doesn't write his code on the board, Carol is a perfect example for getting help from peers, as she not only writes up her solutions alone in her own words, but also credits the person who has inspired her.

(c) No. As long as Erin doesn't copy the website verbatim, she is a perfect example for utilizing online resources since she doesn't copy the answer directly. Instead, she first understands the solution and then writes her solution alone, crediting the resource.

(d) Yes. Both Frank and Grace violated the policy. For Frank, he copied directly from Grace's work, which is not allowed as Course Policies said, "At no time should you be in possession of another student's solution."; for Grace, she shouldn't have given her written solutions. She could explain her ideas and approach, but not show her code.

(e) Yes. Similar to (d), both violated the policy. As said in Course Policies, "At no time should you be in possession of another student's solution." Irene shouldn't use Heidi's solution to write her own, and Heidi shouldn't have sent her work.

3 Use of Piazza

(a) 13

(b) Hi xxx (student's name), you should probably go to the office hours or the homework party this week. This question can't be explained within 5 minutes.

4 LaTeX

(a) $\forall x \exists y \big((P(x) \land Q(x,y)) \implies x \leq \sqrt{y}\big)$

(b) $\sum\limits_{i=0}^{k} i = \frac{k(k+1)}{2}$

CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Alistair Sinclair and Yun Song

HW 1

Due: Friday, August 31, 2018 at 10 PM

Sundry

Before you start your homework, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Always True or Always False?

Classify the following statements as being one of the following, where x and y are arbitrary propositions, and justify your answers (e.g., using a truth table)

- True for all combinations of x and y (Tautology)
- False for all combinations of x and y (Contradiction)
- Neither

(a) $x \wedge (x \implies y) \wedge (\neg y)$

(b) $x \implies (x \vee y)$

(c) $(x \vee y) \vee (x \vee \neg y)$

(d) $(x \implies y) \vee (x \implies \neg y)$

(e) $(x \vee y) \wedge (\neg(x \wedge y))$

(f) $(x \implies y) \wedge (\neg x \implies y) \wedge (\neg y)$

2 Miscellaneous Logic

(a) Let the statement, $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})\ G(x,y)$, be true for predicate $G(x,y)$.

For each of the following statements, decide if the statement is certainly true, certainly false, or possibly true, and justify your solution. (If possibly true, provide a specific example where the statement is false and a specific example where the statement is true.)

(i) $G(3,4)$

(ii) $(\forall x \in \mathbb{R})\ G(x,3)$

(iii) $\exists y\ G(3,y)$

(iv) $\forall y\ \neg G(3,y)$

(v) $\exists x\ G(x,4)$

(b) Give an expression using terms involving $\vee, \wedge$ and $\neg$ which is true if and only if exactly one of X, Y, and Z is true.

3 Propositional Practice

Convert the following English sentences into propositional logic and the following propositions into English. State whether or not each statement is true with brief justification.

(a) There is a real number which is not rational.

(b) All integers are natural numbers or are negative, but not both.

(c) If a natural number is divisible by 6, it is divisible by 2 or it is divisible by 3.

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

(e) $(\forall x \in \mathbb{Z})\ (((2 \mid x) \vee (3 \mid x)) \implies (6 \mid x))$

(f) $(\forall x \in \mathbb{N})\ ((x > 7) \implies ((\exists a, b \in \mathbb{N})\ (a + b = x)))$

4 Proof by?

(a) Prove that if for any two integers x and y, if 10 does not divide xy, then 10 does not divide x and 10 does not divide y. In notation: $(\forall x, y \in \mathbb{Z})\ \ (10 \nmid xy) \implies ((10 \nmid x)\ \ \wedge\ \ (10 \nmid y))$. What proof technique did you use?

(b) Prove or disprove the contrapositive.

(c) Prove or disprove the converse.

5 Prove or Disprove

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

(b) $(\forall x, y \in \mathbb{R})$ $\min(x,y) = (x + y - |x - y|)/2$.

(c) $(\forall a, b \in \mathbb{R})$ if $a + b \leq 10$ then $a \leq 7$ or $b \leq 3$.

(d) $(\forall r \in \mathbb{R})$ if r is irrational then $r + 1$ is irrational.

(e) $(\forall n \in \mathbb{Z}^+)$ $10n^2 > n!$.

6 Preserving Set Operations

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

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

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

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

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

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

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

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

CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Alistair Sinclair and Yun Song

HW 2

Due: Friday, 9/8, 10 PM

Sundry

Before you start your homework, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Hit or Miss?

State which of the proofs below is correct or incorrect. For the incorrect ones, please explain clearly where the logical error in the proof lies. Simply saying that the claim or the induction hypothesis is false is *not* a valid explanation of what is wrong with the proof. You do not need to elaborate if you think the proof is correct.

(a) **Claim:** For all positive numbers $n \in \mathbb{R}$, $n^2 \geq n$.

Proof. The proof will be by induction on n.
Base Case: $1^2 \geq 1$. It is true for $n = 1$.
Inductive Hypothesis: Assume that $n^2 \geq n$.
Inductive Step: We must prove that $(n+1)^2 \geq n+1$. Starting from the left hand side,

$$\begin{aligned}(n+1)^2 &= n^2 + 2n + 1 \\ &\geq n + 1.\end{aligned}$$

Therefore, the statement is true. □

(b) **Claim:** For all negative integers n, $(-1) + (-3) + \cdots + (2n+1) = -n^2$.

Proof. The proof will be by induction on n.
Base Case: $-1 = -(-1)^2$. It is true for $n = -1$.
Inductive Hypothesis: Assume that $(-1) + (-3) + \cdots + (2n+1) = -n^2$.

Inductive Step: We need to prove that the statement is also true for $n-1$ if it is true for n, that is, $(-1)+(-3)+\cdots+(2(n-1)+1) = -(n-1)^2$. Starting from the left hand side,

$$\begin{aligned}(-1)+(-3)+\cdots+(2(n-1)+1) &= ((-1)+(-3)+\cdots+(2n+1))+(2(n-1)+1)\\ &= -n^2+(2(n-1)+1) \quad \text{(Inductive Hypothesis)}\\ &= -n^2+2n-1\\ &= -(n^2-2n+1)\\ &= -(n-1)^2.\end{aligned}$$

Therefore, the statement is true. □

(c) **Claim:** For all nonnegative integers n, $2n = 0$.

Proof. We will prove by strong induction on n.
Base Case: $2 \times 0 = 0$. It is true for $n = 0$.
Inductive Hypothesis: Assume that $2k = 0$ for all $0 \le k \le n$.
Inductive Step: We must show that $2(n+1) = 0$. Write $n+1 = a+b$ where $0 < a, b \le n$. From the inductive hypothesis, we know $2a = 0$ and $2b = 0$, therefore,

$$2(n+1) = 2(a+b) = 2a+2b = 0+0 = 0.$$

The statement is true. □

2 A Coin Game

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.)

3 Grid Induction

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?)

4 Stable Marriage

Consider a set of four men and four women with the following preferences:

men	preferences	women	preferences
A	1>2>3>4	1	D>A>B>C
B	1>3>2>4	2	A>B>C>D
C	1>3>2>4	3	A>B>C>D
D	3>1>2>4	4	A>B>D>C

(a) Run on this instance the stable matching algorithm presented in class. Show each day of the algorithm, and give the resulting matching, expressed as $\{(M,W),\ldots\}$.

(b) Suppose we relax the rules for the men, so that each unpaired man proposes to the next woman on his list at a time of his choice (some men might procrastinate for several days, while others might propose and get rejected several times in a single day). Prove that this modification will not change what pairing the algorithm outputs.

5 Optimal Partners

In the notes, we proved that the Stable Marriage Algorithm always outputs the male-optimal pairing. However, we never explicitly showed why it is guaranteed that putting every man with his best choice results in a pairing at all. Prove by contradiction that no two men can have the same optimal partner. (Note: your proof should not rely on the fact that the Stable Marriage Algorithm outputs the male-optimal pairing.)

6 Examples or It's Impossible

Determine if each of the situations below is possible with the traditional propose-and-reject algorithm. If so, give an example with at least 3 men and 3 women. Otherwise, give a brief proof as to why it's impossible.

(a) Every man gets his first choice.

(b) Every woman gets her first choice, even though her first choice does not prefer her the most.

(c) Every woman gets her last choice.

(d) Every man gets his last choice.

(e) A man who is second on every woman's list gets his last choice.

CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Alistair Sinclair and Yun Song HW 3

Due: September 7, 2018 at 10 PM

Sundry

Before you start your homework, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Short Answer: Graphs

(a) Bob removed a degree 3 node in an n-vertex tree, how many connected components are in the resulting graph? (An expression that may contain n.)

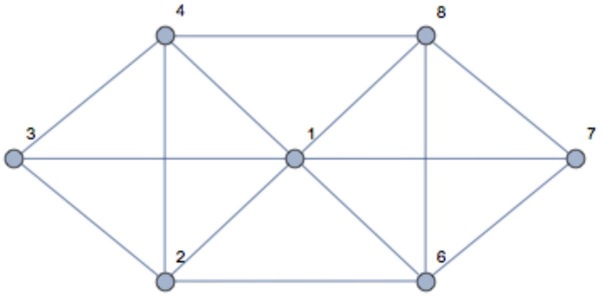
(b) Given an n-vertex tree, Bob added 10 edges to it, then Alice removed 5 edges and the resulting graph has 3 connected components. How many edges must be removed to remove all cycles in the resulting graph? (An expression that may contain n.)

(c) True or False: For all $n \geq 3$, the complete graph on n vertices, K_n has more edges than the n-dimensional hypercube. Justify your answer.

(d) A complete graph with n vertices where n is an odd prime can have all its edges covered with x Hamiltonian cycles (a Hamiltonian cycle is a cycle where each vertex appears exactly once). What is the number, x, of such cycles required to cover the a complete graph? (Answer should be an expression that depends on n.)

(e) Give a set of edge-disjoint Hamiltonian cycles that covers the edges of K_5, the complete graph on 5 vertices. (Each path should be a sequence (or list) of edges in K_5, where an edge is written as a pair of vertices from the set $\{0,1,2,3,4\}$ - e.g: $(0,1),(1,2)$.)

2 Eulerian Tour and Eulerian Walk



(a) Is there an Eulerian tour in the graph above?

(b) Is there an Eulerian walk in the graph above?

(c) What is the condition that there is an Eulerian walk in an undirected graph? Briefly justfy your answer.

3 Bipartite Graph

A bipartite graph consists of 2 disjoint sets of vertices (say L and R), such that no 2 vertices in the same set have an edge between them. For example, here is a bipartite graph (with $L = \{$green vertices$\}$ and $R = \{$red vertices$\}$), and a non-bipartite graph.

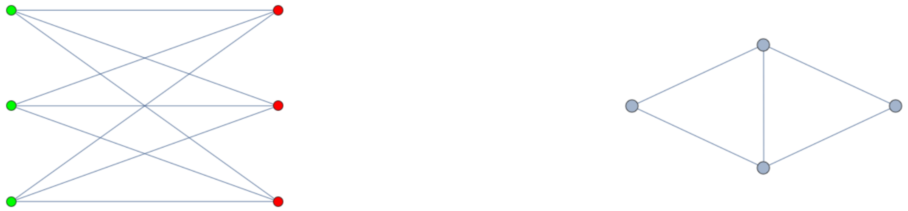


Figure 1: A bipartite graph (left) and a non-bipartite graph (right).

Prove that a graph is bipartite if and only if it has no tours of odd length.

4 Hypercubes

The vertex set of the n-dimensional hypercube $G = (V, E)$ is given by $V = \{0,1\}^n$ (recall that $\{0,1\}^n$ denotes the set of all n-bit strings). There is an edge between two vertices x and y if and only if x and y differ in exactly one bit position. These problems will help you understand hypercubes.

(a) Draw 1-, 2-, and 3-dimensional hypercubes and label the vertices using the corresponding bit strings.

(b) Show that for any $n \geq 1$, the n-dimensional hypercube is *bipartite*: the vertices can be partitioned into two groups so that every edge goes between the two groups.

5 Triangulated Planar Graph

In this problem you will prove that every triangulated planar graph (every face has 3 sides; that is, every face has three edges bordering it, including the unbounded face) contains either (1) a vertex of degree 1, 2, 3, 4, (2) two degree 5 vertices which are adjacent, or (3) a degree 5 and a degree 6 vertices which are adjacent. Justify your answers.

(a) Place a "charge" on each vertex v of value $6 - \text{degree}(v)$. What is the sum of the charges on all the vertices? (*Hint*: Use Euler's formula and the fact that the planar graph is triangulated.)

(b) What is the charge of a degree 5 vertex and of a degree 6 vertex?

(c) Suppose now that we shift $1/5$ of the charge of a degree 5 vertex to each of its neighbors that has a negative charge. (We refer to this as "discharging" the degree 5 vertex.) Conclude the proof under the assumption that, after discharging all degree 5 vertices, there is a degree 5 vertex with positive remaining charge.

(d) If no degree 5 vertices have positive charge after discharging the degree 5 vertices, does there exist any vertex with positive charge after discharging? If there is such a vertex, what are the possible degrees of that vertex?

(e) Suppose there exists a degree 7 vertex with positive charge after discharging the degree 5 vertices. How many neighbors of degree 5 might it have?

(f) Continuing from Part (e). Since the graph is triangulated, are two of these degree 5 vertices adjacent?

(g) Finish the proof from the facts you obtained from the previous parts.

CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Alistair Sinclair and Yun Song **HW 4**

Due: September 21, 2018 at 10 PM

Sundry

Before you start your homework, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Modular Arithmetic Solutions

Find all solutions (modulo the corresponding modulus) to the following equations. Prove that there are no other solutions (in a modular setting) to each equation.

(a) $2x \equiv 5 \pmod{15}$

(b) $2x \equiv 5 \pmod{16}$

(c) $5x \equiv 10 \pmod{25}$

2 Euclid's Algorithm

(a) Use Euclid's algorithm from lecture to compute the greatest common divisor of 527 and 323. List the values of x and y of all recursive calls.

(b) Use extended Euclid's algorithm from lecture to compute the multiplicative inverse of 5 mod 27. List the values of x and y and the returned values of all recursive calls.

(c) Find $x \pmod{27}$ if $5x + 26 \equiv 3 \pmod{27}$. You can use the result computed in (b).

(d) Assume a, b, and c are integers and $c > 0$. Prove or disprove: If a has no multiplicative inverse mod c, then $ax \equiv b \pmod{c}$ has no solution.

3 Modular Exponentiation

Compute the following:

(a) $13^{2018} \pmod{12}$

(b) $8^{11111} \pmod{9}$

(c) $7^{256} \pmod{11}$

(d) $3^{160} \pmod{23}$

4 Euler's Totient Function

Euler's totient function is defined as follows:

$$\phi(n) = |\{i : 1 \leq i \leq n, \texttt{gcd}(n,i) = 1\}|$$

In other words, $\phi(n)$ is the total number of positive integers less than or equal to n which are relatively prime to it. Here is a property of Euler's totient function that you can use without proof:

For m,n such that $\texttt{gcd}(m,n) = 1$, $\phi(mn) = \phi(m) \cdot \phi(n)$.

(a) Let p be a prime number. What is $\phi(p)$?

(b) Let p be a prime number and k be some positive integer. What is $\phi(p^k)$?

(c) Let p be a prime number and a be a positive integer smaller than p. What is $a^{\phi(p)} \pmod{p}$? *(Hint: use Fermat's Little Theorem.)*

(d) Let b be a positive integer whose prime factors are $p_1, p_2, \ldots, p_k$. We can write $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.

Show that for any a relatively prime to b, the following holds:

$$\forall i \in \{1,2,\ldots,k\}, \; a^{\phi(b)} \equiv 1 \pmod{p_i}$$

5 FLT Converse

Recall that the FLT states that, given a prime n, $a^{n-1} \equiv 1 \pmod{n}$ *for all* $1 \leq a \leq n-1$. Note that it says nothing about when n is composite.

Can the FLT condition ($a^{n-1} \equiv 1 \mod n$) hold for some or even all a if n is composite? This problem will investigate both possibilities. It turns out that unlike in the prime case, we need to restrict ourselves to looking at a that are relatively prime to n. (Note that if n is prime, then every $a < n$ is relatively prime to n). Because of this restriction, let's define

$$S(n) = \{i : 1 \leq i \leq n, \texttt{gcd}(n,i) = 1\},$$

so $|\, S \,|$ is the total number of possible choices for a.

(a) Prove that for every a and n that are not relatively prime, FLT condition fails. In other words, for every a and n such that $\texttt{gcd}(n,a) \neq 1$, we have $a^{n-1} \not\equiv 1 \pmod{n}$.

(b) Prove that the FLT condition fails for most choices of a and n. More precisely, show that if we can find a single $a \in S(n)$ such that $a^{n-1} \not\equiv 1 \pmod{n}$, we can find at least $|S(n)|/2$ such a. (Hint: You're almost there if you can show that the set of numbers that fail the FLT condition is at least as large as the set of numbers that pass it. A clever bijection may be useful to compare set sizes.)

The above tells us that if a composite number fails the FLT condition for even one number relatively prime to it, then it fails the condition for most numbers relatively prime to it. However, it doesn't rule out the possibility that some composite number n satisifes the FLT condition entirely: *for all* a relatively prime to n, $a^{n-1} \equiv 1 \mod n$. It turns out such numbers do exist, but they were found through trial-and-error! We will prove one of the conditions on n that make it easy to verify the existence of these numbers.

(c) First, show that if $a \equiv b \mod m_1$ and $a \equiv b \mod m_2$, with $\gcd(m_1, m_2) = 1$, then $a \equiv b \pmod{m_1 m_2}$.

(d) Let $n = p_1 p_2 \cdots p_k$ where p_i are distinct primes and $p_i - 1 \mid n-1$ for all i. Show that $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in S(n)$

(e) Verify that for all a coprime with 561, $a^{560} \equiv 1 \pmod{561}$.

CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Alistair Sinclair and Yun Song **HW 5**

Due: Friday, 9/28, 10pm

Sundry

Before you start your homework, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Quick Computes

Simplify each expression using Fermat's Little Theorem.

(a) $3^{33} \pmod{11}$

(b) $10001^{10001} \pmod{17}$

(c) $10^{10} + 20^{20} + 30^{30} + 40^{40} \pmod{7}$

2 RSA Practice

Bob would like to receive encrypted messages from Alice via RSA.

(a) Bob chooses $p = 7$ and $q = 11$. His public key is (N, e). What is N?

(b) What number is e relatively prime to?

(c) e need not be prime itself, but what is the smallest prime number e can be? Use this value for e in all subsequent computations.

(d) What is $\gcd(e, (p-1)(q-1))$?

(e) What is the decryption exponent d?

(f) Now imagine that Alice wants to send Bob the message 30. She applies her encryption function E to 30. What is her encrypted message?

(g) Bob receives the encrypted message, and applies his decryption function D to it. What is D applied to the received message?

3 Squared RSA

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

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

(c) Prove that this scheme is at least as hard to break as normal RSA; that is, prove that if this scheme can be broken, normal RSA can be as well. We consider RSA to be broken if knowing pq allows you to deduce $(p-1)(q-1)$. We consider squared RSA to be broken if knowing p^2q^2 allows you to deduce $p(p-1)q(q-1)$.

CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Alistair Sinclair and Yun Song **HW 6**

Due: Friday, 7/27, 10pm

Sundry

Before you start your homework, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Polynomial Practice

(a) If f and g are non-zero real polynomials, how many roots do the following polynomials have at least? How many can they have at most? (Your answer may depend on the degrees of f and g.)

(i) $f+g$

(ii) $f \cdot g$

(iii) f/g, assuming that f/g is a polynomial

(b) Now let f and g be polynomials over $\mathrm{GF}(p)$.

(i) If $f \cdot g = 0$, is it true that either $f = 0$ or $g = 0$?

(ii) If $\deg f \geq p$, show that there exists a polynomial h with $\deg h < p$ such that $f(x) = h(x)$ for all $x \in \{0, 1, ..., p-1\}$.

(iii) How many f of degree *exactly* $d < p$ are there such that $f(0) = a$ for some fixed $a \in \{0, 1, \ldots, p-1\}$?

(c) Find a polynomial f over $\mathrm{GF}(5)$ that satisfies $f(0) = 1, f(2) = 2, f(4) = 0$. How many such polynomials are there?

2 The CRT and Lagrange Interpolation

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

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} && (1) \\ x &\equiv a_2 \pmod{n_2} && (2) \\ &\vdots && (\vdots) \\ x &\equiv a_k \pmod{n_k} && (k) \end{aligned}$$

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

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

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

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

(d) For two polynomials $p(x)$ and $q(x)$, mimic the definition of $a \bmod b$ for integers to define $p(x) \bmod q(x)$. Use your definition to find $p(x) \bmod (x-1)$.

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

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

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

3 Old secrets, new secrets

In order to share a secret number s, Alice distributed the values $(1, p(1)), (2, p(2)), \ldots, (n+1, p(n+1))$ of a degree n polynomial p with her friends $\text{Bob}_1, \ldots, \text{Bob}_{n+1}$. As usual, she chose p such that $p(0) = s$. Bob_1 through Bob_{n+1} now gather to jointly discover the secret. Suppose that for some reason Bob_1 already knows s, and wants to play a joke on $\text{Bob}_2, \ldots, \text{Bob}_{n+1}$, making them believe that the secret is in fact some fixed $s' \neq s$. How can he achieve this?

4 Berlekamp-Welch for General Errors

Suppose that Hector wants to send you a length $n = 3$ message, m_0, m_1, m_2, with the possibility for $k = 1$ error. For all parts of this problem, we will work mod 11, so we can encode 11 letters as shown below:

A	B	C	D	E	F	G	H	I	J	K
0	1	2	3	4	5	6	7	8	9	10

Hector encodes the message by finding the degree ≤ 2 polynomial $P(x)$ that passes through $(0, m_0)$, $(1, m_1)$, and $(2, m_2)$, and then sends you the five packets $P(0), P(1), P(2), P(3), P(4)$ over a noisy channel. The message you receive is

$$\text{DHACK} \Rightarrow 3, 7, 0, 2, 10 = r_0, r_1, r_2, r_3, r_4$$

which could have up to 1 error.

(a) First, let's locate the error, using an error-locating polynomial $E(x)$. Let $Q(x) = P(x)E(x)$. Recall that

$$Q(i) = P(i)E(i) = r_i E(i), \quad \text{for} \quad 0 \leq i < n + 2k.$$

What is the degree of $E(x)$? What is the degree of $Q(x)$? Using the relation above, write out the form of $E(x)$ and $Q(x)$ in terms of the unknown coefficients, and then a system of equations to find both these polynomials.

(b) Solve for $Q(x)$ and $E(x)$. Where is the error located?

(c) Finally, what is $P(x)$? Use $P(x)$ to determine the original message that Hector wanted to send.

5 Error-Detecting Codes

Suppose Alice wants to transmit a message of n symbols, so that Bob is able to *detect* rather than *correct* any errors that have occured on the way. That is, Alice wants to find an encoding so that Bob, upon receiving the code, is able to either

(I) tell that there are no errors and decode the message, or

(II) realize that the transmitted code contains at least one error, and throw away the message.

Assuming that we are guaranteed a maximum of k errors, how should Alice extend her message (i.e. by how many symbols should she extend the message, and how should she choose these symbols)? You may assume that we work in GF(p) for very large prime p. Show that your scheme works, and that adding any lesser number of symbols is not good enough.

CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Alistair Sinclair and Yun Song **Homework 7**

Due: Friday, August 3, 2018 at 10 PM

Sundry

Before you start your homework, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Bijective or not?

Decide whether the following functions are bijections or not. Please prove your claims.

(a) $f(x) = 10^{-5}x$

  (i) for domain $\mathbb{R}$ and range $\mathbb{R}$

  (ii) for domain $\mathbb{Z} \cup \{\pi\}$ and range $\mathbb{R}$

(b) $f(x) = p \bmod x$, where $p > 2$ is a prime

  (i) for domain $\mathbb{N} \setminus \{0\}$ and range $\{0, \dots, p\}$

  (ii) for domain $\{(p+1)/2, \dots, p\}$ and range $\{0, \dots, (p-1)/2\}$

(c) $f(x) = \{x\}$, where the domain is $D = \{0, \dots, n\}$ and the range is $\mathscr{P}(D)$, the powerset of D (that is, the set of all subsets of D).

(d) Consider the number $X = 1234567890$, and obtain X' by shuffling the order of the digits of X. Is $f(i) = (\mathrm{i}+1)^{\text{st}}$ *digit of* X' a bijection from $\{0, \dots, 9\}$ to itself?

2 Counting Tools

Are the following sets countable or uncountable? Please prove your claims.

(a) $A \times B$, where A and B are both countable.

(b) $\bigcup_{i \in A} B_i$, where A, B_i are all countable.

(c) The set of all functions f from $\mathbb{N}$ to $\mathbb{N}$ such that f is non-decreasing. That is, $f(x) \leq f(y)$ whenever $x \leq y$.

(d) The set of all functions f from $\mathbb{N}$ to $\mathbb{N}$ such that f is non-increasing. That is, $f(x) \geq f(y)$ whenever $x \leq y$.

(e) The set of all bijective functions from $\mathbb{N}$ to $\mathbb{N}$.

3 Impossible Programs

Show whether the following programs can exist or not.

(a) A program P that takes in any program F, input x and output y and returns true if $F(x)$ outputs y and false otherwise.

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

4 Undecided?

Let us think of a computer as a machine which can be in any of n states $\{s_1, \ldots, s_n\}$. The state of a 10 bit computer might for instance be specified by a bit string of length 10, making for a total of 2^{10} states that this computer could be in at any given point in time. An algorithm $\mathscr{A}$ then is a list of k instructions $(i_0, i_2, \ldots, i_{k-1})$, where each i_l is a function of a state c that returns another state u and a number j. Executing $\mathscr{A}(x)$ means computing

$$(c_1, j_1) = i_0(x), \qquad (c_2, j_2) = i_{j_1}(c_1), \qquad (c_3, j_3) = i_{j_2}(c_2), \qquad \ldots$$

until $j_\ell \geq k$ for some ℓ, at which point the algorithm halts and returns $c_{\ell-1}$.

(a) How many iterations can an algorithm of k instructions perform on an n-state machine (at most) without repeating any computation?

(b) Show that if the algorithm is still running after $2n^2k^2$ iterations, it will loop forever.

(c) Give an algorithm that decides whether an algorithm $\mathscr{A}$ halts on input x or not. Does your contruction contradict the undecidability of the halting problem?

5 Clothing Argument

(a) There are four categories of clothings (shoes, trousers, shirts, hats) and we have ten distinct items in each category. How many distinct outfits are there if we wear one item of each category?

(b) How many outfits are there if we wanted to wear exactly two categories?

(c) How many ways do we have of hanging four of our ten hats in a row on the wall? (Order matters.)

(d) We can pack four hats for travels. How many different possibilities for packing four hats are there? Can you express this number in terms of your answer to part (c)?

(e) If we have exactly 3 red hats, 3 green hats and 4 turquoise hats, and hats of the same colour are indistinguishable, how many distinct sets of three hats can we pack?

CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Alistair Sinclair and Yun Song **HW 8**

Due:

Sundry

Before you start your homework, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Counting, Counting, and More Counting

The only way to learn counting is to practice, practice, practice, so here is your chance to do so. For this problem, you do not need to show work that justifies your answers. We encourage you to leave your answer as an expression (rather than trying to evaluate it to get a specific number).

(a) How many ways are there to arrange n 1s and k 0s into a sequence?

(b) A bridge hand is obtained by selecting 13 cards from a standard 52-card deck. The order of the cards in a bridge hand is irrelevant.
How many different 13-card bridge hands are there? How many different 13-card bridge hands are there that contain no aces? How many different 13-card bridge hands are there that contain all four aces? How many different 13-card bridge hands are there that contain exactly 6 spades?

(c) 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?

(d) How many 99-bit strings are there that contain more ones than zeros?

(e) An anagram of FLORIDA is any re-ordering of the letters of FLORIDA, i.e., any string made up of the letters F, L, O, R, I, D, and A, in any order. The anagram does not have to be an English word.
How many different anagrams of FLORIDA are there? How many different anagrams of ALASKA are there? How many different anagrams of ALABAMA are there? How many different anagrams of MONTANA are there?

(f) How many different anagrams of ABCDEF are there if: (1) C is the left neighbor of E; (2) C is on the left of E (and not necessarily E's neighbor)

(g) We have 9 balls, numbered 1 through 9, and 27 bins. How many different ways are there to distribute these 9 balls among the 27 bins? Assume the bins are distinguishable (e.g., numbered 1 through 27).

(h) We throw 9 identical balls into 7 bins. How many different ways are there to distribute these 9 balls among the 7 bins such that no bin is empty? Assume the bins are distinguishable (e.g., numbered 1 through 7).

(i) How many different ways are there to throw 9 identical balls into 27 bins? Assume the bins are distinguishable (e.g., numbered 1 through 27).

(j) 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?

(k) How many solutions does $x_0 + x_1 + \cdots + x_k = n$ have, if each x must be a non-negative integer?

(l) How many solutions does $x_0 + x_1 = n$ have, if each x must be a *strictly positive* integer?

(m) How many solutions does $x_0 + x_1 + \cdots + x_k = n$ have, if each x must be a *strictly positive* integer?

2 Binomial Beads

(a) Alistair is making school spirit keychains, which consist of a sequence of n beads on a string. He has blue beads and gold beads. How many unique keychains can he make with exactly $k \leq n$ blue beads?

(b) Alistair decides to sell his keychains! He decides on the following pricing scheme:

- Blue beads have a value of x
- Gold beads have a value of y
- The price of a keychain is the product of the values of all of its beads.

What is the price of a keychain with exactly $k \leq n$ blue beads?

(c) Alistair decides to make exactly one of every possible unique keychain. If he sells every keychain he creates, how much revenue will he make? Use parts (a) and (b), and leave your answer in summation form.

(d) Draw a connection between part (c) and the binomial theorem.

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Hint: How do you calculate the product (x + y)(x + y)?

3 Minesweeper

Minesweeper is a game that takes place on a grid of squares. When you click a square, it disappears to reveal either an integer $\in [1,8]$, a mine, or a blank space. If it reveals a mine, you instantly lose. If it reveals a number, that number refers to the number of mines adjacent to that square (including diagonally adjacent). If it reveals a blank space, there were 0 mines adjacent to it.

You are playing on a 8x8 board with 10 mines randomly distributed across the board. In your first move, you click a square near the center of the board.

(a) What is the probability that the square reveals...

i. a mine?

ii. a blank space?

iii. the number k?

(b) The first square you picked revealed the number k. For your next move, you want to minimize the probability of picking a mine. Should you pick a square adjacent to your first pick, or a different square? Your answer should depend on the value of k.

(c) Your first move resulted in the number 1. You pick the square to the right for your next move. What is the probability that this square reveals the number 4?

4 Playing Strategically

Bob, Eve and Carol bought new slingshots. Bob is not very accurate hitting his target with probability $1/3$. Eve is better, hitting her target with probability $2/3$. Carol never misses. They decide to play the following game: They take turns shooting each other. For the game to be fair, Bob starts first, then Eve and finally Carol. Any player who gets shot has to leave the game. The last person standing wins the game. What is Bob's best course of action regarding his first shot?

(a) Compute the probability of the event E_1 that Bob wins in a duel against Eve alone, assuming he shoots first.

(b) Compute the probability of the event E_2 that Bob wins in a duel against Eve alone, assuming he shoots second.

(c) Compute the probability of the same events for a duel of Bob against Carol.

(d) Assuming that both Eve and Carol play rationally, conclude that Bob's best course of action is to shoot into the air (i.e., intentionally miss)! (Hint: What happens if Bob misses? What if he doesn't?)

5 Weathermen

Tom is a weatherman in New York. On days when it snows, Tom correctly predicts the snow 70% of the time. When it doesn't snow, he correctly predicts no snow 95% of the time. In New York, it snows on 10% of all days.

(a) If Tom says that it is going to snow, what is the probability it will actually snow?

(b) What is Tom's overall accuracy?

(c) Tom's friend Jerry is a weatherman in Alaska. Jerry claims that she is a better weatherman than Tom even though her overall accuracy is lower. After looking at their records, you determine that Jerry is indeed better than Tom at predicting snow on snowy days and sun on sunny days. How is this possible?

Hint: what is the weather like in Alaska?

CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Alistair Sinclair and Yun Song — HW 9

Due: Friday, October 26, 2018 at 10 PM

Sundry

Before you start your homework, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Double-Check Your Intuition

(a) (i) Let $X \sim \text{Bin}(5, 1/4)$. Let Y be a random variable equal to $5 - X$. What are the distributions of X and Y?

(ii) Let Z be a random variable denoting the result of a die roll (so $1 \leq Z \leq 6$ uniformly at random). What is $\mathbb{E}[Z^2]$?

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 A and B are integer-valued random variables such that for every integer i, $\mathbb{P}(A = i) = \mathbb{P}(B = i)$, then is $\mathbb{P}(A = B) > 0$?

(c) If C is an integer-valued random variable, then is $\mathbb{E}[C^2] = \mathbb{E}[C]^2$?

(d) If X and Y are random variables and $\mathbb{E}[X] > 100\mathbb{E}[Y]$, then is $\mathbb{P}(X > Y) > 1/100$?

(e) If X and Y are random variables taking positive values, then is $\mathbb{E}[\frac{X}{X+Y}] = \frac{\mathbb{E}[X]}{\mathbb{E}[X+Y]}$?

(f) If A, B, C are events such that $\mathbb{P}(A \cap B \cap C) = \mathbb{P}(A)\mathbb{P}(B)\mathbb{P}(C)$, then are A, B, C mutually independent?

(g) Is an event A never independent with itself?

(h) If A and B are independent events, then are $\overline{A}$ and $\overline{B}$ independent?

2 Airport Revisited

(a) Suppose that there are n airports arranged in a circle. A plane departs from each airport, and randomly chooses an airport to its left or right to fly to. What is the expected number of empty airports after all planes have landed?

(b) Now suppose that we still have n airports, but instead of being arranged in a circle, they form a general graph, where each airport is denoted by a vertex, and an edge between two airports indicates that a flight is permitted between them. There is a plane departing from each airport and randomly chooses a neighboring destination where a flight is permitted. What is the expected number of empty airports after all planes have landed? (Express your answer in terms of $N(i)$ - the set of neighboring airports of airport i, and $\deg(i)$ - the number of neighboring airports of airport i).

3 Fizzbuzz

(a) Fizzbuzz is a classic software engineering interview question. You are given a natural number n, and for each integer i from 1 to n you have to print either "fizzbuzz" if i is divisible by 15, "fizz" if i is divisible by 3 but not 15, "buzz" if i is divisible by 5 but not 15, or the integer itself if i is not divisible by 3 or 5.

If n is a multiple of 15, then how many printed lines will contain an integer?

(Hint: If you pick a line uniformly at random, then what is the probability that the printed line contains an integer?)

(b) Recall the Euler totient function from Homework 4:

$$\phi(n) = |\{i : 1 \leq i \leq n, \texttt{gcd}(i,n) = 1\}|.$$

Suppose $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are positive integers. Prove that

$$\frac{\phi(n)}{n} = \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right)$$

4 Cliques in Random Graphs

Consider a graph $G = (V,E)$ on n vertices which is generated by the following random process: for each pair of vertices u and v, we flip a fair coin and place an (undirected) edge between u and v if and only if the coin comes up heads. So for example if $n = 2$, then with probability $1/2$, $G = (V,E)$ is the graph consisting of two vertices connected by an edge, and with probability $1/2$ it is the graph consisting of two isolated vertices.

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

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

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

Optional: Can you come up with a combinatorial proof? Of course, an algebraic proof would also get full credit.

(d) Prove that the probability that the graph contains a k-clique, for $k \geq 4\log n + 1$, is at most $1/n$. (The log is taken base 2).

Hint: Apply the union bound and part (c).

5 Balls and Bins, All Day Every Day

You throw n balls into n bins uniformly at random, where n is a positive *even* integer.

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

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

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

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

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

CS 70 Fall 2018

Discrete Mathematics and Probability Theory
Alistair Sinclair and Yun Song

HW 10

Due: Monday, November 5, 2018 at 10 PM

Sundry

Before you start your homework, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Family Planning

Mr. and Mrs. Brown decide to continue having children until they either have their first girl or until they have three children. Assume that each child is equally likely to be a boy or a girl, independent of all other children, and that there are no multiple births. Let G denote the numbers of girls that the Browns have. Let C be the total number of children they have.

(a) Determine the sample space, along with the probability of each sample point.

(b) Compute the joint distribution of G and C. Fill in the table below.

	$C=1$	$C=2$	$C=3$
$G=0$			
$G=1$			

(c) Use the joint distribution to compute the marginal distributions of G and C and confirm that the values are as you'd expect. Fill in the tables below.

$\mathbb{P}(G=0)$	
$\mathbb{P}(G=1)$	

$\mathbb{P}(C=1)$	$\mathbb{P}(C=2)$	$\mathbb{P}(C=3)$

(d) Are G and C independent?

(e) What is the expected number of girls the Browns will have? What is the expected number of children that the Browns will have?

2 Will I Get My Package?

A delivery guy in some company is out delivering n packages to n customers, where $n \in \mathbb{N}$, $n > 1$. Not only does he hand a random package to each customer, he opens the package before delivering it with probability $1/2$. Let X be the number of customers who receive their own packages unopened.

(a) Compute the expectation $\mathbb{E}(X)$.

(b) Compute the variance $\text{var}(X)$.

3 Double-Check Your Intuition Again

(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 $\text{var}(X+Y) = \text{var}(X) + \text{var}(Y)$?

(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

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

CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Alistair Sinclair and Yun Song **HW 11**

Due: Friday, November 9, 2018 at 10 PM

Sundry

Before you start your homework, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Random Cuckoo Hashing

Cuckoo birds are parasitic beasts. They are known for hijacking the nests of other bird species and evicting the eggs already inside. Cuckoo hashing is inspired by this behavior. In cuckoo hashing, when we get a collision, the element that was already there gets evicted and rehashed.

We study a simple (but ineffective, as we'll see) version of cuckoo hashing, where all hashes are random. Let's say we want to hash n pieces of data $D_1, D_2, \dots, D_n$ into n possible hash buckets labeled $1, \dots, n$. We hash the $D_1, \dots, D_n$ in that order. When hashing D_i, we assign it a random bucket chosen uniformly from $1, \dots, n$. If there is no collision, then we place D_i into that bucket. If there is a collision with some other D_j, we evict D_j and assign it another random bucket uniformly from $1, \dots, n$. (It is possible that D_j gets assigned back to the bucket it was just evicted from!) We again perform the eviction step if we get another collision. We keep doing this until there is no more collision, and we then introduce the next piece of data, D_{i+1} to the hash table.

(a) What is the probability that there are no collisions over the entire process of hashing $D_1, \dots, D_n$ to buckets $1, \dots, n$? What value does the probability tend towards as n grows very large?

(b) Assume we have already hashed $D_1, \dots, D_{n-1}$, and they each occupy their own bucket. We now introduce D_n into our hash table. What is the expected number of collisions that we'll see while hashing D_n? (*Hint*: What happens when we hash D_n and get a collision, so we evict some other D_i and have to hash D_i? Are we at a situation that we've seen before?)

2 Markov's Inequality and Chebyshev's Inequality

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

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

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

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

(d) $\mathbb{P}[X \geq 6] \leq 9/32$.

3 Easy A's

A friend tells you about a course called "Laziness in Modern Society" that requires almost no work. You hope to take this course next semester to give yourself a well-deserved break after working hard in CS 70. At the first lecture, the professor announces that grades will depend only on two homework assignments. Homework 1 will consist of three questions, each worth 10 points, and Homework 2 will consist of four questions, also each worth 10 points. He will give an A to any student who gets at least 60 of the possible 70 points.

However, speaking with the professor in office hours you hear some very disturbing news. He tells you that, in the spirit of the class, the GSIs are very lazy, and to save time the grading will be done as follows. For each student's Homework 1, the GSIs will choose an integer randomly from a distribution with mean $\mu = 5$ and variance $\sigma^2 = 1$. They'll mark each of the three questions with that score. To grade Homework 2, they'll again choose a random number from the same distribution, independently of the first number, and will mark all four questions with that score.

If you take the class, what will the mean and variance of your total class score be? Use Chebyshev's inequality to conclude that you have less than a 5% chance of getting an A when the grades are randomly chosen this way.

4 Confidence Interval Introduction

We observe a random variable X which has mean μ and standard deviation $\sigma \in (0, \infty)$. Assume that the mean μ is unknown, but σ is known.

We would like to give a 95% confidence interval for the unknown mean μ. In other words, we want to give a random interval (a, b) (it is random because it depends on the random observation X) such that the probability that μ lies in (a, b) is at least 95%.

We will use a confidence interval of the form $(X - \varepsilon, X + \varepsilon)$, where $\varepsilon > 0$ is the width of the confidence interval. When ε is smaller, it means that the confidence interval is narrower, i.e., we are giving a more *precise* estimate of μ.

(a) Using Chebyshev's Inequality, calculate an upper bound on $\mathbb{P}\{|X-\mu| \geq \varepsilon\}$.

(b) Explain why $\mathbb{P}\{|X-\mu| < \varepsilon\}$ is the same as $\mathbb{P}\{\mu \in (X-\varepsilon, X+\varepsilon)\}$.

(c) Using the previous two parts, choose the width of the confidence interval ε to be large enough so that $\mathbb{P}\{\mu \in (X-\varepsilon, X+\varepsilon)\}$ is guaranteed to exceed 95%.

[Note: Your confidence interval is allowed to depend on X, which is observed, and σ, which is known. Your confidence interval is not allowed to depend on μ, which is unknown.]

(d) The previous three parts dealt with the case when you observe one sample X. Now, let n be a positive integer and let $X_1, \dots, X_n$ be i.i.d. samples, each with mean μ and standard deviation $\sigma \in (0, \infty)$. As before, assume that μ is unknown but σ is known.

Here, a good estimator for μ is the *sample mean* $\bar{X} := n^{-1} \sum_{i=1}^{n} X_i$. Calculate the mean and variance of $\bar{X}$.

(e) We will now use a confidence interval of the form $(\bar{X}-\varepsilon, \bar{X}+\varepsilon)$ where $\varepsilon > 0$ again represents the width of the confidence interval. Imitate the steps of (a) through (c) to choose the width ε to be large enough so that $\mathbb{P}\{\mu \in (\bar{X}-\varepsilon, \bar{X}+\varepsilon)\}$ is guaranteed to exceed 95%.

To check your answer, your confidence interval should be *smaller* when n is larger. Intuitively, if you collect more samples, then you should be able to give a more *precise* estimate of μ.

CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Course Notes **HW 12**

Due:

Sundry

Before you start your homework, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Safeway Monopoly Cards

It's that time of the year again - Safeway is offering its Monopoly Card promotion. Each time you visit Safeway, you are given one of n different Monopoly Cards with equal probability. You need to collect them all to redeem the grand prize.

Let X be the number of visits you have to make before you can redeem the grand prize. Show that $\mathrm{var}(X) = n^2 \left(\sum_{i=1}^{n} i^{-2}\right) - \mathbb{E}(X)$. *[Hint: Does this remind you of a particular problem? What is the expectation for this problem?]*

2 Geometric Distribution

Two faulty machines, M_1 and M_2, are repeatedly run synchronously in parallel (i.e., both machines execute one run, then both execute a second run, and so on). On each run, M_1 fails with probability p_1 and M_2 fails with probability p_2, all failure events being independent. Let the random variables X_1, X_2 denote the number of runs until the first failure of M_1, M_2 respectively; thus X_1, X_2 have geometric distributions with parameters p_1, p_2 respectively. Let X denote the number of runs until the first failure of *either* machine.

(a) Show that X also has a geometric distribution, with parameter $p_1 + p_2 - p_1 p_2$.

(b) Now, two technicians are hired to check on the machines every run. They decide to take turns checking on the machines every hour. What is the probability that the first technician is the first one to find a faulty machine?

3 Geometric and Poisson

Let X be geometric with parameter p, Y be Poisson with parameter λ, and $Z = \max(X,Y)$. Assume X and Y are independent. For each of the following parts, your final answers should not have summations.

(a) Compute $P(X > Y)$.

(b) Compute $P(Z \geq X)$.

(c) Compute $P(Z \leq Y)$.

4 Darts

Alvin is playing darts. His aim follows an exponential distribution; that is, the probability density that the dart is x distance from the center is $f_X(x) = \exp(-x)$. The board's radius is 4 units.

(a) What is the probability the dart will stay within the board?

(b) Say you know Alvin made it on the board. What is the probability he is within 1 unit from the center?

(c) If Alvin is within 1 unit from the center, he scores 4 points, if he is within 2 units, he scores 3, etc. In other words, Alvin scores $\lfloor 5-x \rfloor$, where x is the distance from the center. What is Alvin's expected score after one throw?

5 Exponential Practice

(a) Let $X_1, X_2 \sim \text{Exponential}(\lambda)$ be independent, $\lambda > 0$. Calculate the density of $Y := X_1 + X_2$. [*Hint*: One way to approach this problem would be to compute the CDF of Y and then differentiate the CDF.]

(b) Let $t > 0$. What is the density of X_1, conditioned on $X_1 + X_2 = t$? [*Hint*: Once again, it may be helpful to consider the CDF $\mathbb{P}(X_1 \leq x \mid X_1 + X_2 = t)$. To tackle the conditioning part, try conditioning instead on the event $\{X_1 + X_2 \in [t, t+\varepsilon]\}$, where $\varepsilon > 0$ is small.]

6 Uniform Means

Let $X_1, X_2, \ldots, X_n$ be n independent and identically distributed uniform random variables on the interval $[0,1]$ (where n is a positive integer).

(a) Let $Y = \min\{X_1, X_2, \ldots, X_n\}$. Find $\mathbb{E}(Y)$. [*Hint*: Use the tail sum formula, which says the expected value of a nonnegative random variable is $\mathbb{E}(X) = \int_0^\infty \mathbb{P}(X > x)\,\mathrm{d}x$. Note that we can use the tail sum formula since $Y \geq 0$.]

(b) Let $Z = \max\{X_1, X_2, \ldots, X_n\}$. Find $\mathbb{E}(Z)$. [*Hint*: Find the CDF.]

CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Course Notes **HW 13**

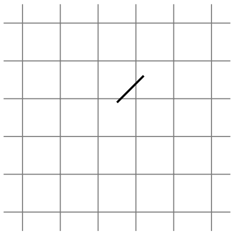
Due: Friday, November 30, 2018 at 10PM

Sundry

Before you start your homework, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Buffon's Needle on a Grid

In this problem, we will consider Buffon's Needle, but with a catch. We now drop a needle at random onto a large grid, and example of which is shown below.



The length of the needle is 1, and the space between the grid lines is 1 as well.

Recall from class that a random throw means that the position of the center of the needle and its orientation are independent and uniformly distributed.

(a) Given that the angle between the needle and the horizontal lines is θ, what is the probability that the needle does not intersect any grid lines? Justify your answer.

(b) Continue part (a) to find the probability that the needle, when dropped onto the grid at random (with the angle chosen uniformly at random), intersects a grid line. Justify your answer.

Hint: You may use the fact that $\sin\theta\cos\theta = \frac{1}{2}\sin(2\theta)$ without proof.

(c) Let X be the number of times the needle intersects a gridline (so, in the example shown above, $X = 2$). Find $\mathbb{E}[X]$. Justify your answer.

Hint: Can you do this without using your answer from part (b)?

(d) Combine the previous parts to figure out the probability that $X = 1$, i.e. the needle will only intersects one gridline. Justify your answer.

(e) We will fold the needle into an equilateral triangle, where each side is length $\frac{1}{3}$. What is the expected number of intersections that this triangle will have with the gridlines, when dropped onto the grid? Justify your answer.

2 Variance of the Minimum of Uniform Random Variables

Let n be a positive integer and let $X_1, \dots, X_n \overset{\text{i.i.d.}}{\sim} \text{Uniform}[0,1]$. Find $\operatorname{var} Y$, where

$$Y := \min\{X_1, \dots, X_n\}.$$

Hint: You may need to perform integration by parts.

3 Erasures, Bounds, and Probabilities

Alice is sending 1000 bits to Bob. The probability that a bit gets erased is p, and the erasure of each bit is independent of the others.

Alice is using a scheme that can tolerate up to one-fifth of the bits being erased. That is, as long as Bob receives at least 801 of the 1000 bits correctly, he can decode Alice's message.

In other words, Bob becomes unable to decode Alice's message only if 200 or more bits are erased. We call this a "communication breakdown", and we want the probability of a communication breakdown to be at most 10^{-6}.

1. Use Markov's inequality to upper bound p such that the probability of a communications breakdown is at most 10^{-6}.
2. Use Chebyshev's inequality to upper bound p such that the probability of a communications breakdown is at most 10^{-6}.
3. As the CLT would suggest, approximate the fraction of erasures by a Gaussian random variable (with suitable mean and variance). Use this to find an approximate bound for p such that the probability of a communications breakdown is at most 10^{-6}.

4 Sampling a Gaussian With Uniform

In this question, we will see one way to generate a normal random variable if we have access to a random number generator that outputs numbers between 0 and 1 uniformly at random.

As a general comment, remember that showing two random variables have the same CDF or PDF is sufficient for showing that they have the same distribution.

(a) First, let us see how to generate an exponential random variable with a uniform random variable. Let $U_1 \sim Uniform(0,1)$. Prove that $-\ln U_1 \sim Expo(1)$.

(b) Let $N_1, N_2 \sim \mathscr{N}(0,1)$, where N_1 and N_2 are independent. Prove that $N_1^2 + N_2^2 \sim Expo(1/2)$.

Hint: You may use the fact that over a region R, if we convert to polar coordinates $(x,y) \to (r,\theta)$, then the double integral over the region R will be

$$\iint_R f(x,y)\,dx\,dy = \iint_R f(r\cos\theta, r\sin\theta)\cdot r\,dr\,d\theta.$$

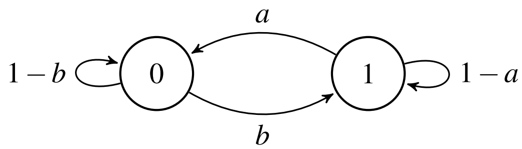
(c) Suppose we have two uniform random variables, U_1 and U_2. How would you transform these two random variables into a normal random variable with mean 0 and variance 1?

Hint: What part (b) tells us is that the point (N_1, N_2) will have a distance from the origin that is distributed as the square root of an exponential distribution. Try to use U_1 to sample the radius, and then use U_2 to sample the angle.

5 Markov Chain Terminology

In this question, we will walk you through terms related to Markov chains.

1. (Irreducibility) A Markov chain is irreducible if, starting from any state i, the chain can transition to any other state j, possibly in multiple steps.
2. (Periodicity) $d(i) := \gcd\{n > 0 \mid P^n(i,i) = \mathbb{P}[X_n = i \mid X_0 = i] > 0\}$, $i \in \mathscr{X}$. If $d(i) = 1\ \forall i \in \mathscr{X}$, then the Markov chain is aperiodic; otherwise it is periodic.
3. (Matrix Representation) Define the transition probability matrix P by filling entry (i,j) with probability $P(i,j)$.
4. (Invariance) A distribution π is invariant for the transition probability matrix P if it satisfies the following balance equations: $\pi = \pi P$.



(a) For what values of a and b is the above Markov chain irreducible? Reducible?

(b) For $a = 1$, $b = 1$, prove that the above Markov chain is periodic.

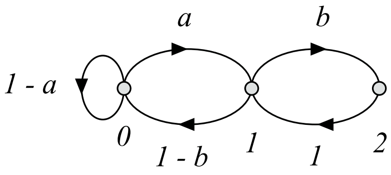
(c) For $0 < a < 1$, $0 < b < 1$, prove that the above Markov chain is aperiodic.

(d) Construct a transition probability matrix using the above Markov chain.

(e) Write down the balance equations for this Markov chain and solve them. Assume that the Markov chain is irreducible.

6 Analyze a Markov Chain

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



(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;

(d) Let $T_i = \min\{n \geq 0 \mid X(n)=i\}$, T_i is the number of steps until we transit to state i for the first time. Calculate $\mathbb{E}[T_2 \mid X(0)=1]$.

7 Boba in a Straw

Imagine that Jonathan is drinking milk tea and he has a very short straw: it has enough room to fit two boba (see figure).

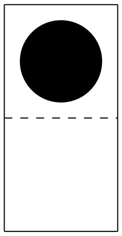


Figure 1: A straw with one boba currently inside. The straw only has enough room to fit two boba.

Here is a formal description of the drinking process: We model the straw as having two "components" (the top component and the bottom component). At any given time, a component can contain nothing, or one boba. As Jonathan drinks from the straw, the following happens every second:

1. The contents of the top component enter Jonathan's mouth.

2. The contents of the bottom component move to the top component.

3. With probability p, a new boba enters the bottom component; otherwise the bottom component is now empty.

Help Jonathan evaluate the consequences of his incessant drinking!

(a) At the very start, the straw starts off completely empty. What is the expected number of seconds that elapse before the straw is completely filled with boba for the first time? [Write down the equations; you do not have to solve them.]

(b) Consider a slight variant of the previous part: now the straw is narrower at the bottom than at the top. This affects the drinking speed: if either (i) a new boba is about to enter the bottom component or (ii) a boba from the bottom component is about to move to the top component, then the action takes two seconds. If both (i) and (ii) are about to happen, then the action takes three seconds. Otherwise, the action takes one second. Under these conditions, answer the previous part again. [Write down the equations; you do not have to solve them.]

(c) Jonathan was annoyed by the straw so he bought a fresh new straw (the straw is no longer narrow at the bottom). What is the long-run average rate of Jonathan's calorie consumption? (Each boba is roughly 10 calories.)

(d) What is the long-run average number of boba which can be found inside the straw? [Maybe you should first think about the long-run distribution of the number of boba.]