Final Exam

Friday, August 16, 5:10pm–8:10pm

CS 70: Discrete Mathematics and Probability Theory, Summer 2013

Your name _____

Your student ID # _____

Your section # _____

This exam has 8 questions and a total of 100 points.
Do not open the exam until you are told to.
Do not write below this line.

Q1	
Q2	
Q3	
Q4	
Q5	
Q6	
Q7	
Q8	
Total	

1. [30 points] **MULTIPLE CHOICE.** Circle the correct answer. You don't need to show work.

1a. [2 points] $\big((P \Leftrightarrow Q) \Rightarrow P\big) \quad \equiv \quad \big(\neg P \wedge \neg Q\big)$

TRUE FALSE

1b. [2 points] Suppose no two people in the room have the same height or the same age. Let $\text{Taller}(x, y)$ mean "x is taller than y", and $\text{Older}(x, y)$ mean "x is older than y". Which one of the following correctly expresses "The tallest person is not the youngest"?

$$\forall x \ \big(\forall y \ (\text{Taller}(x, y) \Rightarrow \neg\text{Older}(y, x))\big)$$

$$\forall x \ \exists y \ \big(\text{Taller}(y, x) \vee \text{Older}(x, y)\big)$$

$$\forall y \ \exists x \ \big((x \neq y) \Rightarrow (\text{Taller}(x, y) \vee \neg\text{Older}(y, x))\big)$$

1c. [2 points] Suppose you want to prove $(\forall n \in \mathbb{N}) \ P(n)$. Which one of the following is *not* a valid proof strategy?

Prove $P(0) \wedge P(1) \wedge (\forall n \in \mathbb{N}) \ (\neg P(n) \Leftrightarrow \neg P(n+1))$

Prove $P(0) \wedge P(1) \wedge P(2) \wedge (\forall n \in \mathbb{N}) \ (P(n) \Rightarrow P(2n))$

Prove $P(0) \wedge P(1) \wedge (\forall n \in \mathbb{N}) \ (P(n) \Rightarrow P(n+2))$

1d. [2 points] Suppose the male-optimal propose-and-reject algorithm is run on a uniformly random stable marriage instance with n men and n women. That is, each man (independently of the others) picks a uniformly random permutation of the women for his preference list, and similarly for the women. What is the probability that in the resulting pairing, each man gets the first woman on his list and each woman gets the first man on her list?

$$\frac{n!}{2n^n} \qquad \frac{1}{(n!)^2} \qquad \frac{n!}{(n^n)^2} \qquad \frac{1}{n! \cdot (2n)^n} \qquad \frac{n^n}{(n!)^2}$$

1e. [2 points] For all positive integers a, b, c: If a has an inverse mod b then ac has an inverse mod bc.

TRUE FALSE

1f. [2 points] For all $n \geq 2$ there exists an n-node directed graph such that for every node, either the indegree is 0 or the outdegree is 0 but not both.

TRUE FALSE

1g. [2 points] A 6-sided die is rolled nine times. The probability that at least eight of the outcomes are the same is

$$\frac{6 \cdot \binom{9}{8}}{6^9} \qquad 6 \cdot 5 \cdot \frac{1}{6^8} \qquad \frac{6 \cdot (9 \cdot 5 + 1)}{6^9} \qquad \left(\binom{9}{8} + \binom{9}{9}\right) \cdot \frac{1}{6^8}$$

1h. [2 points] You're writing an email spam detector. 20% of the email you receive is spam, and the other 80% is not spam. For a spam email, the probability it comes from an address not in your list of contacts is 1. For a non-spam email, the probability it comes from an address not in your list of contacts is 0.25. A new email comes in, and your program sees that it comes from an address not in your list of contacts. What is the posterior probability it is spam?

$$\frac{1}{5} \qquad \frac{1}{4} \qquad \frac{1}{2} \qquad \frac{3}{4}$$

1i. [2 points] A casino game costs \$1 to play. I win with probability 1/5, in which case I earn \$4 (hence \$3 profit). If I lose, I get nothing (\$-1 profit). If I play the game n times, the expected value of my total profit (in dollars) is

$$-\frac{3n}{5} \qquad -\frac{n}{5} \qquad \frac{n}{5} \qquad \frac{3n}{5}$$

1j. [2 points] Suppose X is an unbiased estimator for p with absolute error ϵ and confidence parameter δ ("$1 - \delta$ confident"). Which one of the following is guaranteed to be true?

$2X$ is an unbiased estimator for $2p$ with absolute error ϵ and confidence δ

$2X$ is an unbiased estimator for $2p$ with absolute error 2ϵ and confidence δ

$2X$ is an unbiased estimator for $2p$ with absolute error ϵ and confidence 2δ

1k. [2 points] You throw a dart at a 2×2 square (where x ranges between 0 and 2, and y also ranges between 0 and 2). You win iff the dart's location has $x \geq 1$ or $y \geq x$. Assuming your dart lands uniformly at random within the square, the probability you win is

11/12 7/8 5/6 3/4 1/2

1l. [2 points] Suppose that X has an exponential distribution with parameter λ. Then $\Pr\left[X > 3 \;\middle|\; X \leq 5\right] =$

$$\frac{e^{-3\lambda} - e^{-5\lambda}}{1 - e^{-5\lambda}} \qquad \frac{e^{-5\lambda} - e^{-3\lambda}}{1 - e^{-3\lambda}} \qquad \frac{\lambda e^{-3\lambda} - \lambda e^{-5\lambda}}{1 - \lambda e^{-5\lambda}} \qquad \frac{\lambda e^{-5\lambda}}{1 - \lambda e^{-3\lambda}}$$

1m. [2 points] $\Pr\left[\text{Bin}(10000, p) \leq 10000p + 50\sqrt{p(1-p)}\right]$ is, according to the Central Limit Theorem, approximately

$\Pr\left[N(0,1) \leq -0.5\right]$ $\Pr\left[N(0,1) \leq 0.25\right]$ $\Pr\left[N(0,1) \leq 0.5\right]$

1n. [2 points] There exists a surjection (i.e., an "onto function") from the set of even natural numbers to the set of all computer programs.

TRUE FALSE

1o. [2 points] Which one of the following is *not* proved using the diagonalization technique?

The set of rationals $\mathbb{Q}$ has the same cardinality as the set of natural numbers $\mathbb{N}$

The set of reals $\mathbb{R}$ has greater cardinality than the set of natural numbers $\mathbb{N}$

The halting problem is not computable

2. [10 points] **PROOFS AND GRAPHS.**

Consider undirected graphs with no multi-edges and no self-loops.

2a. [2 points] Prove that for every graph on $n+1$ nodes, if it has at least $\binom{n}{2}+1$ edges, then there does not exist a node of degree 0. What proof technique are you using?

2b. [1 point] Prove that for every graph on $n+1$ nodes, if there exists a node of degree n, then the graph is connected. (Recall that "connected" means for every two nodes there exists a path between them.)

2c. [7 points] Prove the following by simple induction on n:

For all $n \geq 3$, if a graph G on n nodes has $\geq \binom{n-1}{2}+1$ edges, then G is connected.

(Hint: Use parts (a) and (b) of this problem! In the inductive step going from n to $n+1$, pick an arbitrary node v and consider the possibilities for its degree.)

3. [12 points] **MODULAR ARITHMETIC AND POLYNOMIALS.**

3a. [2 points] Evaluate $\dfrac{9002}{7 + (11 \times 12)}$ in modulo 9 arithmetic. Show your work.

3b. [3 points] Consider RSA with $p = 7$, $q = 11$. Use the Euclidean algorithm to determine whether or not $e = 21$ is a valid encryption exponent. Show your work and clearly label your answer and justification.

3c. [4 points] Solve the following modular equation. (Hint: think RSA decryption.)

$$x^5 \equiv 6 \pmod{35}$$

3d. [3 points] Alice has a polynomial P of degree ≤ 2 over $GF(7)$. She sends packets to Bob indicating the values $P(1), \ldots, P(6)$, but Bob only receives packets indicating that $P(1) = 1$, $P(3) = 0$, $P(4) = 0$. Use Lagrange interpolation to find the coefficients of P. Show your work, and clearly label your answer.

4. [10 points] **COUNTING AND PROBABILITY.**

You are the human resources director for a company. There are n job applicants, of which k are qualified and $n - k$ are unqualified. You need to hire r people, and you just pick a uniformly random subset of r out of all n applicants. You may assume that $n > k \geq r \geq 2$.

4a. [2 points] What is the probability that everyone you hire is qualified?

4b. [3 points] What is the probability that you hire exactly one unqualified applicant?

4c. [3 points] What is the probability that you hire exactly two unqualified applicants, given that you hire at least one unqualified applicant?

4d. [2 points] In how many ways can you assign m identical tasks to the r new employees, so that each employee gets at least one task? (Assume $m \geq r$.)

5. [8 points] **DISCRETE DISTRIBUTIONS.**

5a. [4 points] A missile launch code has been shared among 20 officers using a secret-sharing scheme, such that the code can be recovered iff at least 5 officers combine their shares. You are not one of the officers. Each day you have a meeting with a uniformly random officer (independently of other days). If you have not previously met with that officer, then you bribe him to get his share of the secret. In expectation, how many days does it take before you can recover the secret? Give an exact expression and show your work.

5b. [4 points] Your web server occasionally crashes, at random times, with an average of three times *per week*. What is the probability it will crash *at least* twice *tomorrow*?

6. [12 points] **CONCENTRATION.**

You are teaching a class with n students. Before handing homeworks back to your students, you pick up each homework and put a sticker on it with probability $\frac{1}{2}$ (independently of the other homeworks). Then you hand back the homeworks according to a uniformly random permutation. Let X be the number of students who get their own homework back AND it has a sticker on it. In the following problems, show all your work and clearly label your answer.

6a. [3 points] Compute the expectation $\mathrm{E}(X)$.

6b. [2 points] Use Markov's Inequality to prove an upper bound on the probability that at least 3 students get their own homework back and it has a sticker on it.

6c. [5 points] Compute the variance $\text{Var}(X)$.

6d. [2 points] Use Chebyshev's Inequality to prove an upper bound on the probability that at least 3 students get their own homework back and it has a sticker on it.

7. [8 points] **CONTINUOUS DISTRIBUTIONS.**

After this exam is over, you will need to walk home. Suppose there are two routes you can take from Valley LSB to your dorm/apartment. Route A is a shorter distance than route B, but route A has a higher variance due to unpredictable traffic lights. You know from past experience that the time to walk route A can be modeled as a normal distribution with mean 10 minutes and standard deviation 2 minutes, and the time for route B is normal with mean 12 minutes and standard deviation 1 minute. Suppose you leave the exam at exactly 8:15pm.

7a. [4 points] Suppose you want to maximize the probability that you are home by 8:30pm, since that's when your favorite TV show starts. Which route is best? Justify your answer. (Note: You do *not* need to calculate the value of the maximum probability, only figure out which probability is higher.)

7b. [4 points] Suppose instead that you want to find the earliest time x such that you can be home by that time with probability 0.9. What is this time x, and which route achieves it? Justify your answer. You may assume that $\Pr\left[N(0,1) \leq 1.3\right] = 0.9$.

8. [10 points] **THE FINAL BOSS.**

Can you synthesize different topics from throughout the course?

8a. [3 points] You pick a uniformly random node in the n-dimensional hypercube, and let a be its label (a bit string). Then you pick a uniformly random edge that's attached to a, and let b be the label of the other endpoint of the edge. Given that b has more 1's than a does, what is the probability that a has exactly k 1's?

8b. [3 points] You have proposition variables $P_1, P_2, \ldots, P_n$, and each is set independently to true or false uniformly at random. Compute the variance of the number of pairs $\{i, j\}$ for which the formula $(P_i \Rightarrow P_j) \wedge (P_j \Rightarrow P_i)$ is true.

8c. [4 points] Suppose $p > d > 1$ and p is prime (note that $p \geq 3$). Consider the following undirected graph with no multi-edges and no self-loops. The nodes represent all the polynomials of degree $\leq d$ over $GF(p)$. There is an edge between two of these polynomials iff they have no roots in common. Prove that this graph has an eulerian cycle.

8d. [0 points] Go Bears?

TRUE FALSE