1 T/F

(3 points each) Circle T for True or F for False. We will only grade the answers, and are unlikely to even look at any justifications or explanations.

(a) T F $\forall x(P(x) \vee Q(x))$ is equivalent to $(\forall x, P(x)) \vee (\forall x, Q(x))$.

False. For instance, let $P(x)$ be "x is nonegative" and $Q(x)$ be "x is positive."

(b) T F $\forall x(P(x) \wedge Q(x))$ is equivalent to $(\forall x, P(x)) \wedge (\forall x, Q(x))$.

True. If $P \wedge Q$ holds for all x, then clearly P must hold for all x, and so must Q.

(c) T F If $b \equiv c \pmod{d}$, then $a^b \equiv a^c \pmod{d}$.

False. $1 \equiv 6 \pmod{5}$, but $2^1 = 2 \equiv 2 \pmod{5}$ and $2^6 = 64 \equiv 4 \pmod{5}$.

(d) T F The multiplicative inverse of 3 modulo 5 is 2.

True. $3 * 2 = 6 \equiv 1 \pmod{5}$.

(e) T F It is safe to send the number 1 using the RSA protocol.

False. 1 just encrypts to 1 no matter what your key is. This is why people use padding (adding extra bits) in actual applications.

(f) T F If events A and B are independent then $Pr[A|B] = Pr[A]$.

True, immediately from definition.

(g) T F It is always the case that $Pr[A \cup B] \leq Pr[A] + Pr[B]$

True. Union bound.

(h) T F The set of all polynomials over prime fields is countable.

True. Any polynomial over a finite field can be represented as a finite string. Another way too go about proving this is to do a spiral enumeration, similar to what we did to prove that pairs of integers are countable. At coordinate (i, j), enumerate all the polynomials of degree i in $GF(j)$ if j is a prime, and don't enumerate anything if j isn't.

(i) T F It is possible to write a program that takes a program P and a string x as input and correctly returns either "P(x) definitely halts" or "P(x) may or may not loop infinitely".

True. A very simple way to do this is to always return "P(x) may or may not loop infinitely".

(j) T F Let A, B and C be 3 events. Suppose that $\Pr[B|A] = \Pr[C|A]$, and that $Pr[B] < Pr[C]$. Then the probability that A happens (given that we observe B) is greater than the probability that A happens (given that we observe C).

False. A,B and C can be disjoint.

(k) T F In all stable matching problems, there are at most two stable matchings: the male optimal and the female optimal.

False. Heres' a simple example: consider a case with two men and two women with two unique stable pairings (M1 likes W1 best, M2 likes W2 best, but W2 likes M1 best and W1 likes M2 best).

Make two instances of this and put them together in a way that the men from each instance all have the women from the other instance at the bottom of their preference lists, and vice versa.

There are four stable pairings here.

(l) T F The probability $\frac{1}{k}$ of being k times away from the expectation, given by Markov's inequality, is never tight. In other words, there is no random variable X, such that $Pr[X \geq a] = \frac{E[X]}{a}$.

False. See MT2.

(m) T F I have a coin with unknown probability p of coming up H. I flip it 100 times, and get H 50 times. If I flip the coin 1000 times, the expected number of H is 500.

False. The coin is never guaranteed to come up with some number of heads.

2 Short Answers

(a) **(4 points)** A student retakes classes until they get a good grade, and ceases to take a class once a good grade in that class is attained. The probability that they get a good grade in class A is $\frac{1}{2}$. The probability that they get a good grade in class B is $\frac{3}{4}$. The probability that they get a good grade in class C with probability $\frac{4}{5}$. How many classes should they expect to take?
Considering sum of the expectations of geometric random variables we get: $2 + \frac{4}{3} + \frac{5}{4}$.

(b) **(4 points)** I have a pile of six pens, four highlighters, ten pencils, and five styluses. I pick five at random from the pile. What is the probability that I end up with at least one of each kind of writing implement?

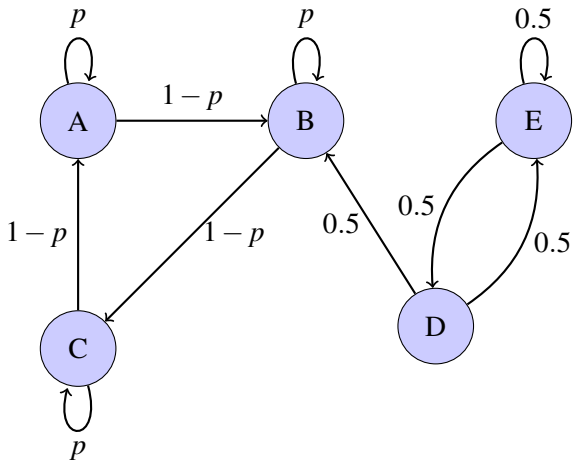
$$\frac{\frac{6*4*5*10*(25-4)}{2}}{\binom{25}{5}}$$

(c) **(4 points)** What is the last digit of 2016^{70}?
6. This is because every number that ends in 6 when multiplied by 6 has a last digit of 6.

(d) **(4 points)** Calculate $12^{136} \pmod 7$. 2. Through the multiplication property of modular arithmetic, we have that $12^{136} = 5^{136} \pmod 7$. An application of Fermat's Little Theorem yields $5^{136} = 5^{6(22)+4} = 5^4 \pmod 7$. Then we can use exponentiation by squaring to get $5^4 = 25^2 = 4^2 = 2 \pmod 7$.

(e) **(4 points)** Compute $\gcd(512, 480)$. $32 = 512 \pmod{480}$. $0 = 480 \pmod{32}$. $gcd(512,480) = gcd(480,32) = gcd(32,0) = 32$.

(f) **(4 points)** Find a stationary distribution of the following Markov Chain $(1 > p > 0)$:



$(1/3,1/3,1/3,0,0)$

(g) **(4 points)** Let $G=(V,E)$ be an undirected graph with $V=\{0,\ldots,6\}$ and $E=\{(i,i+1 \pmod 7)\}\cup\{(i,j):ij=1 \pmod 7, i\neq j\}$. There are no self-loops. How many edges does the graph have? It's a cycle with 7 vertices, plus all $(i,j):ij=1 \pmod 7$, so 7 plus 2 (from 3,5 and 2,4) edges.

(h) **(4 points)** You and 6 friends have a bag of 7 distinct chocolates. You have a favorite chocolate. Everyone takes turns and picks a chocolate at random, but unfortunately you pick last. What is the probability that you pick your favorite chocolate? $\frac{1}{7}$, by symmetry

(i) **(4 points)** You have a coin that has probability of coming up heads $p=Pr[H]=0.35$. You flip the coin 100 times. Use CLT to get an estimate of the probability that the number of heads is more than the number of tails. You can approximate $\sqrt{0.35\cdot 0.65}$ by 0.5. You can also use the $68-95-99.7$ rule. Evaluate to a number. Let X be the number of H. Then, $\frac{X-100p}{10\sqrt{p(1-p)}}\approx N(0,1)$.

$$Pr[X>50]=Pr\left[\frac{X-100p}{10\sqrt{p(1-p)}}>\frac{50-100p}{10\sqrt{p(1-p)}}\right]$$

$100p=35$. $\sqrt{p(1-p)}=\sqrt{0.35*0.65}\approx 0.5$. Therefore, $\frac{50-100p}{10\sqrt{p(1-p)}}\approx\frac{50-35}{100.5}=\frac{15}{5}=3$. The probability that a $N(0,1)$ takes value bigger than 3 is approximately $\frac{1-0.997}{2}=\frac{0.003}{2}=0.0015$.

(j) **(4 points)** Suppose Alex and Grace are using Blum's coin toss scheme. Alex sends Grace $n=pq$, the product of two primes each congruent to 3 mod 4 as in the normal protocol. Grace is feeling lazy that day and, instead of choosing an x and sending back $a=x^2$, just picks random a directly. Luckily for her, a is indeed a perfect square, although she doesn't know what its square root is. Who wins the coin toss, and why?Alex wins, because Grace has even less information in this case than she does in the losing case of the normal Blum protocol. Instead of having one square root she has zero! (remember that she needs two to win).

In the case that Grace's number is not relatively prime to n, she can "win" by cheating at the scheme and calling GCD to factor n, but the chances of this are extremely unlikely (see Question 8).

(k) **(6 points)** Prove or disprove: The variance of a random variable that only attains nonnegative values cannot exceed the expectation of the random variable.
F - A long tail distribution will disprove the following statement. In particular we can consider a

geometric distribution.
It is sufficient to show that there exists a $p \in [0,1]$ such that $\frac{1-p}{p^2} > \frac{1}{p}$:

$$\frac{1-p}{p^2} > \frac{1}{p} \iff \frac{p-p^2}{p^2} > 1 \iff \frac{1}{p} - 1 > 1 \iff \frac{1}{p} > 2 \iff p > \frac{1}{2}$$

Thus choosing a geometric distribution with $p > 1/2$ we disprove the above claim.

3 Short proofs

(a) **(4 points)** Prove that if n^2+2 and n^2-2 are prime, for some natural number n, then n is divisible by 3. Proof by contraposition. If n is not divisible by 3, then n can be represented as $n \neq 0 \pmod 3$. We split all of our possible n into cases where $n = 1 \pmod 3$ and $n = 2 \pmod 3$. In the case where $n = 1 \pmod 3$, $n^2+2 = 1^2+2 = 3 = 0 \pmod 3$. n^2+2 is a multiple of 3 and thus, not a prime. In the second case where $n = 2 \pmod 3$, $n^2+2 = 2^2+2 = 6 = 0 \pmod 3$. n^2+2 is a multiple of 3 and thus, not a prime. Therefore, our original claim is proven true.

(b) **(4 points)** Prove that $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$, for all $n \in \mathbb{N}$. Proof by induction on n. For the base case let $n = 1$ where $\frac{1}{1\cdot 2} = \frac{1}{2} = \frac{1}{1+1}$. Suppose for induction that $n = k$,

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{k(k+1)} = \frac{k}{k+1}$$

It suffices to show that our claim hold for $n = k+1$. An application of our hypothesis reveals

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{k(k+1)} + \frac{1}{k+1(k+2)} = \frac{k}{k+1} + \frac{1}{k+1(k+2)}$$

$$= \frac{k(k+2)+1}{(k+1)(k+2)} = \frac{(k+1)(k+1)}{(k+1)(k+2)} = \frac{k+1}{k+2}$$

which proves our claim.

(c) **(4 points)** A connected graph G is k-edge-connected, if the minimum number of edge removals necessary to make it disconnected is k. For example, trees are 1-connected, since any edge removal disconnects them.

Prove or disprove: There exists a 6-edge-connected planar graph. The minimum degree is 6, and therefore it's not planar, since we know that every planar graph has a vertex of at least degree 5.

(d) **(4 points)** Prove that if you put n items in $k < n$ boxes, there is a box with at least (inclusive) $\lceil \frac{n}{k} \rceil$ number of items. Recall that $\lceil x \rceil$ is the smallest number $y \geq x$, such that $y \in \mathbb{Z}$. For example, $\lceil 1.9 \rceil = 2$, and $\lceil 3 \rceil = 3$.Assume this is not the case. Then, every box has at most $\lceil \frac{n}{k} \rceil - 1$ items. Therefore, the total number of items is $\left(\lceil \frac{n}{k} \rceil - 1\right) k < \frac{n}{k} k = n$, a contradiction.

(e) **(4 points)** Let $a, b \in \mathbb{N}$, and let k be the smallest positive integer such that $a^k = 1 \pmod b$. Prove that if $a^n = 1 \pmod b$ then k divides n. Suppose that this is not the case. Then $n = kq + r$, for $0 < r < k$. Then

$$1 = a^n = a^{kq} a^r = (a^k)^q a^r = 1^q a^r = a^r \pmod b,$$

a contradiction, since k is the smallest positive integer such that $a^k = 1 \pmod b$

(f) **(4 points)** Prove that if Alex sends a message m_a to Fan, encrypted with Fan's (public) RSA key, Grace can send another message $m_d = qm_a$ for some q of her choice, without knowing either m_a or Fan's private key, assuming she knows the (encrypted) ciphertext that Alex sent to Fan. Alex sends $m_a^e \bmod pq$, so Grace can send the encryted message $q^e m_a^e \equiv (qm_a)^e \equiv m_d^e \bmod pq$

(g) **(4 points)** Prove **combinatorially** that for $n > 2$:

$$(n-2)! \sum_{i=1}^{n-1} i = \frac{n!}{2} \ .$$

Hint: How many ordered permutations of $\{1,2,3,...,n\}$ *are there such that* 1 *occurs earlier than* 2*?*

Start from the hint: How many ordered permutations of $\{1,2,3,...,n\}$ are there such that 1 occurs earlier than 2?

Answer 1: $n!/2$ because there are $n!$ permutations, and exactly half of them have 1 occurring before 2 (for every permutation with 1 occurring before 2, we can exchange their positions to get a permutation with 2 before 1.)

Answer 2: If 1 in the first place, then there are $n-1$ options for 2. If 1 is in the second place, $n-2$ options for 2, and so on. That means that there are $1+2+...+(n-1)$ ways to place 1 and 2 both.

Once we have placed 1 and 2, there are $(n-2)!$ ways to place the remainder. Therefore, the total number of permutations with 1 before 2 is $(n-2)!\sum_{i=1}^{n-1} i$.

4 Random graphs

Define $G_{n,p}$ as a *random graph* with $n \geq 5$ vertices, where a pair of distinct vertices (u,v) forms an edge independently with probability p (there are no self-loops).

(a) **(5 points)** What is the probability that the path $u_1 \to u_2 \to \cdots \to u_n$ exists? $(p)^{n-1}$

(b) **(5 points)** In terms of n, p, what is the expected number of times K_5 (the complete graph of size 5) appears in $G_{n,p}$ as a subgraph? Note that K_5 appears 6 times in a K_6. The probability that a fixed set of 5 vertices form a K_5 is $p^{4+3+2+1} = p^{10}$. Let X_i be an indicator for the event that a certain group of 5 vertices form a K_5. There are $\binom{n}{5}$ such groups, and X_i takes value 1 w.p. p^{10}. $E[\text{number of cliques}] = E[\sum X_i] = \sum_i E[X_i] = \binom{n}{5} p^{10}$.

(c) **(5 points)** Fix a vertex v. The degree of v is a random variable. In terms of n, p, what is the expected degree of v? $(n-1)p$

(d) **(5 points)** What is the probability that the degree of v is equal to k? $\binom{n-1}{k} p^k (1-p)^{n-k-1}$

(e) **(5 points)** What is the variance of the degree of v? $(n-1)p(1-p)$. It's a binomial distribution.

5 Magic Box

(20 points) For your birthday you get a magic box. The box works as follows: you ask a yes or no question, and the box replies with a "YES" or a "NO". The box says the correct answer with probability $\frac{2}{3}$. The probability that the box makes a mistake is independent of all the past and previous mistakes.

You decide to use this box to figure out whether P is equal to NP. You devise the following algorithm: You'll ask the box n times whether or not P is equal to NP. The box will answer "YES" some number of times x, and "NO" some number of times y. If $x \geq y$ you'll conclude that P equal NP, otherwise you'll conclude that P does not equal NP.

Prove that you'll arrive at the correct conclusion with probability exponentially (in n) close to 1. This means that the probability of coming to the correct conclusion is at least $1 - c^n$, for some $c < 1$.

You can assume that $e^{-\frac{1}{k}} < 1$, for all $k > 0$.

Let X_i be a random variable that takes value 1 if the box is correct (i.e. with probability $2/3$) and 0 otherwise.

We want to bound the probability of being wrong, i.e. the event that $\sum X_i \leq \frac{n}{2}$. Clearly, $E[\sum X_i] = \frac{2n}{3}$. By Chernoff bounds we have

$$Pr[\sum X_i \leq (1-\delta)\mu] \leq e^{-\frac{\delta^2\mu}{2}}$$

Setting $\delta = \frac{1}{4}$, and $\mu = \frac{2n}{3}$ we get

$$Pr[\sum X_i \leq \frac{n}{2}] \leq e^{-\frac{\frac{1}{16}\frac{2n}{3}}{2}} = e^{-\frac{1}{48}n}$$

Therefore, the probability of being correct is at least $1 - c^n$, where $c = e^{-\frac{1}{48}}$.

6 Magikarps Can't Keep Secrets

(20 points) Suppose a trainer has 100 Pokemon and wants to share a secret with them. He knows that exactly 10 of the Pokemon are Magikarps (but doesn't know which ones are Magikarps).

Magikarps aren't the best at remembering things. When asked for the secrets that they were given, they'll just give an arbitrary number instead of the actual secret that they were entrusted with.

Pokemon who are not Magikarps will honestly give the numbers that they were entrusted with by the trainer.

The trainer wants a scheme with the following properties:

- Any group of 40 Pokemon can reveal the secret if they carry out the protocol correctly, even if some of them are Magikarps and reveal incorrect numbers.
- Anyone who obtains the correct secrets of all 10 Magikarps will not be able to recover any information about the secret.
- Any group of less than 40 Pokemon who get together cannot recover the secret, as long as nobody in the group knows who the Magikarps are.

Devise an efficient protocol (no brute forcing) that follows these constraints, and justify why it works. Essentially it's Shamir's secret sharing scheme plus decoding from BW. Find some polynomial of degree 19 in some Galois field greater than 100. Encode the secret S as $P(0) = S$ and give the ith Pokemon the point $(i, P(i))$. Now if you have 40 pokemon getting together, you have 40 points, and among those points at most 10 are corrupted, so you can recover the polynomial using the Berlekamp Welch ECC procedure. If you have all the 10 Magikarps providing the correct information, you only have 10 points and would not be able to recover the degree 19 polynomial. We can have at most 10 corrupted points, so we need to get 40 points to recover the degree 19 polynomial. If we get less than 40 points, it is not guaranteed that we can recover the polynomial.

7 Error Correction (with Codes, not Erasers)

Alice sends a message to Bob over a channel that corrupts $k = 2$ numbers. Alice computes a polynomial P and sends a number of points x, $P(0), P(1), \ldots, P(x-1)$, to Bob. Bob applies the Berlekamp-Welch algorithm to the message he receives and correctly recovers the message that Alice sent. The message is $(2,0,0)$. Everything is $GF(11)$.

If you get an incorrect answer for (a), you can still get full credit for (b) and (c) if your math for those parts is correct.

(a) **(10 points)** What are the points Alice sent? We're looking for a degree 2 polynomial that goes through points $(0,2)$, $(1,0)$, and $(2,0)$.

$$D_0(x) = \frac{(x-1)(x-2)}{(-1)(-2)} = \frac{(x-1)(x-2)}{2}$$

$$D_1(x) = \frac{(x-0)(x-2)}{(1-0)(1-2)} = -x(x-2)$$

$$D_2(x) = \frac{(x-0)(x-1)}{(2-0)(2-1)} = \frac{x(x-1)}{2}$$

$$P(x) = 2D_0(x) + 0D_1(x) + 0D_2(x) = (x-1)(x-2)$$

Alice will send $x = n + 2k = 3 + 4 = 7$ points. We can easily find: $P(0) = 2$, $P(1) = 0$, $P(2) = 0$, $P(3) = 2 \cdot 1 = 2$, $P(4) = 3 \cdot 2 = 6$, $P(5) = 4 \cdot 3 = 12 = 1 \pmod{11}$, $P(6) = 5 \cdot 4 = 20 = 9 \pmod{11}$,

She sent: $(2,0,0,2,6,1,9)$

(b) **(10 points)** What is the probability that Bob received message $(2,0,0,2,1,3,0)$? You may assume that the channel picks 2 packets at random and corrupts them to a random number in $GF(11)$. The new number could be the same as the old one. For example, if Alice sent $(1,2,3)$, the channel could pick 1 and 3 and change 1 to 5 and 3 to 3, and thus Bob receives $(5,2,3)$. 0. That would require 3 corruptions, since 3 packets are different.

(c) **(10 points)** What is the probability that Bob received message $(2,0,0,2,6,1,9)$? Let A be the event that no packets change, and B_i the event that the channel picked the i-th pair of packets.

Then $Pr[A] = \sum_{i=1}^{\binom{7}{2}} Pr[A|B_i]Pr[B_i]$.

Given that packets x and y were picked by the channel, the probability that they remain unchanged is $\frac{1}{11^2}$. The probability that the channel picked packets x and y is $\frac{1}{\binom{7}{2}}$.

Therefore, $Pr[A] = \frac{1}{11^2}$.

8 Special, General, and... Primal Relativity?

(22 points) Let p and q be distinct prime numbers. Show that if you pick a number x uniformly at random between 0 and $pq-1$ (inclusive), then the probability that x is relatively prime to pq is $\frac{(p-1)(q-1)}{pq}$. *Hint: Use the Chinese remainder theorem.* There are $p-1$ numbers in $\mathbb{Z}_p$ that are relatively prime to p and there are

$q-1$ numbers in $\mathbb{Z}_q$ relatively prime to q. Any number that is relatively prime to pq must be congruent to some $j \not\equiv 0 \pmod{p}$ and also congruent to some $k \not\equiv 0 \pmod{q}$; each such congruence has a single solution mod pq by the Chinese remainder theorem. Therefore, since there are $p-1$ possible values of j and $q-1$ possible values of k, there are $(p-1)(q-1)$ numbers in $\mathbb{Z}_{pq}$ relatively prime to pq.

Therefore, the chance of picking a number x that is relatively prime to pq is $\frac{(p-1)(q-1)}{pq}$.

Alternate Solution: Total number of ways to choose a number mod pq is pq; The numbers not relatively prime to pq are $0, p, 2p, ...p(q-1)$ and similarly for q. However, 0 is counted twice, so we have $p+q-1$ total number of numbers mod pq not relatively prime to pq. Thus, the probability of picking a number relatively prime to pq is $\frac{pq-(p+q-1)}{pq} = \frac{pq-(p+q)+1}{pq} = \frac{(p-1)(q-1)}{pq}$.

9 Chicken Business

In any flock, every pair of chickens will engage in barnyard squabble to determine which of the two is dominant over the other (hence the origin of the phrase "pecking order"). In other words, for every pair of chickens i, j, either i pecks j or j pecks i.

In general, pecking is not transitive, meaning that if C_1 pecks C_2, who pecks C_3, then it is not necessarily the case that C_1 pecks C_3.

Define a chicken K as a king if, for any other chicken C, either K pecks C directly (which we will abbreviate as $K \to C$), or there exists a field marshal F such that K pecks F, who pecks C (denoted by $K \to F \to C$). We'll call the second type of pecking *indirect* pecking. **You may assume that a king always exists.**

Notice that there may be multiple king chickens in a flock. For instance, if Alex pecks Grace, who pecks Fan, who pecks Alex, then Alex, Grace, and Fan are all kings.

You may assume the following lemma: given a chicken C in a particular flock G, if C is pecked by other chickens, then one of the chickens that pecks C must be a king.

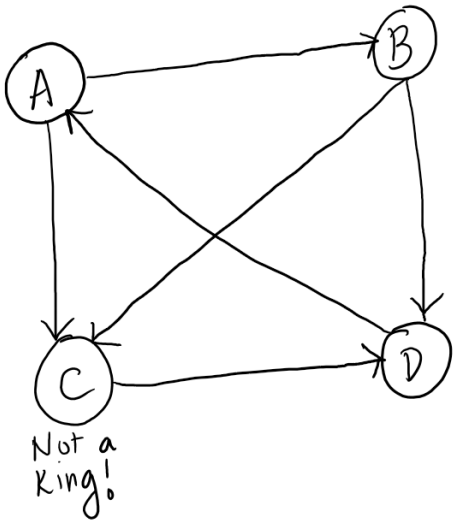
(a) **(7 points)** Prove that a flock of four chickens cannot have exactly four kings.

Problem from https://precollegiate.stanford.edu/circle/math/notes06f/kingchicken.pdf.

Suppose for contradiction we have a flock of four chickens with exactly four kings. No chicken can have outdegree of exactly 3; otherwise this chicken cannot be pecked by others so no other chicken can be a king. Similarly, none of them can have 0 outdegree, since any chicken with outdegree 0 cannot be a king.

Since we have 6 pecking pairs, we must have exactly two chickens with outdegree 2 and exactly two chickens with outdegree 1. Why? If we have three chickens with outdegree 2, then there would be a chicken with outdegree 0 (otherwise we'd run out of edges). On the other hand, if we have three chickens with outdegree 1, then the remaining chicken would have to have outdegree 3.

Furthermore, one of the chickens with outdegree 2 must peck the other chicken with outdegree 2 (since for every pair of chickens, one must peck another). This uniquely determines a graph (below), and the graph does not have 4 kings.



(b) **(7 points)** Use the lemma to prove that no flock can have exactly two kings.

We'll show that if a flock has two kings, we can find a third one. Let k_1 and k_2 be the two kings. Either k_1 pecks k_2, or k_2 pecks k_1. Without loss of generality, assume that k_1 pecks k_2. Since k_2 is king, it must directly or indirectly peck k_1; it doesn't do so directly, therefore there must exist a chicken x, such that $k_2 \to x \to k_1$. Consider the set of chickens A that peck k_1. $k_2 \notin A$, and A is not empty, since $x \in A$. Therefore, there must be a third king $k_3 \in A$, by the previous lemma.

(c) **(7 points)** Use the lemma to prove that if a flock has exactly one king, then that king must peck all the other chickens.

Assume this is not the case, i.e. there is a chicken x that pecks the unique king k. Therefore the set of chickens A that peck k is non-empty, and hence, by the lemma, there must be another king in A. Contradiction.

10 Expected Distance

(19 points) Let X and Y be two random variables in $Exponential(1)$. X and Y are independent. Find $E[|X-Y|]$.

$$E[|X-Y|] = E[\max\{X,Y\} - \min\{X,Y\}] = E[\max\{X,Y\}] - E[\min\{X,Y\}]$$

Therefore, we only have to compute the expected minimum and the expected maximum of X and Y. We have that $f_X(x) = f_Y(x) = e^{-x}$, $F_X(x) = F_Y(x) = Pr[X \le x] = Pr[Y \le x] = 1 - e^{-x}$, for $x \ge 1$.

$$Pr[\min\{X,Y\} \le w] = 1 - Pr[\min\{X,Y\} \ge w] = 1 - Pr[X \ge w]Pr[Y \ge w] = 1 - e^{-w}e^{-w} = 1 - e^{-2w}$$

.

Therefore, $\min\{X,Y\}$ follows the exponential distribution with parameter 2, and therefore $E[\min\{X,Y\}] = \frac{1}{2}$.

Now, notice that $\min\{X,Y\} + \max\{X,Y\} = X + Y$. Therefore, $E[\max\{X,Y\}] = E[X+Y] - E[\min\{X,Y\}] = E[X] + E[Y] - E[\min\{X,Y\}] = 2 - \frac{1}{2} = \frac{3}{2}$

Therefore, we have that $E[|X-Y|] = \frac{3}{2} - \frac{1}{2} = 1$.

Alternate Answer

Here's a really beautiful answer we found during grading, from Kyusang (Michael) Soh:

What's the distribution of $1 - \text{CDF of } |X-Y|$?

This is $\Pr[|X-Y| > t] = \Pr[X-Y > t] + \Pr[Y-X > t]$. By symmetry (since both Y and X are drawn from the same distribution), this is equal to $2\Pr[X-Y > t] = 2\Pr[X > Y+t]$. By memorylessness of the exponential distribution, this is $2\Pr[X > Y]\Pr[X > t] = \Pr[X > t]$ (by symmetry, since we must have $\Pr[X > Y] = 1/2$).

Therefore, $1 - F_{|X-Y|}(t) = \Pr[|X-Y| > t] = \Pr[X > t]$, which immediately implies that $|X-Y|$ must be identically distributed as X.

It immediately follows that $E[|X-Y|] = 1$.

11 Extra Pages

If you use this page as extra space for answers to problems, please indicate clearly which problem(s) you are answering here, and indicate **in the original space for the problem** that you are continuing your work on an extra sheet. You can also use this page to give us feedback or suggestions, report cheating or other suspicious activity, or to draw doodles.

More extra paper. If you fill this sheet up you can request extra sheets from a proctor (just make sure to write your SID on each one, and to staple the extra sheets to your exam when you submit it).

More extra paper. If you fill this sheet up you can request extra sheets from a proctor (just make sure to write your SID on each one, and to staple the extra sheets to your exam when you submit it).

Equation Sheet - PLEASE REMOVE THIS SHEET

Discrete Distributions

Bernoulli Distribution

- 1 with probability p, 0 with probability $1-p$
- Expectation: p
- Variance: $p(1-p)$

Binomial Distribution with parameters n, p

- $\Pr[X = k] = \binom{n}{k} p^k (1-p)^{n-k}$
- Expectation: np
- Variance: $np(1-p)$

Geometric Distribution with parameters p

- $\Pr[X = k] = (1-p)^{k-1} p$

- Expectation: $1/p$
- Variance: $\frac{1-p}{p^2}$

Uniform Distribution with parameters a, b ($a \leq b$)

- $\Pr[X = k] = \frac{1}{b-a+1}$ for $k \in [a,b]$, 0 otherwise.
- Expectation: $(a+b)/2$
- Variance: $\frac{(b-a+1)^2-1}{12}$

Poisson Distribution with parameter λ

- $\Pr[X = k] = \frac{\lambda^k e^{-\lambda}}{k!}$
- Expectation: λ
- Variance: λ

Continuous Distributions

Uniform Distribution with parameters a, b ($a < b$).

- PDF: $\frac{1}{b-a}$ for $x \in [a,b]$, 0 otherwise.
- Expectation: $(a+b)/2$
- Variance: $\frac{(b-a)^2}{12}$

Exponential Distribution with parameter λ

- PDF: $\lambda e^{-\lambda x}$ for $x > 0$, 0 otherwise
- Expectation: $1/\lambda$
- Variance: $1/\lambda^2$

Normal Distribution with parameters μ, σ^2

- PDF: $\frac{1}{\sqrt{2\sigma^2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$
- Expectation: μ
- Variance: σ^2

Chernoff Bounds

Theorem: Let $X_1, \ldots, X_n$ be independent indicator random variables such that $Pr[X_i = 1] = p_i$, and $Pr[X_i = 0] = 1 - p_i$. Let $X = \sum_{i=1}^{n} X_i$ and $\mu = E[X]$. Then the following Chernoff bounds hold:

- For any $\delta > 0$:
$$Pr[X \geq (1+\delta)\mu] \leq \left(\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}} \right)^{\mu}$$
- For any $1 > \delta > 0$:
$$Pr[X \leq (1-\delta)\mu] \leq \left(\frac{e^{-\delta}}{(1-\delta)^{(1-\delta)}} \right)^{\mu}$$
- For any $1 > \delta > 0$:
$$Pr[X \geq (1+\delta)\mu] \leq e^{-\frac{\mu\delta^2}{3}}$$
- For any $1 > \delta > 0$:
$$Pr[X \leq (1-\delta)\mu] \leq e^{-\frac{\mu\delta^2}{2}}$$
- For $R > 6\mu$:
$$Pr[X \geq R] \leq 2^{-R}$$

Please remove this sheet before submitting.