CS 70 Discrete Mathematics and Probability Theory
Summer 2016 Dinh, Psomas, and Ye Final Exam

PRINT Your Name: _____, _____
(last) (first)

By signing below, I agree that (a) I will not give or receive help from others during the exam, (b) that I will not use any electronic devices or other prohibited resources during the exam, and (c) that I will not discuss or disclose the contents of the exam before 2:30 PM PDT on Friday, August 12 2016.

SIGN Your Name: _____ DATE: _____

PRINT Your Student ID: _____

CIRCLE your exam room: 1 Pimentel 120 Latimer 540 Cory 293 Cory Other

Name of the person sitting to your left: _____

Name of the person sitting to your right: _____

- After the exam starts, please write your student ID (or name) on every sheet (we will remove the staple when scanning your exam).
- We will not grade anything outside of the space provided for a problem unless we are clearly told in the space provided for the question to look elsewhere.
- You may consult three **handwritten** pages of notes (one double-sided sheet+one single-sided sheet; or three single-sided sheets) sheet of notes. Apart from that, you may not look at books, notes, etc. Calculators, phones, computers, and other electronic devices are not permitted.
- There are 28 pages (14 sheets) on the exam, including 3 pages of extra paper and an 2-page (1 sheet) equation reference at the end containing tables of distributions and bounds. Notify a proctor immediately if a page is missing.
- There are 10 questions on this exam, worth a total of 270 points.
- **You may, without proof, use theorems and facts that were proven in the notes and/or in lecture.**
- **If you cannot solve a problem whose answer is required for a subsequent one, you may reference the answer to the previous problem by, for instance, saying "Let y be the answer to part a".**
- **You have 170 minutes.**

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

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 $(\forall x, P(x)) \vee (\forall x, Q(x))$.

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

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

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

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

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

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

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

(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".

(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).

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

(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 $Pr[X \geq a] = \frac{E[X]}{a}$.

(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.

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?

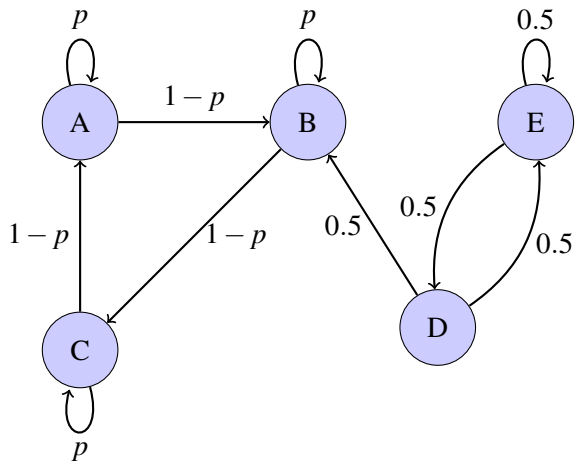
(b) **(4 points)** I have a pile of six pens, four highlighters, ten pencils, and five styluses. I pick five at random from the pile. What is the probability that I end up with at least one of each kind of writing implement?

(c) **(4 points)** What is the last digit of 2016^{70}?

(d) **(4 points)** Calculate $12^{136} \pmod 7$.

(e) **(4 points)** Compute $\gcd(512, 480)$.

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



(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?

(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?

(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.

(j) **(4 points)** Suppose Alex and David are using Blum's coin toss scheme. Alex sends David $n = pq$, the product of two primes each congruent to 3 mod 4 as in the normal protocol. David is feeling lazy that day and, instead of choosing an x and sending back $a = x^2$, just picks random a directly. Luckily for him, a is indeed a perfect square, although he doesn't know what its square root is. Who wins the coin toss, and why?

(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.

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.

(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 $n\in\mathbb{N}$.

(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.

(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 $\lceil 3 \rceil = 3$.

(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.

(f) **(4 points)** Prove that if Alex sends a message m_a to Fan, encrypted with Fan's (public) RSA key, David can send another message $m_d = qm_a$ for some q of David's choice, without knowing either m_a or Fan's private key, assuming he knows the (encrypted) ciphertext that Alex sent to Fan.

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

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

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

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?

(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.

(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?

(d) **(5 points)** What is the probability that the degree of v is equal to k?

(e) **(5 points)** What is the variance of the degree of v?

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 $k > 0$.

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.

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?

(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 $(5,2,3)$.

(c) **(10 points)** What is the probability that Bob received message $(2,0,0,2,6,1,9)$?

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.*

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 David, who pecks Fan, who pecks Alex, then Alex, David, 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.

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

(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.

10 Expected Distance

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

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.