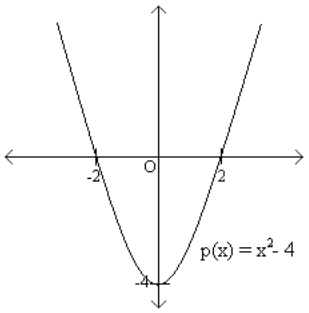
CS 70 Discrete Mathematics for CS
Spring 2008 David Wagner
Note 10

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 note.

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:

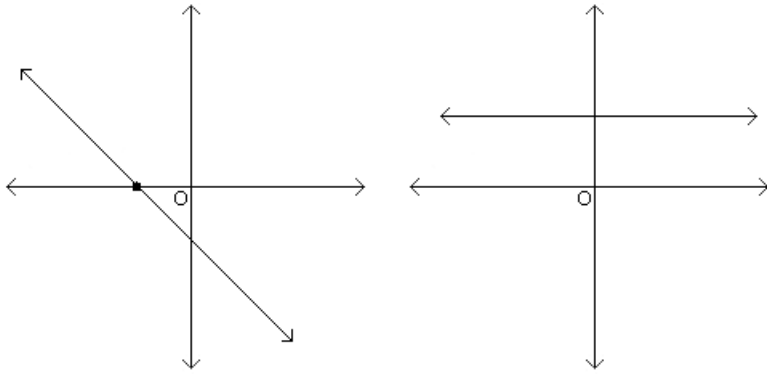


We now state two fundamental properties of polynomials that we will prove in due course.

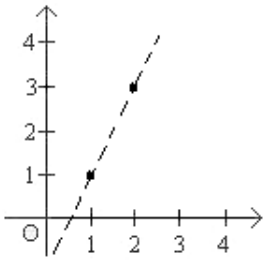
Property 1: A non-zero polynomial of degree d has at most d roots.

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

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, and so on. Given $d+1$ pairs $(x_1,y_1),\ldots,(x_{d+1},y_{d+1})$, how do we determine the 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 $p(x)$. Because these algorithms always work, this will take us partway towards proving that Property 2 is true.

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 ith 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 $2 \leq j \leq d+1$. 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). It's easy to see that $q(x_j) = 0$ for $2 \leq j \leq d+1$. But what is $q(x_1)$? Well, $q(x_1) = (x_1-x_2)(x_1-x_3)\cdots(x_1-x_{d+1})$, which is some constant that's different from 0 (since the x_i are all distinct). 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. In other words, if we want to find a polynomial such that $y_i = 1$ and $y_j = 0$ for $j \neq i$, we can do that. Let us introduce some notation: let us denote by $\Delta_i(x)$ the degree d polynomial that goes through these $d+1$ points, i.e., $\Delta_i(x_i) = 1$ and $\Delta_i(x_j) = 0$ when $j \neq i$. Then

$$\Delta_i(x) = \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)}.$$

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 the polynomial we are looking for is

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

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 ith term evaluates to y_i times 1 as required.

For instance, suppose $d = 2$ and $x_1 = 1$, $x_2 = 2$, $x_3 = 3$. Then

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

Consequently the polynomial $p(x)$ we are looking for can be expressed as $p(x) = y_1\Delta_1(x) + y_2\Delta_2(x) + y_3\Delta_3(x)$.

Property 2 and Uniqueness

We have shown how to find a polynomial $p(x)$ through any given $d+1$ points. This proves part of Property 2 (the existence of the polynomial). How do we prove the second part, that the polynomial is unique? Suppose for contradiction that there is another polynomial $q(x)$ that also passes through the $d+1$ points. Now

consider the polynomial $r(x) = p(x) - q(x)$. This is a non-zero polynomial of degree at most d. So by Property 1 it can have at most d roots. But on the other hand $r(x_i) = p(x_i) - q(x_i) = 0$ for $i = 1, \ldots, d+1$, so $r(x)$ has $d+1$ distinct roots. Contradiction. Therefore $p(x)$ is the unique polynomial that satisfies the $d+1$ conditions.

Property 1

Now let us turn to Property 1. We will prove this property in two steps.

Theorem: a is a root of $p(x)$ if and only if the polynomial $x-a$ divides $p(x)$.

Proof: Dividing $p(x)$ by the polynomial $x-a$ yields

$$p(x) = (x-a)q(x) + r(x)$$

for some polynomials $q(x)$ and $r(x)$, 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 (i.e., $x-a$). Therefore $r(x)$ must have degree 0 and therefore is some constant c, so $r(x) = c$. Now substituting $x = a$, we see $p(a) = 0 \cdot q(a) + r(a) = c$. If a is a root of $p(x)$, then $p(a) = 0$, so $c = 0$ and therefore $p(x) = (x-a)q(x)$, showing that $x-a$ divides $p(x)$.

On the other hand, if $x-a$ divides $p(x)$, then we know that $r(x) = 0$ and $p(x) = (x-a)q(x)$, hence $p(a) = 0 \cdot q(a) = 0$ and in particular a is a root of $p(x)$. □

Theorem: If $a_1, \ldots, a_d$ are d distinct roots of a polynomial $p(x)$ of degree d, then $p(x)$ has no other roots.

Proof: We will show that $p(x) = c(x-a_1)(x-a_2)\cdots(x-a_d)$ for some constant c. First, observe 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. Also $0 = p(a_2) = (a_2-a_1)q_1(a_2)$ 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, we find 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. A polynomial of degree 0 must be of the form $q_d(x) = c$ for some constant c, so we've shown that $p(x) = c(x-a_1)(x-a_2)\cdots(x-a_d)$ for some constant c, as claimed.

The theorem follows immediately. If a is any other value, different from $a_1, \ldots, a_d$, then $a - a_i \neq 0$ for all i and hence $p(a) = c(a-a_1)(a-a_2)\cdots(a-a_d) \neq 0$. In other words, no other value a can be a root of the polynomial $p(x)$. □

This completes the proof that a polynomial of degree d has at most d roots.

Finite Fields

Property 1 and Property 2 were stated under the assumption that the coefficients of the polynomials and the variable x range over the real numbers. These properties also hold if we use the set of rational numbers, or even the set of complex numbers, instead of the real numbers.

However, the properties do not hold if the values are restricted to the set of 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. As a result, our proof of Property 1 does not generalize to the case where the values are restricted to $\mathbb{N}$ or $\mathbb{Z}$.

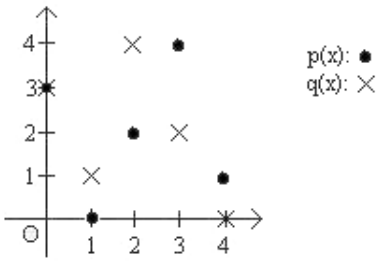
But if we work with numbers modulo a prime m, then we can add, subtract, multiply and divide (by any non-zero number modulo m). To check this, recall from our discussion of modular arithmetic in the previous

lectures that x has an inverse mod m if $\gcd(m,x) = 1$. Thus if m is prime *all* the numbers $\{1,\ldots,m-1\}$ have an inverse mod 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 an example of these properties holding in the case of polynomials of degree $d = 1$ modulo 5. Consider the polynomial $p(x) \equiv 4x+3 \pmod 5$. The roots of this polynomial are all values x such that $4x+3 \equiv 0 \pmod 5$. 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 $\Delta_1(x) \equiv \frac{x-x_2}{x_1-x_2} \equiv \frac{x-1}{0-1} \equiv -(x-1) \pmod 5$, and $\Delta_2(x) \equiv \frac{x-x_1}{x_2-x_1} \equiv \frac{x-0}{1-0} \equiv x \pmod 5$. Thus, $p(x) \equiv 3 \cdot \Delta_1(x) + 2 \cdot \Delta_2(x) \equiv -3(x-1) + 2x \equiv -x+3 \equiv 4x+3 \pmod 5$.

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. Intuitively, a field is a set where we can add, subtract, multiply, and divide any pair of elements from the set, and we will get another element in the set (as long as we don't try to divide by 0). If you would like to learn more about fields and the axioms they 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`.

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 $p(x) \equiv 2x+3 \pmod 5$ and $q(x) \equiv 3x-2 \pmod 5$ over $GF(5)$. We can represent these polynomials in the x-y plane as follows:



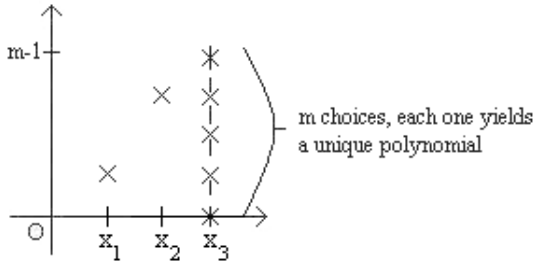
Notice that these two "lines" intersect in exactly one point, even though the picture looks nothing at all like lines in the Euclidean plane! Modulo 5, two lines can still intersect in at most one point, and that is thanks to the properties of addition, subtraction, multiplication, and division modulo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

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 when we are working modulo 6, if $a - a_1 \equiv 2 \pmod 6$ and $a - a_2 \equiv 3 \pmod 6$, these factors are non-zero, but $(a-a_1)(a-a_2) \equiv 2 \cdot 3 \equiv 0 \pmod 6$. Working modulo a prime ensures that this disaster cannot happen.

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, so there are a total of $m \times m \times m = m^3$ such polynomials.

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 $i = 1,2,3$. 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 y_3. Once three points are 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 the 2 points $(x_1,y_1),(x_2,y_2)$. This is illustrated 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 a total of 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 given	# of polynomials
$d+1$	1
d	m
$d-1$	m^2
$\vdots$	$\vdots$
$d-k$	m^{k+1}

The reason that we can 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.

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 decides that a nuclear strike can be initiated only if at least k major officials agree to it, for some $k > 1$. Suppose that missiles are protected by a secret launch code; the missile will

only launch if it is supplied with the proper launch code. Let's 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 (not even partial information), even if they pool their knowledge. For example, a group of $k-1$ conspiring officials should not be able to tell whether the secret launch code is odd or even; whether it is a prime number or not; whether it is divisible by some number a; or whether its least significant bit is 0 or 1. How can we accomplish this?

We'll presume that there are n officials indexed from 1 to n and that the secret launch code is some natural number s. Let q be a prime number larger than n and s, where $0 \leq s \leq q-1$. We will work over $GF(q)$ from now on, i.e., we will be working modulo q.

The scheme is simple. We pick a random polynomial $P(x)$ of degree $k-1$ such that $P(0) = s$. Then, we give the share $P(1)$ to the first official, $P(2)$ to the second official, ..., $P(n)$ to the nth official.

This satisfies our two desiderata:

1. Any k officials, having the values of the polynomial at k points, can use Lagrange interpolation to find $P(x)$. Once they know the polynomial $P(x)$, they can recover the secret s by computing $s = P(0)$.

2. What about some group of $k-1$ conspiring officials? They don't have enough information to recover polynomial $P(x)$. All they know is that there is some polynomial of degree $k-1$ passing through their $k-1$ points. 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 that also satisfies the constraint that $P(0) = b$. This means that any conjectured value of the secret is consistent with the information available to the $k-1$ conspirators, so the conspirators cannot rule out any hypothesized value for $P(0)$ as impossible. In short, the conspirators learn nothing about $P(0) = s$.

This scheme is known as Shamir secret sharing, in honor of its inventor, Adi Shamir.

Example. Suppose you are in charge of setting up a secret sharing scheme, with secret $s = 1$, 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 two or fewer cannot. We will need a polynomial of degree $k-1 = 2$. Let's say we are working over $GF(7)$ and you randomly choose the polynomial $P(x) = 3x^2 + 5x + 1$. (Notice: $P(0) = 1 = s$, 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 $P(1) \equiv 3 \cdot 1^2 + 5 \cdot 1 + 1 \equiv 9 \equiv 2 \pmod 7$ to the first official, $P(2) \equiv 3 \cdot 2^2 + 5 \cdot 2 + 1 \equiv 23 \equiv 2 \pmod 7$ to the second, $P(3) \equiv 3 \cdot 3^2 + 5 \cdot 3 + 1 \equiv 43 \equiv 1 \pmod 7$ to the third, $P(4) \equiv 6 \pmod 7$ to the fourth, and $P(5) \equiv 3$ 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 functions:

$$\Delta_3(x) \equiv \frac{(x-4)(x-5)}{(3-4)(3-5)} \equiv \frac{(x-4)(x-5)}{2} \equiv 4(x-4)(x-5) \pmod 7$$
$$\Delta_4(x) \equiv \frac{(x-3)(x-5)}{(4-3)(4-5)} \equiv \frac{(x-3)(x-5)}{-1} \equiv -(x-3)(x-5) \pmod 7$$
$$\Delta_5(x) \equiv \frac{(x-3)(x-4)}{(5-3)(5-4)} \equiv \frac{(x-3)(x-4)}{2} \equiv 4(x-3)(x-4) \pmod 7.$$

They then compute the polynomial $P(x) = 1 \cdot \Delta_3(x) + 6 \cdot \Delta_4(x) + 3 \cdot \Delta_5(x) \equiv 3x^2 + 5x + 1$ (you should verify this 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:

$$P(1) \equiv a_2 + a_1 + s \equiv 2 \pmod 7$$
$$P(5) \equiv 4a_2 + 5a_1 + s \equiv 3 \pmod 7$$

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 have guessed the secret ($0 \leq s \leq 6$) and identified a unique degree 2 polynomial that's consistent with their guess (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—in particular, these two people have no information about the secret, not even partial information.