

Wonderful and Crazy Ideas in Computer Science and Math
Virginia Vassilevska and Ryan Williams July 13, 2009

Polynomials, Secret Sharing, And Error-Correcting Codes

$$P(X) = \text{👤} X^3 + \text{👤} X^2 + \text{👤} X^1 + \text{👤}$$

Polynomials in one variable over the reals

$$P(x) = 3x^2 + 7x - 2$$

$$Q(x) = x^{123} - \frac{1}{2}x^{25} + 19x^3 - 1$$

$$R(y) = 2y + \sqrt{2}$$

$$S(z) = z^2 - z - 1$$

$$T(x) = 0$$

$$W(x) = \pi$$

Representing a polynomial

A degree- d polynomial is represented by its $(d+1)$ coefficients:

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x^1 + a_0$$

The numbers a_d, a_{d-1}, \dots, a_0 are the coefficients.

E.g. $P(x) = 3x^4 - 7x^2 + 12x - 19$

Coefficients are:

$$3, 0, -7, 12, -19$$

Are we working over the reals?

We could work over any "field"
(set with addition, multiplication, division defined.)

E.g., we could work with the rationals, or the reals.

Or with \mathbb{Z}_p , the integers mod prime p .

In the next few slides I'll remind you what we learned about $+$ and $*$ mod p , and I'll tell you how to do division.

Recall:
($a \bmod p$) means
"the remainder when a is
divided by p "

$$(a \bmod p) = 0$$


is equivalent to
 $p \mid a$




If $a = b \bmod p$, then a are
in the same equivalence
class mod p .

Given a , to get another
number b such that
 $a = b \bmod p$,
just add some multiple of p
to a .





Recall:
**Fundamental Lemma of plus,
 minus, and times modulo p:**
 If
 $(x = y \pmod p)$ and $(a = b \pmod p)$
 Then: $x + a = y + b \pmod p$
 $x - a = y - b \pmod p$
 $x * a = y * b \pmod p$



**Fundamental Lemma of plus
 minus, and times modulo p:**
 When doing plus, minus, and times
 modulo n, at any time in the
 calculation we can replace a
 number with another number in
 the same equiv. class modulo p

The Set Z_p for prime p

$Z_p = \{0, 1, 2, \dots, p-1\}$ These are all the
 remainders when you
 divide by p

In Z_5 :
 $7 \equiv 1 + 4 \pmod 5 = 1 + 4 \pmod 5 = 5 \pmod 5 = 0 \pmod 5$
 $7 \equiv 1 * 3 \pmod 5 = 3 \pmod 5$

New: The set Z_p^*

$Z_p^* = \{1, 2, 3, \dots, p-1\}$

**This is the set of the numbers in Z_p which
 one can divide by, mod p.**

How to divide b by a mod p:
 1. Find a number c such that $a * c = 1 \pmod p$.
 2. Multiply b by c.

Division mod p

How to divide b by a mod p:
 1. Find a number c such that $a * c = 1 \pmod p$.
 2. Multiply b by c.

That's all about
 mod p for now.

For example:
 We want to divide 5 by 2 mod 7

$4 * 2 \pmod 7 = 1 \pmod 7$
 Hence, $2^{-1} \pmod 7 = 4$.

$5/2 \pmod 7 = 5 * 4 \pmod 7 = 20 \pmod 7 = 6 \pmod 7$

Simple Facts about Polynomials

Let $P(x), Q(x)$ be two polynomials.

The sum $P(x) + Q(x)$ is also a polynomial.
 (i.e., polynomials are "closed under addition")

Their product $P(x)Q(x)$ is also a polynomial.
 ("closed under multiplication")

$P(x)/Q(x)$ is not necessarily a polynomial.

Multiplying Polynomials

$$(x^2+2x-1)(3x^3+7x)$$

$$= 3x^5 + 7x^3 + 6x^4 + 14x^2 - 3x^3 - 7x$$

$$= 3x^5 + 6x^4 + 4x^3 + 14x^2 - 7x$$

When you do it mod p, you can again replace the coefficients at any point by elements of the same equivalence class!

$$(x^2+2x-1)(3x^3+7x) \pmod 7 = (x^2+2x-1)(3x^3) \pmod 7$$

$$= 3x^5 + 6x^4 - 3x^3 \pmod 7$$

$$= 3x^5 + 6x^4 + 4x^3 \pmod 7$$

Evaluating a polynomial

Suppose:

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x^1 + a_0$$

E.g. $P(x) = 3x^4 - 7x^2 + 12x - 19 \pmod 7$

$$P(5) = 3 \cdot 5^4 + 12 \cdot 5 - 19 = 3 \cdot (-2)^4 + (-2) \cdot (-2) + 2 \\ = 3 \cdot 16 + 4 + 2 = 3 \cdot 2 + 6 = 12 = 5 \pmod 7$$

$$P(-1) = 3 \cdot (-1)^4 + 12 \cdot (-1) - 19 = 3 \pmod 7$$

$$P(0) = -19 = 2 \pmod 7$$

The roots of a polynomial

Suppose:

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x^1 + a_0$$

Definition: r is a "root" of P(x) if P(r) = 0

$$P(x) = 3x + 7 \quad \text{root} = -(7/3).$$

$$P(x) = x^2 - 2x + 1 \quad \text{roots} = 1, 1$$

$$P(x) = 3x^3 - 10x^2 + 10x - 2 \quad \text{roots} = 1/3, 1, 2.$$

Linear Polynomials

$$P(x) = ax + b, \quad a \neq 0$$

One root: $P(x) = ax + b = 0 \Rightarrow x = -b/a \pmod{11}$

For example: $P(x) = 7x - 9 \pmod{11}$ (over \mathbb{Z}_{11})

$$x = (-(-9)/7) \pmod{11} \\ = 9 \cdot 7^{-1} \pmod{11} \\ = 9 \cdot (-3) = -27 \pmod{11} \\ = 6 \pmod{11}.$$

Recall: dividing by 7 mod 11 can be done!
 $7 \cdot (-3) = -21 = 1 \pmod{11}$

Check: $P(6) = 7 \cdot 6 - 9 = 42 - 9 = 33 = 0 \pmod{11}$

The Single Most Important Fact About Low-degree Polynomials

at most d
A non-zero degree-d polynomial P(x) has at most d roots.



If you give me pairs $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ then there is at most one degree-d polynomial P(x) such that:

$$P(x_k) = y_k \quad \text{for all } k$$

Here x_i s are all distinct




Theorem: Let $P(x)$ and $Q(x)$ be polynomials of degree at most d . Suppose there are $d+1$ distinct points x_1, x_2, \dots, x_{d+1} such that $P(x_1)=Q(x_1), P(x_2)=Q(x_2), \dots, P(x_{d+1})=Q(x_{d+1})$. Then $P(x)=Q(x)$ for all x .

Proof: Look at the polynomial $R(x) = P(x) - Q(x)$.
 $R(x)$ has $d+1$ roots: $R(x_1) = R(x_2) = \dots = R(x_{d+1}) = 0$.

A non-zero degree- d polynomial $P(x)$ has at most d roots.

$R(x)$ has degree at most d .
 So $R(x)$ must be 0!
 $R(x) = 0 \Rightarrow P(x) = Q(x)$




x's are all distinct

If you give me pairs $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$

then there is at most one degree- d polynomial $P(x)$ such that:

$P(x_k) = y_k$ for all k





Hmm: at most one?

So perhaps for some $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ there are no degree- d polynomials with

$P(x_k) = y_k$

for all the $d+1$ values of k ?





Lagrange Interpolation

Given any $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), \dots, (x_{d+1}, y_{d+1})$

then there exists exactly one degree- d polynomial $P(x)$ such that

$P(x_k) = y_k$ for all k

k-th "Switch" polynomial

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), \dots, (x_{d+1}, y_{d+1})$

$$g_k(x) = (x-x_1)(x-x_2)\dots(x-x_{k-1})(x-x_{k+1})\dots(x-x_{d+1})$$

Degree of $g_k(x)$ is: d

$g_k(x)$ has d roots: $x_1, \dots, x_{k-1}, x_{k+1}, \dots, x_{d+1}$

Evaluate g_k at x_k :

$$g_k(x_k) = (x_k-x_1)(x_k-x_2)\dots(x_k-x_{k-1})(x_k-x_{k+1})\dots(x_k-x_{d+1}) \neq 0$$

For all $i \neq k, g_k(x_i) = 0$

k-th "Switch" polynomial: example

Given 3 pairs $(0, 1), (1, 2), (2, 0)$

$$g_0(x) = (x-1)(x-2), \quad g_1(x) = x(x-2), \quad g_2(x) = x(x-1)$$

Degree of each $g_k(x)$ is 2, and each $g_k(x)$ has 2 roots.

$g_0(x)$ has 2 roots: 1, 2

Evaluate g_0 at 0:

$$g_0(0) = (0-1)(0-2) = 2 \neq 0$$

$$g_0(1) = (1-1)(1-2) = 0 \text{ and } g_0(2) = (2-1)(2-2) = 0$$

k-th "Switch" polynomial

For every x_k from x_1, x_2, \dots, x_{d+1} we have a polynomial $g_k(x)$ such that

- $g_k(x_k) \neq 0$, and
- $g_k(x_i) = 0$ for all $i \neq k$

$$h_k(x) = g_k(x)/g_k(x_k)$$

We will define a new polynomial $h_k(x)$ with

- $h_k(x_k) = 1$, and
- $h_k(x_i) = 0$ for all $i \neq k$

k-th "Switch" polynomial

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), \dots, (x_{d+1}, y_{d+1})$

$$g_k(x) = (x-x_1)(x-x_2)\dots(x-x_{k-1})(x-x_{k+1})\dots(x-x_{d+1})$$

$$h_k(x) = g_k(x)/g_k(x_k)$$

$$h_k(x) = \frac{(x-x_1)(x-x_2)\dots(x-x_{k-1})(x-x_{k+1})\dots(x-x_{d+1})}{(x_k-x_1)(x_k-x_2)\dots(x_k-x_{k-1})(x_k-x_{k+1})\dots(x_k-x_{d+1})}$$

$$h_k(x_k) = 1$$

$$\text{For all } i \neq k, h_k(x_i) = 0$$

The Lagrange Polynomial

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), \dots, (x_{d+1}, y_{d+1})$

$$h_k(x) : \quad h_k(x_k) = 1$$

$$\text{For all } i \neq k, h_k(x_i) = 0$$

$$P(x_2) = y_1 \cdot 0 + y_2 \cdot 1 + y_3 \cdot 0 + \dots + y_{d+1} \cdot 0 = y_2$$

$$P(x) = y_1 h_1(x) + y_2 h_2(x) + \dots + y_{d+1} h_{d+1}(x)$$

$P(x)$ is the unique polynomial of degree d such that $P(x_1) = y_1, P(x_2) = y_2, \dots, P(x_{d+1}) = y_{d+1}$

Example

Input: $(5,1), (6,2), (7,9)$ $x_1 = 5 \quad x_2 = 6 \quad x_3 = 7$
 $y_1 = 1 \quad y_2 = 2 \quad y_3 = 9$

Switch polynomials:

$$h_1(x) = (x-6)(x-7)/(5-6)(5-7) = \frac{1}{2} (x-6)(x-7)$$

$$h_2(x) = (x-5)(x-7)/(6-5)(6-7) = -(x-5)(x-7)$$

$$h_3(x) = (x-5)(x-6)/(7-5)(7-6) = \frac{1}{2} (x-5)(x-6)$$

$$P(x) = 1 \times h_1(x) + 2 \times h_2(x) + 9 \times h_3(x)$$

$$= (6x^2 - 77x + 237)/2$$

Lagrange interpolation

We can always construct the unique polynomial $P(x)$ given $d+1$ point evaluations $(x_1, y_1), (x_2, y_2), \dots, (x_{d+1}, y_{d+1})$.

This is not only true over the real numbers, but also mod a prime (over Z_p).

Two different representations

$P(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x^1 + a_0$
 can be represented either by

a) $d+1$ coefficients

$$a_d, a_{d-1}, \dots, a_2, a_1, a_0$$

b) Its value at any $d+1$ points

$$P(x_1), P(x_2), \dots, P(x_d), P(x_{d+1})$$

(e.g., $P(0), P(1), P(2), \dots, P(d+1)$.)

Converting Between The Two Representations

Coefficients to Evaluation:

Evaluate $P(x)$ at $d+1$ points

Evaluation to Coefficients:

Use Lagrange Interpolation

Difference in the Representations

$P(x)$ can be represented by:

- $d+1$ coefficients $a_d, a_{d-1}, \dots, a_1, a_0$
- Value at $d+1$ points $P(x_1), \dots, P(x_{d+1})$

Adding two polynomials:

Both representations are equally good, since in both cases the new polynomial can be represented by the sum of the representations

$$\begin{aligned} P &= (5, 9, 6), \text{ that is: } P(0) = 5 \quad P(1) = 9 \quad P(2) = 6 \\ P &= (3, -9, 5), \text{ that is: } Q(0) = 3 \quad Q(1) = -9 \quad Q(2) = 5 \\ (P+Q) &= (8, 0, 11) \end{aligned}$$

Difference in the Representations

$P(x)$ can be represented by:

- $d+1$ coefficients $a_d, a_{d-1}, \dots, a_1, a_0$
- Value at $d+1$ points $P(x_1), \dots, P(x_{d+1})$

Multiplying two polynomials:

Representation (a) requires $(d+1)^2$ multiplications

$$\begin{aligned} P(x) &= a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0 \\ Q(x) &= b_d x^d + b_{d-1} x^{d-1} + \dots + b_1 x + b_0 \end{aligned}$$

$P(x) \cdot Q(x)$: Coefficient in front of x^k is
(Sum over $i=0, \dots, k$: $a_i b_{k-i}$)

Difference in the Representations

$P(x)$ can be represented by:

- $d+1$ coefficients $a_d, a_{d-1}, \dots, a_1, a_0$
- Value at $d+1$ points $P(x_1), \dots, P(x_{d+1})$

Multiplying two polynomials:

Representation (b) just requires $(d+1)$ multiplications

$$\begin{aligned} P(x_i) &= p_1, \dots, P(x_{d+1}) = p_{d+1} \\ Q(x_i) &= q_1, \dots, Q(x_{d+1}) = q_{d+1} \end{aligned}$$

$$(P \cdot Q)(x_i) = (p_1 \cdot q_1), \dots, (P \cdot Q)(x_{d+1}) = p_{d+1} \cdot q_{d+1}$$

Difference in the Representations

$P(x)$ can be represented by:

- $d+1$ coefficients $a_d, a_{d-1}, \dots, a_1, a_0$
- Value at $d+1$ points $P(x_1), \dots, P(x_{d+1})$

Multiplying two polynomials:

Representation (a) requires $(d+1)^2$ multiplications

Representation (b) just requires $(d+1)$ multiplications (if the two polynomials are already evaluated at the same points)

Difference in the Representations

$P(x)$ can be represented by:

- $d+1$ coefficients $a_d, a_{d-1}, \dots, a_1, a_0$
- Value at $d+1$ points $P(x_1), \dots, P(x_{d+1})$

Evaluating the polynomial at some point:

Is easy with representation (a): plug in

Requires Lagrange interpolation with (b)

The value-representation is tolerant to "erasures"

I want to send you a polynomial $P(x)$ of degree d .

Suppose your mailer drops my emails once in a while.



Now hang on a minute!
Why would I ever want to send you a polynomial?

The value-representation is tolerant to "erasures"

I want to send you a polynomial $P(x)$ of degree d .

Suppose your mailer drops my emails once in a while.

Say, I wanted to send you a message "hello"

I could write it as "8 5 12 12 15", or
 $8x^4 + 5x^3 + 12x^2 + 12x + 15$



The value-representation is tolerant to "erasures"

I want to send you a polynomial $P(x)$ of degree d .

Suppose your mailer drops my emails once in a while.

I could evaluate $P(x)$ at $n > d+1$ points and send $\langle k, P(k) \rangle$ to you for all $k = 1, 2, \dots, n$.

As long you get at least $(d+1)$ of these, choose any $(d+1)$ of the ones you got, and reconstruct $P(x)$.

But is it tolerant to "corruption" ?

I want to send you a polynomial $P(x)$.

Suppose your mailer corrupts my emails once in a while.

Suppose $P(x) = 2x^2 + 1$, and I chose $n = 4$.

I evaluated $P(0) = 1, P(1) = 3, P(2) = 9, P(3) = 19$.

So I sent you $\langle 0, 1 \rangle, \langle 1, 3 \rangle, \langle 2, 9 \rangle, \langle 3, 19 \rangle$

Corrupted email says $\langle 0, 1 \rangle, \langle 1, 2 \rangle, \langle 2, 9 \rangle, \langle 3, 19 \rangle$

You choose $\langle 0, 1 \rangle, \langle 1, 2 \rangle, \langle 2, 9 \rangle$

and get $Q(x) = 3x^2 - 2x + 1$. **$Q(3) = 22 \neq 19$**

Error-Detecting Representation

The above scheme does detect errors!

If we send the value of degree- d polynomial $P(x)$ at $n \geq d+1$ different points,

$\langle x_1, P(x_1) \rangle, \langle x_2, P(x_2) \rangle, \dots, \langle x_n, P(x_n) \rangle$

then we can detect corruptions as long as there fewer than $(n-d)$ of them

Why? If only $n-d-1$ corruptions, then $d+1$ correct points, and we'll notice an inconsistency!

And that's not all:
polynomials are amazing
in other ways as well...

Secret Sharing

Missile has random secret number S encoded into its hardware. It will not arm without being given S .

n officers have memorized a private "share" of S . Any k out of n of them should be able to assemble their shares so as to obtain S .

Any $\leq k-1$ of them should not be able to jointly determine any information about S .

A k -out-of- n secret sharing scheme

Let S be a random "secret" from Z_p

Want to give shares z_1, z_2, \dots, z_n to the n officers such that:

- if we have k of the z_i 's, then we can find out S .
- if we have $k-1$ z_i 's, then any secret S is equally likely to have produced this set of z_i 's.

Our k -out-of- n S.S.S.

Let S be a random "secret" from Z_p

Pick $k-1$ random coefficients R_1, R_2, \dots, R_{k-1} from Z_p

Let

$$P(x) = R_{k-1} x^{k-1} + R_{k-2} x^{k-2} + \dots + R_1 x^1 + S$$

For any j in $\{1, 2, \dots, n\}$, officer j 's share $z_j = P(j)$

Our k -out-of- n S.S.S.

Let S be a random "secret" from Z_p

Pick $k-1$ random coefficients R_1, R_2, \dots, R_{k-1} from Z_p

Let $P(x) = R_{k-1} x^{k-1} + R_{k-2} x^{k-2} + \dots + R_1 x^1 + S$

For any j in $\{1, 2, \dots, n\}$, officer j 's share $z_j = P(j)$

$P(0) =$ where P hits y -axis $= S$.

$P(x)$ chosen to be a random degree $k-1$ polynomial given that f hits the y -axis at S .

Since S is random, each *such* polynomial is equally likely to be chosen

Our k -out-of- n S.S.S.

Let S be a random "secret" from Z_p

Pick $k-1$ random coefficients R_1, R_2, \dots, R_{k-1} from Z_p

Let $P(x) = R_{k-1} x^{k-1} + R_{k-2} x^{k-2} + \dots + R_1 x^1 + S$

For any j in $\{1, 2, \dots, n\}$, officer j 's share $z_j = P(j)$

If k officers get together, they can figure out $P(x)$ by Lagrange interpolation, and then evaluate $P(0) = S$.

Our k -out-of- n S.S.S.

Let S be a random "secret" from Z_p

Pick $k-1$ random coefficients R_1, R_2, \dots, R_{k-1} from Z_p


Let $P(x) = R_{k-1} x^{k-1} + R_{k-2} x^{k-2} + \dots + R_1 x^1 + S$

For any j in $\{1, 2, \dots, n\}$, officer j 's share $z_j = P(j)$

If $k-1$ officers get together, they know $P(x)$ at $k-1$ different points.

For each value of S' , we can get a unique polynomial P' passing through their points, and $P'(0) = S'$.

And so each S' equally is likely!!!



Polynomials

Fundamental Theorem of polynomials:
Degree- d polynomial has at most d roots.
Two different deg- d polys agree on $\leq d$ points.

Lagrange Interpolation:
Given $d+1$ pairs (x_k, y_k) , can find unique poly P
such that $P(x_k) = y_k$ for all these k .
Gives us alternative representation for polys.

Many Applications of this representation
Error detecting/correcting codes
Secret sharing.

Summary Bee