Math 96:
Polynomials Techniques

October 18th, 2024

1 Introduction

A polynomial in one variable is a function of the form $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ for some constants $a_0, a_1, \ldots, a_n$. More generally, a polynomial in several variables is a function $f(x_1, \ldots, x_k)$ that is a sum of monomials, that is functions of the form $cx_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}$ for c some constant and e_i non-negative integers. These functions show up in many places and are popular both as topics of questions and tools that can be used in problem solving.

2 Factorization and Roots

Like with integers, polynomials exhibit a form of unique factorization. In particular, if you have a polynomial f whose coefficients lie in $\mathbb{Z}$ or $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$ (or any other field or unique factorization domain) in any number of variables, then f can always be written as a product of *irreducibles*, that is polynomials that cannot be written as a product of two non-constant polynomials, with coefficients in the same ring as f. Furthermore, this factorization is unique up to reordering the factors and multiplying the factors by constants.

This factorization is particularly interesting for univariate polynomials. A polynomial $f(x)$ has a root at r if $f(r) = 0$. It is not hard to show that this happens if and only if $(x-r)$ is a factor of f. This implies for example that if $f(x)$ is of degree-d (i.e. the largest power of x with a non-zero coefficient is d), then f can have at most d roots (since it can admit at most d linear factors). This is particularly interesting over $\mathbb{C}$, where the *Fundamental Theorem of Algebra* says that every polynomial f factors into linear factors. Furthermore, over $\mathbb{R}$, every polynomial factors into linear and quadratic factors.

1999 A2: Let $p(x)$ be a polynomial that is nonnegative for all real x. Prove that for some k, there are polynomials $f_1(x), \ldots, f_k(x)$ such that

$$p(x) = \sum_{j=1}^{k} (f_j(x))^2.$$

3 Equality Testing

The fact that a nonzero univariate polynomial of degree at most d can have at most d roots can be quite powerful. In particular, this tells us that if f is a polynomial of degree at most d with *more* than d roots, then f must be uniquely the zero polynomial. More generally, if f and g are two polynomials of degree at most d and if we can find values $x_1, x_2, \ldots, x_{d+1}$ where $f(x_i) = g(x_i)$ for each i, then applying the above result to $f - g$, we can conclude that f and g must be identically the same. But verifying that f and g agree at these $d+1$ points, you can show that f and g agree. This is particularly useful as you can often pick these points to make the evaluation easier.

This kind of thinking can also often be generalized to polynomials in multiple variables. The idea being that by finding ways to evaluate at certain points or evaluate certain coefficients one can often determine what the polynomial in question is without ever having to carefully evaluate it.

1984 A3: Let n be a positive integer. Let a, b, x be real numbers, with $a \neq b$, and let M_n denote the $2n \times 2n$ matrix whose (i, j) entry $m_{i,j}$ is given by

$$m_{i,j} = \begin{cases} x & \text{if } i = j \\ a & \text{if } i \neq j \text{ and } i + j \text{ is even} \\ b & \text{if } i \neq j \text{ and } i + j \text{ is odd.} \end{cases}$$

Thus, for example, $M_2 = \begin{pmatrix} x & b & a & b \\ b & x & b & a \\ a & b & x & b \\ b & a & b & x \end{pmatrix}$. Express $\lim_{x \to a} \det M_n/(x-a)^{2n-2}$ as a polynomial in a, b, and n, where $\det M_n$ denotes the determinant of M_n.

4 Finite Differences

Let $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_d x^d$ be a degree-d univariate polynomial. Consider the finite difference $f(x+n) - f(x)$ for some non-zero number n. By the Binomial Theorem this is

$$\sum_{i=0}^{d} a_i \sum_{j=0}^{i} x^j n^{i-j} \binom{i}{j} - \sum_{i=0}^{d} a_i x^i = \sum_{i=0}^{d} a_i \sum_{j=0}^{i-1} x^j n^{i-j} \binom{i}{j}.$$

In particular, note that the highest degree, x^d terms here cancel out, leading to a polynomial with degree $d-1$, and leading coefficient dna_d. It is also possible (though somewhat more cumbersome) to track the next few highest coefficients. This is a very useful thing to know, especially when one repeatedly takes such finite differences until the resulting polynomial becomes a constant.

1984 B5: For each nonnegative integer k, let $d(k)$ denote the number of 1's in the binary expansion of k (for example $d(0) = 0$ and $d(5) = 2$). Let m be a positive integer. Express

$$\sum_{k=0}^{2^m-1} (-1)^{d(k)} k^m$$

in the form $(-1)^m a^{f(m)}(g(m))!$, where a is an integer and f and g are polynomials.

5 The Intermediate Value Theorem

One nice way to prove the existence of roots of a polynomial is by the intermediate value theorem. In particular, if we can find points where the polynomial is positive and negative, we know that there must be a root somewhere in between.

2014 B4: Show that for each positive integer n, all the roots of the polynomial

$$\sum_{k=0}^{n} 2^{k(nk)} x^k$$

are real numbers.