CS/Math 240: Introduction to Discrete Mathematics	8/6/2007

Exam 2 - Sample Exam

Instructor: Jeff Kinne — TA: Mike Kowalczyk

The exam will be closed-notes and no calculators will be allowed. You will be allowed a 4x6 inch index card cheat sheet. This sample exam is much longer than the actual exam will be.

1. In this problem, you prove Boole's inequality.

   (a) Show that for any events E_1 and E_2 of a random experiment, $\Pr[E_1 \cup E_2] \leq \Pr[E_1] + \Pr[E_2]$.

   (b) Use induction to show that this holds for any finite number of events. That is, let $E_1, E_2, ..., E_n$ be any events. Prove by induction that

   $$\Pr[E_1 \cup E_2 \cup ... \cup E_n] \leq \Pr[E_1] + \Pr[E_2] + ... + \Pr[E_n].$$

2. Consider the experiment of rolling 5 independent 6-sided dice. What is the probability none of the dice ever come up even?

3. Consider rolling either two or three independent 6-sided dice. Is it more likely to roll a total of 8 when rolling two dice or three dice?

4. Consider flipping n independent fair coins. What is the probability that at some point there are at least 2 heads in a row?

5. Consider the situation where we view each person's birthday as having an equal chance of being on any of the 366 days in the year. Determine a formula for the probability that if n people enter a room, at least one of them has a birthday today.

6. Consider the situation where we view each person's birthday as having an equal chance of being on any of the 366 days in the year. Determine a formula for the probability that if n people enter a room, at least two of them have a birthday today.

7. Consider the experiment of rolling n fair dice. Compute the expected number of dice that come up even.

8. Show that for any random variable X and non-empty event E, $E[X] = \Pr[E] \cdot E[X|E] + \Pr[\overline{E}] \cdot E[X|\overline{E}]$, where $E[X|E]$ is defined as $E[X|E] = \sum_{\text{possible values } r \text{ of } X} r \cdot \Pr[X = r|E]$.

9. Consider the following randomized algorithm for determining if an integer is prime.

   Is-Prime
   Input: integer n that is at least 2
   Output: "yes" iff n is prime

   Let $S = \{2, 3, ..., \lfloor\sqrt{n}\rfloor\}$.
   while S is non-empty
       Pick a number k at random from S.
       if $k|n$ **then** return "no"
           else remove k from S
   return "yes"

   You may take for granted that this algorithm is correct. We will analyze the running time of this algorithm when the input is a product of two primes, so let $n = p_1 \cdot p_2$ where $p_1 \leq p_2$ and both p_1 and p_2 are primes. Let X be the number of iterations of the while loop when running the algorithm on input $n = p_1 \cdot p_2$.

   (a) What are the possible values for X? What is the probability of occurring for each?

   (b) Compute $E[X]$.

   (c) Use Markov's inequality to give an upper bound for the probability that $X \geq \sqrt{n} - 10$.

10. For this problem, we consider the situation of randomly guessing on an exam. Suppose you are taking a 10 question multiple choice exam, where each question has 4 possible answers. For each question, you pick your answer completely randomly from the 4 choices.

    (a) For each value $i = 0, 1, 2, ..., 10$, compute the probability that you get i questions right on the exam.

    (b) Compute the expected number of answers you get right on the exam.

    (c) If 60% is a passing grade, what is the probability you pass the exam?

11. Consider a drug test with the following properties. If you have used the drug recently, the test is positive with probability 95%. If you have not used the drug recently, the test is positive with probability 1%. And approximately 0.5% of the population uses the drug (has used the drug recently).

    Compute the probability that you have used the drug recently given the fact that you have taken the test and it came back negative (indicating an absence of the drug in your system).

12. In this problem, you use the Chinese remainder theorem to compute $2^{10} \pmod{35}$. Note that $2^{10} = 1024$.

    (a) Compute $2^{10} \pmod 5$ and $2^{10} \pmod 7$.

    (b) Now use the Chinese remainder theorem to determine $2^{10} \pmod{35}$.

13. Use the Euclidean algorithm to show that 100 and 77 are relatively prime.

14. Show that for any integers a and b, if $a|b$ and $b|a$ then either $a = b$ or $a = -b$.

15. Give an example of integers a and m so that a does not have a multiplicative inverse (mod m).

16. List all integers that are $\equiv 5 \pmod{17}$.

17. List all integers less than 36 that are relatively prime with 36.

18. Show that 15 is a multiplicative inverse of 7 modulo 26.

19. Use Fermat's little theorem to show that 33 is not prime.

20. In this problem, we consider the task of finding a 1000 bit prime number.

   (a) Using the prime number theorem, give a formula estimating the probability of a random 1000 bit integer being prime.

   (b) Assume that we have an algorithm that determines whether a given integer is prime or not. We aim to find a prime that is about 1000 bits long by randomly picking integers that are about this size until we find one that is prime. Give an estimate for the expected number of trials needed before finding a prime.

   Hint: use the geometric distribution.

   (c) Use Markov's inequality to give a formula that is an upper bound on the probability that at least 10,000 trials are needed.