CS 70 Discrete Mathematics and Probability Theory
Summer 2021

HW 3

Due: Sunday 7/18, 10:00 PM
Grace period until Sunday 7/18, 11:59 PM

Sundry

Before you start writing your final homework submission, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Lagrange? More like Lamegrange.

In this problem, we walk you through an alternative to Lagrange interpolation.

(a) Let's say we wanted to interpolate a polynomial through a single point, (x_0, y_0). What would be the polynomial that we would get? (This is not a trick question.)

(b) Call the polynomial from the previous part $f_0(x)$. Now say we wanted to define the polynomial $f_1(x)$ that passes through the points (x_0, y_0) and (x_1, y_1). If we write $f_1(x) = f_0(x) + a_1(x - x_0)$, what value of a_1 causes $f_1(x)$ to pass through the desired points?

(c) Now say we want a polynomial $f_2(x)$ that passes through (x_0, y_0), (x_1, y_1), and (x_2, y_2). If we write $f_2(x) = f_1(x) + a_2(x - x_0)(x - x_1)$, what value of a_2 gives us the desired polynomial?

(d) Suppose we have a polynomial $f_i(x)$ that passes through the points (x_0, y_0), ..., (x_i, y_i) and we want to find a polynomial $f_{i+1}(x)$ that passes through all those points and also (x_{i+1}, y_{i+1}). If we define $f_{i+1}(x) = f_i(x) + a_{i+1} \prod_{j=0}^{i} (x - x_j)$, what value must a_{i+1} take on?

2 Polynomials over Galois Fields

Real numbers, complex numbers, and rational numbers are all examples of *fields*. A field is a set of numbers that has some nice properties over some operations. Galois fields are fields with only a finite number of elements, unlike fields such as the real numbers. Galois fields are denoted by GF(q), where q is the number of elements in the field.

(a) In the field GF(p), where p is a prime, how many roots does $q(x) = x^p - x$ have? Use this fact to express $q(x)$ in terms of degree one polynomials. Justify your answers.

(b) Prove that in GF(p), where p is a prime, whenever $f(x)$ has degree $\geq p$, it is equivalent to some polynomial $\tilde{f}(x)$ with degree $< p$.

(c) Show that if P and Q are polynomials over the reals (or complex numbers, or rationals) and $P(x)Q(x) = 0$ for all x, then either $P(x) = 0$ for all x, $Q(x) = 0$ for all x, or both.

(d) Show that the claim in part (c) is false for finite fields GF(p), where p is a prime.

3 How Many Polynomials?

Let $P(x)$ be a polynomial of degree at most 2 over GF(5). As we saw in lecture, we need $d+1$ distinct points to determine a unique d-degree polynomial, so knowing the values for say, $P(0)$, $P(1)$, and $P(2)$ would be enough to recover P. (For this problem, we consider two polynomials to be distinct if they return different values for any input.)

(a) Assume that we know $P(0) = 1$, and $P(1) = 2$. Now consider $P(2)$. How many values can $P(2)$ have? How many distinct possibilities for P do we have?

(b) Now assume that we only know $P(0) = 1$. We consider $P(1)$ and $P(2)$. How many different $(P(1), P(2))$ pairs are there? How many distinct possibilities for P do we have?

(c) Now, let P be a polynomial of degree at most d on GF(p) for some prime p with $p > d$. Assume we only know P evaluated at $k \leq d+1$ different values. How many different possibilities do we have for P?

(d) A polynomial with integer coefficients that cannot be factored into polynomials of lower degree on a finite field, is called an irreducible or prime polynomial.

Show that $P(x) = x^2 + x + 1$ is a prime polynomial on GF(5).

4 Counting, Counting, and More Counting

The only way to learn counting is to practice, practice, practice, so here is your chance to do so. Although there are many subparts, each subpart is fairly short, so this problem should not take any longer than a normal CS70 homework problem. You do not need to show work, and **Leave your answers as an expression** (rather than trying to evaluate it to get a specific number).

(a) How many ways are there to arrange n 1s and k 0s into a sequence?

(b) How many 7-digit ternary (0,1,2) bitstrings are there such that no two adjacent digits are equal?

(c) A bridge hand is obtained by selecting 13 cards from a standard 52-card deck. The order of the cards in a bridge hand is irrelevant.

i. How many different 13-card bridge hands are there? ii. How many different 13-card bridge hands are there that contain no aces? iii. How many different 13-card bridge hands are there that contain all four aces? iv. How many different 13-card bridge hands are there that contain exactly 6 spades?

(d) Two identical decks of 52 cards are mixed together, yielding a stack of 104 cards. How many different ways are there to order this stack of 104 cards?

(e) How many 99-bit strings are there that contain more ones than zeros?

(f) An anagram of ALABAMA is any re-ordering of the letters of ALABAMA, i.e., any string made up of the letters A, L, A, B, A, M, and A, in any order. The anagram does not have to be an English word.
i. How many different anagrams of ALABAMA are there? ii. How many different anagrams of MONTANA are there?

(g) How many different anagrams of ABCDEF are there if: (1) C is the left neighbor of E; (2) C is on the left of E (and not necessarily E's neighbor)

(h) We have 9 balls, numbered 1 through 9, and 27 bins. How many different ways are there to distribute these 9 balls among the 27 bins? Assume the bins are distinguishable (e.g., numbered 1 through 27).

(i) How many different ways are there to throw 9 identical balls into 27 bins? Assume the bins are distinguishable (e.g., numbered 1 through 27).

(j) We throw 9 identical balls into 7 bins. How many different ways are there to distribute these 9 balls among the 7 bins such that no bin is empty? Assume the bins are distinguishable (e.g., numbered 1 through 7).

(k) There are exactly 20 students currently enrolled in a class. How many different ways are there to pair up the 20 students, so that each student is paired with one other student? Solve this in at least 2 different ways. **Your final answer must consist of two different expressions.**

(l) How many solutions does $x_0 + x_1 + \cdots + x_k = n$ have, if each x must be a non-negative integer?

(m) How many solutions does $x_0 + x_1 = n$ have, if each x must be a *strictly positive* integer?

(n) How many solutions does $x_0 + x_1 + \cdots + x_k = n$ have, if each x must be a *strictly positive* integer?

5 Functional Counting

In each of the following questions, assume that n is a positive integer.

(a) How many strictly increasing functions are there from the set $\{1,2,\ldots,n-1,n\}$ to the set $\{1,2,\ldots,2n-1,2n\}$?

(b) How many surjective functions are there from the set $\{1,2,\ldots,2n-1,2n\}$ to the set $\{1,2,\ldots,n-1,n\}$?

6 Good Khalil Hunting

As a sidejob, Khalil is also working as a janitor in Berkeley EECS. One day, he notices a problem on the board and decides to solve it. The problem is as follows: **Find all homeomorphically irreducible trees having 10 vertices.** A tree is homeomorphically irreducible if it has no vertices of degree 2. Assume all vertices and edges are indistinguishable from another.

Let's help Khalil solve this using strategic **casework**. We will partition the problem based off the number of the leaves in the tree. For sake of clarity, label the vertices $v_1, \ldots, v_{10}$ and their degrees $d_1, \ldots, d_{10}$ in decreasing order of degree.

(a) Show that the number of leaves, ℓ, we can have is $6 \leq \ell \leq 9$. (*Hint*: What do you know about the degrees of a leaf? What about a non-leaf in this case?)

For the following parts, drawings are neither necessary nor sufficient for your answer, but are highly encouraged to help you get the answer. Please briefly justify your answers by formulating equations involving the degrees of the vertices, along with short explanations.

(b) How many 10 vertex, homeomorphically irreducible trees of 9 leaves are there? Justify your answer.

(c) How many 10 vertex, homeomorphically irreducible trees of 8 leaves are there? Justify your answer.

(d) How many 10 vertex, homeomorphically irreducible trees of 7 leaves are there? Justify your answer.

(e) How many 10 vertex, homeomorphically irreducible trees of 6 leaves are there? Justify your answer.

In total, you should have counted 10 trees. Great work!

7 Proofs of the Combinatorial Variety

Prove each of the following identities using a combinatorial proof.

(a) For every positive integer $n > 1$,

$$\sum_{k=0}^{n} k \cdot \binom{n}{k} = n \cdot \sum_{k=0}^{n-1} \binom{n-1}{k}.$$

(b) For each positive integer m and each positive integer $n > m$,

$$\sum_{a+b+c=m} \binom{n}{a} \cdot \binom{n}{b} \cdot \binom{n}{c} = \binom{3n}{m}.$$

(Notation: the sum on the left is taken over all triples of nonnegative integers (a, b, c) such that $a + b + c = m$.)