Algebraic Structures and Polynomials

CS70 Summer 2016 - Lecture 7C

David Dinh

03 August 2016

UC Berkeley

Today

Review: Chinese Remainder Theorem and Blum Coin Flipping

Algebraic Structures: Groups, Rings, and Fields

Galois Fields

Polynomials

Applications: Secret Sharing and Erasure Codes

Motivation

We’ve been talking about manipulating numbers in modular arithmetic and congruences as in a manner similar to talking about ordinary numbers.

Motivation

We’ve been talking about manipulating numbers in modular arithmetic and congruences as in a manner similar to talking about ordinary numbers.

Can we express turn numbers and congruences in modular arithmetic into their own “number system”?

Motivation

We’ve been talking about manipulating numbers in modular arithmetic and congruences as in a manner similar to talking about ordinary numbers.

Can we express turn numbers and congruences in modular arithmetic into their own “number system”?

Define *algebraic structures* through axioms that define how they behave.

Groups

A **group** $(G, +)$ is a pair consisting of a set G and a binary operation $\cdot$ that satisfies the following axioms:

- **Closure**: If $a, b \in G$, then $a + b \in G$.

Groups

A **group** $(G, +)$ is a pair consisting of a set G and a binary operation $\cdot$ that satisfies the following axioms:

- **Closure**: If $a, b \in G$, then $a + b \in G$.
- **Associativity:** For all $a, b, c \in G$: $a + (b + c) = (a + b) + c$.

Groups

A **group** $(G,+)$ is a pair consisting of a set G and a binary operation $\cdot$ that satisfies the following axioms:

- **Closure**: If $a, b \in G$, then $a+b \in G$.
- **Associativity:** For all $a, b, c \in G$: $a+(b+c) = (a+b)+c$.
- **Existence of Identity:** There exists some element $e \in G$ such that for all $a \in G$, $e+a = a$.

Groups

A **group** $(G,+)$ is a pair consisting of a set G and a binary operation $\cdot$ that satisfies the following axioms:

- **Closure**: If $a,b \in G$, then $a+b \in G$.
- **Associativity:** For all $a,b,c \in G$: $a+(b+c)=(a+b)+c$.
- **Existence of Identity:** There exists some element $e \in G$ such that for all $a \in G$, $e+a=a$.
- **Existence of inverse:** For all $a \in G$, exists $b \in G$ such that $a+b=b+a=e$.

Groups

A **group** $(G, +)$ is a pair consisting of a set G and a binary operation $\cdot$ that satisfies the following axioms:

- **Closure**: If $a, b \in G$, then $a + b \in G$.
- **Associativity:** For all $a, b, c \in G$: $a + (b + c) = (a + b) + c$.
- **Existence of Identity:** There exists some element $e \in G$ such that for all $a \in G$, $e + a = a$.
- **Existence of inverse:** For all $a \in G$, exists $b \in G$ such that $a + b = b + a = e$.

Notice that there no commutativity requirement. "$\cdot$" may be non-commutative! If it is commutative, we refer to the group as *abelian*. Formally, Abelian groups must satisfy requires another axiom:

- **Commutativity:** For all $a, b \in G$: $a + b = b + a$.

Groups

A **group** $(G,+)$ is a pair consisting of a set G and a binary operation $\cdot$ that satisfies the following axioms:

- **Closure**: If $a,b \in G$, then $a+b \in G$.
- **Associativity:** For all $a,b,c \in G$: $a+(b+c) = (a+b)+c$.
- **Existence of Identity:** There exists some element $e \in G$ such that for all $a \in G$, $e+a = a$.
- **Existence of inverse:** For all $a \in G$, exists $b \in G$ such that $a+b = b+a = e$.

Notice that there no commutativity requirement. "$\cdot$" may be non-commutative! If it is commutative, we refer to the group as *abelian*. Formally, Abelian groups must satisfy requires another axiom:

- **Commutativity:** For all $a,b \in G$: $a+b = b+a$.

Also, note that $+$ doesn't necessarily have to represent addition in the normal sense. Elements of G may not even be numbers!

Rings and Fields

Start with an Abelian group $(R, +)$. Turn it into a ring by adding another binary operation, "$\cdot$" (that it is closed on). In addition to the Abelian group axioms for $(R, +)$, a ring must satisfy the following:

Start with an Abelian group $(R, +)$. Turn it into a ring by adding another binary operation, "$\cdot$" (that it is closed on). In addition to the Abelian group axioms for $(R, +)$, a ring must satisfy the following:

- **Associativity:** For all $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Rings and Fields

Start with an Abelian group $(R, +)$. Turn it into a ring by adding another binary operation, "$\cdot$" (that it is closed on). In addition to the Abelian group axioms for $(R, +)$, a ring must satisfy the following:

- **Associativity:** For all $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **Multiplicative identity:** There exists an element $1 \in R$ such that for all $a \in R$, $1 \cdot a = a \cdot 1 = a$.

Rings and Fields

Start with an Abelian group $(R,+)$. Turn it into a ring by adding another binary operation, "$\cdot$" (that it is closed on). In addition to the Abelian group axioms for $(R,+)$, a ring must satisfy the following:

- **Associativity:** For all $a,b,c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **Multiplicative identity:** There exists an element $1 \in R$ such that for all $a \in R$, $1 \cdot a = a \cdot 1 = a$.
- **Left and right distributivity:** For all $a,b,c \in R$, $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$.

Rings and Fields

Start with an Abelian group $(R,+)$. Turn it into a ring by adding another binary operation, "$\cdot$" (that it is closed on). In addition to the Abelian group axioms for $(R,+)$, a ring must satisfy the following:

- **Associativity:** For all $a,b,c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **Multiplicative identity:** There exists an element $1 \in R$ such that for all $a \in R$, $1 \cdot a = a \cdot 1 = a$.
- **Left and right distributivity:** For all $a,b,c \in R$, $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$.

A ring is **commutative** if for all $a,b \in r$, $a \cdot b = b \cdot a$.

Rings and Fields

Start with an Abelian group $(R, +)$. Turn it into a ring by adding another binary operation, "$\cdot$" (that it is closed on). In addition to the Abelian group axioms for $(R, +)$, a ring must satisfy the following:

- **Associativity:** For all $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **Multiplicative identity:** There exists an element $1 \in R$ such that for all $a \in R$, $1 \cdot a = a \cdot 1 = a$.
- **Left and right distributivity:** For all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

A ring is **commutative** if for all $a, b \in r$, $a \cdot b = b \cdot a$.

Add **multiplicative inverses** to get a *field*: for all $a \neq 0 \in R$, exists $a^{-1} \in R$ such that $a \cdot a^{-1} = 1$.

Rings and Fields

Start with an Abelian group $(R,+)$. Turn it into a ring by adding another binary operation, "$\cdot$" (that it is closed on). In addition to the Abelian group axioms for $(R,+)$, a ring must satisfy the following:

- **Associativity:** For all $a,b,c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **Multiplicative identity:** There exists an element $1 \in R$ such that for all $a \in R$, $1 \cdot a = a \cdot 1 = a$.
- **Left and right distributivity:** For all $a,b,c \in R$, $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$.

A ring is **commutative** if for all $a,b \in r$, $a \cdot b = b \cdot a$.

Add **multiplicative inverses** to get a *field*: for all $a \neq 0 \in R$, exists $a^{-1} \in R$ such that $a \cdot a^{-1} = 1$.

Examples: With addition and multiplication defined in the usual sense $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{C}$ are fields. $\mathbb{Z}$ is a commutative ring but not a field.

How do we apply fields to modular arithmetic?

[1] Also known as Galois or finite fields for prime p, although those are more general objects that have different meanings for non-prime p as well.

Galois Fields

How do we apply fields to modular arithmetic?

Let $\mathbb{Z}_n$ denote the set $\{0, 1, 2, \ldots, n-1\}$ and consider $(\mathbb{Z}_n, +, \cdot)$ where $+$ and $\cdot$ are defined as standard addition and multiplication $\pmod{n}$. It follows immediately from the standard properties of addition and multiplication that this is a commutative ring.

[1] Also known as Galois or finite fields for prime p, although those are more general objects that have different meanings for non-prime p as well.

Galois Fields

How do we apply fields to modular arithmetic?

Let $\mathbb{Z}_n$ denote the set $\{0, 1, 2, \ldots, n-1\}$ and consider $(\mathbb{Z}_n, +, \cdot)$ where $+$ and $\cdot$ are defined as standard addition and multiplication $\pmod{n}$. It follows immediately from the standard properties of addition and multiplication that this is a commutative ring.

Is it a field?

[1]Also known as Galois or finite fields for prime p, although those are more general objects that have different meanings for non-prime p as well.

Galois Fields

How do we apply fields to modular arithmetic?

Let $\mathbb{Z}_n$ denote the set $\{0, 1, 2, \dots, n-1\}$ and consider $(\mathbb{Z}_n, +, \cdot)$ where $+$ and $\cdot$ are defined as standard addition and multiplication $\pmod{n}$. It follows immediately from the standard properties of addition and multiplication that this is a commutative ring.

Is it a field? How do we guarantee that there's a multiplicative inverse for each $k \in \mathbb{Z}_n$?

[1] Also known as Galois or finite fields for prime p, although those are more general objects that have different meanings for non-prime p as well.

Galois Fields

How do we apply fields to modular arithmetic?

Let $\mathbb{Z}_n$ denote the set $\{0, 1, 2, \ldots, n-1\}$ and consider $(\mathbb{Z}_n, +, \cdot)$ where $+$ and $\cdot$ are defined as standard addition and multiplication $\pmod{n}$. It follows immediately from the standard properties of addition and multiplication that this is a commutative ring.

Is it a field? How do we guarantee that there's a multiplicative inverse for each $k \in \mathbb{Z}_n$?

To be a multiplicative inverse: $\gcd(k, n) = 1$. How do we make sure that this holds for all $k \in \mathbb{Z}_n$?

[1] Also known as Galois or finite fields for prime p, although those are more general objects that have different meanings for non-prime p as well.

Galois Fields

How do we apply fields to modular arithmetic?

Let $\mathbb{Z}_n$ denote the set $\{0, 1, 2, \ldots, n-1\}$ and consider $(\mathbb{Z}_n, +, \cdot)$ where $+$ and $\cdot$ are defined as standard addition and multiplication $\pmod{n}$. It follows immediately from the standard properties of addition and multiplication that this is a commutative ring.

Is it a field? How do we guarantee that there's a multiplicative inverse for each $k \in \mathbb{Z}_n$?

To be a multiplicative inverse: $\gcd(k, n) = 1$. How do we make sure that this holds for all $k \in \mathbb{Z}_n$? Make n prime.

[1] Also known as Galois or finite fields for prime p, although those are more general objects that have different meanings for non-prime p as well.

Galois Fields

How do we apply fields to modular arithmetic?

Let $\mathbb{Z}_n$ denote the set $\{0, 1, 2, \ldots, n-1\}$ and consider $(\mathbb{Z}_n, +, \cdot)$ where $+$ and $\cdot$ are defined as standard addition and multiplication $\pmod{n}$. It follows immediately from the standard properties of addition and multiplication that this is a commutative ring.

Is it a field? How do we guarantee that there's a multiplicative inverse for each $k \in \mathbb{Z}_n$?

To be a multiplicative inverse: $\gcd(k, n) = 1$. How do we make sure that this holds for all $k \in \mathbb{Z}_n$? Make n prime.

Definition: For prime p, the field $(\mathbb{Z}_p, +, \cdot)$, with $+$ and $\cdot$ defined as modular arithmetic $\pmod{p}$, is known as the prime field[1] of order p, denoted $GF(p)$.

[1] Also known as Galois or finite fields for prime p, although those are more general objects that have different meanings for non-prime p as well.

Galois Fields

How do we apply fields to modular arithmetic?

Let $\mathbb{Z}_n$ denote the set $\{0,1,2,\ldots,n-1\}$ and consider $(\mathbb{Z}_n,+,\cdot)$ where $+$ and $\cdot$ are defined as standard addition and multiplication $\pmod{n}$. It follows immediately from the standard properties of addition and multiplication that this is a commutative ring.

Is it a field? How do we guarantee that there's a multiplicative inverse for each $k \in \mathbb{Z}_n$?

To be a multiplicative inverse: $\gcd(k,n)=1$. How do we make sure that this holds for all $k \in \mathbb{Z}_n$? Make n prime.

Definition: For prime p, the field $(\mathbb{Z}_p,+,\cdot)$, with $+$ and $\cdot$ defined as modular arithmetic $\pmod{p}$, is known as the prime field[1] of order p, denoted $GF(p)$.

[1] Also known as Galois or finite fields for prime p, although those are more general objects that have different meanings for non-prime p as well.

Polynomials

Polynomials

Now that we have a framework for modular math (mod some prime): let's extend this to polynomials.

Polynomials

Now that we have a framework for modular math (mod some prime): let's extend this to polynomials.

We'll be working with polynomials in prime fields.

Polynomials

Now that we have a framework for modular math (mod some prime): let's extend this to polynomials.

We'll be working with polynomials in prime fields.

A polynomial of *degree d* over some commutative ring R is an expression of the form

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$$

where the coefficients a_i are elements of R.

Polynomials

Now that we have a framework for modular math (mod some prime): let's extend this to polynomials.

We'll be working with polynomials in prime fields.

A polynomial of *degree d* over some commutative ring R is an expression of the form

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$$

where the coefficients a_i are elements of R.

A polynomial is said to contain a point (x, y) if $p(x) = y$.

Specifying a Polynomial

How do we describe polynomials?

Specifying a Polynomial

How do we describe polynomials?

One way: just give me the coefficients. $a_0, a_1, \ldots, a_d$. $d+1$ numbers.

Specifying a Polynomial

How do we describe polynomials?

One way: just give me the coefficients. $a_0, a_1, \ldots, a_d$. $d+1$ numbers.

Another way to think about it: specify polynomials by points that it contains. Obviously if we specify every single point that it does (in a finite ring there are only finitely many points, so we can list them all) that fully specifies the polynomial.

Specifying a Polynomial

How do we describe polynomials?

One way: just give me the coefficients. $a_0, a_1, \ldots, a_d$. $d+1$ numbers.

Another way to think about it: specify polynomials by points that it contains. Obviously if we specify every single point that it does (in a finite ring there are only finitely many points, so we can list them all) that fully specifies the polynomial. Can we do it in fewer points?

Specifying a Polynomial

How do we describe polynomials?

One way: just give me the coefficients. $a_0, a_1, \ldots, a_d$. $d+1$ numbers.

Another way to think about it: specify polynomials by points that it contains. Obviously if we specify every single point that it does (in a finite ring there are only finitely many points, so we can list them all) that fully specifies the polynomial. Can we do it in fewer points?

What's a polynomial of degree 0?

Specifying a Polynomial

How do we describe polynomials?

One way: just give me the coefficients. $a_0, a_1, \ldots, a_d$. $d+1$ numbers.

Another way to think about it: specify polynomials by points that it contains. Obviously if we specify every single point that it does (in a finite ring there are only finitely many points, so we can list them all) that fully specifies the polynomial. Can we do it in fewer points?

What's a polynomial of degree 0? Just a constant function. $p(x) = a_0$.

Specifying a Polynomial

How do we describe polynomials?

One way: just give me the coefficients. $a_0, a_1, \ldots, a_d$. $d+1$ numbers.

Another way to think about it: specify polynomials by points that it contains. Obviously if we specify every single point that it does (in a finite ring there are only finitely many points, so we can list them all) that fully specifies the polynomial. Can we do it in fewer points?

What's a polynomial of degree 0? Just a constant function. $p(x) = a_0$. How many points to I need to specify a constant function?

Specifying a Polynomial

How do we describe polynomials?

One way: just give me the coefficients. $a_0, a_1, \ldots, a_d$. $d+1$ numbers.

Another way to think about it: specify polynomials by points that it contains. Obviously if we specify every single point that it does (in a finite ring there are only finitely many points, so we can list them all) that fully specifies the polynomial. Can we do it in fewer points?

What's a polynomial of degree 0? Just a constant function. $p(x) = a_0$. How many points to I need to specify a constant function? Just 1. $(\text{anything}, a_0)$.

Specifying a Polynomial

How do we describe polynomials?

One way: just give me the coefficients. $a_0, a_1, \ldots, a_d$. $d+1$ numbers.

Another way to think about it: specify polynomials by points that it contains. Obviously if we specify every single point that it does (in a finite ring there are only finitely many points, so we can list them all) that fully specifies the polynomial. Can we do it in fewer points?

What's a polynomial of degree 0? Just a constant function. $p(x) = a_0$. How many points to I need to specify a constant function? Just 1. $(\text{anything}, a_0)$.

What about a polynomial of degree 1? It's a

Specifying a Polynomial

How do we describe polynomials?

One way: just give me the coefficients. $a_0, a_1, \ldots, a_d$. $d+1$ numbers.

Another way to think about it: specify polynomials by points that it contains. Obviously if we specify every single point that it does (in a finite ring there are only finitely many points, so we can list them all) that fully specifies the polynomial. Can we do it in fewer points?

What's a polynomial of degree 0? Just a constant function. $p(x) = a_0$. How many points to I need to specify a constant function? Just 1. $(\text{anything}, a_0)$.

What about a polynomial of degree 1? It's a line.

Specifying a Polynomial

How do we describe polynomials?

One way: just give me the coefficients. $a_0, a_1, \ldots, a_d$. $d+1$ numbers.

Another way to think about it: specify polynomials by points that it contains. Obviously if we specify every single point that it does (in a finite ring there are only finitely many points, so we can list them all) that fully specifies the polynomial. Can we do it in fewer points?

What's a polynomial of degree 0? Just a constant function. $p(x) = a_0$. How many points to I need to specify a constant function? Just 1. $(\text{anything}, a_0)$.

What about a polynomial of degree 1? It's a line. How many points do I need to specify a line?

Specifying a Polynomial

How do we describe polynomials?

One way: just give me the coefficients. $a_0, a_1, \ldots, a_d$. $d+1$ numbers.

Another way to think about it: specify polynomials by points that it contains. Obviously if we specify every single point that it does (in a finite ring there are only finitely many points, so we can list them all) that fully specifies the polynomial. Can we do it in fewer points?

What's a polynomial of degree 0? Just a constant function. $p(x) = a_0$. How many points to I need to specify a constant function? Just 1. $(\text{anything}, a_0)$.

What about a polynomial of degree 1? It's a line. How many points do I need to specify a line? 2.

Specifying a Polynomial

How do we describe polynomials?

One way: just give me the coefficients. $a_0, a_1, \ldots, a_d$. $d+1$ numbers.

Another way to think about it: specify polynomials by points that it contains. Obviously if we specify every single point that it does (in a finite ring there are only finitely many points, so we can list them all) that fully specifies the polynomial. Can we do it in fewer points?

What's a polynomial of degree 0? Just a constant function. $p(x) = a_0$. How many points to I need to specify a constant function? Just 1. $(\text{anything}, a_0)$.

What about a polynomial of degree 1? It's a line. How many points do I need to specify a line? 2.

Beginning to see a pattern here? How many points do I need to specify a polynomial of degree 2?

Specifying a Polynomial

How do we describe polynomials?

One way: just give me the coefficients. $a_0, a_1, \ldots, a_d$. $d+1$ numbers.

Another way to think about it: specify polynomials by points that it contains. Obviously if we specify every single point that it does (in a finite ring there are only finitely many points, so we can list them all) that fully specifies the polynomial. Can we do it in fewer points?

What's a polynomial of degree 0? Just a constant function. $p(x) = a_0$. How many points to I need to specify a constant function? Just 1. (anything, a_0).

What about a polynomial of degree 1? It's a line. How many points do I need to specify a line? 2.

Beginning to see a pattern here? How many points do I need to specify a polynomial of degree 2? 3.

Specifying a Polynomial

How do we describe polynomials?

One way: just give me the coefficients. $a_0, a_1, \ldots, a_d$. $d+1$ numbers.

Another way to think about it: specify polynomials by points that it contains. Obviously if we specify every single point that it does (in a finite ring there are only finitely many points, so we can list them all) that fully specifies the polynomial. Can we do it in fewer points?

What's a polynomial of degree 0? Just a constant function. $p(x) = a_0$. How many points to I need to specify a constant function? Just 1. $(\text{anything}, a_0)$.

What about a polynomial of degree 1? It's a line. How many points do I need to specify a line? 2.

Beginning to see a pattern here? How many points do I need to specify a polynomial of degree 2? 3. Degree d?

Specifying a Polynomial

How do we describe polynomials?

One way: just give me the coefficients. $a_0, a_1, \ldots, a_d$. $d+1$ numbers.

Another way to think about it: specify polynomials by points that it contains. Obviously if we specify every single point that it does (in a finite ring there are only finitely many points, so we can list them all) that fully specifies the polynomial. Can we do it in fewer points?

What's a polynomial of degree 0? Just a constant function. $p(x) = a_0$. How many points to I need to specify a constant function? Just 1. $(\text{anything}, a_0)$.

What about a polynomial of degree 1? It's a line. How many points do I need to specify a line? 2.

Beginning to see a pattern here? How many points do I need to specify a polynomial of degree 2? 3. Degree d? $d+1$.

Specifying Polynomials with Points

If I have some degree-d polynomial, and I give you $d+1$ points for it, how do you get the coefficients back from the points?

Specifying Polynomials with Points

If I have some degree-d polynomial, and I give you $d+1$ points for it, how do you get the coefficients back from the points?

One way to do it: try plugging in the points and solving for the coefficients.

Specifying Polynomials with Points

If I have some degree-d polynomial, and I give you $d+1$ points for it, how do you get the coefficients back from the points?

One way to do it: try plugging in the points and solving for the coefficients. Say I give you $(x_1, y_1), (x_2, y_,), \ldots, (x_{d+1}, y_{d+1})$.

$$\begin{aligned} y_1 &= a_0 + a_1 x_1 + a_2 x_1^2 + \cdots + a_d x_1^d \\ &\vdots \\ y_{d+1} &= a_0 + a_1 x_{d+1} + a_2 x_{d+1}^2 + \cdots + a_d x_{d+1}^d \end{aligned}$$

Or in matrix form:

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^d \\ 1 & x_2 & x_2^2 & \ldots & x_2^d \\ 1 & x_3 & x_3^2 & \ldots & x_3^d \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{d+1} & x_{d+1}^2 & \ldots & x_{d+1}^d \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_d \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_{d+1} \end{bmatrix}$$

(This matrix is called the *Vandermonde matrix*.)

Lagrange Interpolation (1/2)

How do we know the system of equations on the previous slide has a solution? Unfortunately, we don't. (If you know linear algebra you can prove directly through determinants or through linear independence that the Vandermonde matrix is nonsingular, but that's beyond the scope of this course.)

Lagrange Interpolation (1/2)

How do we know the system of equations on the previous slide has a solution? Unfortunately, we don't. (If you know linear algebra you can prove directly through determinants or through linear independence that the Vandermonde matrix is nonsingular, but that's beyond the scope of this course.)

Let's try another way to get the polynomial: set the value at each x-coordinate, one at a time.

Lagrange Interpolation (1/2)

How do we know the system of equations on the previous slide has a solution? Unfortunately, we don't. (If you know linear algebra you can prove directly through determinants or through linear independence that the Vandermonde matrix is nonsingular, but that's beyond the scope of this course.)

Let's try another way to get the polynomial: set the value at each x-coordinate, one at a time.

Notice that $(x - x_2)(x - x_3)\ldots(x - x_{d+1})$ is zero at $x_2, x_3, \ldots, x_{d+1}$ (but not at x_1).

Lagrange Interpolation (1/2)

How do we know the system of equations on the previous slide has a solution? Unfortunately, we don't. (If you know linear algebra you can prove directly through determinants or through linear independence that the Vandermonde matrix is nonsingular, but that's beyond the scope of this course.)

Let's try another way to get the polynomial: set the value at each x-coordinate, one at a time.

Notice that $(x-x_2)(x-x_3)\dots(x-x_{d+1})$ is zero at $x_2, x_3, \dots, x_{d+1}$ (but not at x_1). What if we divide by its value at $x = x_1$ and then multiply by y_1?

Lagrange Interpolation (1/2)

How do we know the system of equations on the previous slide has a solution? Unfortunately, we don't. (If you know linear algebra you can prove directly through determinants or through linear independence that the Vandermonde matrix is nonsingular, but that's beyond the scope of this course.)

Let's try another way to get the polynomial: set the value at each x-coordinate, one at a time.

Notice that $(x-x_2)(x-x_3)\dots(x-x_{d+1})$ is zero at $x_2, x_3, \dots, x_{d+1}$ (but not at x_1). What if we divide by its value at $x = x_1$ and then multiply by y_1?

$$\Delta_1(x) \coloneqq y_1 \frac{(x-x_2)(x-x_3)\dots(x-x_{d+1})}{(x_1-x_2)(x_1-x_3)\dots(x_1-x_{d+1})}$$

Value at x_1?

Lagrange Interpolation (1/2)

How do we know the system of equations on the previous slide has a solution? Unfortunately, we don't. (If you know linear algebra you can prove directly through determinants or through linear independence that the Vandermonde matrix is nonsingular, but that's beyond the scope of this course.)

Let's try another way to get the polynomial: set the value at each x-coordinate, one at a time.

Notice that $(x-x_2)(x-x_3)\dots(x-x_{d+1})$ is zero at $x_2, x_3, \dots, x_{d+1}$ (but not at x_1). What if we divide by its value at $x = x_1$ and then multiply by y_1?

$$\Delta_1(x) \coloneqq y_1 \frac{(x-x_2)(x-x_3)\dots(x-x_{d+1})}{(x_1-x_2)(x_1-x_3)\dots(x_1-x_{d+1})}$$

Value at x_1? y_1.

Lagrange Interpolation (1/2)

How do we know the system of equations on the previous slide has a solution? Unfortunately, we don't. (If you know linear algebra you can prove directly through determinants or through linear independence that the Vandermonde matrix is nonsingular, but that's beyond the scope of this course.)

Let's try another way to get the polynomial: set the value at each x-coordinate, one at a time.

Notice that $(x-x_2)(x-x_3)\ldots(x-x_{d+1})$ is zero at $x_2, x_3, \ldots, x_{d+1}$ (but not at x_1). What if we divide by its value at $x = x_1$ and then multiply by y_1?

$$\Delta_1(x) \coloneqq y_1 \frac{(x-x_2)(x-x_3)\ldots(x-x_{d+1})}{(x_1-x_2)(x_1-x_3)\ldots(x_1-x_{d+1})}$$

Value at x_1? y_1. Value at $x_2, \ldots, x_{d+1}$?

Lagrange Interpolation (1/2)

How do we know the system of equations on the previous slide has a solution? Unfortunately, we don't. (If you know linear algebra you can prove directly through determinants or through linear independence that the Vandermonde matrix is nonsingular, but that's beyond the scope of this course.)

Let's try another way to get the polynomial: set the value at each x-coordinate, one at a time.

Notice that $(x-x_2)(x-x_3)\dots(x-x_{d+1})$ is zero at $x_2, x_3, \dots, x_{d+1}$ (but not at x_1). What if we divide by its value at $x = x_1$ and then multiply by y_1?

$$\Delta_1(x) \coloneqq y_1 \frac{(x-x_2)(x-x_3)\dots(x-x_{d+1})}{(x_1-x_2)(x_1-x_3)\dots(x_1-x_{d+1})}$$

Value at x_1? y_1. Value at $x_2, \dots, x_{d+1}$? 0.

Lagrange Interpolation (1/2)

How do we know the system of equations on the previous slide has a solution? Unfortunately, we don't. (If you know linear algebra you can prove directly through determinants or through linear independence that the Vandermonde matrix is nonsingular, but that's beyond the scope of this course.)

Let's try another way to get the polynomial: set the value at each x-coordinate, one at a time.

Notice that $(x-x_2)(x-x_3)\dots(x-x_{d+1})$ is zero at $x_2, x_3, \dots, x_{d+1}$ (but not at x_1). What if we divide by its value at $x = x_1$ and then multiply by y_1?

$$\Delta_1(x) \coloneqq y_1 \frac{(x-x_2)(x-x_3)\dots(x-x_{d+1})}{(x_1-x_2)(x_1-x_3)\dots(x_1-x_{d+1})}$$

Value at x_1? y_1. Value at $x_2, \dots, x_{d+1}$? 0. General idea behind interpolation: make these polynomials for all i and add them together.

Lagrange Interpolation (2/2)

Generally, define:

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

Lagrange Interpolation (2/2)

Generally, define:

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

From construction we know that $\Delta_i(x_i) = 1$ and $\Delta_i(x_j) = 0$ for $j \neq i$.

Lagrange Interpolation (2/2)

Generally, define:

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

From construction we know that $\Delta_i(x_i) = 1$ and $\Delta_i(x_j) = 0$ for $j \neq i$. Therefore,

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

must contain $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$.

Lagrange Interpolation (2/2)

Generally, define:

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

From construction we know that $\Delta_i(x_i) = 1$ and $\Delta_i(x_j) = 0$ for $j \neq i$. Therefore,

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

must contain $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$. Degree of this polynomial?

Lagrange Interpolation (2/2)

Generally, define:

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

From construction we know that $\Delta_i(x_i) = 1$ and $\Delta_i(x_j) = 0$ for $j \neq i$. Therefore,

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

must contain $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$. Degree of this polynomial? Just number of terms in each product, d.

Lagrange Interpolation (2/2)

Generally, define:

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

From construction we know that $\Delta_i(x_i) = 1$ and $\Delta_i(x_j) = 0$ for $j \neq i$. Therefore,

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

must contain $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$. Degree of this polynomial? Just number of terms in each product, d. So we have a polynomial of degree d that passes through all our points.

Lagrange Interpolation (2/2)

Generally, define:

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

From construction we know that $\Delta_i(x_i) = 1$ and $\Delta_i(x_j) = 0$ for $j \neq i$. Therefore,

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

must contain $(x_1, y_1), (x_2, y_2), \dots, (x_{d+1}, y_{d+1})$. Degree of this polynomial? Just number of terms in each product, d. So we have a polynomial of degree d that passes through all our points.

When does interpolation work? Notice that we need division also.

Lagrange Interpolation (2/2)

Generally, define:

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

From construction we know that $\Delta_i(x_i) = 1$ and $\Delta_i(x_j) = 0$ for $j \neq i$. Therefore,

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

must contain $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$. Degree of this polynomial? Just number of terms in each product, d. So we have a polynomial of degree d that passes through all our points.

When does interpolation work? Notice that we need division also. **Polynomial must be over a field in order to guarantee that interpolation works.**

Uniqueness?

Now we have a polynomial passing through a collection of $d+1$ points. Is it the *only* polynomial passing through these points? Or: we know the system given by the Vandermonde matrix has a solution. Is it a unique solution or is the system underdetermined?

Uniqueness?

Now we have a polynomial passing through a collection of $d+1$ points. Is it the *only* polynomial passing through these points? Or: we know the system given by the Vandermonde matrix has a solution. Is it a unique solution or is the system underdetermined?

Two theorems:

Theorem 1: A nonzero polynomial of degree d has at most d roots.

Uniqueness?

Now we have a polynomial passing through a collection of $d+1$ points. Is it the *only* polynomial passing through these points? Or: we know the system given by the Vandermonde matrix has a solution. Is it a unique solution or is the system underdetermined?

Two theorems:

Theorem 1: A nonzero polynomial of degree d has at most d roots.

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

Uniqueness?

Now we have a polynomial passing through a collection of $d+1$ points. Is it the *only* polynomial passing through these points? Or: we know the system given by the Vandermonde matrix has a solution. Is it a unique solution or is the system underdetermined?

Two theorems:

Theorem 1: A nonzero polynomial of degree d has at most d roots.

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

We already know there is such a polynomial (we constructed one). Remains to show uniqueness.

Proof of Theorem 2

Let's just assume Theorem 1 for now and do 2 first to show uniqueness.

Proof of Theorem 2

Let's just assume Theorem 1 for now and do 2 first to show uniqueness.

Suppose that I have two polynomials $p(x)$, $q(x)$ with degree at most d that both contain $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$.

Proof of Theorem 2

Let's just assume Theorem 1 for now and do 2 first to show uniqueness.

Suppose that I have two polynomials $p(x)$, $q(x)$ with degree at most d that both contain $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$. Consider $r(x) = p(x) - q(x)$. It suffices to show that $r(x) = 0$ (i.e. $p(x) = q(x)$).

Proof of Theorem 2

Let's just assume Theorem 1 for now and do 2 first to show uniqueness.

Suppose that I have two polynomials $p(x)$, $q(x)$ with degree at most d that both contain $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$. Consider $r(x) = p(x) - q(x)$. It suffices to show that $r(x) = 0$ (i.e. $p(x) = q(x)$).

Notice that $r(x) = 0$ at $x_1, x_2, \ldots, x_{d+1}$ ($d+1$ points) since $p(x)$ and $q(x)$ take the same values there.

Proof of Theorem 2

Let's just assume Theorem 1 for now and do 2 first to show uniqueness.

Suppose that I have two polynomials $p(x)$, $q(x)$ with degree at most d that both contain $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$. Consider $r(x) = p(x) - q(x)$. It suffices to show that $r(x) = 0$ (i.e. $p(x) = q(x)$).

Notice that $r(x) = 0$ at $x_1, x_2, \dots, x_{d+1}$ ($d+1$ points) since $p(x)$ and $q(x)$ take the same values there.

Since $r(x)$ is the sum of two degree-at-most-d polynomials, its degree must also be at most d. As shown above it has at least $d+1$ points where it's zero, so it has at least $d+1$ roots.

Proof of Theorem 2

Let's just assume Theorem 1 for now and do 2 first to show uniqueness.

Suppose that I have two polynomials $p(x)$, $q(x)$ with degree at most d that both contain $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$. Consider $r(x) = p(x) - q(x)$. It suffices to show that $r(x) = 0$ (i.e. $p(x) = q(x)$).

Notice that $r(x) = 0$ at $x_1, x_2, \ldots, x_{d+1}$ ($d+1$ points) since $p(x)$ and $q(x)$ take the same values there.

Since $r(x)$ is the sum of two degree-at-most-d polynomials, its degree must also be at most d. As shown above it has at least $d+1$ points where it's zero, so it has at least $d+1$ roots. But we know that a nonzero polynomial of degree d has at most d roots.

Proof of Theorem 2

Let's just assume Theorem 1 for now and do 2 first to show uniqueness.

Suppose that I have two polynomials $p(x)$, $q(x)$ with degree at most d that both contain $(x_1,y_1),\ldots,(x_{d+1},y_{d+1})$. Consider $r(x)=p(x)-q(x)$. It suffices to show that $r(x)=0$ (i.e. $p(x)=q(x)$).

Notice that $r(x)=0$ at $x_1,x_2,\ldots,x_{d+1}$ ($d+1$ points) since $p(x)$ and $q(x)$ take the same values there.

Since $r(x)$ is the sum of two degree-at-most-d polynomials, its degree must also be at most d. As shown above it has at least $d+1$ points where it's zero, so it has at least $d+1$ roots. But we know that a nonzero polynomial of degree d has at most d roots. That means $r(x)=0$, as desired. $\square$

Polynomial Division

Given a degree-d polynomial $f(x)$ and a polynomial $g(x)$ of degree at most d, we can use long division to write $f(x) = g(x)q(x) + r(x)$ for some polynomials $q(x), r(x)$ such that the degree of $r(x)$ is strictly smaller than the degree of $f(x)$. Method: same as elementary-school long division for numbers!

Polynomial Division

Given a degree-d polynomial $f(x)$ and a polynomial $g(x)$ of degree at most d, we can use long division to write $f(x) = g(x)q(x) + r(x)$ for some polynomials $q(x), r(x)$ such that the degree of $r(x)$ is strictly smaller than the degree of $f(x)$. Method: same as elementary-school long division for numbers!

Example: divide $x^3 - 2x^2 - 4$ by $x - 3$.

Polynomial Division

Given a degree-d polynomial $f(x)$ and a polynomial $g(x)$ of degree at most d, we can use long division to write $f(x) = g(x)q(x) + r(x)$ for some polynomials $q(x), r(x)$ such that the degree of $r(x)$ is strictly smaller than the degree of $f(x)$. Method: same as elementary-school long division for numbers!

Example: divide $x^3 - 2x^2 - 4$ by $x - 3$.

$$
\begin{array}{rrrrr}
 & x^2 & +\ x & +3 & \\
\cline{2-5}
x-3 \big) & x^3 - 2x^2 & +0x & -4 & \\
 & x^3 - \ 3x^2 & & & \\
\cline{1-2}
 & +x^2 & +0x & & \\
 & \underline{+x^2} & \underline{-3x} & & \\
 & & +3x & -4 & \\
 & & \underline{+3x} & \underline{-9} & \\
 & & & & +5
\end{array}
$$

Polynomial Division

Given a degree-d polynomial $f(x)$ and a polynomial $g(x)$ of degree at most d, we can use long division to write $f(x) = g(x)q(x) + r(x)$ for some polynomials $q(x), r(x)$ such that the degree of $r(x)$ is strictly smaller than the degree of $f(x)$. Method: same as elementary-school long division for numbers!

Example: divide $x^3 - 2x^2 - 4$ by $x - 3$.

$$
\begin{array}{rrrrr}
 & & x^2 & +x & +3 \\ \cline{2-5}
x-3 \big) & x^3 & -2x^2 & +0x & -4 \\
 & x^3 & -3x^2 & & \\ \cline{1-3}
 & & +x^2 & +0x & \\
 & & +x^2 & -3x & \\ \cline{3-4}
 & & & +3x & -4 \\
 & & & +3x & -9 \\ \cline{4-5}
 & & & & +5
\end{array}
$$

So $x^3 - 2x^2 - 4 = (x-3)(x^2 + x + 3) + 5.$

Proof of Theorem 1 (1/3)

Lemma 1: Suppose a is a root of some degree-d polynomial $p(x)$. Then $p(x) = (x-a)q(x)$ for some degree-$d-1$ polynomial $q(x)$.

Proof of Theorem 1 (1/3)

Lemma 1: Suppose a is a root of some degree-d polynomial $p(x)$. Then $p(x) = (x-a)q(x)$ for some degree-$d-1$ polynomial $q(x)$.

Proof of Lemma: Divide $p(x)$ by $(x-a)$ using polynomial long division: $p(x) = (x-a)q(x) + r(x)$.

Proof of Theorem 1 (1/3)

Lemma 1: Suppose a is a root of some degree-d polynomial $p(x)$. Then $p(x) = (x-a)q(x)$ for some degree-$d-1$ polynomial $q(x)$.

Proof of Lemma: Divide $p(x)$ by $(x-a)$ using polynomial long division: $p(x) = (x-a)q(x) + r(x)$. The degree of $r(x)$ is necessarily smaller than that of $x-a$, so it's a constant, i.e. $r(x) = c$ for some constant c.

Lemma 1: Suppose a is a root of some degree-d polynomial $p(x)$. Then $p(x) = (x-a)q(x)$ for some degree-$d-1$ polynomial $q(x)$.

Proof of Lemma: Divide $p(x)$ by $(x-a)$ using polynomial long division: $p(x) = (x-a)q(x) + r(x)$. The degree of $r(x)$ is necessarily smaller than that of $x-a$, so it's a constant, i.e. $r(x) = c$ for some constant c. Substitute $x = a$: $p(a) = (a-a)q(a) + c = 0$.

Proof of Theorem 1 (1/3)

Lemma 1: Suppose a is a root of some degree-d polynomial $p(x)$. Then $p(x) = (x-a)q(x)$ for some degree-$d-1$ polynomial $q(x)$.

Proof of Lemma: Divide $p(x)$ by $(x-a)$ using polynomial long division: $p(x) = (x-a)q(x) + r(x)$. The degree of $r(x)$ is necessarily smaller than that of $x-a$, so it's a constant, i.e. $r(x) = c$ for some constant c. Substitute $x = a$: $p(a) = (a-a)q(a) + c = 0$. But we know that a is a root of p, so $p(a) = 0$. So $c = 0$, i.e. $p(x) = (x-a)q(x)$, as desired. $\square$

Proof of Theorem 1 (2/3)

Lemma 2: If a degree-d polynomial $p(x)$ has d distinct roots $a_1, ..., a_d$, then it can be written as $p(x) = c(x - a_1)...(x - a_d)$ for some constant c.

Proof of Theorem 1 (2/3)

Lemma 2: If a degree-d polynomial $p(x)$ has d distinct roots $a_1, ..., a_d$, then it can be written as $p(x) = c(x - a_1)...(x - a_d)$ for some constant c.

Proof of Lemma 2: Idea: just keep dividing by $(x - a_i)$.

Proof of Theorem 1 (2/3)

Lemma 2: If a degree-d polynomial $p(x)$ has d distinct roots $a_1, \ldots, a_d$, then it can be written as $p(x) = c(x - a_1) \ldots (x - a_d)$ for some constant c.

Proof of Lemma 2: Idea: just keep dividing by $(x - a_i)$.Formally: proceed by induction on d.

Proof of Theorem 1 (2/3)

Lemma 2: If a degree-d polynomial $p(x)$ has d distinct roots $a_1, \ldots, a_d$, then it can be written as $p(x) = c(x - a_1)\ldots(x - a_d)$ for some constant c.

Proof of Lemma 2: Idea: just keep dividing by $(x - a_i)$.Formally: proceed by induction on d.

For the base case, consider a degree-1 polynomial with a single root a_1. It immediately follows from Lemma 1 that it must be expressible as $c(x - a_1)$.

Proof of Theorem 1 (2/3)

Lemma 2: If a degree-d polynomial $p(x)$ has d distinct roots $a_1, ..., a_d$, then it can be written as $p(x) = c(x - a_1)...(x - a_d)$ for some constant c.

Proof of Lemma 2: Idea: just keep dividing by $(x - a_i)$.Formally: proceed by induction on d.

For the base case, consider a degree-1 polynomial with a single root a_1. It immediately follows from Lemma 1 that it must be expressible as $c(x - a_1)$.

Proof of Theorem 1 (3/3)

Now suppose for induction that the lemma holds for some d. It suffices to show that we can express a degree-$d+1$ polynomial $p(x)$ with $d+1$ roots $a_1,...,a_{d+1}$ as $p(x) = c(x-a_1)...(x-a_{d+1})$.

Proof of Theorem 1 (3/3)

Now suppose for induction that the lemma holds for some d. It suffices to show that we can express a degree-$d+1$ polynomial $p(x)$ with $d+1$ roots $a_1, \ldots, a_{d+1}$ as $p(x) = c(x - a_1)\ldots(x - a_{d+1})$.

Apply Lemma 1: $p(x) = (x - a_{d+1})q(x)$ for some degree-d polynomial $q(x)$.

Proof of Theorem 1 (3/3)

Now suppose for induction that the lemma holds for some d. It suffices to show that we can express a degree-$d+1$ polynomial $p(x)$ with $d+1$ roots $a_1, \ldots, a_{d+1}$ as $p(x) = c(x - a_1) \ldots (x - a_{d+1})$.

Apply Lemma 1: $p(x) = (x - a_{d+1})q(x)$ for some degree-d polynomial $q(x)$.

Roots of $q(x)$? $a_1, \ldots, a_d$. Why? $p(x)$ is zero at those points, and $x - a_{d+1}$ isn't, so $q(x)$ has to be.

Proof of Theorem 1 (3/3)

Now suppose for induction that the lemma holds for some d. It suffices to show that we can express a degree-$d+1$ polynomial $p(x)$ with $d+1$ roots $a_1, \ldots, a_{d+1}$ as $p(x) = c(x-a_1)\ldots(x-a_{d+1})$.

Apply Lemma 1: $p(x) = (x-a_{d+1})q(x)$ for some degree-d polynomial $q(x)$.

Roots of $q(x)$? $a_1, \ldots, a_d$. Why? $p(x)$ is zero at those points, and $x-a_{d+1}$ isn't, so $q(x)$ has to be. $q(x)$: d distinct roots, degree d. So by inductive hypothesis, $q(x) = c(x-a_1)\ldots(x-a_d)$.

Proof of Theorem 1 (3/3)

Now suppose for induction that the lemma holds for some d. It suffices to show that we can express a degree-$d+1$ polynomial $p(x)$ with $d+1$ roots $a_1,...,a_{d+1}$ as $p(x) = c(x-a_1)...(x-a_{d+1})$.

Apply Lemma 1: $p(x) = (x-a_{d+1})q(x)$ for some degree-d polynomial $q(x)$.

Roots of $q(x)$? $a_1,...,a_d$. Why? $p(x)$ is zero at those points, and $x-a_{d+1}$ isn't, so $q(x)$ has to be. $q(x)$: d distinct roots, degree d. So by inductive hypothesis, $q(x) = c(x-a_1)...(x-a_d)$.

So $p(x) = c(x-a_1)...(x-a_d)(x-a_{d+1})$ as desired. $\square$

Proof of Theorem 1 (3/3)

Now suppose for induction that the lemma holds for some d. It suffices to show that we can express a degree-$d+1$ polynomial $p(x)$ with $d+1$ roots $a_1, \ldots, a_{d+1}$ as $p(x) = c(x-a_1)\ldots(x-a_{d+1})$.

Apply Lemma 1: $p(x) = (x-a_{d+1})q(x)$ for some degree-d polynomial $q(x)$.

Roots of $q(x)$? $a_1, \ldots, a_d$. Why? $p(x)$ is zero at those points, and $x-a_{d+1}$ isn't, so $q(x)$ has to be. $q(x)$: d distinct roots, degree d. So by inductive hypothesis, $q(x) = c(x-a_1)\ldots(x-a_d)$.

So $p(x) = c(x-a_1)\ldots(x-a_d)(x-a_{d+1})$ as desired. $\square$

It immediately follows that a nonzero polynomial of degree d has at most d roots. Why?

Now suppose for induction that the lemma holds for some d. It suffices to show that we can express a degree-$d+1$ polynomial $p(x)$ with $d+1$ roots $a_1, \ldots, a_{d+1}$ as $p(x) = c(x-a_1)\ldots(x-a_{d+1})$.

Apply Lemma 1: $p(x) = (x - a_{d+1})q(x)$ for some degree-d polynomial $q(x)$.

Roots of $q(x)$? $a_1, \ldots, a_d$. Why? $p(x)$ is zero at those points, and $x - a_{d+1}$ isn't, so $q(x)$ has to be. $q(x)$: d distinct roots, degree d. So by inductive hypothesis, $q(x) = c(x-a_1)\ldots(x-a_d)$.

So $p(x) = c(x-a_1)\ldots(x-a_d)(x-a_{d+1})$ as desired. $\square$

It immediately follows that a nonzero polynomial of degree d has at most d roots. Why? Suppose for contradiction that it has more than d. Take first d roots and write the polynomial as $c(x-a_1)\ldots(x-a_d)$. Plug in the $d+1$st root, a_{d+1}. Since it's distinct from $a_1, \ldots, a_d$ this polynomial must be nonzero, contradicting our assertion that a_{d+1} was a root. Therefore, we've proven Theorem 1.

Up next...

Counting polynomials.

Applications: Shamir's secret sharing and error-correcting codes.

Polynomial identity testing and the Schwartz-Zippel lemma