CS 70 Spring 2006 | Discrete Mathematics for CS Vazirani | Lecture 11

Polynomials

You are all familiar with polynomials of the form $p(x) = a_0x^d + a_1x^{d-1} + \ldots + a_d$, where the coefficients a_i and the variable x are real numbers (or perhaps rationals or complex numbers). In this lecture we will review some of the fundamental properties of polynomials, as well as the crucial properties of real numbers (and rationals and complex numbers) that are used to prove these properties.

Property 1: A non-zero polynomial of degree d has at most d roots.

Property 2: Given $d+1$ pairs $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$, there is a unique polynomial $p(x)$ of degree d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

Moreover, in property 2, there is an efficient algorithm for determining the polynomial $p(x)$. Let us sketch two different ways this can be done:

In the first method, we write a system of $d+1$ linear equations in $d+1$ variables: the coefficients of the polynomial $a_0, \ldots, a_d$. The i^{th} equation is: $a_0x_i^d + a_1x_i^{d-1} + \ldots + a_0 = y_i$.

Since x_i and y_i are constants, the this is a linear equation in the $d+1$ unknowns $a_0, \ldots, a_d$. Now solving these equations gives the coefficients of the polynomial $p(x)$. To do this carefully, we must show that the equations do have a solution and that it is unique. This involves showing that a certain determinant is non-zero. We will leave that as an exercise, and turn to the second method.

Here is the second method for determining the polynomial $p(x)$: Suppose we could write down $d+1$ different polynomials each of degree d as follows:

$$\Delta_i(x) = 1 \text{ if } x = x_i, \text{and } 0 \text{ if} x = x_j, j \neq i$$

Then we can write $p(x) = \sum_{i=1}^{d+1} y_i \Delta_i(x)$.

The polynomial $\Delta_i(x)$ is easy to write down. It is simply $\Delta_i(x) = \frac{\Pi j \neq i (x - x_j)}{\Pi j \neq i (x_i - x_j)}$

How do we show that $p(x)$ is the unique polynomial that satisfies these $d+1$ conditions? Suppose for contradiction that there is another polynomial $q(x)$ that satisfies the $d+1$ conditions as well. Now consider the polynomial $r(x) = p(x) - q(x)$. This is a non-zero polynomial of degree d. So by property 1 it can have at most d roots. But on the other hand $r(x_i) = p(x_i) - q(x_i) = 0$ on $d+1$ distinct points. Contradiction. Therefore $p(x)$ is the unique polynomial that satisfies the $d+1$ conditions.

Now let us turn to property 1. To prove this property we first show that a is root of $p(x)$ iff $(x-a)$ divides $p(x)$. The proof is simple: dividing $p(x)$ by $(x-a)$ gives $p(x) = (x-a)q(x) + r(x)$, where $q(x)$ is the quotient and $r(x)$ is the remainder. The degree of $r(x)$ is necessarily smaller than the degree of the divisor $(x-a)$. Therefore $r(x)$ must have degree 0 and therefore is some constant c. But now substituting $x = a$, we get $p(a) = c$. But since a is a root, $p(a) = 0$. Thus $c = 0$ and therefore $p(x) = (x-a)q(x)$, thus showing that $(x-a)|p(x)$.

Now suppose that $a_1, \ldots, a_d$ are d distinct roots of $p(x)$. Let us show that $p(x)$ can have no other roots. We will show that $p(x) = c(x-a_1)(x-a_2)\cdots(x-a_d)$. Now if $p(a) = c(a-a_1)(a-a_2)\cdots(a-a_d) \neq 0$ if $a \neq a_i$

for all i.

To show that $p(x) = c(x-a_1)(x-a_2)\cdots(x-a_d)$, we start by observing that $p(x) = (x-a_1)q_1(x)$ for some polynomial $q_1(x)$ of degree $d-1$, since a_1 is a root. But now $0 = p(a_2) = (a_2-a_1)q_1(a_2)$ since a_2 is a root. But since $a_2 - a_1 \neq 0$, it follows that $q_1(a_2) = 0$. So $q_1(x) = (x-a_2)q_2(x)$, for some polynomial $q_2(x)$ of degree $d-2$. Proceeding in this manner by induction (do this formally!), we get that $p(x) = (x-a_1)(x-a_2)\cdots(x-a_d)q_d(x)$ for some polynomial $q_d(x)$ of degree 0, thus showing what we want. This completes the proof that a polynomial of degree d has at most d roots.

0.1 Finite Fields

Why did we assume that the coefficients and variables in a polynomial ranged over the reals or rationals or complex numbers? This is because we need the operations of $+,-,x,\div$. In particular, we need the property that we can divide by any non-zero number. Sets of numbers which satisfy these properties are called fields.

But for our applications, we want all these properties of polynomials to hold, but we want the coefficients and variables to range only over a finite set of values. One way to achieve this is to choose some prime number m, a and work with numbers modulo m. So now there are only m different choices for any coefficient or for x $(0,1,\ldots,m-1)$. But we can still add, subtract, multiply and divide by any non-zero value. It turns out that the proofs of both the properties above continue to hold while working modulo m.

Let us briefly consider what would go wrong if we chose m not to be prime, for example $m = 6$. Now we can no longer divide by 2 or 3. In the proof of property 1, we asserted that $p(a) = c(a-a_1)(a-a_2)\cdots(a-a_d) \neq 0$ if $a \neq a_i$ for all i. But if we were working modulo 6, and if $a-a_1 = 2$ and $a-a_2 = 3$, each non-zero, but $(a-a_1)(a-a_2) = 2\cdot 3 = 0 \bmod 6$.

Secret Sharing

Suppose the U.S. government finally decides that a nuclear strike can be initiated only if at least $k > 1$ major officials agree to it (what a “major official” is doesn’t really matter to us). We want to devise a scheme such that (1) any group of k of these officials can pool their information to figure out the launch code and initiate the strike but (2) no group of $k-1$ or fewer can conspire to find the code. How can we accomplish this?

Suppose that there are n officials and that launch code is some natural number s. Let q be a prime number larger than n and s —we will work over $GF(q)$ from now on.

Now pick a random polynomial P of degree $k-1$ such that $P(0) = s$ and give the pair $(1,P(1))$ to the first official, $(2,P(2))$ to the second, …, $(n,P(n))$ to the nth. Then

- Any k officials, having the values of the polynomial at k points, can use Lagrange interpolation to find P, and once they know what P is, they can compute $P(0) = s$ to learn the secret.
- Any group of $k-1$ officials has no information about P. All they know is that there is a polynomial of degree $k-1$ passing through their $k-1$ points such that $P(0) = s$. However, for each possible value $P(0) = b$, there is a unique polynomial that is consistent with the information of the $k-1$ officials, and satisfies the constraint that $P(0) =$.