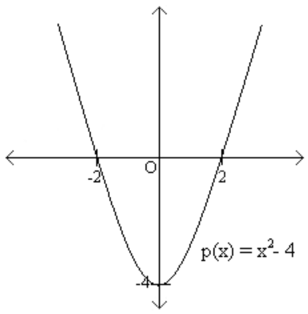
CS 70 Discrete Mathematics for CS
Fall 2006 Papadimitriou & Vazirani **Lecture 11**

Polynomials

Recall from your high school math that a polynomial in a single variable is of the form $p(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0$. Here the variable x and the coefficients a_i are usually real numbers. For example, $p(x) = 5x^3 + 2x + 1$, is a polynomial of degree $d = 3$. Its coefficients are $a_3 = 5$, $a_2 = 0$, $a_1 = 2$, and $a_0 = 1$. Polynomials have some remarkably simple, elegant and powerful properties, which we will explore in this lecture.

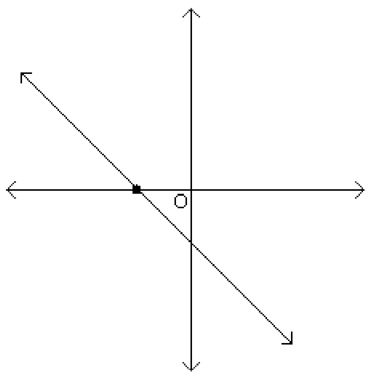
First, a definition: we say that a is a root of the polynomial $p(x)$ if $p(a) = 0$. For example, the degree 2 polynomial $p(x) = x^2 - 4$ has two roots, namely 2 and -2, since $p(2) = p(-2) = 0$. If we plot the polynomial $p(x)$ in the x-y plane, then the roots of the polynomial are just the places where the curve crosses the x axis:

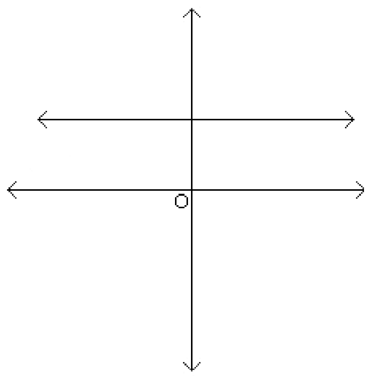


Property 1: A non-zero polynomial of degree d has at most d roots.

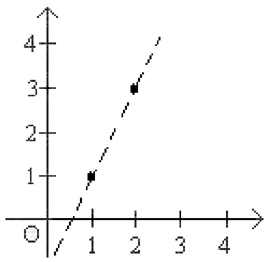
Property 2: Given $d+1$ pairs $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$, there is a unique polynomial $p(x)$ of degree (at most) d such that $p(x_i) = y_i$ for $1 \le i \le d+1$.

Let us consider what these two properties say in the case that $d = 1$. A graph of a linear (degree 1) polynomial $y = a_1 x + a_0$ is a line. Property 1 says that if a line is not the x-axis (i.e. if the polynomial is not $y = 0$), then it can intersect the x-axis in at most one point.





Property 2 says that two points uniquely determine a line.



Polynomial Interpolation

Property 2 says that two points uniquely determine a degree 1 polynomial (a line), three points uniquely determine a degree 2 polynomial, four points uniquely determine a degree 3 polynomial, ... Given $d+1$ pairs $(x_1,y_1),\ldots,(x_{d+1},y_{d+1})$, how do we determine a polynomial $p(x) = a_d x^d + \ldots + a_1 x + a_0$ such that $p(x_i) = y_i$ for $i = 1$ to $d+1$. We will give two different efficient algorithms for reconstructing the coefficients $a_0,\ldots,a_d$ and therefore the polynomial $p(x)$.

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: $a_d x_i^d + a_{d-1} x_i^{d-1} + \ldots + a_0 = y_i$.

Since x_i and y_i are constants, 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 $p(x)$. For example, given the 3 pairs $(-1,2)$, $(0,1)$, and $(2,5)$, we will construct the degree 2 polynomial $p(x)$ which goes through these points. The first equation says $a_2(-1)^2 + a_1(-1) + a_0 = 2$. Simplifying, we get $a_2 - a_1 + a_0 = 2$. Applying the same technique to the second and third equations, we get the following system of equations:

$$\begin{aligned} a_2 - a_1 + a_0 &= 2 \\ a_0 &= 1 \\ 4a_2 + 2a_1 + a_0 &= 5 \end{aligned}$$

Substituting for a_0 and multiplying the first equation by 2 we get:

$$\begin{aligned} 2a_2 - 2a_1 &= 2 \\ 4a_2 + 2a_1 &= 4 \end{aligned}$$

Then, adding down we find that $6a_2 = 6$, so $a_2 = 1$, and plugging back in we find that $a_1 = 0$. Thus, we have determined the polynomial $p(x) = x^2 + 1$. To do this method more 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.

The second method is called *Lagrange interpolation*: Let us start by solving an easier problem. Suppose that we are told that $y_1 = 1$ and $y_j = 0$ for $2 \le j \le d+1$. Now can we reconstruct $p(x)$? Yes, this is easy! Consider $q(x) = (x-x_2)(x-x_3)\cdots(x-x_{d+1})$. This is a polynomial of degree d (the x_i's are constants, and x appears d times). $q(x_j) = 0$ for $2 \le j \le d+1$. But what is $q(x_1)$? $q(x_1) = (x_1-x_2)(x_1-x_3)\cdots(x_1-x_{d+1})$, which is some constant not equal to 0. Thus if we let $p(x) = q(x)/q(x_1)$ (dividing is ok since $q(x_1) \neq 0$), we have the polynomial we are looking for. For example, suppose you were given the pairs $(1,1)$, $(2,0)$, and $(3,0)$. Then we can construct the degree $d = 2$ polynomial $p(x)$ by letting $q(x) = (x-2)(x-3) = x^2 - 5x + 6$, and $q(x_1) = q(1) = 2$. Thus, we can now construct $p(x) = q(x)/q(x_1) = (x^2 - 5x + 6)/2$.

Of course the problem is no harder if we single out some arbitrary index i instead of 1: i.e. $y_i = 1$ and $y_j = 0$ for $j \neq i$. Let us introduce some notation: let us denote by $\Delta_i(x)$ the degree d polynomial that goes through these $d+1$ points. Then $\Delta_i(x) = \frac{\Pi j \neq i (x - x_j)}{\Pi j \neq i (x_i - x_j)}$.

Let us now return to the original problem. Given $d+1$ pairs $(x_1,y_1),\ldots,(x_{d+1},y_{d+1})$, we first construct the $d+1$ polynomials $\Delta_1(x),\ldots,\Delta_{d+1}(x)$. Now we can write $p(x)=\sum_{i=1}^{d+1} y_i\Delta_i(x)$. Why does this work? First notice that $p(x)$ is a polynomial of degree d as required, since it is the sum of polynomials of degree d. And when it is evaluated at x_i, d of the $d+1$ terms in the sum evaluate to 0 and the *i-th* term evaluates to y_i times 1 as required.

If $d=2$, and $x_i=i$, for instance, then

$$\begin{aligned}
\Delta_1(x) &= \frac{(x-2)(x-3)}{(1-2)(1-3)} = \frac{(x-2)(x-3)}{2}\\
\Delta_2(x) &= \frac{(x-1)(x-3)}{(2-1)(2-3)} = \frac{(x-1)(x-3)}{-1}\\
\Delta_3(x) &= \frac{(x-1)(x-2)}{(3-1)(3-2)} = \frac{(x-1)(x-2)}{2}.
\end{aligned}$$

Uniqueness

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.

Property 1

Now let us turn to property 1. To prove this property we first show that a is a 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.

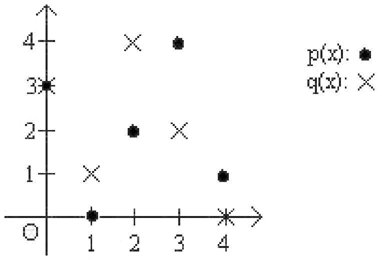
0.1 Finite Fields

Both property 1 and property 2 also hold when the values of the coefficients and the variable x are chosen from the complex numbers instead of the real numbers or even the rational numbers. They do not hold if the values are restricted to being natural numbers or integers. Let us try to understand this a little more closely. The only properties of numbers that we used in polynomial interpolation and in the proof of property 1 is that we can add, subtract, multiply and divide any pair of numbers as long as we are not dividing by 0. We cannot subtract two natural numbers and guarantee that the result is a natural number. And dividing two integers does not usually result in an integer.

But if we work with numbers modulo a prime m, then we can add, subtract, multiply and divide (by any non-zero number modulo m). So both property 1 and property 2 hold if the coefficients and the variable x are restricted to take on values modulo m. This remarkable fact that these properties hold even when we restrict ourselves to a *finite* set of values is the key to several applications that we will presently see. First, let's see examples of these properties holding in the case of degree $d = 1$ polynomials modulo 5. Consider the polynomial $p(x) = 4x+3 \pmod 5$. The roots of this polynomial are all values x such that $4x+3 \equiv 0 \pmod 5$ holds. Solving for x, we get that $4x \equiv 2 \pmod 5$, or $x \equiv 3 \pmod 5$. Thus, we found only 1 root for a degree 1 polynomial. Now, given the points $(0,3)$ and $(1,2)$, we will reconstruct the degree 1 polynomial $p(x)$ modulo 5. Using Lagrange interpolation, we get that $\Delta_1(x) = -(x-1)$, and $\Delta_2(x) = x$. Thus, $p(x) = (3)\Delta_1(x) + (2)\Delta_2(x) = -x+3 \equiv 4x+3 \pmod 5$.

When we work with numbers modulo a prime m, we are working over finite fields, denoted by F_m or GF_m (for Galois Field). In order for a set to be called a field, it must satisfy certain axioms which are the building blocks that allow for these amazing properties and others to hold. If you would like to learn more about fields and the axioms which a set must satisfy, you can visit Wikipedia's site and read the article on fields: `http://en.wikipedia.org/wiki/Field_%28mathematics%29`. While you are there, you can also read the article on Galois Fields and learn more about some of its applications and elegant properties which will not be covered in this lecture: `http://en.wikipedia.org/wiki/Galois_field`. These articles provide further insight into these incredible algebraic structures and discuss powerful facts which are often taken for granted.

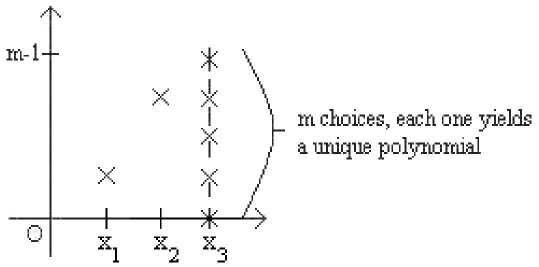
We said above that it is remarkable that properties 1 and 2 continue to hold when we restrict all values to a finite set modulo a prime number m. To see why this is remarkable let us see what the graph of a linear polynomial (degree 1) looks like modulo 5. There are now only 5 possible choices for x, and only 5 possible choices for y. Consider the polynomials $p(x) = 2x+3$ and $q(x) = 3x-2$ over GF_5. We can represent these polynomials on the x-y plane as follows:



Notice that these two "lines" intersect in exactly one point, even though the picture looks nothing at all like lines in the Euclidean plane. Modulo 5, two lines can still intersect in at most one point, and that is thanks to the properties of addition, subtraction, multiplication, and division modulo 5.

Counting

How many degree 2 polynomials are there modulo m? This is easy; there are 3 coefficients, each of which can take on m distinct values for a total of m^3. Now suppose we are given three pairs $(x_1,y_1),(x_2,y_2),(x_3,y_3)$, then by property 2, there is a unique polynomial of degree 2 such that $p(x_i) = y_i$ for $1 \le i \le 3$. Suppose we were only given two pairs $(x_1,y_1),(x_2,y_2)$; how many distinct degree 2 polynomials are there that go through these two points? Here is a slick way of working this out. Fix any x_3, and notice that there are exactly m choices for fixing y_3. Now with three points specified, by property 2 there is a unique polynomial of degree 2 that goes through these three points. Since this is true for each of the m ways of choosing y_3, it follows that there are m polynomials of degree at most 2 that go through 2 points, as shown below:



What if you were only given one point? Well, there are m choices for the second point, and for each of these there are m choices for the third point, yielding m^2 polynomials of degree at most 2 that go through the point given. A pattern begins to emerge, as is summarized in the following table:

Polynomials of degree $\leq d$ over F_m	
# of points	# of polynomials
$d+1$	1
d	m
$d-1$	m^2
$\vdots$	$\vdots$
$d-k$	m^{k+1}

The reason that we can now count the number of polynomials is because we are working over a finite field. If we were working over an infinite field such as the rationals, there would be infinitely many polynomials of degree d that can go through d points! Think of a line, which has degree one. If you were just given one point, there would be infinitely many possibilities for the second point, each of which uniquely defines a line.

Finally, you might wonder why we chose m to be a prime. 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 $(a-a_1)(a-a_2) = 2\cdot 3 = 0$ mod 6.

Secret Sharing

In the late 1950's and into the 1960's, during the Cold War, President Dwight D. Eisenhower approved instructions and authorized top commanding officers for the use of nuclear weapons under very urgent emergency conditions. Such measures were set up in order to defend the United States in case of an attack in which there was not enough time to confer with the President and decide on an appropriate response. This would allow for a rapid response in case of a Soviet attack on U.S. soil. This is a perfect situation in which a secret sharing scheme could be used to ensure that a certain number of officials must come together in order to successfully launch a nuclear strike, so that for example no single person has the power and control over such a devastating and destructive weapon. 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. 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 have any information about the launch code, even if they pool their knowledge. For example, they should not learn whether the secret is odd or even, a prime number, divisible by some number a, or the secret's least significant bit. How can we accomplish this?

Suppose that there are n officials indexed from 1 to n and the launch code is some natural number s. Let q be a prime number larger than n and s, where $0 \le s \le q-1$ —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 share $P(1)$ to the first official, $P(2)$ to the second, $\ldots$, $P(n)$ 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 $P(0) = b$.

Example. Suppose you are in charge of setting up a secret sharing scheme where you want to distribute $n = 5$ shares to 5 people such that any $k = 3$ or more people can figure out the secret, but 2 or fewer cannot. Let's say we are working over $GF(7)$ and you randomly choose the polynomial of degree $k-1 = 2 : P(x) = 3x^2 + 5x + 1$ (here, $P(0) = 1 = s$, the secret). So you know everything there is to know about the secret and the polynomial, but what about the people that receive the shares? Well, the shares handed out are $P(1) = 2$ to the first official, $P(2) = 2$ to the second, $P(3) = 1$ to the third, $P(4) = 6$ to the fourth, and $P(5) = 3$ to the fifth official. Let's say that officials 3, 4, and 5 get together (we expect them to be able to recover the secret). Using Lagrange interpolation, they compute the following delta functions:

$$
\begin{aligned}
\Delta_3(x) &= \frac{(x-4)(x-5)}{(3-4)(3-5)} = \frac{(x-4)(x-5)}{2} \\
\Delta_4(x) &= \frac{(x-3)(x-5)}{(4-3)(4-5)} = \frac{(x-3)(x-5)}{-1} \\
\Delta_5(x) &= \frac{(x-3)(x-4)}{(5-3)(5-4)} = \frac{(x-3)(x-4)}{2}.
\end{aligned}
$$

They then compute the polynomial over $GF(7)$: $P(x) = (1)\Delta_3(x) + (6)\Delta_4(x) + (3)\Delta_5(x) = 3x^2 + 5x + 1$ (verify the computation!). Now they simply compute $P(0)$ and discover that the secret is 1.

Let's see what happens if two officials try to get together, say persons 1 and 5. They both know that the polynomial looks like $P(x) = a_2x^2 + a_1x + s$. They also know the following equations:

$$
\begin{aligned}
P(1) &= a_2 + a_1 + s = 2 \\
P(5) &= 4a_2 + 5a_1 + s = 3
\end{aligned}
$$

But that is all they have, 2 equations with 3 unknowns, and thus they cannot find out the secret. This is the case no matter which two officials get together. Notice that since we are working over $GF(7)$, the two people could've guessed the secret ($0 \le s \le 6$) and constructed a unique degree 2 polynomial (by property 2). But the two people combined have the same chance of guessing what the secret is as they do individually. This is important, as it implies that two people have no more information about the secret than one person does.