

15-251

Great Theoretical Ideas in Computer Science

m

Algebraic Structures II: Rings and Fields and Polynomials

Lecture 16 (October 14, 2010)

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

more
Few things about group theory
^

Permutations

A permutation of a set X is a bijection $\alpha : X \rightarrow X$

We denote the set of all permutations of $X = \{1, 2, \dots, n\}$ by S_n

$$|S_n| = n!$$

Notation:

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{bmatrix} \text{ means } \alpha(1)=2, \alpha(2)=3, \dots, \alpha(5)=5$$

Composition

Define the operation “ \circ ” on S_n to mean the composition of two permutations

As shorthand, we will write $\alpha \circ \beta$ as $\alpha\beta$

To compute $\alpha\beta$, first apply β and then α :

$$\alpha\beta(i) = \alpha(\beta(i))$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \leftarrow \text{This permutation "fixes 2"}$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

Groups

A group G is a pair (S, \diamond) , where S is a set and \diamond is a binary operation on S such that:

1. \diamond is associative
2. (Identity) There exists an element $e \in S$ such that:
 $e \diamond a = a \diamond e = a$, for all $a \in S$
3. (Inverses) For every $a \in S$ there is $b \in S$ such that: $a \diamond b = b \diamond a = e$

If \diamond is commutative, then G is called a commutative group

(S_n, \bullet) is a Group

Is \bullet associative on S_n ? YES!

Is there an identity? YES: The identity function

$$\begin{bmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{bmatrix}$$

Does every element have an inverse? YES!

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{bmatrix}$$

Is the group commutative? No! (for $n > 2$)

Cycles

Let i_1, i_2, \dots, i_r be distinct integers between 1 and n . Define $(i_1 i_2 \dots i_r)$ to be the permutation α that fixes the remaining $n-r$ integers and for which:

$$\alpha(i_1) = i_2, \alpha(i_2) = i_3, \dots, \alpha(i_{r-1}) = i_r, \alpha(i_r) = i_1$$

$$(5)(1\ 2\ 3\ 4) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} \quad \left(\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{array} \right)$$

$$(1\ 5\ 3\ 4\ 2) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{bmatrix}$$

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$ **Examples** $\rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix}$

$$(1\ 5\ 2)(2\ 4\ 3) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{bmatrix} = (1\ 5\ 2\ 4\ 3)$$

$$(1\ 2\ 3)(4\ 5) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{bmatrix}$$

Two cycles are disjoint if every x moved by one is fixed by the other

$(i_1\ i_2\ \dots\ i_r)$ is called a cycle or an r -cycle

Express α as the product of disjoint cycles

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 2 & 5 & 3 & 8 & 9 & 7 \end{bmatrix}$$

$$= (1\ 6\ 3)(2\ 4)(5)(7\ 8\ 9)$$

Theorem: Every permutation can be uniquely factored into the product of disjoint cycles

Express β as the product of disjoint cycles

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 3 & 2 & 4 & 6 & 1 & 8 & 9 & 5 \end{bmatrix}$$

$$= (1\ 7\ 8\ 9\ 5\ 6)(2\ 3)(4)$$

Now for the new stuff...

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

Definition:

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

1. $(R, +)$ is a commutative group
2. \times is associative ← Minimal requirements from "product"
3. The distributive laws hold in R :

$$(a + b) \times c = (a \times c) + (b \times c)$$

$$c \times (a + b) = (c \times a) + (c \times b)$$

Examples:

Is $(Z, +, *)$ a ring?

Yes. $(Z, +)$ is commutative group
 $*$ is associative
 $+$ distributes over $*$

Is $(Z, +, \min)$ a ring?

No $(Z, +)$ is commutative group
 \min is associative
 but $+$ does not distribute over \min
 $\min(1+3, 2) \neq \min(1, 2) + \min(3, 2)$

Examples:

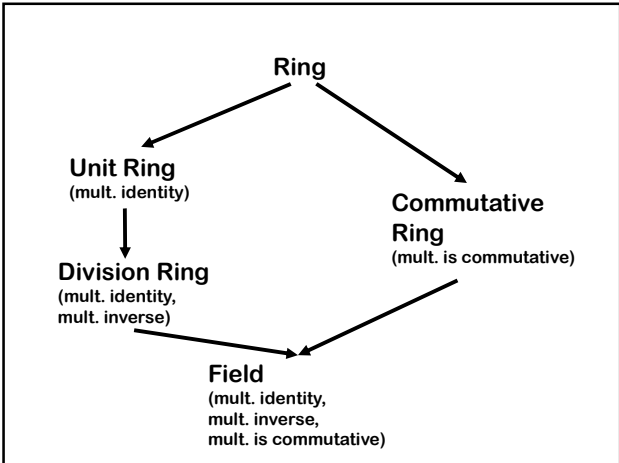
(Set of $m \times n$ Z -valued matrices, $+$, $*$)?
for $m=n$
 It is commutative group with respect to $+$

Yes. $*$ is associative
 $+$ distributes over $*$

(Set of polynomials with real coefficients, $+$, $*$)?

It is commutative group with respect to $+$

Yes. $*$ is associative
 $+$ distributes over $*$



Fields

Definition:

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

1. $(F, +)$ is a commutative group
2. $(F - \{0\}, \times)$ is a commutative group
3. The distributive law holds in F :
 $(a + b) \times c = (a \times c) + (b \times c)$

Examples:

Is $(\mathbb{Z}, +, *)$ a field?

No. $(\mathbb{Z}, *)$ not a group

How about $(\mathbb{R}, +, *)$?

Yes.

How about $(\mathbb{Z}_n, +_n, *_n)$?

Only when n is prime.
 $(\mathbb{Z}_n, *_n)$ is a group
only for prime n .

Polynomials, Lagrange, and Error-correction

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:

$$P(x) = c_d x^d + c_{d-1} x^{d-1} + \dots + c_1 x^1 + c_0$$

The $d+1$ numbers c_d, c_{d-1}, \dots, c_0 are 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 this lecture, we will work with \mathbb{Z}_p

the field $(\mathbb{Z}_p, +, \cdot)$

$(\mathbb{Z}_p = \{0, 1, 2, \dots, p-1\}, +)$
is a commutative group

$(\mathbb{Z}_p^\times = \{1, 2, 3, \dots, p-1\} = \mathbb{Z}_p \setminus \{0\}, \cdot)$
is also a commutative group

$(\mathbb{Z}_p, +, \cdot)$
is a field

Addition distributes over multiplication.

Let $\mathbb{Z}_p[x]$ denote the set of polynomials with variable x and coefficients from \mathbb{Z}_p

Multiplying Polynomials

(say from $\mathbb{Z}_{11}[x]$)

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

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

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

$$= 3x^5 + 6x^4 + 4x^3 + 3x^2 + 4x \quad \left\{ \begin{array}{l} \text{reduce} \\ \text{mod } 11 \end{array} \right.$$

Adding, Multiplying 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.

$\mathbb{Z}_p[x]$ is a commutative ring with identity

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")

Addition is associative

0 (the "zero" polynomial) is the additive identity

$-P(x)$ is the additive inverse of $P(x)$

Also, addition is commutative

$(\mathbb{Z}_p[x], +)$ is a commutative group

$\mathbb{Z}_p[x]$ is a commutative ring with identity

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

The sum $P(x)*Q(x)$ is also a polynomial.

(i.e., polynomials are "closed under multiplication")

Multiplication is associative

1 (the "unit" polynomial) is the multiplicative identity

Multiplication is commutative

Finally, addition distributes over multiplication

$(\mathbb{Z}_p[x], +, \cdot)$ is a commutative ring with identity

(mult. inverses may not exist)

Evaluating a polynomial

Suppose:

$$P(x) = c_d x^d + c_{d-1} x^{d-1} + \dots + c_1 x^1 + c_0$$

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

$$P(5) = 3 \times 5^4 - 7 \times 5^2 + 12 \times 5 - 19$$

$$P(-1) = 3 \times (-1)^4 - 7 \times (-1)^2 + 12 \times (-1) - 19$$

$$P(0) = -19$$

The roots of a polynomial

Suppose:

$$P(x) = c_d x^d + c_{d-1} x^{d-1} + \dots + c_1 x^1 + c_0$$

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

E.g., $P(x) = 3x + 7$ root = $-(7/3)$.

$P(x) = x^2 - 2x + 1$ roots = 1, 1

$P(x) = 3x^3 - 10x^2 + 10x - 2$ roots = $1/3, 1, 2$.

Linear Polynomials

$$P(x) = ax + b$$

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

E.g., $P(x) = 7x - 9$ in $Z_{11}[x]$

$$\begin{aligned} \text{root} &= (-(-9)/7) = 9 * 7^{-1} \\ &= 9 * 8 = 72 \\ &= 6 \pmod{11}. \end{aligned}$$

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

The Single Most Important Theorem About Low-degree Polynomials

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

This fact has many applications...

An application: Theorem

Given pairs $(a_1, b_1), \dots, (a_{d+1}, b_{d+1})$ of values there is at most one degree- d polynomial $P(x)$ such that:
 $P(a_k) = b_k$ for all k

$(4, 17)$
 $(5, 9)$
 $(6, 28)$

when we say "degree- d ", we mean degree at most d .

we'll always assume $a_i \neq a_k$ for $i \neq k$

An application: Theorem

Given pairs $(a_1, b_1), \dots, (a_{d+1}, b_{d+1})$ of values there is at most one degree- d polynomial $P(x)$ such that:
 $P(a_k) = b_k$ for all k

Let's prove the contrapositive

Assume $P(x)$ and $Q(x)$ have degree at most d
 Suppose a_1, a_2, \dots, a_{d+1} are $d+1$ points such that $P(a_k) = Q(a_k)$ for all $k = 1, 2, \dots, d+1$

Then $P(x) = Q(x)$ for all values of x

Proof: Define $R(x) = P(x) - Q(x)$

$R(x)$ has degree (at most) d

$R(x)$ has $d+1$ roots, so it must be the zero polynomial □

Theorem:

Given pairs $(a_1, b_1), \dots, (a_{d+1}, b_{d+1})$ of values
there is at most one
degree-d polynomial $P(x)$
such that:
 $P(a_k) = b_k$ for all k

do there exist $d+1$ pairs
for which there are
no such polynomials??

Revised Theorem:

Given pairs $(a_1, b_1), \dots, (a_{d+1}, b_{d+1})$ of values
there is exactly one
degree-d polynomial $P(x)$
such that:
 $P(a_k) = b_k$ for all k



The algorithm to construct $P(x)$
is called Lagrange Interpolation

Two different representations

$P(x) = c_d x^d + c_{d-1} x^{d-1} + \dots + c_1 x^1 + c_0$
can be represented either by

a) its $d+1$ coefficients

$c_d, c_{d-1}, \dots, c_2, c_1, c_0$

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

$P(a_1), P(a_2), \dots, P(a_d), P(a_{d+1})$

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

**Converting Between The
Two Representations**

Coefficients to Evaluation:

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

Evaluation to Coefficients:

Use Lagrange Interpolation

Revised Theorem:

Given pairs $(a_1, b_1), \dots, (a_{d+1}, b_{d+1})$ of values
there is exactly one
degree-d polynomial $P(x)$
such that:
 $P(a_k) = b_k$ for all k



The algorithm to construct $P(x)$
is called Lagrange Interpolation

An Application:**Error Correcting Codes**

Error Correcting Codes

Messages as sequences of numbers in Z_{29} :

HELLO 8 5 12 12 15

I want to send a sequence of $d+1$ numbers

Suppose your mailer may corrupt any k among all the numbers I send.

How should I send the numbers to you?

In Particular

Suppose I just send over the numbers

8 5 12 12 15

and you get

8 9 0 12 15

say $k=2$ errors

How do you correct errors?

How do you even detect errors?

A Simpler Case: Erasures

Suppose I just send over the numbers

8 5 12 12 15

and you get

8 * * 12 15

say $k=2$ erasures

(Numbers are either correct or changed to *)

What can you do to correct errors?

A Simple Solution

Repetition: repeat each number $k+1$ times

8 8 8 5 5 5 12 12 12 12 12 12 15 15 15

At least one copy of each number will reach

8 8 8 5 * * 12 12 12 12 12 12 15 15 15

For arbitrary corruptions, repeat $2k+1$ times and take majority

Very wasteful!

To send $d+1$ numbers with erasures, we sent $(d+1)(k+1)$ numbers

Can we do better?

Note that to send 1 number with k erasures we need to send $k+1$ numbers.

maybe for d numbers, sending $d+k+1$ numbers suffices??

Think polynomials...

Encoding messages as polynomials:

HELLO

8 5 12 12 15

$$8x^4 + 5x^3 + 12x^2 + 12x + 15 \in Z_{29}[x]$$

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

Send it in the value representation!

Want to send a polynomial of degree-d subject to at most k erasures.

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

Send P(0), P(1), P(2), ..., P(d+k)

At least d+1 of these values will reach

Say P(0), *, P(2), *, ..., *, P(d+k)

Can recover P(x) from these d+1 values

Example

$f(x) = 8x^4 + 5x^3 + 12x^2 + 12x + 15$

$x=0$	15
$x=1$	23
$x=2$	23
$x=3$	14
$x=4$	13
$x=5$	26
$x=6$	19

Example

$f(x) = 8x^4 + 5x^3 + 12x^2 + 12x + 15$

$f(0) \text{ mod } 29$	15	(1)
$f(1) \text{ mod } 29$	23	(2)
$f(2) \text{ mod } 29$	23	(3)
$f(3) \text{ mod } 29$	14	(4)
$f(4) \text{ mod } 29$	13	(5)
$f(5) \text{ mod } 29$	26	(6)
$f(6) \text{ mod } 29$	19	(7)

Curve Fitting: Polynomial Interpolation ([[0, 15], [1, 23], [4, 13], [5, 26], [6, 19]]), x_form = Lagrange ;

$\frac{1}{0} (x-1)(x-4)(x-5)(x-6) - \frac{23}{60} x(x-4)(x-5)(x-6) + \frac{13}{24} x(x-1)(x-5)(x-6) - \frac{13}{10} x(x-1)(x-4)(x-6) + \frac{19}{60} x(x-1)(x-4)(x-5)$

$g := \text{eval}(\text{expand}(\% \text{ mod } 29))$

$8x^4 + 5x^3 + 12x^2 + 12x + 15$

Much better!!!

Naïve Repetition:

To send d+1 numbers with k erasures, we sent (d+1)(k+1) numbers

Polynomial Coding:

To send d+1 numbers with k erasures, we sent (d+k+1) numbers

What about corruptions?

Want to send a polynomial of degree-d subject to at most k corruptions.

Similar ideas suffice, see the supplementary material

This technique (encoding using polynomials) is called Reed-Solomon coding...

It's used in practice...

TO: TELECOM SUPPLIER
155 BORNHOUTER HWY
W ICHU BEACH, FL
07764-1394

TO: TELECOM CUSTOMER
2020 VALLEYDALE ROAD
BIRMINGHAM, AL
35244

(S) TRACK ID: 0662742MV96421234

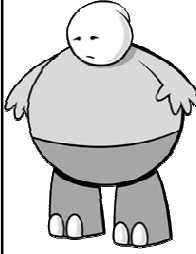
(P) CUST TRACK ID: AA00211211 RINGER C4C

(Q) QUANTITY: 1 EA PACKAGE COUNT: 1 OF 1
PACKAGE WEIGHT: 3 LBS

(R) TRACK ID: [Barcode]

Maxicodes = "UPS codes" = another 2-d Reed-Solomon codes

PDF417 codes = 2-d Reed-Solomon codes



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

Lagrange Interpolation:
 Given $d+1$ pairs (a_k, b_k) , can find
 unique poly P with $P(a_k) = b_k$
 for all these k .
 Gives us value represent'n for polys.

Here's What You Need to Know...

Error Correction
 Erasure codes
 Detection and correction

Supplementary Material

What about corruptions?

Want to send a polynomial of degree-d
 subject to at most k corruptions.

Suppose we try the same idea

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

Send $P(0), P(1), P(2), \dots, P(d+k)$

At least $d+1$ of these values will be unchanged

Example

$P(x) = 2x^2 + 1$, and $k = 1$.

So I sent $P(0)=1, P(1)=3, P(2)=9, P(3)=19$

Corrupted email says $(1, 4, 9, 19)$

Choosing $(1, 4, 9)$ will give us $Q(x) = x^2 + 2x + 1$

But we can at least detect errors!

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

Send $P(0), P(1), P(2), \dots, P(d+k)$

At least $d+1$ of these values will be correct

Say $P(0), P(1), P(2), P(3), P(4), \dots, P(d+k)$

Using these $d+1$ correct values will give $P(x)$

Using any of the incorrect values will
 give something else

Quick way of detecting errors

Interpolate first $d+1$ points to get $Q(x)$

Check that all other received values are
 consistent with this polynomial $Q(x)$

If all values consistent, no errors!

In that case, we know $Q(x) = P(x)$
 else there were errors...

Number of numbers?

Naïve Repetition:

To send $d+1$ numbers with error detection,
sent $(d+1)(k+1)$ numbers

Polynomial Coding:

To send $d+1$ numbers with error detection,
sent $(d+k+1)$ numbers

How about error correction?

requires more work

To send $d+1$ numbers in such a way
that we can correct up to k errors,
need to send $d+1+2k$ numbers.

Similar encoding scheme

Evaluate degree- d $P(x)$ at $d+1+2k$ points

Send $P(0), P(1), P(2), \dots, P(d+2k)$

At least $d+1+k$ of these values will be correct

Say $P(0), P(1), P(2), P(3), P(4), \dots, P(d+2k)$

How do we know which are correct?

how do we do this fast?

Theorem: A unique degree- d polynomial $R(x)$
can agree with the received data on
at least $d+1+k$ points

Clearly, the original polynomial $P(x)$
agrees with data on $d+1+k$ points
(since at most k errors, total $d+1+2k$ points)

And if two different degree- d polynomials did so,
they would have to agree with each other on
 $d+1$ points, and hence be the same.

So any such $R(x) = P(x)$

Theorem: A unique degree- d polynomial $R(x)$
can agree with the received data on
at least $d+1+k$ points

Brute-force Algorithm:

Interpolate each subset of $(d+1)$ points

Check if the resulting polynomial agrees
with received data on $d+1+k$ pts

Takes too much time...

A fast algorithm to decode was given
by Berlekamp and Welch
which solves a system of linear equations

Recent research has given very fast
encoding and decoding algorithms

BTW, this coding scheme is called
Reed-Solomon encoding