EECS 70 Discrete Mathematics and Probability Theory
Fall 2015 Walrand/Rao Final

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

SIGN Your Name: ____________________________________

PRINT Your Student ID: ____________________________________

CIRCLE your exam room: 220 Hearst 230 Hearst 237 Hearst !!!!

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 odd page (we will remove the staple when scanning your exam).
- We will not grade anything outside of the space provided for a problem. Please use scratch paper as necessary and clearly indicate your answer.
- There are two Parts: Discrete Math and Probability. Do in the order you feel best suits you.
- For Part I.
  - Problem 1 has instructions for what to indicate.
  - Problem 2 is short answer; no need to justify. Partial credit may be awarded if appropriate.
  - Problem 3 is short answer; no need to justify. Partial credit may be awarded if appropriate.
  - Problem 4 requires proofs.
- For Part II.
  - Questions 1(a)-(d). You need only circle True or False.
  - For the other questions, you should indicate clearly your derivation in the space provided.
- You may not look at books, notes, etc. Calculators, phones, and computers are not permitted.
- There are 22 pages on the exam, including this first page. Notify a proctor immediately if a page is missing.
- **You may, without proof, use theorems and facts that were proven in the notes and/or in lecture.**
- **You have 180 minutes; there are 25 parts in Part I and 20 parts in Part II.**

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

Part I: Discrete Math.

1. **Propositions. 10 points. 3/3/4**

(a) The following statement expresses the fact that there is a smallest number in the natural numbers, $(\exists y \in N)\ (\forall x \in N)\ (y \leq x)$. Write a statement that expresses the fact that there is no smallest number in the integers, Z.

(b) The following statement could express Fermats Little Theorem, fill in the blank so that it does.
Let $\textbf{Prime}(p) = \forall d \in N; d \geq 2, d < p \implies \neg(d|p)$,
$(\forall p \in N)\ [\textbf{Prime}(p) \implies$
$((\forall a \in N)(\ (\underline{\hspace{2cm}}) \implies \ a^{p-1} \equiv 1 \pmod{p}))]$

(c) The statements,
$(\exists x \in S)\ ((\forall y \in S)\ P(x,y) \wedge (\forall y \in S)\ Q(x,y))$

and

$((\exists x \in S)\ (\forall y \in S)\ P(x,y)) \wedge ((\exists x \in S)(\forall y \in S)\ Q(x,y))$,

are not equivalent. Give a counterexample. That is, define an S, $P(x,y)$, and $Q(x,y)$ which cause the above statements to have different values.

2. Quick Short Answer. 34 points. Breakdown below.

Clearly indicate your correctly formatted answer: this is what is to be graded. No need to justify!

(a) **[4 Points.]** What is the number of different n-men, n-women stable marriage *instances*? (Here the men and women are distinguishable. This, for example, means switching the preference lists of two different men corresponds to two different instances, as does switching the order of two women in a man's preference list.)

(b) **[3 Points.]** In any run of the stable marriage algorithm, where the men propose, it is the case that the number of women recieving a proposal on each day is non-decreasing. This includes women recieving old proposals. (True/False)

(c) **[3 Points.]** What is the inverse of 2 modolo n, if n is odd? (You should write an expression that may involve n. Simplicity matters.)

(d) **[3 Points.]** If $gcd(x,y) = 13$, what is $gcd(x, x-13y)$?

(e) **[4 Points.]** What is $3^{26} \pmod{35}$?

(f) **[4 Points.]** What is d for the RSA scheme where $p = 5$, and $q = 7$, and e is 5? (Do not worry about the security of such a scheme, just follow the definition of RSA.)

(g) **[3 Points.]** What degree polynomial should you use to tolerate 3 errors (corruptions) when sending a message consisting of 7 packets?

Consider a hypercube of dimension $d \geq 2$ for the next two parts. Recall that the vertices correspond to all the length d binary (bit) strings, and each vertex is adjacent to all vertices that differ in one bit position.

(h) **[2 Points.]** Remove all vertices (and their incident edges) where the number of ones in the binary representation is even. How many connected components are in the remaining graph?

(i) **[2 Points.]** Remove all vertices (and their incident edges) where the first bit is a 1. How many connected components are in the remaining graph?

The hypercube problems are complete now.

(j) **[3 Points.]** If you take a walk in a graph until you reach a vertex with no unused edges, this vertex is either the starting vertex or has ____ degree. (Possible answers: odd or even.)

(k) **[3 Points.]** What is the minimum number of edges one needs to remove from K_{2n} (the complete graph on $2n$ vertices) to leave exactly two components of equal size.

3. More Short Answer. 33 points. Breakdown below.

Clearly indicate your correctly formatted answer: this is what is to be graded. No need to justify!

(a) **[4 Points.]** How many different anagrams of MISSISSIPPI are there that do not start or end with I? (For example, MISSISSIPPI should not be counted, as it ends with I. Note there are 11 characters: 1 M, 4 S's, 4 I's, and 2 P's. No need to simplify your expression.)

(b) **[4 Points.]** If $ax+by=6$ and $cx+dy=5$, for integers a,b,c,d,x and y, what is the multiplicative inverse of x modulo y? (Answer should be in terms of a,b,c and/or d modulo y.)

(c) **[4 Points.]** What is the maximum number of solutions for the equation $10x = y \pmod{35}$, for any value of y, for $x,y \in \{0,1,\ldots,34\}$.

(d) **[5 Points.]** A degree 2 polynomial, $P(x)$, over arithmetic modulo 7 goes through points $(1,0)$, $(2,4)$, $(3,0)$, what is $P(0)$?

(e) **[6 Points.]** How many polynomials of degree exactly 2 modulo p are there that cannot be factored into two or more polynomial factor; are "irreducible"? (For example, $x^2 - 1$ is reducible as it factors into $(x-1)(x+1)$, x^2 is also reducible, $x^2 + 1$ is irreducible modulo 3 since it has no roots. Answer should be an expression involving p.)

(f) **[5 Points.]** The problem of determining whether a program uses more than n^2 space (in bits) on an input of size n is undecidable. (True/False)

(g) **[5 Points.]** In any stable pairing where exactly half the men are paired with their optimal partner, at least half the women are paired with their pessimal partner. (True/False)

4. Proofs. 22 points. 6/8/9

(a) Show that if $n^2 - 1$ is not a multiple of d, than neither $n-1$ nor $n+1$ is a multiple of d.

(b) Prove that there the problem of determining whether a program has *any* input which causes it to halt is undecidable. (True/False.)

(c) Given a necklace of n red and n blue beads. Show that you can cut the necklace at a place such that every prefix of the resulting string of beads has at least as many red beads as blue. For example, the (circular) necklace *BBRR* can be cut between the blue beads and red beads producing a string *RRBB* where every prefix (*R*, *RR*, *RRB*, and *RRBB*) has more red beads than blue beads. (Advice: if you don't have an idea, maybe come back later.)

Part II: Probability.

1. **True or False. No justification needed. 10 points. 2/2/3/3.**

   Clearly indicate your correctly formatted answer: this is what is to be graded. No need to justify!

   (a) If $var[X] \leq 1$, then $Pr[X \geq 10] \leq 1\%$. (True or False.)

   (b) Let X be uniform in $[0,1]$. Then $E[X^5] = 1/6$. (True or False.)

   (c) Let X,Y,Z be i.i.d.. Then $E[X+Y|X+Y+Z] = (2/3)(X+Y+Z)$. (True or False.)

   (d) Let X,Y be two random variables and $Z = \min\{X,Y\}$. Then $E[Z] \leq \min\{E[X],E[Y]\}$. (True or False)

2. **Short Answers. 14 points: 3/4/3/4**

Clearly indicate your answer and your derivation.

(a) Let $\Omega = [0,1]$ with the uniform distribution. Find $0 < a < b < 1$ so that the following two events of Ω are independent: $[0,0.5]$ and $[a,b]$. [*Hint:* $(a,b) = (0,1)$ do not satisfy the requirements and neither do $(a,b) = (0,0)$ nor $(a,b) = (1,1)$.]

(b) Let X,Y be independent and $U[0,1]$. Calculate $E[|X-Y|]$. [*Hint:* Note the absolute value!]

(c) A coin is equally likely to be fair or biased with $Pr[H] = 0.7$. You flip the coin 100 times. What is the expected number of heads?

(d) A coin is equally likely to be fair or biased with $Pr[H] = 0.7$. You flip it twice and only get Ts. Find the expected number of additional flips until you get H.

3. **Short Problems. 18 points. 4/4/4/6**

Clearly indicate your answer and your derivation.

(a) Choose m real numbers uniformly at random in $[0,1]$. Let X be the largest one of these numbers. What is the pdf $f_X(x)$? Find $E[X]$.

(b) Let X be a random variable with mean μ and variance σ^2. Find the value a that minimizes $E[(X-a)^2]$.

(c) Let X be $Expo(1)$. Recall that this means that $f_X(x) = e^{-x}1\{x \geq 0\}$, so that $E[X] = 1$ and $F_X(x) = [1 - e^{-x}]1\{x \geq 0\}$.

(a) Show that $Pr[X > t + s|X > s] = Pr[X > t]$ for $s, t \geq 0$.

(b) Use that result to calculate $E[X|X > 5]$.

(d) Let X, Y, Z be i.i.d. $\mathcal{N}(0,1)$ and $V = 2X + 3Y + 4Z, W = X + Y + Z$. Find $L[V|W]$.

4. Less Short Problems. 58 points: 8/7/7/7/7/7/8/7

Clearly indicate your answer and your derivation.

(a) Let $\Omega = \{1,2,3,4,5,6\}$ be a uniform probability space. Let also $X(\omega)$ and $Y(\omega)$, for $\omega \in \Omega$, be the random variables defined as follows:

Table 1: The random variables X and Y.

ω	1	2	3	4	5	6
$X(\omega)$	0	0	1	1	2	2
$Y(\omega)$	0	2	3	5	2	0

(i) Calculate $V = L[Y|X]$;

(ii) Calculate $W = E[Y|X]$;

(iii) Calculate $E[(Y-V)^2]$;

(iv) Calculate $E[(Y-W)^2]$.

[*Hint:* Recall that $L[Y|X]$ and $E[Y|X]$ are functions of X and that you need to specify their value as a function of X.]

(b) A dart player is equally likely to be good or bad. If he is good, he shoots the dart uniformly in a circle with radius $1/2$. If he is bad, he shoots the dart uniformly in a circle with radius 1. The first dart of the player is at distance $1/3$ from the center. What is the expected distance of the second dart to the center of the target? [*Hint:* Condition on the distance being in $[1/3, 1/3+\delta]$ for a small δ. Call that event A.]

(c) You roll a balanced die n times. Let X_n be the number of different values that you got in the first n steps. For instance, if the successive rolls yield $5,2,5,4,2,1$, then $X_1 = 1, X_2 = 2, X_3 = 2, X_4 = 3, X_5 = 3$, and $X_6 = 4$. Calculate $E[X_n]$.

(d) One bin has 100 red balls. At step 1, you pick a ball at random from the bin and you replace it with a ball that is equally likely to be red or blue. You repeat that process. Let X_n be the number of red balls in the bin after n steps. Thus, $E[X_1] = 99.5$. Calculate $E[X_n]$. [*Hint:* Recall that $1 + a + \cdots + a^k = (1 - a^{k+1})(1 - a)$ for $a \neq 1$.]

(e) Let X,Y be i.i.d. $U[-1,1]$. Calculate $L[Y|Y+2X]$. [*Hint:* Note that $var(X) = var[2Z]$ where $Z = U[0,1]$.]

(f) Let $\{X_1, \ldots, X_n\}$ be the lifetimes of lightbulbs. We know that they are exponentially distributed with parameter λ and we know that $\lambda \geq 10$. Recall that $E[X_m] = \lambda^{-1}$ and $var[X_m] = \lambda^{-2}$.

(1) Use Chebyshev's inequality to construct a 95%-confidence interval for λ^{-1} based on $\{X_1, \ldots, X_n\}$.

(2) Use the CLT to construct such a confidence interval.

[*Hint:* The answers should not contain λ, since this is what we are trying to estimate.]

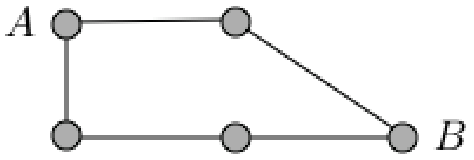

Figure 1: Circuit for problem.

(g) Consider the circuit in Figure 1. Nodes A and B are connected via five links. The links fail independently, each after an exponentially distributed time with mean 1. Calculate the expected time until the nodes A and B are disconnected, i.e., when there is no longer a path of working links between them. [*Hint:* Note that the time until the top path fails is the minimum of independent random variables; similarly for the bottom path. Recall what we know about the minimum of exponential random variables. Also, recall that if $X = Expo(\lambda)$, then $f_X(x) = \lambda e^{-\lambda x} 1\{x \geq 0\}$; also, for $x > 0$, $Pr[X \leq x] = 1 - e^{-\lambda x}$ and $Pr[X > x] = e^{-\lambda x}, E[X] = \int_0^\infty x\lambda e^{-\lambda x} dx = \lambda^{-1}, var(X) = \lambda^{-2}$.]

(h) Let $X_n, n \geq 1$ be $Expo(1)$. Use Chernoff's inequality to find an upper bound on

$$Pr[\frac{X_1 + \cdots + X_n}{n} \geq 2].$$

The bound should be of the form α^n for some $0 < \alpha < 1$. [*Hint:* Recall that $\int_0^\infty e^{-ax} dx = 1/a$ for $a > 0$.]