Sharing secrets

1 Polynomials

Recall that a polynomial in a single variable is of the form

$$P(x) = a_d \cdot x^d + a_{d-1} \cdot x^{d-1} + \ldots + a_2 \cdot x^2 + a_1 \cdot x + a_0$$

The variable x and the coefficients a_i are usually real numbers. So a polynomial P can be seen as a function $\mathbb{R} \to \mathbb{R}$.

Example 1. *$P(x) = 3x^3 + 2x + 1$ is a polynomial of degree $d = 3$. Its coefficients are $a_3 = 3$, $a_2 = 0$, $a_1 = 2$, $a_0 = 1$, and $P(1) = 6$, and $P(0) = 1$.*

Polynomials have some remarkably simple, elegant and powerful properties, which we will explore below.

First, a definition: we say that a is a root of the polynomial $P(x)$ if $P(a) = 0$. For example, the degree two polynomial $P(x) = x^2 - 9$ two roots, namely 3 and -3, since $P(3) = P(-3) = 0$. 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), (x_2, y_2), $\ldots (x_d, y_d)$, (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 $1 \leq i \leq d + 1$.*

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), (x_2, y_2), $\ldots (x_d, y_d)$, (x_{d+1}, y_{d+1}), how do we determine a polynomial $P(x) = a_d \cdot x^d + a_{d-1} \cdot x^{d-1} + \ldots + a_2 \cdot x^2 + a_1 \cdot x + a_0$ such that $P(x_i) = y_i$ for $1 \leq i \leq d + 1$?

We will give two different efficient algorithms for reconstructing the coefficients $a_0, a_1, \ldots a_d$, and therefore the polynomial $P(x)$.

First method

We write a system of $d+1$ linear equations in $d+1$ variables: the coefficients of the polynomial $a_0, a_1, \ldots, a_d$. The i-th equation is:

$$a_d x_i^d + a_{d-1} x_i^{d-1} + \ldots + a_2 x_i^2 + a_1 x_i + a_0 = P(x_i)$$

or

$$a_d x_i^d + a_{d-1} x_i^{d-1} + \ldots + a_2 x_i^2 + a_1 x_i + a_0 = y_i$$

Since x_i, and y_i, are constants, this is a linear equation in the $d+1$ unknowns $a_0, a_1, \ldots a_d$. Now solving these equations gives the coefficients of the polynomial $P(x)$.

For example, given the three pairs $(-1, 1)$, $(1, 1)$ and $(2, 7)$, we will construct the degree 2 polynomial $P(x) = 2a_2 \cdot (x)^2 + a_1 \cdot (x) + a_0$ which goes through these points.

The first equation $P(-1) = 1$ yields $a_2 \cdot (-1)^2 + a_1 \cdot (-1) + a_0 = 1$. Simplifying, we get $a_2 - a_1 + a_0 = 1$. Applying the same technique to the second and third equations, we get the following system of equations:

$$\begin{aligned} a_2 - a_1 + a_0 &= 1 \quad (1) \\ a_2 + a_1 + a_0 &= 1 \quad (2) \\ 4a_2 + 2a_1 + a_0 &= 7 \quad (3) \end{aligned}$$

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.

Lagrange interpolation

Given $d+1$ pairs (x_1, y_1), (x_2, y_2), $\ldots (x_d, y_d)$, (x_{d+1}, y_{d+1}), the *Lagrange polynomial* (or, more precisely, *interpolation polynomial in Lagrange form*) is the polynomial

$$P(x) = \sum_{i=1}^{d+1} y_i \cdot L_i(x)$$

which a linear combination of *Lagrange basis polynomials*

$$L_i(x) = \frac{x - x_1}{x_i - x_1} \cdots \frac{x - x_{i-1}}{x_i - x_{i-1}} \cdot \frac{x - x_{i+1}}{x_i - x_{i+1}} \cdots \frac{x - x_{d+1}}{x_i - x_{d+1}} = \prod_{j=1, j \neq i}^{d+1} \frac{x - x_j}{x_i - x_j}$$

Theorem 1. *$P(x)$ is a unique polynomial of degree (at most) d such that $P(x_i) = y_i$ for $1 \leq i \leq d+1$.*

The proof is based on the folowing properties of $L_i(x) = \frac{x-x_1}{x_i-x_1} \cdots \frac{x-x_{i-1}}{x_i-x_{i-1}} \cdot \frac{x-x_{i+1}}{x_i-x_{i+1}} \cdots \frac{x-x_{d+1}}{x_i-x_{d+1}}$.

Proposition 1.

- *$L_i(x_i) = 1$ for any $i \in \{1, 2, \ldots, d+1\}$*

- $L_i(x_j) = 0$ *for any* $i, j \in \{1, 2, \ldots, d+1\}$, $j \neq i$.
- $y_i \cdot L_i(x_i) = y_i$ *for any* $i \in \{1, 2, \ldots, d+1\}$
- $y_i \cdot L_i(x_j) = 0$ *for any* $i, j \in \{1, 2, \ldots, d+1\}$, $j \neq i$.

Example Let $d = 3$ and the four control points be

$$\begin{aligned}(x_1, y_2) &= (-9, 5)\\ (x_2, y_2) &= (-4, 2)\\ (x_3, y_3) &= (-1, -2)\\ (x_4, y_4) &= (7, 9)\end{aligned}$$

- $L_1(x) = \frac{x-x_2}{x_1-x_2}\frac{x-x_3}{x_1-x_3}\frac{x-x_4}{x_1-x_4} = \frac{x+4}{-9+4}\frac{x+1}{-9+1}\frac{x-7}{-9-7}$ and so,
  $L_1(x) = \begin{cases} 1 & \text{if} \quad x = -9, \\ 0 & \text{if} \quad x \in \{-4, -1, 7\} \end{cases}$ and $5 \cdot L_1(x) = \begin{cases} 5 & \text{if} \quad x = -9, \\ 0 & \text{if} \quad x \in \{-4, -1, 7\} \end{cases}$
  The graphic of $5L_1(x)$ is shown in red in the graphic below.
- $2 \cdot L_2(x) = \begin{cases} 2 & \text{if} \quad x = -4, \\ 0 & \text{if} \quad x \in \{-9, -1, 7\} \end{cases}$
  The graphic of $2L_2(x)$ is shown in blue in the graphic.
- $-2 \cdot L_3(x) = \begin{cases} -2 & \text{if} \quad x = -1, \\ 0 & \text{if} \quad x \in \{-9, -1, 7\} \end{cases}$
  The graphic of $-2L_3(x)$ is shown in green in the graphic.
- $9 \cdot L_4(x) = \begin{cases} 9 & \text{if} \quad x = 7, \\ 0 & \text{if} \quad x \in \{-9, -4, -1\} \end{cases}$
  The graphic of $9L_4(x)$ is shown in yellow in the graphic.
- Finally, $P(x) = 5 \cdot L_1(x) + 2 \cdot L_2(x) + 2 \cdot L_3(x) + 9 \cdot L_4(x)$.

  The graphic of $P(x)$ is shown in black in the graphic.

2 Finite field

A field is an algebraic structure in which the operations of addition, subtraction, multiplication and division (except division by zero) may be performed, and the same rules hold which are familiar from the arithmetic of ordinary numbers.

The prototypical example of a field is $\mathbb{Q}$ (the field of rational numbers). Other important examples include the field of real numbers $\mathbb{R}$, the field of complex numbers $\mathbb{C}$ and, for any prime number p, the finite field of integers modulo p, denoted $\mathbb{Z}/p\mathbb{Z}$, F_p or $GF(p)$. The mathematical discipline concerned with the study of fields is called field theory.

Definition 1. *A field is a set F with two operations $+$ and $\cdot$ with the properties:*

1. *Closure of F under $+$ and $\cdot$. For all a, b belonging to F, both $a + b$ and $a \cdot b$ belong to F (or more formally, $+$ and $\cdot$ are binary operations on F).*

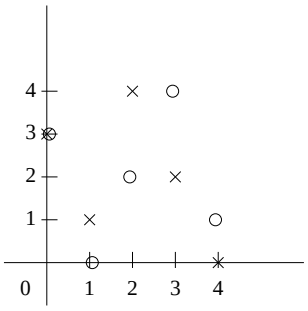

Figure 1: The graphic of polynomials $p(x) = 2x + 3$ and $q(x) = 3x - 2$ over F_5.

2. *Both $+$ and $\cdot$ are associative.s For all a, b, c in F, $a+(b+c) = (a+b)+c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.*

3. *Both $+$ and $\cdot$ are commutative. For all a, b belonging to F, $a + b = b + a$ and $a \cdot b = b \cdot a$.*

4. *The operation $\cdot$ is distributive over the operation $+$. For all a, b, c, belonging to F, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.*

5. *Existence of an additive identity. There exists an element 0 in F, such that for all a belonging to F, $a + 0 = a$.*

6. *Existence of a multiplicative identity There exists an element 1 in F different from 0, such that for all a belonging to F, $a \cdot 1 = a$.*

7. *Existence of additive inverses. For every a belonging to F, there exists an element $-a$ in F, such that $a + (-a) = 0$.*

8. *Existence of multiplicative inverses. For every $a \neq 0$ belonging to F, there exists an element a^{-1} in F, such that $a \cdot a^{-1} = 1$.*

The field F_5

The field F_5 is the set $\{0, 1, 2, 3, 4\}$ with the operation of addition $+$ and and multiplication $\cdot$ modulo 5.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Example

1. Calculate in F_5: $2 \cdot 4$; $\frac{2}{4}$; $\frac{1}{4}$; $-\frac{3}{4}$.

2. Solve in F_5 the equations: $2x + 1 = 3$; $2 - 3x = 1$.

3 Secret Sharing

During the Cold War, in the 1950's and 1960's, President Dwight D. Elsenhower 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, 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. 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, ..., $P(n)$ 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 $s = P(0)$ 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. For each possible value of 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 F_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 L_i functions:

$L_3(x) = \frac{(x-4)(x-5)}{(3-4)(3-5)} = \frac{(x-4)(x-5)}{2}$

$L_4(x) = \frac{(x-3)(x-5)}{(4-3)(4-5)} = \frac{(x-3)(x-5)}{-1}$

$L_5(x) = \frac{(x-3)(x-4)}{(5-3)(5-4)} = \frac{(x-3)(x-4)}{2}$

They then compute the polynomial over F_7

$$P(x) = 1 \times L_3(x) + 6 \cdot L_4(x) + 3 \cdot L_5(x) = 3x^2 + 5x + 1$$

(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:
$P(1) = a_2 + a_1 + s = 2$
$P(5) = 4a_2 + 5a_1 + s = 3$ 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 F_7, the two people could've guessed the secret ($0 < s < 6$) 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.