CS 70 Discrete Mathematics and Probability Theory
Spring 2016 Walrand and Rao Midterm 2

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

SIGN Your Name: ______________________

PRINT Your Student ID: ______________________

CIRCLE your exam room:
2050 VLSB 10 Evans 159 Mulford 145 Dwinelle 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 odd page (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. Scratch paper is not allowed to be used for answers.
- Give justifications as noted.
- You may consult two single-sided sheet of notes. Apart from that, you may not look at books, notes, etc. Calculators, phones, and computers are not permitted.
- There are 12 single sided pages on the exam. 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 120 minutes: there are 52 parts on this exam.**
  - **Problems 1-3: 26 parts. 55 points.**
  - **Problem 4-7: 25 parts. 45 points.**

  Do relax, they are mostly quite short. Though do keep moving.

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

1. Short Questions: 2/2/2/2/2 Provide a clear and concise justification of your answer.

In this problem, you roll two balanced six-sided dice. *Hint: Draw a picture.*

1. What is the probability that the number of pips (dots) on the second die is equal to the number on the first?

2. What is the probability that the number of pips (dots) on the second die is strictly larger than the number on the first?

3. What is the probability that the first die yields a value less than or equal to 2 given that the sum of the two values is strictly larger than 5?

4. What is the probability that the two values differ by 4 or more in absolute value?

5. What is the probability that the maximum of the two values is 5 or 6?

2. Short Questions: 3/3/3/3/3/3/3 Provide a clear and concise justification of your answer.

In this problem, there is a probability space with sample space Ω.

1. True or False (and justification): Two disjoint events A and B with $Pr[A] > 0$ and $Pr[B] > 0$ cannot be independent.

2. True or False (and justification): Let $\{A_1, \ldots, A_N\}$ be a partition of Ω. That is, the events $\{A_1, \ldots, A_N\}$ are pairwise disjoint and their union is Ω. Let also B and C be two other events. If $Pr[B|A_n] > Pr[C|A_n]$, then it must be that $Pr[A_n|B] > Pr[A_n|C]$.

3. True or False (and justification): If A and B are positively correlated and so are B and C, then A and C are necessarily positively correlated. (Recall that, by definition, two events A and B are positively correlated if $Pr[A \cap B] > Pr[A]Pr[B]$.)

4. There is a bag with 50 red and 50 blue balls. You pick four balls, without replacement. Given that the first ball is red, what is the probability that the fourth ball is also red?

5. True or False (and justification): For any event A, the events A and Ω are independent.

6. True or False (and justification): If the events A, B, C are such that $A \cap B \cap C = \emptyset$, then $Pr[A \cup B \cup C] = Pr[A] + Pr[B] + Pr[C]$.

7. (a) Let $\Omega = \{1,2,3,4,5,6\}$ be a uniform probability space. Find two independent events A and B with $0 < Pr[A] < 1$ and $0 < Pr[B] < 1$.

   (b) Let $\Omega = \{1,2,\ldots,n\}$ be a uniform probability space. Assume that n is not a prime number. Find two independent events A and B with $0 < Pr[A] < 1$ and $0 < Pr[B] < 1$.

3. Longer Questions: 8/8/8 Provide a clear and concise justification of your answer.

1. You select a three digit decimal number uniformly in $\{000, 001, \ldots, 999\}$. Note that we consider 023 to be a three digit decimal number, etc.

   (a) What is the probability that the number has three identical digits given that it has at least two identical digits?

   (b) What is the probability that the sum of the three digits is 9.

2. There are two bags. One contains 4 red and 6 blue balls. The other contains 6 red and 4 blue balls. You select one of the two bags with equal probabilities and pick three balls without replacement.

   Hint: Give names to the appropriate events. For instance, let A_1 be the event that you selected the first bag, etc.

   (a) Given that you selected the first bag, what is the probability that the first two balls are red?

   (b) Given that you selected the first bag, what is the probability that the three balls are red?

   (c) Given that you selected the second bag, what is the probability that the first two balls are red?

   (d) Given that you selected the second bag, what is the probability that the three balls are red?

   (e) What is the probability that the first two balls are red?

   (f) What is the probability that the three balls are red?

   (g) Given that the first two balls are red, what is the probability that the third one is also red?

   (h) What is the probability that you selected the first bag given that the first two balls are red?

4. A car mechanic is great with probability 0.2 and ordinary otherwise. A great mechanic is great every day and an ordinary one is ordinary every day. The car mechanic works on one car at a time and, when he starts working on a car, he works on it day after day until he finishes. If he is great, he finishes a car repair with probability 0.6 independently on each day. If he is ordinary, he finishes it with probability 0.4 independently on each day. You ask two friends who used that mechanic. He completed their car repairs in 3 and 4 days, respectively.

(a) What is the probability p that the mechanic is great?

(b) What is the probability that he would repair your car repair in at most 2 days?

Note: The expression for p is a bit complicated. We don't want you to spend time evaluating its value. You can express the answer to (b) in terms of p.

5. How many? (1/1/2/3/3/4)

1. How many length 10 ternary strings are there? (A ternary number has three possible symbols: 0,1,2. The first digit can be 0! So, 0000000000 is a 10 symbol string.)

2. How many length 10 ternary strings are there with a 1 as the first symbol?

3. How many 10 digit ternary numbers are there with a 1 in either of the first two digits. (You should count the numbers starting with 1 in both of the first two.)

4. How many length ternary strings are there where the symbols add up to 10? (Recall the symbols are $0,1$ and 2. An example of such a string is 2222200000, since there are five 2's and five 0's and the sum of their numeric values is 10.)

5. How many ways are there to split up n dollars among r friends where each friend gets at least 1 dollar and no friend gets half or more of the dollars. (You may assume that n is even and $k \geq 3$. If convenient you can assume that $\binom{n}{m} = 0$ for $m > n$.)

6. Give a combinatorial proof that

$$3^n = \sum_{i=0}^{n} \binom{n}{i} 2^{n-i}.$$

6. Polynomials (1/1/1/5/4/1)

Consider two polynomials, $P(x)$ of degree d and $E(x)$ of degree k over $GF(p)$ (modulo p) for a prime p where $p > d > k$.

1. What is the maximum number of solutions to $P(x) = 5 \pmod{p}$?

2. What is the maximum number of solutions to $E(x)P(x) = 5 \pmod{p}$?

3. What is the maximum number of solutions to $E(x) + P(x) = 5 \pmod{p}$?

4. Assume that $d = 2$, $P(1) = 1$, $P(2) = 2$, and $P(3) = 2$ and $p = 7$, what is $P(0)$?

5. Assume that $d = 1$, and we are told that $P(1) = 2$, $P(2) = 3$, $P(3) = 2$, $P(4) = 0$ and $p = 5$, but we know there is exactly one incorrect point.

   (a) What is $P(0)$?

   (b) What is the error locator polynomial for Berlekamp-Welsh Algorithm for this situation?

7. Countability/Computability (1/1/1/1/1/1/1)

For the following problems, a computer program may run forever, and if it eventually prints every element of a set or every digit of a real number at a finite, specific time, it is said to print out that set or that number. For example, there is a computer program that prints out every natural number. We also allow a computer program access to an infinite amount of memory.

1. The power set (the set of all subsets) of any infinite set is uncountable. (True/False)

2. There is a computer program that prints all rational numbers. (True/False)

3. A computer program can print out $\sqrt{2}$. (True/False)

4. There is a computer program that prints all real numbers. (True/False)

5. There is an efficiency checking program that takes another program P and an input n and verifies that P halts within 2^n steps for all inputs of size n. (True/False)

6. There is a computer program that prints all computer programs and the inputs where they halt. (True/-False.)

7. There is a computer program that given a program P and input x can check if all the subroutines of P are called. (True/False.)

8. Schemes (3/3/3/1/1)

1. Bob saw a show about twin primes, primes p and q where $q = p+2$. Thinking these were cool, he decided to use twin primes to construct his RSA key pair. Give a polynomial time method to break his scheme. Recall that he makes (N,e) public and that $N = pq$ for his twin primes p and q.

2. A secret has been shared among 10 people using the scheme from class with a degree 3 polymonial. Recall that any 4 people can reconstruct the secret. But say all 10 agree to cooperate but some remember incorrectly (or are just lying). What is the largest number of people who can be incorrect where the group can still correctly reconstruct the secret?

3. Consider that some CS70 students want to vote for their favorite superhero: Batman or Superman. If a student i likes Batman, they construct a polynomial $P_i(x) = r_i x + 1$, otherwise they construct a polynomial of $r_i x - 1$ where r_i is chosen uniformly at random in $\{0, \ldots, p-1\}$. The polynomials are in $GF(p)$, that is considered to be evaluated modulo p.

   Then each student gives Professor Walrand $P_i(1)$ and Professor Rao $P_i(2)$. The professors serve as vote counters.

   (a) The professors' compute the sum of the values given to each and each professor announces the result. Professor Walrand announces that his sum (or $\sum_i P_i(1) \pmod{11}$) is 3 and Professor Rao announces that his sum (or $\sum_i P_i(2) \pmod{11}$) is 5. If $p = 11$ (the student's polynomials are modulo 11) and 5 students voted, who is the students' favorite? (Justify briefly.)

   (b) Can either professor know who a student voted for, given that they do not reveal any individual student's value to the other professor? (Justify briefly.)

   (c) How could a student have cheated?