Math 96:
Polynomials Techniques

October 27th, 2023

1 Introduction

A polynomial in one variable is a function of the form $f(x) = \sum_{i=0}^{n} a_i x^i$ for some constants a_i (called the coefficients) taken from some ring (like $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$). The degree of such a polynomial is the largest k so that $a_k \neq 0$.

A multivariate polynomial is a function of several variables $x_1, x_2, \ldots, x_n$ that can be written as a finite sum of monomials, where each monomial is a product of powers of the x_i's times some coefficient.

Given two polynomials you can add or multiply them, using basic algebra to simplify the result. Also, given a polynomial and some values for its variables, you can evaluate the polynomial at those values.

2 Roots and Factorization

Consider the collection of polynomials in variables $x_1, \ldots, x_n$ with coefficients in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$ (or more generally any field or unique factorization domain). Such a polynomial f is called *irreducible* if it cannot be written as a product of two other polynomials $f = gh$ unless either g or h is a constant. Much like integers, such polynomials have unique factorization. In particular any such polynomial can be written as a product of irreducibles, and this representation is unique up to (i) reordering the factors and (ii) multiplying the factors by constants.

This is particularly relevant for univariate polynomials. In particular r is a root of a polynomial f (meaning that $f(r) = 0$) if and only if $(x - r)$ is a factor of $f(x)$. This has a number of consequences, including importantly the fact that a degree-d polynomial has at most d roots. The *Fundamental Theorem of Algebra* says that any univariate polynomial over $\mathbb{C}$ factors into linear factors, while any polynomial over $\mathbb{R}$ factors into linear and quadratic factors.

1963 B1: For what integers a does $x^2 - x + a$ divide $x^{13} + x + 90$?

3 Identity Testing

The previous fact that a univariate polynomial of degree d has at most d roots is actually quite important. In particular, if f and g are two univariate polynomials of degree at most d and you want to show that $f(x) = g(x)$, you can do this by showing that $f(x_i) = g(x_i)$ for at least $d+1$ different values of x_i. This would mean that $(f - g)$ is a degree at most d polynomial with more than d roots, which is only possible if it is identically 0.

1978 A2: Let $a, b, p_1, \ldots, p_n$ be real numbers with $a \neq b$. Define $f(x) = (x - p_1)(x - p_2)(x - p_3)\cdots(x - p_n)$. Show that

$$\det \begin{bmatrix} p_1 & a & a & a & \cdots & a & a \\ b & p_2 & a & a & \cdots & a & a \\ b & b & p_3 & a & \cdots & a & a \\ b & b & b & p_4 & \cdots & a & a \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ b & b & b & b & \cdots & p_{n-1} & a \\ b & b & b & b & \cdots & b & p_n \end{bmatrix} = \frac{bf(a) - af(b)}{b - a}.$$

4 Roots, Coefficients, and Symmetric Polynomials

Suppose that a polynomial $p(x)$ factors completely as $p(x) = (x - r_1)(x - r_2)\cdots(x - r_n)$. How do the roots $r_1, r_2, \ldots, r_n$ of p relate to its coefficients?

Well expanding p out we find that $p(x) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + \ldots + (-1)^n \sigma_n$ where σ_t is the tth elementary symmetric polynomial in the roots. That is the sum of every possible product of t of the r_i's. In particular σ_1 is the sum of the roots and σ_n is their product.

The elementary symmetric polynomials are also quite useful for other reasons. In particular the *Fundamental Theorem of Symmetric Polynomials* says that any symmetric polynomial in $r_1, \ldots, r_n$ (that is a polynomial that stays the same if you switch two of the r_i's) is a polynomial in the elementary symmetric polynomials. Furthermore, if the symmetric polynomial in question has integer coefficients, so does the way of writing it in terms of the elementary symmetric polynomials.

1968 A6: Determine all polynomials of the form $\sum_{i=0}^{n} a_I x^{n-i}$ with $a_i = \pm 1$ $(0leqi \leq n, 1 \leq n < \infty)$ such that each has only real zeroes.

5 Polynomial Interpolation

Our discussion of identity testing implies that a univariate polynomial of degree-d is determined by its values at any $d+1$ points. It turns out, that given these values it is not too hard to find the polynomial. In particular, suppose that $p(x_i) = y_i$ for all $i = 1, 2, \ldots, d+1$. You can show that

$$p(x) = \sum_{i=1}^{d+1} y_i \prod_{j \neq i} \frac{(x - x_j)}{(x_i - x_j)}.$$

This is because it is not hard to show that for the above p that $p(x_i) = y_i$ for all i. Given this, this is the only polynomial that takes those values at those points.

2008 A5: Let $n \geq 3$ be an integer. Let $f(x)$ and $g(x)$ be polynomials with real coefficients such that the points $(f(1), g(1)), (f(2), g(2)), \ldots, (f(n), g(n))$ in $\mathbb{R}^2$ are the vertices of a regular n-gon in counterclockwise order. Prove that at least one of $f(x)$ and $f(x)$ has degree greater than or equal to $n-1$.