Chris Piech
CS109

Homework #1
April 5, 2017

Problem Set #1
Due: 10:30am on Friday, April 14th

For each problem, briefly explain/justify how you obtained your answer. Brief explanations of your answer are necessary to get full credit for a problem even if you have the correct numerical answer. The explanations help us determine your understanding of the problem whether or not you got the correct answer. Moreover, in the event of an incorrect answer, we can still try to give you partial credit based on the explanation you provide. It is fine for your answers to include summations, products, factorials, exponentials, or combinations; you don't need to calculate those all out to get a single numeric answer.

Note: all assignment submissions will be made online. If you handwrite your solutions, you are responsible for making sure that you can produce clearly legible scans of them for submission. You may optionally use any word processing software you like for writing up your solutions. On the CS109 webpage we provide a template file and tutorial for the LaTex system.

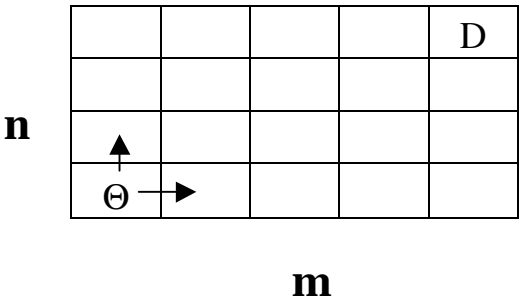
1. Many modern encryption algorithms are based on products of prime numbers. The key insight is that, for a large number N which is the product of 2 or more prime numbers, it is infeasible to factorize N into those prime numbers. An efficient algorithm to do so would break most of the internet (lookup RSA for more details)! For this problem, assume that there are *k* prime numbers less than N.
   a. How many ways are there of choosing two prime numbers less than N (note: the two prime numbers may be the same)?
   b. How many ways are there of choosing *r* prime numbers less than N (any of which may be the same)?
   c. How many ways are there of choosing *r* **distinct** prime numbers less than N?

2. A substitution cypher is derived from orderings of the alphabet. How many ways can the 26 letters be ordered if each letter appears exactly once and:
   a. There are no other restrictions?
   b. The letters Q and U must be next to each other (but in any order)?
   c. There are 5 vowels and no two vowels can be next to each other?
   d. There are 5 vowels and they must be next to each other?
   e. The position of the three most common letters (E, T and A) are fixed?

3. You are counting cards in a card game that uses **four** standard decks of cards. There are 208 cards total. Each deck has 52 cards (13 values each with 4 suits). Cards are only distinguishable based on their suit and value, not which deck they came from.
   a. In how many distinct ways can the cards be ordered?
   b. You are dealt two cards. How many distinct pairs of cards can you be dealt (the order of the two cards you are dealt does not matter)?
   c. You are dealt two cards. Cards with values 10, Jack, Queen, King and Ace are considered "good" cards. How many ways can you get two "good" cards?

Errata: the wording of question (b) has been updated for clarity

4. Imagine you have a robot (Θ) that lives on an ***n*** x ***m*** grid (it has n rows and m columns):



The robot starts in cell (1, 1) and can take steps either to the right or up (no left or down steps). How many distinct paths can the robot take to the destination in cell (n, m):
   a. If there are no additional constraints?
   b. The robot must start by moving to the right?
   c. If the robot changes direction exactly 3 times? As an example: moving up two times in a row is not changing directions but switching from moving up to moving right is. Moving [Up, Right, Right, Up] would count as having two direction switches.

5. Given all the start-up activity going on in high-tech, you realize that applying combinatorics to investment strategies might be an interesting idea to pursue. Say you have $20 million that must be invested among 4 possible companies. Each investment must be in integral units of $1 million, and there are minimal investments that need to be made if one is to invest in these companies. The minimal investments are $1, $2, $3, and $4 million dollars, respectively for company 1, 2, 3, and 4. How many different investment strategies are available if
   a. an investment must be made in each company?
   b. investments must be made in at least 3 of the 4 companies?

6. Determine the number of vectors $(x_1, x_2, \ldots, x_n)$ such that each x_i is a non-negative integer and $\sum_{i=1}^{n} x_i \le k$, where k is some constant non-negative integer. Note that you can think of n (the size of the vector) as a constant that can be used in your answer.

7. In how many ways can n identical server requests ("identical balls") be distributed among r servers ("urns") so that the ith server receives at least m_i requests, for each $i = 1, 2, \ldots, r$? You can assume that $n \ge \sum_{i=1}^{r} m_i$.

8. If we assume that all possible poker hands (comprised of 5 cards from a standard 52 card deck) are equally likely, what is the probability of being dealt:
   a. a flush? (A hand is said to be a flush if all 5 cards are of the same suit. Note that this definition means that *straight flushes* (five cards of the same suit in numeric sequence) are also considered flushes.)

b. one pair? (This occurs when the cards have numeric values a, a, b, c, d, where a, b, c, and d are all distinct.)
c. two pairs? (This occurs when the cards have numeric values a, a, b, b, c, where a, b and c are all distinct.)
d. three of a kind? (This occurs when the cards have numeric values a, a, a, b, c, where a, b and c are all distinct.)
e. four of a kind? (This occurs when the cards have numeric values a, a, a, a, b.)

9. Say we roll a fair 6-sided die six times, what is the probability that:
   a. we will roll three different numbers, *twice* each?
   b. we will roll some number *exactly* 4 times?

10. To get good performance when working binary search trees (BST), we must consider the probability of producing completely degenerate BSTs (where each node in the BST has at most one child). See Handout #2, Example 7 for more details on binary search trees.
    a. If the integers 1 through n are inserted in arbitrary order into a BST (where each possible order is equally likely), what is the probability (as an expression in terms of n) that the resulting BST will have completely degenerate structure?
    b. Using your expression from part (a), determine the smallest value of n for which the probability of forming a completely degenerate BST is less than 0.01 (i.e., 1%).

11. Say a hacker has a list of n distinct password candidates, only one of which will successfully log her into a secure system.
    a. If she tries passwords from the list at random, deleting those passwords that do not work, what is the probability that her first successful login will be (exactly) on her k-th try?
    b. Now say the hacker tries passwords from the list at random, but does **not** delete previously tried passwords from the list. She stops after her first successful login attempt. What is the probability that her first successful login will be (exactly) on her k-th try?

12. Say a university is offering 3 programming classes: one in Java, one in C++, and one in Python. The classes are open to any of the 100 students at the university. There are:
    - a total of 27 students in the Java class
    - a total of 26 students in the C++ class
    - a total of 18 students in the Python class
    - 12 students in both the Java and C++ classes
    - 5 students in both the Java and Python classes
    - 7 students in both the C++ and Python classes
    - 3 students in all three classes (note: these students are also counted as being in each pair of classes in the numbers above).

    a. If a student is chosen randomly at the university, what is the probability that he or she is not in any of the 3 programming classes?
    b. If a student is chosen randomly at the university, what is the probability that he or she is taking *exactly one* of the three programming classes?
    c. If two students are chosen randomly at the university, what is the probability that at least one of the chosen students is taking at least one programming class?

13. A binary string containing M 0's and N 1's (in arbitrary order, where all orderings are equally likely) is sent over a network. What is the probability that the first r bits of the received message contain exactly k 1's?

14. A computer generates two random integers in the range 1 to 12, inclusive, where each value in the range 1 to 12 is equally likely to be generated. What is the probability that the second randomly generated integer has a value that is greater than the first?

15. Suppose that m strings are hashed (randomly) into N buckets, assuming that all N^m arrangements are equally likely. Find the probability that exactly k strings are hashed to the first bucket.