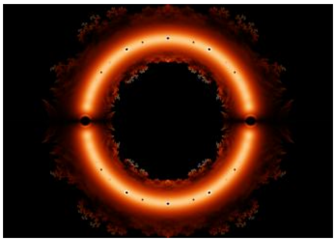
Great Theoretical Ideas In Computer Science

Victor Adamchik CS 15-251

Lecture 26 Carnegie Mellon University

Polynomials, Error Correction



Outline

Finite Fields

Polynomial Ring

Lagrange Interpolation

Reed-Solomon encoding

Group

A group G is a pair (S, •), where S is a set and • is a binary operation $S \times S \to S$ such that:

1. (Closure) For all a and b $\in$ S, a • b$\in$S

2. ♦ is associative, (a • b) • c= a • (b • c)

3. (Identity) There exists an element e $\in$ S s.t.

   e • a = a • e = a, for all a $\in$ S

4. (Inverses) For every a $\in$ S there is b $\in$ S s.t.

   a • b = b • a = e

Rings

We often define more than one operation on a set

For example, in Z_n we can do both addition and multiplication modulo n

A ring is a set together with two operations

Rings

A ring R is a set together with two binary operations + and ×, satisfying the following properties:

1. (R,+) is a commutative group

2. × is associative

3. The distributive laws hold in R:

   (a + b) × c = (a × c) + (b × c)

   c × (a + b) = (c × a) + (c × b)

Examples: (Z, +, *) a ring

Fields

A field F is a set together with two binary operations + and ×, satisfying the following properties:

1. (F,+) is a commutative group

2. (F-{0},×) is a commutative group

3. The distributive law holds in F:

   (a + b) × c = (a × c) + (b × c)

Fields

Informally, it's a place where you can add, subtract, multiply, and divide.

Examples:

Real numbers	$\mathbb{R}$
Rational numbers	$\mathbb{Q}$
Complex numbers	$\mathbb{C}$
(Finite field) Integers mod *prime*	Z_p aka $\mathbb{F}_p$

NON-examples: Integers $\mathbb{Z}$ division??

Non-negative reals $\mathbb{R}^+$ subtraction??

Another Example

Quadratic "number field"

$\mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} : a,b \in \mathbb{Q} \}$

Addition: $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a+c) + (b+d)\sqrt{2}$

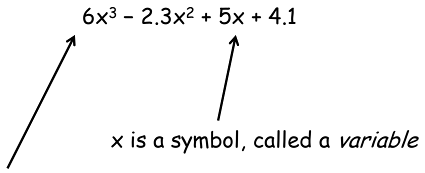
Multiplication:

$(a + b\sqrt{2}) \bullet (c + d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2}$

Polynomials

Polynomials

Informally, a polynomial is an expression that looks like this:



$6x^3 - 2.3x^2 + 5x + 4.1$

x is a symbol, called a *variable*

a number standing next to x are called a *coefficient*

Polynomials

Informally, a polynomial is an expression that looks like this:

$6x^3 - 2.3x^2 + 5x + 4.1 \quad \in \mathbb{R}[x]$

Coefficients can come from any *field*.

Can allow multiple variables, but we won't.

Set of polynomials with variable x and coefficients from field F is denoted F[x].

Polynomials – formal definition

Let F be a field and let x be a variable symbol.

F[x] is the set of polynomials over F,

defined to be expressions of the form

$c_d x^d + c_{d-1} x^{d-1} + \cdots + c_2 x^2 + c_1 x + c_0$

where each c_i is in F, and $c_d \neq 0$.

We call d the degree of the polynomial.

Also, the expression 0 is a polynomial.

(By convention, we call its degree $-\infty$.)

Adding and multiplying polynomials

Example.

Here are two polynomials in $\mathbb{F}_{11}[x]$

$$P(x) = x^2 + 5x - 1$$
$$Q(x) = 3x^3 + 10x$$

$$\begin{aligned} P(x) + Q(x) &= 3x^3 + x^2 + 15x - 1 \\ &= 3x^3 + x^2 + 4x - 1 \\ &= 3x^3 + x^2 + 4x + 10 \end{aligned}$$

Adding and multiplying polynomials

Example.

Here are two polynomials in in $\mathbb{F}_{11}[x]$

$$P(x) = x^2 + 5x - 1$$
$$Q(x) = 3x^3 + 10x$$

$$\begin{aligned} P(x) \cdot Q(x) &= (x^2 + 5x - 1)(3x^3 + 10x) \\ &= 3x^5 + 15x^4 + 7x^3 + 50x^2 - 10x \\ &= 3x^5 + 4x^4 + 7x^3 + 6x^2 + x \end{aligned}$$

F[x] is not a field

Polynomial addition is associative and commutative.

So (F[x], +) is an abelian group!

Polynomial multiplication is associative and commutative.

Multiplication distributes over addition:

$$P(x) \cdot (Q(x) + R(x)) = P(x) \cdot Q(x) + P(x) \cdot R(x)$$

If P(x) / Q(x) were always a polynomial, then F[x] would be a field!

Dividing polynomials?

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

So F[x] is not quite a field.

It's a commutative ring

Same with $\mathbb{Z}$, the integers:
it has everything except division.

Dividing polynomials?

$\mathbb{Z}$ has the concept of "division with remainder":

Given $a,b \in \mathbb{Z}$, $b \neq 0$, can write $a = q \cdot b + r$, $r < b$

F[x] has the same concept:

Given $A(x), B(x) \in F[x]$, $B(x) \neq 0$, can write

$$A(x) = Q(x) \cdot B(x) + R(x),$$

where $\deg(R(x)) < \deg(B(x))$.

"Division with remainder" for polynomials

Example: Divide $6x^4+8x+1$ by $2x^2+4$ in $\mathbb{F}_{11}[x]$

$$\begin{array}{r|l} & 3x^2 + 5 \\ \hline 2x^2+4 & 6x^4+8x+1 \\ - & 6x^4+x^2 \\ \hline & -x^2+8x+1 \\ - & 10x^2+9 \\ \hline & 8x-8 = 8x + 3 \end{array}$$

Check:

$$6x^4+8x+1$$
$$= (3x^2+5)(2x^2+4)+(8x+3)$$

“Division with remainder” for polynomials

Similar to integers, you can do modular arithmetic with polynomials over a field.

For example,

$2x^2 = 2 \bmod (x^2-1)$ $2x^2 = 2(x^2-1) + 2$

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

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

Enough algebraic theory.

Let’s play with polynomials!

Evaluating polynomials

Given a polynomial $P(x) \in F[x]$,
$P(a)$ means its evaluation at element a.

E.g., if $P(x) = x^2+3x+5$ in $\mathbb{F}_{11}[x]$

$P(6) = 6^2+3\cdot 6+5 = 36+18+5 = 59 = 4$

$P(4) = 4^2+3\cdot 4+5 = 16+12+5 = 33 = 0$

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

Polynomial roots

Theorem:
Let $P(x) \in F[x]$ have degree 1.
Then $P(x)$ has exactly 1 root.

Proof:
Write $P(x) = cx + d$ (where $c \neq 0$).
Then $P(r) = 0 \Leftrightarrow c \cdot r + d = 0$
$\Leftrightarrow c \cdot r = -d$
$\Leftrightarrow r = -d/c$.

Polynomial roots

Let $P(x) \in F[x]$ have degree 2.
Then $P(x)$ has… how many roots??

E.g.: $P(x)=x^2+1$...

# of roots over $\mathbb{C}[x]$: 2 (namely, i and $-i$)

# of roots over $\mathbb{R}[x]$: 0

# of roots over $\mathbb{F}_2[x]$: 1 (namely, 1)

# of roots over $\mathbb{F}_3[x]$: 0

The single most important theorem about polynomials over fields:

A degree d
polynomial has
at most d roots.

Theorem: Over a field, for all $d \geq 0$, degree d polynomials have at most d roots.

Proof by induction on $d \in \mathbb{N}$:

Base case: If $P(x)$ is degree 0 . This has 0 roots.
Assume true for $d \geq 0$. Let $P(x)$ have degree d+1.
If $P(x)$ has 0 roots: we're done! Else let b be a root.
Divide with remainder: $P(x) = Q(x)(x-b) + R(x)$. $(*)$
$\deg(R) < \deg(x-b) = 1$, so $R(x)$ is a constant.
Plug $x = b$ into $(*)$ to see that constant is zero
So $P(x) = Q(x)(x-b)$, where by IH Q has $\leq$ d roots.
$\therefore$ $P(x)$ has $\leq$ d+1 roots, completing the induction.

An important corollary

Corollary: Suppose a polynomial $R(x) \in F[x]$ is s.t.
(i) R has degree $\leq$ d and
(ii) R has $\geq$ d+1 roots
Then R must be the 0 polynomial

Theorem: Over a field, degree d polynomials have at most d roots.

Reminder:

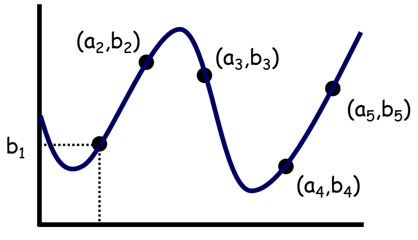
This is only true over a field.

E.g., consider $P(x) = 3x$ over Z_6.

It has degree 1, but 3 roots: 0, 2, and 4.

Interpolation

Say you're given a bunch of "data points"



Can you find a (low-degree) polynomial which "fits the data"?

Interpolation

Let pairs $(a_1,b_1), (a_2,b_2), \ldots, (a_{d+1},b_{d+1})$ from a field F be given (with all a_i's distinct).

Theorem:

There is exactly one polynomial $P(x)$ of degree at most d such that $P(a_i) = b_i$ for all $i = 1,\ldots,d+1$.

E.g. there is a unique linear polynomial going through 2 points

Theorem Proof

There are two things to prove.

1. There is at *least* one polynomial of degree $\leq$ d passing through all d+1 data points.
2. There is at *most* one polynomial of degree $\leq$ d passing through all d+1 data points.

Let's prove #2 first.

Proof #2

Suppose P(x) and Q(x) both do the trick.

Let $R(x) = P(x)-Q(x)$.

Since deg(P), deg(Q) $\le$ d we must have deg(R) $\le$ d.

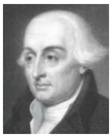
But $R(a_i) = b_i-b_i = 0$ for all i = 1…d+1.

Thus R(x) has more roots than its degree.

Thus, R(x) must be the 0 polynomial, i.e.,
P(x)=Q(x).

Proof #1

The method for constructing the polynomial
is called Lagrange Interpolation.



Discovered in 1795
by J.-L. Lagrange.

Lagrange Interpolation

a_1	b_1
a_2	b_2
a_3	b_3
…	…
a_d	b_d
a_{d+1}	b_{d+1}

Want P(x) with degree $\le$ d
such that $P(a_i) = b_i$ $\forall$i.

Special Case

a_1	1
a_2	0
a_3	0
…	…
a_d	0
a_{d+1}	0

Once we solve this special case,
the general case is very easy.

Special Case

a_1	1
a_2	0
a_3	0
…	…
a_d	0
a_{d+1}	0

Let $Q(x) = (x-a_2)(x-a_3)\cdots(x-a_{d+1})$

$Q(a_1)$ =??

Degree is d. ✔

$Q(a_2) = Q(a_3) = \cdots = Q(a_{d+1}) = 0$. ✔

Lagrange Interpolation

a_1	1
a_2	0
a_3	0
…	…
a_d	0
a_{d+1}	0

Numerator
is a deg. d
polynomial

Denominator
is a nonzero
field element

$$S_1(x) = \frac{Q(x)}{Q(a_1)} = \frac{(x-a_2)\ldots(x-a_{d+1})}{(a_1-a_2)\ldots(a_1-a_{d+1})}$$

Call this the selector polynomial for a_1.

Another special case

a_1	0
a_2	1
a_3	0
…	…
a_d	0
a_{d+1}	0

$$S_2(x) = \frac{(x-a_1)(x-a_3)\ldots(x-a_{d+1})}{(a_2-a_1)(a_2-a_3)\ldots(a_2-a_{d+1})}$$

Lagrange Interpolation

a_1	0
a_2	0
a_3	0
…	…
a_d	0
a_{d+1}	1

$$S_{d+1}(x) = \frac{(x-a_1)\ldots(x-a_d)}{(a_{d+1}-a_1)\ldots(a_{d+1}-a_d)}$$

Great! But what about this data?

a_1	b_1
a_2	b_2
a_3	b_3
…	…
a_d	b_d
a_{d+1}	b_{d+1}

$P(x) = b_1 S_1(x) + \ldots + b_{d+1} S_{d+1}(x)$

This formula is called Lagrange's Interpolation

Recall: Lagrange Interpolation

Let pairs $(a_1,b_1), (a_2,b_2), \ldots, (a_{d+1},b_{d+1})$ from a field F be given (with all a_i's distinct).

Theorem:

There is exactly one polynomial P(x) of degree at most d such that $P(a_i) = b_i$ for all i = 1,…,d+1.

Correspondence between a set of points and a polynomial

Application:

Error-correcting codes

Sending messages on a noisy channel

The channel may corrupt up to k symbols.

How can Alice still read the message?

Sending messages on a noisy channel

Let's say messages are sequences

118 114 120 85 66 78

noisy channel ↓

118 114 ? 85 ? 78

The channel may erase (replace by ?) up to k symbols.

How to correct the errors?

How to even detect that there *are* errors?

Repetition code

Have Bob repeat each symbol k+1 times.

118 114 120 85 66 78

becomes

118 118 118 114 114 114 120 120 120 85 85 85 66 66 66 78 78 78

Noisy channel ↓

118 118 118 ? ? 114 120 120 120 85 85 85 66 66 66 78 78 78

If at most k errors, Alice can figure out each symbol.

This is pretty wasteful!

To send message of d+1 symbols and guard against k errors, we had to send (d+1)(k+1) total symbols.

Can we do better?

Enter polynomials

Say Bob's message is d+1 elements from

118 114 120 85 66 78

Bob thinks of it as the coefficients of a degree d polynomial $P(x) \in F_{257}[x]$

$P(x) = 118x^5 + 114x^4 + 120x^3 + 85x^2 + 66x + 78$

Bob sends the polynomial P(x).

How??

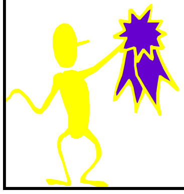
Send it in the Values Representation!

$P(x) = 118x^5 + 114x^4 + 120x^3 + 85x^2 + 66x + 78$

Bob sends P(x)'s values on d+k+1 inputs:

P(1), P(2), P(3), …, P(d+k+1)

This is called the Reed-Solomon encoding.



Reed-Solomon encoding

$P(x) = 118x^5 + 114x^4 + 120x^3 + 85x^2 + 66x + 78$

Bob sends P(x)'s values on d+k+1 inputs:

P(1), P(2), P(3), …, P(d+k+1)

If there are at most k errors, then Alice still knows P's value on d+1 points.

Alice recovers P(x) using Lagrange Interpolation!

Application of Reed–Solomon encoding

Storage devices (CD, DVD, Barcodes, etc)
Mobile communications
Satellite communications
Digital television / DVB
High-speed modems.

Here's What You
Need to Know…

Finite Fields
Polynomial Ring
Lagrange Interpolation
Reed–Solomon encoding