

Secure Computation - Part I
Prof. Ashish Choudhury
Department of Computer Science
International Institute of Information Technology, Bangalore

Module - 1
Lecture - 10
Polynomials Over Fields

(Refer Slide Time: 00:32)

Lecture Overview

- Polynomials over fields
 - ❖ Properties
 - ❖ Lagrange's interpolation



Hello everyone. Welcome to this lecture. Plan for this lecture is as follows: In this lecture, we will see some basic properties regarding polynomials over fields. And we will also discuss about Lagrange's interpolation. The reason we want to discuss these concepts is that, looking ahead, this will be useful when we want to design an efficient threshold secret-sharing scheme for any given threshold t which is less than n .

(Refer Slide Time: 01:04)

Polynomials Over a Field

□ Let $(\mathbb{F}, +, \cdot)$ be a field

□ Definition: a t -degree polynomial $f(X)$ over \mathbb{F} is of the form

$$f(X) = \underbrace{a_0}_{\text{"0"}} + \underbrace{a_1}_{\text{"0"}} \cdot X + \dots + \underbrace{a_t}_{\text{"0"}} \cdot X^t$$

$\sim \dots + 0X^t$

($t+1$) Coefficients

$a_0, \dots, a_t \in \mathbb{F}$

All operations are field operations



So, what are polynomials over a field? So, imagine you are given a field with an abstract plus operation and an abstract multiplication operation. So, the polynomials over a field are very similar to usual polynomials that we are aware of, where we have integer coefficients or coefficients which are real number. So, if I say that I have a polynomial whose degree is t , and if the polynomial is over the field \mathbb{F} , then basically I am talking about a polynomial $f(X)$ which has $t + 1$ coefficients.

So, those coefficients a_0, a_1, \dots, a_t , they are elements over the fields. And a_1 will be the coefficient of X to the power 1; a_2 will be the coefficient of X to the power 2; and a_t will be the coefficient of X power t . So, in total you have $t + 1$ coefficients, and that is why this will be called a t -degree polynomial. And all these coefficients are elements of field. So, it could be the case that all your coefficients are the 0 element.

That is quite possible, but still we will call such a polynomial as a t -degree polynomial. Or it could be the case that only a_0 is, say a_t , the coefficient a_t is 0, but remaining other coefficients are non-zero elements. So, all such polynomials will be called as t -degree polynomials.

(Refer Slide Time: 02:56)

Polynomials Over a Field

Let $(\mathbb{F}, +, \cdot)$ be a field

Definition: a t -degree polynomial $f(X)$ over \mathbb{F} is of the form

$$f(X) = a_0 \oplus a_1 \otimes X \oplus \dots \oplus a_t \otimes X^t$$

$a_0, \dots, a_t \in \mathbb{F}$

All operations are field operations

Ex: consider the field $(\mathbb{Z}_7, +_7, \cdot_7)$ --- addition/multiplication modulo 7

$$f(X) = 6 + 2X + 3X^4 \quad \text{4-degree polynomial}$$

Handwritten notes: $\mathbb{F} = \{0, 1, 2, 3, 4, 5, 6\}$, $0X^2 + 0X^3$



And here, the plus and the dot operation that we have in the definition of this $f(X)$ are not the integer addition and integer multiplication, but rather they are the field plus and the field multiplication operation. So, let us see an example here. So, imagine I consider my field \mathbb{F} to be the set \mathbb{Z}_7 , which has the elements 0, 1, 2, 3, 4, 5 and 6. And my plus operation in this field is the addition modulo 7, and my multiplication operation here is the multiplication modulo 7.

So, this will be an example of a polynomial over the field \mathbb{Z}_7 which is a 4-degree polynomial. Even though it does not have coefficients for, or it does not have terms like X^2 and X^3 , I can implicitly assume that it has terms like 0 times X^2 and 0 times X^3 to be implicitly present in this polynomial $f(X)$. So, this is an example of a polynomial over the field \mathbb{Z}_7 .

(Refer Slide Time: 04:22)

Polynomials Over a Field

Let $(\mathbb{F}, +, \cdot)$ be a field

Definition: a t -degree polynomial $f(X)$ over \mathbb{F} is of the form

$$f(X) = a_0 \oplus a_1 \otimes X \oplus \dots \oplus a_t \otimes X^t$$

$a_0, \dots, a_t \in \mathbb{F}$

All operations are field operations

Ex: consider the field $(\mathbb{Z}_7, +_7, \cdot_7)$ --- addition/multiplication modulo 7

$$f(X) = 6 + 2X + 3X^4$$

$$f(1) = (6 + 2 + 3) \bmod 7 = 4$$

Handwritten: $f(1) \neq 11$

Handwritten: $8 \notin \mathbb{Z}_7$

$$f(8) = f(1) = (6 + 2 + 3) \bmod 7 = 4$$

Handwritten: $(6 + 2 \cdot 8 + 3 \cdot 8^4) \bmod 7 =$



And here, the plus operation and the dot operation; so, dot operations are here; are the integer, are the addition modulo 7 operation and the multiplication modulo 7 operation. So, let us evaluate or compute the value of this polynomial, let us say $x = 1$. So, if I want to compute the value of the polynomial at $x = 1$, I substitute $x = 1$ everywhere. But remember, all the addition and multiplication operations are performed modulo 7; so, $f(1)$ will be 11 modulo 7.

So, $f(1)$ would not be 11, because the plus and the multiplication operations are performed modulo 7. If I want to compute $f(8)$, then there are 2 ways to compute that. I could compute 6 plus 2 times 8, plus 3 times 8 to the power 4. And then, everything I can reduce modulo 7. But that will require me to perform a little bit large computations. Instead, what I can do is the following:

The element 8 can be reduced modulo 7 itself, because the element 8 is actually not a member of the field \mathbb{Z}_7 . But I can make it a member of \mathbb{Z}_7 by reducing it modulo 7, because my operations here are performed modulo 7. So, $f(8)$ will be the same value as $f(1)$, and we have already calculated $f(1)$. So, you can verify. That does not matter whether you compute $f(1)$ and then equate it with $f(8)$; that will give you the same result.

Or if you directly plug in the value of X to be 8 everywhere and then compute everything, and then do modulo 7, you will get the same result. So, that is an example of a field and polynomial over a field, you can have any abstract field with an abstract plus, an abstract dot operation, and then you can define polynomials.

(Refer Slide Time: 06:26)

Polynomials Over a Field

□ Let $(\mathbb{F}, +, \cdot)$ be a field

□ Definition: a t -degree polynomial $f(X)$ over \mathbb{F} is of the form

$$f(X) = a_0 + a_1 \cdot X + \dots + a_t \cdot X^t$$

$a_0, \dots, a_t \in \mathbb{F}$

All operations are field operations

□ Ex: consider the field $(\mathbb{Z}_7, +_7, \cdot_7)$ --- addition/multiplication modulo 7

$$f(X) = 6 + 2X + 3X^4$$

$$f(1) = (6 + 2 + 3) \bmod 7 = 4$$

$$f(8) = f(1) = (6 + 2 + 3) \bmod 7 = 4$$

$$X^4 + ax + b$$

$$X^4 + 2X + 6$$

□ Definition (root of a polynomial): an element $v \in \mathbb{F}$ is called a root of $f(X)$, if $f(v) = 0$

No roots $\left\{ \begin{array}{l} f(X) = 6 + 2X + 3X^4 \\ f(0), f(1), \dots, f(6) \neq 0 \end{array} \right.$

$\exists \alpha \in \mathbb{Z}_7$ such that $f(\alpha) = 0$
 $f(x \bmod 7) = f(x)$

Next, we define what we call as root of a polynomial. And this is again similar to root of an equation that we are familiar with in the integer world. So, if we are given an equation, say $X^2 + 2X + a$; or an arbitrary equation $X^2 + aX + b$, then we say that Z is the root of this equation, if I substitute $X = Z$ and get 0. So, I carry over this definition for polynomials over field.

So, imagine $f(X)$ is a polynomial over a field in the variable X , then a value v from the field or an element $f v$ from the field will be called as the root of this polynomial, if the polynomial evaluated at $x = v$ gives you the 0 element of the field. Again, this is not the numeric 0, this is the 0 element of your field. So, again, let us take the example of the polynomial that we have defined, that we have written down over, where my field is \mathbb{Z}_7 .

And now, it is easy to see that this polynomial has no root. Because $f(0)$ is not 0, $f(1)$ is not 0, $f(2)$ is not 0, $f(3)$ is not 0, and like that $f(6)$ is also not 0. Now, you might be wondering, why cannot I say f, why I am only restricting to $X = 0$ up to $X = 6$. It could be possible that there is some value greater than 6, such that $f(X)$ takes the value 0 for this particular f .

Well, that is not possible, because if you take any $X > 6$, and try to compute the value of $f(X)$ for such an X , then that will be one of these 7 possible values. It will be either $f(0)$ or $f(1)$ or $f(6)$, because $f(X)$ will be same as $f(X \text{ modulo } 7)$. And this will be either $f(0)$ or $f(1)$ or $f(6)$. But all these 7 values, none of them is equal to 0. And hence, it does not matter whether your $X > 6$. Also if you evaluate $f(X)$ for such an X , it will give you a non-zero value. So, that shows that this polynomial does not have any root.

(Refer Slide Time: 09:05)

Polynomials Over a Field

Let $(\mathbb{F}, +, \cdot)$ be a field

Definition: a t-degree polynomial $f(X)$ over \mathbb{F} is of the form $f(X) = a_0 + a_1 \cdot X + \dots + a_t \cdot X^t$ where $a_0, \dots, a_t \in \mathbb{F}$. All operations are field operations.

Ex: consider the field $(\mathbb{Z}_7, +_7, \cdot_7)$ --- addition/multiplication modulo 7

$$f(X) = 6 + 2X + 3X^4$$

$$f(1) = (6 + 2 + 3) \bmod 7 = 4$$

$$f(8) = f(1) = (6 + 2 + 3) \bmod 7 = 4$$

$X^2 + ax + b$
 ~~$X^2 + aX + b$~~

Definition (root of a polynomial): an element $v \in \mathbb{F}$ is called a root of $f(X)$, if $f(v) = 0$

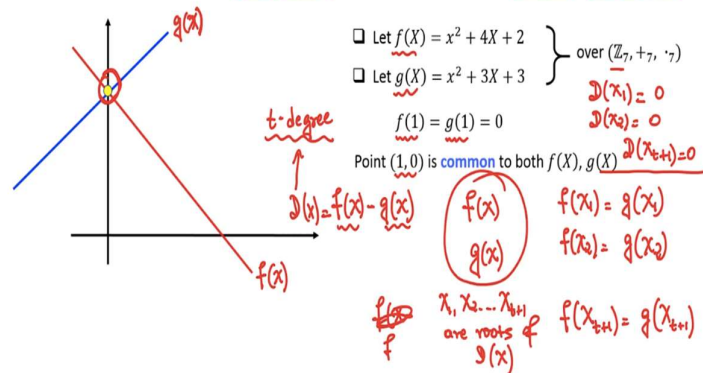
No roots $\left\{ \begin{array}{l} f(X) = 6 + 2X + 3X^4 \\ f(0), f(1), \dots, f(6) \neq 0 \end{array} \right.$ $\left\{ \begin{array}{l} g(X) = X + 4X^2 + X^3 + X^4 \\ g(0) = g(1) = g(2) = g(3) = 0 \end{array} \right.$ 4 roots

Whereas, if I consider another polynomial $g(X)$ over the same field and compute the value of $g(0), g(1), g(2), g(3)$; all of them turn out to be 0. That means, this polynomial has 4 roots. Now, you might be wondering, is it possible that this polynomial have more than 4 roots? (Refer Slide Time: 09:29)

Polynomials Over a Field : Properties

Theorem (Abstract algebra): a t-degree polynomial over \mathbb{F} has at most t roots. Ex: $t=1$

Theorem (Abstract algebra): two distinct t-degree polynomials over \mathbb{F} can have at most t common values



Well, we have a general result, which is similar to the results regarding the number of roots that you may have for an integer polynomial. By integer polynomial, I mean, where you have the integer coefficients and the plus and the multiplication or the integer plus and the integer multiplication. So, this result is regarding the number of roots that you may have for a polynomial over a field.

And the result says that, if you take a t-degree polynomial over the field, then it can have at most t roots. That means, either it can have 0 number of roots or it can have 1 root or it could

have 2 roots or maximum it could have, it can have t roots. Now, it may be the case that some of them are, all of them are distinct, some are repeated; you may have different possible cases.

But in total, the number of roots that you may have for a t -degree polynomial over a field is upper bounded by t ; that is the maximum number of roots you can have. So, I will not be going into the proof of that theorem. That is not required. But we can prove it. If you are interested, you can refer to any standard text in abstract algebra. Another interesting result regarding polynomials over the field, which we will be using is the following:

If I consider 2 different t -degree polynomials; and when I say different t -degree polynomials, by that I mean there is at least 1 power of X for which the corresponding coefficients are different in the 2 polynomials. It is not the case that all the coefficients of both the polynomials are identical, because, if that is the case, then basically they are the same polynomial.

When I am saying that they are different polynomials, at least 1 of the coefficients or 1 of the power of X will have different coefficients in the 2 polynomials. So, the result says that, if you take 2 different t -degree polynomials over the field, then they can have at most t common values. You cannot have more than t common values for 2 different t -degree polynomials. So, how to interpret this result?

Again, I would not be going into the proof, but let me give you a pictorial interpretation. Let us take the case of $t = 1$ to understand this result. So, for $t = 1$, a polynomial of degree-1 is nothing but a straight line. So, the result says the following: That if you take 2 straight line, if you take; so, this red line, this is a straight line equation. Imagine that the corresponding equation is $f(X)$.

And you have this blue line which is again a straight line. So, its corresponding equation, say it is $g(X)$ or it will be a 1-degree polynomial. Now, it is a well-known fact that if I take 2 different straight lines, they can have at most 1 point common, at most. It is not necessary that definitely they should have 1 common point. It could be the case that the 2 straight lines, they never intersect, they are parallel, or they never intersect at all.

It could be the case as well. But if at all they intersect, they can intersect at most at 1 point. And that 1 point will be common; common in the sense, it lies both on the blue straight line as well as on the red straight line. That means, I can say that this point belongs to g of X as well as f of X . So, again, let us see an example to make it more clear. So, consider 2 polynomials $f(X)$ and $g(X)$ here.

Both are over this field \mathbb{Z}_7 and where the operations are addition modulo 7 and multiplication modulo 7. Now, it is easy to see that if I evaluate the f polynomial at $x = 1$, and if I evaluate the g polynomial at $x = 1$, I get the value 0. Hence, I can say that the point 1, 0 is common to both the polynomial $f(X)$ as well as $g(X)$. In general, if you have 2 different t -degree polynomials, they can have at most t common values.

And how we can prove it? Actually, we can prove this second theorem using the help of the first theorem here. If you consider 2 different polynomials $f(X)$ and $g(X)$, the claim is as per the theorem that they can have at most t common values. So, we can prove it by contradiction. So, on contrary, assume that they have $t + 1$ or more common values. That means, you have, say $f(X_1) = g(X_1)$; you have $f(X_2) = g(X_2)$; and like that, you have, say $f(X_{t+1}) = g(X_{t+1})$, where this X_1, X_2, \dots, X_{t+1} , all are different.

Now, if this is the case, what can I say about the polynomial $f(X) - g(X)$? So, you consider the polynomial $f(X) - g(X)$. Let us call this polynomial as $D(X)$. Now, what will be the degree of $D(X)$ polynomial? Since, $f(X)$ is a t -degree polynomial, $g(X)$ is also a t -degree polynomial, I can say that $D(X)$ is also a t -degree polynomial. Now, what can I say about $D(X_1)$? $D(X_1)$ will be $f(X_1) - g(X_1)$.

But $f(X_1)$ and $g(X_1)$ are same. Hence, $D(X_1)$ is the 0 element. In the same way, $D(X_2)$ will be the 0 element. And like that, $D(X_{t+1})$ is also the 0 element. That means, I get the conclusion that X_1, X_2, \dots, X_{t+1} are roots of the polynomial $D(X)$. But $D(X)$ has degree- t , hence it can have at most t roots, as per this first theorem. But I am showing you that $D(X)$ will have more than t roots. That is not possible.

That means, whatever I assumed regarding $f(X)$ and $g(X)$, that is incorrect. I assumed that $f(X)$ and $g(X)$ have $t + 1$ common values; that is an incorrect assumption. Hence, they can

have at most t common values. So, that is another interesting result regarding polynomials over the fields. We have 2 interesting properties here. So, now, we will see some more properties here, which will be useful for us.

(Refer Slide Time: 17:08)

Polynomials Over a Field : Properties

□ Theorem (Abstract algebra): a t -degree polynomial over \mathbb{F} has **at most t roots**

□ Theorem (Abstract algebra): two **distinct** t -degree polynomials over \mathbb{F} can have **at most t common values**

□ Let $f(X) = x^2 + 4X + 2$

□ Let $g(X) = x^2 + 3X + 3$

$f(1) = g(1) = 0$

Point $(1, 0)$ is **common** to both $f(X), g(X)$

$x_1 \neq x_2 \neq x_3$
 $\dots \neq x_{d+1}$

□ Theorem (Abstract algebra): Let $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ be pairs of elements from \mathbb{F} , where x_1, \dots, x_{d+1} are **distinct**. Then there exists a **unique d -degree polynomial** $f(X)$ over \mathbb{F} , such that $f(x_i) = y_i$, for $1 \leq i \leq d + 1$

The last property that we require for our secret-sharing scheme later is the following: If you are given $d + 1$ points from \mathbb{F} . So, you can imagine $(x_1, y_1), (x_1, y_2), \dots, (x_{d+1}, y_{d+1})$ as $d + 1$ points in two-dimension plane, where it is given that the x-coordinates, all of them are distinct and elements from the field. That means, $x_1 \neq x_2 \neq x_3 \neq \dots \neq x_{d+1}$; all of them are different elements and elements from the field.

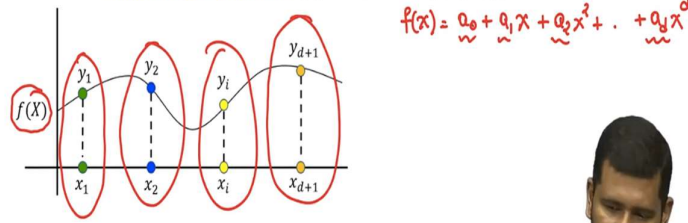
Then this theorem says that, there always exists a unique polynomial of degree- d , call it $f(X)$, such that this x, y pairs which are given to you constitute points on that polynomial $f(X)$ or lie on the polynomial $f(X)$. So, basically, what I am saying is the following: It is a well-known fact that if I give you 2 distinct points, in the x, y plane; so, this is your, say (x_1, y_1) and (x_2, y_2) ; there always exists a unique straight line passing through it; let us all be aware of.

I am just generalising that result over fields, because now I am saying that this result holds even if the x, y elements, x, y pairs are elements from the field. What I am saying is, if you are given $d + 1$ such x, y pairs, where the x-coordinates are distinct, that ensures that your $d + 1$ x, y pairs, they are distinct elements, none of them are the same. Then, you can find a unique curve; that curve I am calling it as $f(X)$, whose degree will be d and which passes through those $d + 1$ x, y pairs.

(Refer Slide Time: 19:33)

Lagrange's Polynomial Interpolation

□ **Theorem:** Let $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ be pairs of elements from \mathbb{F} , where x_1, \dots, x_{d+1} are **distinct**. Then there exists a **unique d-degree polynomial** $f(X)$ over \mathbb{F} , such that $f(x_i) = y_i$, for $1 \leq i \leq d+1$

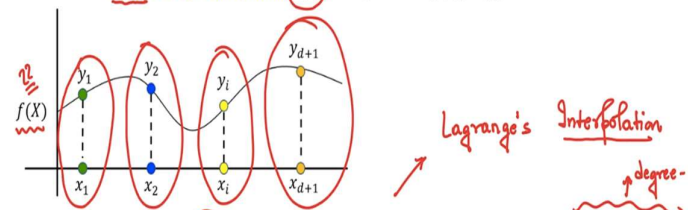


So, this is what I am claiming pictorially. You are given (x_1, y_1) ; (x_2, y_2) ; (x_i, y_i) ; and (x_{d+1}, y_{d+1}) . Then you can always find the curve, call it $f(X)$ whose degree will be d . That means, your $f(X)$ will be of the form $a_0 + a_1X + a_2X^2 + \dots + a_dX^{d+1}$, where all this a_0, a_1, a_2 are elements from the field, such that this f polynomial evaluated at $x = x_1$ will give you y_1 , this f polynomial evaluated at $x = x_2$ gives you y_2 , and so on. That is what is the claim.

(Refer Slide Time: 20:42)

Lagrange's Polynomial Interpolation

□ **Theorem:** Let $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ be pairs of elements from \mathbb{F} , where x_1, \dots, x_{d+1} are **distinct**. Then there exists a **unique d-degree polynomial** $f(X)$ over \mathbb{F} , such that $f(x_i) = y_i$, for $1 \leq i \leq d+1$



□ **Idea:** Express the unknown $f(X)$ as a **linear combination** of $d+1$ **d-degree polynomials** $\delta_1(X), \dots, \delta_{d+1}(X)$

$$f(x) \cong y_1 \cdot \delta_1(x) + \dots + y_i \cdot \delta_i(x) + \dots + y_{d+1} \cdot \delta_{d+1}(x)$$

All elements except x_i are its roots

$$\delta_1(x_1) = 1 \quad \delta_i(x_i) = 1$$

$$\delta_1(x_2) = \dots = \delta_1(x_{d+1}) = 0 \quad \delta_i(x_1) = \dots = \delta_i(x_{i-1}) = \delta_i(x_{i+1}) = \dots = \delta_i(x_{d+1}) = 0$$

Now, and the fact is that, not only there is a polynomial, that polynomial is a unique polynomial. That is also, is one of the implications of this term. That means, you cannot have 2 different curves $f(X)$ and $g(X)$ passing through this x, y pairs. And that comes from our previous results. Because, in the previous 2 theorems, we have already argued that 2 different

d -degree polynomials cannot have more than d common values, they can have at most d common values.

But here we are given $d + 1$ x, y pairs, so, that is why there can be only 1 and only 1 polynomial of degree- d passing through this $d + 1$ x, y pairs. So, now, how do we prove this theorem? There are several ways to prove it. We will be interested basically to construct this polynomial $f(X)$. This $f(X)$ polynomial is not given to us. We are given only the x, y pairs. x_1, y_1 is given to you; x_2, y_2 is given to you; x_{d+1}, y_{d+1} is given to you.

Your goal is now to find out this polynomial $f(X)$, because that is what we will require in our secret-sharing protocol later. How do you get this $f(X)$ polynomial? So, there are several ways to do this. The most, the easiest method is what we call as Lagrange's interpolation attributed to Lagrange, who invented this method. And why it is called interpolation?

Because you are basically interpolating the points x_1, y_1, x_2, y_2 and getting the unknown curve $f(X)$. Now, it turns out that students often try to memorise the Lagrange's interpolation formula, because, for many of them find it slightly difficult to interpret. But there is nothing to memorise the Lagrange's interpolation formula. It is a very simple formula based on a very cute idea. So, our goal is the following:

Our goal is to find out this unknown $f(X)$ polynomial passing through the given $d + 1$ x, y pairs. So, the idea behind the Lagrange's interpolation is that we should try to express this unknown $f(X)$ polynomial which we want to compute as a linear combination of $d + 1$ number of d -degree polynomials. So, I will be finding $d + 1$ polynomials. I am calling them as δ_1 polynomial, δ_2 polynomial and δ_{d+1} th polynomial.

Each of them have individually degree- d . We will see what will be the structure of this δ_1 polynomial, δ_2 polynomial and so on. So, the idea is that, whatever is the $f(X)$ polynomial you want to compute, that can be expressed as a linear combination of these delta polynomials, where the linear combiners are your y elements which are given to you. So, remember, you are given $d + 1$ number of y elements.

Now, these delta polynomials, they are not arbitrary polynomials, they are not arbitrary d polynomials, they are not arbitrary d-degree polynomials, but they are some special type of d-degree polynomials. What is the speciality of this d-degree delta polynomials? So, the speciality is the following: If I consider the $\delta_1(X)$ polynomial, then it has d number of roots. And what are the roots? The roots are $x_2, x_3, x_4, \dots, x_{d+1}$

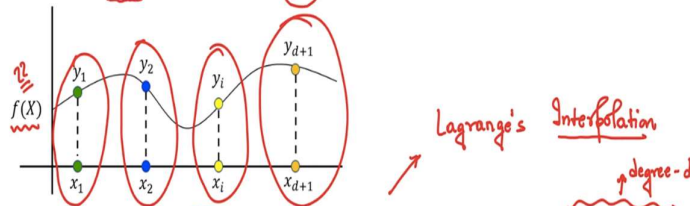
That means, you are given $d + 1$ number of x elements. This $\delta_1(X)$ polynomial has all the elements except x_1 as its root. That means, if you evaluate this δ_1 polynomial at $X = x_2$, you will get the value 0. If you evaluate this δ_1 polynomial at $X = x_3$, you will get the 0 value. And if you evaluate this δ_1 polynomial at $X = x_{d+1}$, you will get 0. And, if you evaluate this δ_1 polynomial at $X = x_1$, you should get the multiplicative identity element namely 1.

That is the property of this δ_1 polynomial. In the same way, if I consider the δ_i polynomial, it has the property that all elements except x_i are its roots. Namely, if you evaluate this δ_i polynomial at $X = x_1$, you get 0; if you evaluate this δ_i polynomial at $X = x_2$, you get 0 and so on. But, if you evaluate this δ_i polynomial at $X = x_i$, you should get the multiplicative identity element.

(Refer Slide Time: 26:56)

Lagrange's Polynomial Interpolation

□ **Theorem:** Let $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ be pairs of elements from \mathbb{F} , where x_1, \dots, x_{d+1} are distinct. Then there exists a unique d-degree polynomial $f(X)$ over \mathbb{F} , such that $f(x_i) = y_i$, for $1 \leq i \leq d + 1$



□ **Idea:** Express the unknown $f(X)$ as a linear combination of $d + 1$ d degree polynomials $\delta_1(X), \dots, \delta_{d+1}(X)$

$$f(X) \cong y_1 \cdot \delta_1(X) + \dots + y_i \cdot \delta_i(X) + \dots + y_{d+1} \cdot \delta_{d+1}(X)$$

All elements except x_{d+1} are roots
 $\delta_{d+1}(x_{d+1}) = 1$

$$\delta_1(x_1) = 1 \qquad \delta_i(x_i) = 1$$

$$\delta_1(x_2) = \dots = \delta_1(x_{d+1}) = 0 \qquad \delta_i(x_1) = \dots = \delta_i(x_{i-1}) = \delta_i(x_{i+1}) = \dots = \delta_{d+1}(x_1) = \dots = \delta_{d+1}(x_d) = 0$$

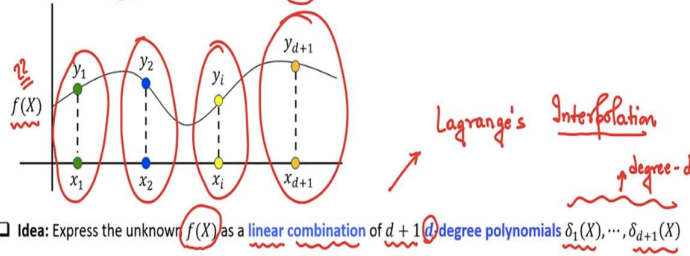
$$= \delta_i(x_{d+1}) = 0$$

And in the same way, if you take the d plus 1th delta polynomial δ_{d+1} , it has the property that all elements, all the x elements which are given to you except x_{d+1} are the roots. And it is easy to see that the way I have defined this δ_i polynomial; by definition itself, each of this δ_i polynomial will have the degree-d. Why? Because, for each δ_i polynomial;

(Refer Slide Time: 27:40)

Lagrange's Polynomial Interpolation

□ Theorem: Let $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ be pairs of elements from \mathbb{F} , where x_1, \dots, x_{d+1} are distinct. Then there exists a unique d -degree polynomial $f(X)$ over \mathbb{F} , such that $f(x_i) = y_i$, for $1 \leq i \leq d+1$



□ Idea: Express the unknown $f(X)$ as a linear combination of $d+1$ d -degree polynomials $\delta_1(X), \dots, \delta_{d+1}(X)$

$$f(X) \cong y_1 \cdot \delta_1(X) + \dots + y_i \cdot \delta_i(X) + \dots + y_{d+1} \cdot \delta_{d+1}(X)$$

$$\begin{aligned} \delta_1(x_1) &= 1 & \delta_i(x_i) &= 1 & \delta_{d+1}(x_{d+1}) &= 1 \\ \delta_1(x_2) &= \dots = \delta_1(x_{d+1}) = 0 & \delta_i(x_1) &= \dots = \delta_i(x_{i-1}) = \delta_i(x_{i+1}) = \dots & \delta_{d+1}(x_1) &= \dots = \delta_{d+1}(x_d) = 0 \\ & & & = \delta_i(x_{d+1}) = 0 & & \end{aligned}$$

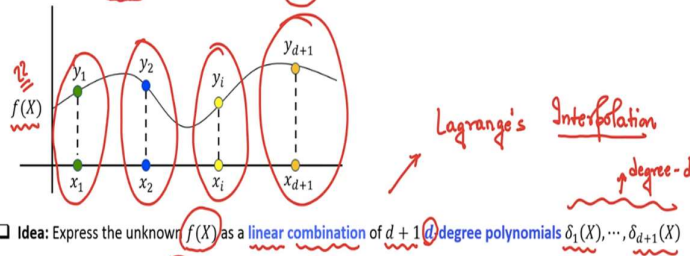
⊙ ⊙ ⊙ ⊙ ⊙ ⊙

So, each δ_i polynomial has exactly d roots, and hence, degree- d . Because I know that a d -degree polynomial can have at most d roots, but since I have defined my δ_i polynomials in such a way that they, each of them has indeed exactly d roots, that automatically ensures that each of my δ_1 polynomial, δ_2 polynomial, δ_i polynomial, δ_{d+1} th polynomial, each of them has degree- d .

(Refer Slide Time: 28:31)

Lagrange's Polynomial Interpolation

□ Theorem: Let $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ be pairs of elements from \mathbb{F} , where x_1, \dots, x_{d+1} are distinct. Then there exists a unique d -degree polynomial $f(X)$ over \mathbb{F} , such that $f(x_i) = y_i$, for $1 \leq i \leq d+1$



□ Idea: Express the unknown $f(X)$ as a linear combination of $d+1$ d -degree polynomials $\delta_1(X), \dots, \delta_{d+1}(X)$

$$f(X) \cong y_1 \cdot \delta_1(X) + \dots + y_i \cdot \delta_i(X) + \dots + y_{d+1} \cdot \delta_{d+1}(X)$$

$$\begin{aligned} \delta_1(x_1) &= 1 & \delta_i(x_i) &= 1 & \delta_{d+1}(x_{d+1}) &= 1 \\ \delta_1(x_2) &= \dots = \delta_1(x_{d+1}) = 0 & \delta_i(x_1) &= \dots = \delta_i(x_{i-1}) = \delta_i(x_{i+1}) = \dots & \delta_{d+1}(x_1) &= \dots = \delta_{d+1}(x_d) = 0 \\ & & & = \delta_i(x_{d+1}) = 0 & & \end{aligned}$$

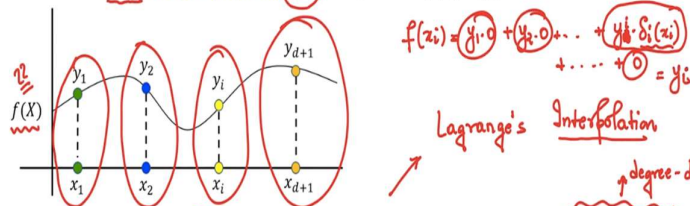
So, now, my claim is that this unknown $f(X)$ polynomial is nothing but this linear combination, namely $y_1 \cdot \delta_1(X)$ polynomial, $y_2 \cdot \delta_2(X)$ polynomial and so on. So, why $f(X)$ will have degree- d , because each of these delta polynomials they have degree- d 's. And now, if I multiply a polynomial with some constant, y_1 is a constant. So, overall, this is a degree- d polynomial.

Similarly, $y_2 \cdot \delta_2(X)$, that will be a degree-d polynomial. And in the same way, $y_i \cdot \delta_i(X)$ polynomials, that will be a degree-d polynomial. And this last linear combination, it will be a degree-d polynomial. And now, if I sum up several d-degree polynomials, I will again get a degree-d polynomial. So, it is given, guaranteed that whatever $f(X)$ I compute, by computing this linear combination, that will be a degree-d polynomial.

(Refer Slide Time: 29:40)

Lagrange's Polynomial Interpolation

□ **Theorem:** Let $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ be pairs of elements from \mathbb{F} , where x_1, \dots, x_{d+1} are distinct. Then there exists a unique d-degree polynomial $f(X)$ over \mathbb{F} , such that $f(x_i) = y_i$, for $1 \leq i \leq d+1$



□ **Idea:** Express the unknown $f(X)$ as a linear combination of $d+1$ d-degree polynomials $\delta_1(X), \dots, \delta_{d+1}(X)$

$$f(X) \cong y_1 \cdot \delta_1(X) + \dots + y_i \cdot \delta_i(X) + \dots + y_{d+1} \cdot \delta_{d+1}(X)$$

$$f(x_1) = y_1 \cdot 1 + y_2 \cdot 0 + \dots + y_i \cdot 0 + \dots + y_{d+1} \cdot 0 = y_1$$

$$\delta_1(x_1) = 1, \quad \delta_1(x_2) = \dots = \delta_1(x_{d+1}) = 0$$

$$\delta_i(x_1) = \dots = \delta_i(x_{i-1}) = \delta_i(x_{i+1}) = \dots = \delta_i(x_{d+1}) = 0, \quad \delta_i(x_i) = 1$$

$$\delta_{d+1}(x_{d+1}) = 1, \quad \delta_{d+1}(x_1) = \dots = \delta_{d+1}(x_d) = 0$$

And now, do I get the guarantees that I have in the theorem? What can I say about $f(x_1)$? So, if I evaluate $f(x_1)$, then that will be same as y_1 times δ_1 polynomial evaluated at x_1 . But δ_1 polynomial evaluated at x_1 gives me 1. Plus y_2 times δ_2 polynomial evaluated at x_1 . But δ_2 polynomial has the property that x_2 constitutes its root. So, δ_2 polynomial evaluated at x_1 will give me overall 0.

That means, all the remaining terms here will give me 0. And 0 added with a non-zero element will give this non-zero element; and y_1 multiplied with 1 will give me y_1 . In the same way, $f(x_i)$ will be y_1 times δ_1 polynomial evaluated at x_i . But x_i is 1 of the roots of delta 1 polynomial. So, I will get y_1 times 0 plus y_2 times 0, because δ_2 polynomial evaluated at x_i will give me 0.

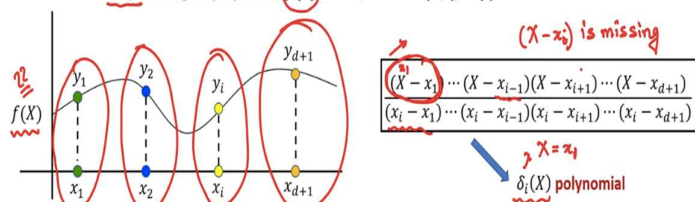
And like that, it is only the i th term in this $f(X)$, which is y_i times δ_i polynomial evaluated at x_i will survive. And remaining everything will become 0. So, this becomes 0, this becomes 0, last term becomes 0. It is only the i th term which will survive. So, sorry, this should be y_i . And δ_i polynomial has the property that x_i does not constitute its root. When it is evaluated at x_i , it gives me 1.

So, y_i into 1 will give me y_i . So, indeed, this $f(X)$ has all the properties. It has degree- d . And indeed, when evaluated at x_1 , it gives me y_1 ; when evaluated at x_2 , it gives me y_2 and so on.

(Refer Slide Time: 31:56)

Lagrange's Polynomial Interpolation

□ **Theorem:** Let $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ be pairs of elements from \mathbb{F} , where x_1, \dots, x_{d+1} are **distinct**. Then there exists a **unique d -degree polynomial** $f(X)$ over \mathbb{F} , such that $f(x_i) = y_i$, for $1 \leq i \leq d+1$



□ **Idea:** Express the unknown $f(X)$ as a **linear combination** of $d+1$ **degree polynomials** $\delta_1(X), \dots, \delta_{d+1}(X)$

$$f(X) \cong y_1 \cdot \delta_1(X) + \dots + y_i \cdot \delta_i(X) + \dots + y_{d+1} \cdot \delta_{d+1}(X)$$

$$\begin{aligned} \delta_1(x_1) &= 1 & \delta_i(x_i) &= 1 & \delta_{d+1}(x_{d+1}) &= 1 \\ \delta_1(x_2) = \dots = \delta_1(x_{d+1}) &= 0 & \delta_i(x_1) = \dots = \delta_i(x_{i-1}) = \delta_i(x_{i+1}) = \dots &= \delta_{d+1}(x_1) = \dots = \delta_{d+1}(x_d) &= 0 \\ & & &= \delta_i(x_{d+1}) = 0 & \end{aligned}$$

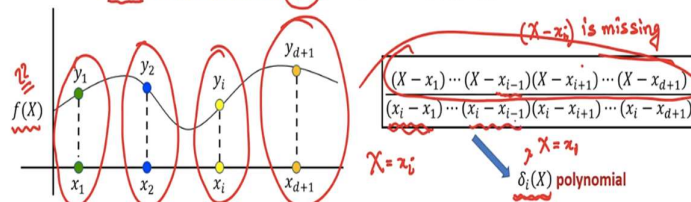
Now, if you want to see the structure of the $\delta_i(X)$ polynomial, this will be the structure of your $\delta_i(X)$ polynomial. So, all the elements you can see. In the numerator, I have the terms of the form $X - x_1$; $X - x_2$; $X - x_{i-1}$. So, basically, the term $X - x_i$ is missing in the numerator. Why it is missing? Because I do not want x_i to be the root of this polynomial; remaining all elements should be the root.

So, x_1 should be root, x_2 should be root, x_{i-1} should be root, x_{i+1} should be root, and so on. So, that is why, in the numerator I have d terms like this. And in the denominator, I have terms like $x_i - x_1$; $x_i - x_2$. So, now, you can see. Indeed, if I substitute $X = x_1$ say; then because, since I have in the numerator $X - x_1$, if I substitute $X = x_1$, I get 0 in the numerator; and hence, overall it becomes 0. So, like that, you substitute any value of x except x_i , this δ_i polynomial will vanish; it will become 0.

(Refer Slide Time: 33:13)

Lagrange's Polynomial Interpolation

□ **Theorem:** Let $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ be pairs of elements from \mathbb{F} , where x_1, \dots, x_{d+1} are **distinct**. Then there exists a **unique d -degree polynomial** $f(X)$ over \mathbb{F} , such that $f(x_i) = y_i$, for $1 \leq i \leq d+1$



□ **Idea:** Express the unknown $f(X)$ as a **linear combination** of $d+1$ d -degree polynomials $\delta_1(X), \dots, \delta_{d+1}(X)$

$$f(X) \cong y_1 \cdot \delta_1(X) + \dots + y_i \cdot \delta_i(X) + \dots + y_{d+1} \cdot \delta_{d+1}(X)$$

$$\delta_i(x_i) = 1 \quad \delta_i(x_1) = \dots = \delta_i(x_{i-1}) = \delta_i(x_{i+1}) = \dots = \delta_i(x_{d+1}) = 0$$

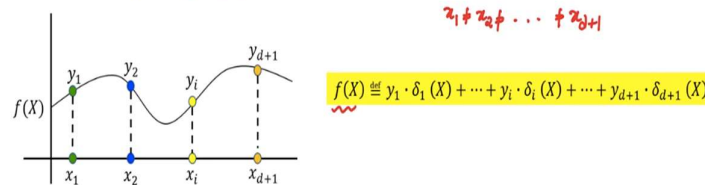
$$\delta_{d+1}(x_{d+1}) = 1 \quad \delta_{d+1}(x_1) = \dots = \delta_{d+1}(x_d) = 0$$

Whereas, if you substitute X , capital $X = x_i$, then both your numerator and denominator will become same. And hence, it will take the value 1. So, there is nothing to memorise here. You just need to ensure; just remember this property that $\delta_i(X)$ has the property that all the elements except the i th x element should be root. And that is possible if you write all this product terms in the numerator. And to ensure that, this δ_i polynomial takes the value 1 at $X = x_i$. You write down the corresponding differences in the denominator. As simple as that.

(Refer Slide Time: 33:55)

Lagrange's Interpolation : Discussion

□ **Theorem:** Let $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ be pairs of elements from \mathbb{F} , where x_1, \dots, x_{d+1} are **distinct**. Then there exists a **unique d -degree polynomial** $f(X)$ over \mathbb{F} , such that $f(x_i) = y_i$, for $1 \leq i \leq d+1$



$$\delta_i(X) = \frac{(X-x_1) \dots (X-x_{i-1})(X-x_{i+1}) \dots (X-x_{d+1})}{(x_i-x_1) \dots (x_i-x_{i-1})(x_i-x_{i+1}) \dots (x_i-x_{d+1})}$$

$$= c_i^{-1} \cdot (X-x_1) \dots (X-x_{i-1})(X-x_{i+1}) \dots (X-x_{d+1})$$

$$c_i \cong (x_i-x_1) \dots (x_i-x_{i-1})(x_i-x_{i+1}) \dots (x_i-x_{d+1}) \neq 0$$

So, this is your Lagrange's interpolation and this is the general form of your $\delta_i(X)$ polynomial. So, now, if you are wondering that this; whatever is there in the denominator, I am dividing the numerator by the denominator, that is not the case. Remember, all the operations are the field operation. In the field operation, we do not have what we call as division.

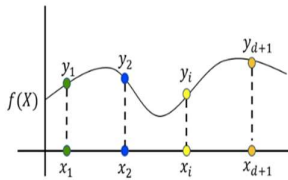
Division should be interpreted as if I am multiplying the numerator with the multiplicative inverse of the denominator. So, let me call this entire denominator as c_i . And it will be a non-zero value, non-zero element from the field. Why? Because of the fact that none of the given x values are same, all of them are distinct. So, if I take differences, pairwise differences, I will get a non-zero element.

And since c_i is a non-zero element, this δ_i polynomial should be interpreted as if I am dividing by 1 over c_i , and remaining whatever in the numerator. But 1 over c_i should be interpreted as if I am multiplying the numerator by the multiplicative inverse of my denominator. And since c_i is non-zero; remember, one of the properties of the field is that all the non-zero elements are guaranteed to have its multiplicative inverse; so, multiplicative inverse here is possible.

(Refer Slide Time: 35:39)

Lagrange's Interpolation : Discussion

□ **Theorem:** Let $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ be pairs of elements from \mathbb{F} , where x_1, \dots, x_{d+1} are distinct. Then there exists a **unique d -degree polynomial** $f(X)$ over \mathbb{F} , such that $f(x_i) = y_i$, for $1 \leq i \leq d+1$



$x_1 \neq x_2 \neq \dots \neq x_{d+1}$

$f(X) \cong y_1 \cdot \delta_1(X) + \dots + y_i \cdot \delta_i(X) + \dots + y_{d+1} \cdot \delta_{d+1}(X)$

□ Given $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$, the value of $f(X)$ can be easily computed for any given x_{new}

$f(x_{new}) = y_1 \delta_1(x_{new}) + \dots + y_{d+1} \delta_{d+1}(x_{new})$

$\delta_i(X) = \frac{(X-x_2) \dots (X-x_{i-1})(X-x_{i+1}) \dots (X-x_{d+1})}{(x_i-x_2) \dots (x_i-x_{i-1})(x_i-x_{i+1}) \dots (x_i-x_{d+1})}$

$= c_i^{-1} \cdot (X-x_2) \dots (X-x_{i-1})(X-x_{i+1}) \dots (X-x_{d+1})$

$c_i \cong (x_i-x_2) \dots (x_i-x_{i-1})(x_i-x_{i+1}) \dots (x_i-x_{d+1}) \neq 0$

Another interesting property of Lagrange's interpolation which we will require later is the following: Imagine you are given $d + 1$ x, y pairs, where the x -coordinates are distinct. We know as per the Lagrange's interpolation that we can compute a curve $f(X)$ passing through this x, y pairs. And now, imagine you are given a new x value, say you are given a new x -coordinate x_{new} , which is different from all the given previous x -coordinates.

And you want to compute the value of this $f(X)$ curve at $X = x_{new}$. That means, you want to find out that what should be the corresponding y value. Now, since my $f(X)$ curve is this, as per the Lagrange's interpolation, the value of $f(x_{new})$ can be computed as follows: I just substitute $X = x_{new}$ in the Lagrange's interpolation formula, and then I get the value of the f curve at $X = x_{new}$.

(Refer Slide Time: 36:49)

Properties of t -degree Polynomial

- Let $\mathcal{P}^{s,t}$ be set of all t -degree polynomials over \mathbb{F} , with s as the constant term $|\mathbb{F}| = 7$
- ◆ Each $f(X) \in \mathcal{P}^{s,t}$ is of the form $f(X) = s + a_1 \cdot X + \dots + a_t \cdot X^t$, where each $a_1, \dots, a_t \in \mathbb{F}$
- $|\mathcal{P}^{s,t}| = |\mathbb{F}|^t$
- a_1 can take any of $|\mathbb{F}|$ values
 a_2 can be any of $|\mathbb{F}|$ —
- $|\mathbb{F}| \times |\mathbb{F}| \times |\mathbb{F}| \times \dots \times |\mathbb{F}|$
 $|\mathbb{F}|^t$

Now, let us see some more interesting properties of t -degree polynomials over field. So, let me call this set $\mathcal{P}^{s,t}$ to be the set of all t -degree polynomials over the field whose constant term, a constant coefficient is the element s . So, each such polynomial, each polynomial from this collection $\mathcal{P}^{s,t}$ will be a polynomial which will have $t + 1$ coefficients.

It will have the coefficient a_0 , it will have the coefficient a_1 , it will have the coefficient a_t . But since I want the constant term to be the value s , I do not have a choice for a_0 . My a_0 has to be compulsorily s . Remaining other t coefficients can be any element from the field. So, that is why, it follows that the number of polynomials $f(X)$ which are elements of this bigger set of polynomials whose constant term is the element s ; the number of such polynomials is the number of elements that you can have in the field raised to the power t .

Why so? Because a_1 can take any of these many values. So, if, say for instance, the cardinality of \mathbb{F} is 10, if there are 10 elements in your field, or say 7 elements in your field, then a_1 could be any of those 7 elements; a_2 also can be any of those 7 elements, and so on. So, that is why, how many possible polynomials I can have? I can have these many options for the first coefficient.

I have these many options for the coefficients for X^2 . I have these many options for the coefficients for X^3 . And like that, I have these many options for the coefficient of X^t . So, this is basically the number of elements in the field raised to the power t . These many possible polynomials you can have.

(Refer Slide Time: 39:48)

Properties of t -degree Polynomial

- Let $\mathcal{P}^{s,t}$ $\hat{=}$ set of all t -degree polynomials over \mathbb{F} , with s as the constant term
- ◆ Each $f(X) \in \mathcal{P}^{s,t}$ is of the form $f(X) = s + a_1 \cdot X + \dots + a_t \cdot X^t$, where each $a_1, \dots, a_t \in \mathbb{F}$
- Ex: $t = 2, \mathbb{F} = (\mathbb{Z}_3, +_3, \cdot_3)$ and $s = 1$

$1+X$	$1+X^2$	$1+X+X^2$	$1+2X+X^2$
$1+2X$	$1+2X^2$	$1+X+2X^2$	$1+2X+2X^2$

$|\mathcal{P}^{s,t}| = |\mathbb{F}|^t$ $|\mathbb{F}| = 3 \Rightarrow 3^2 = 9$ $f(0)=s$ $g(0)=s$

- $\{(x_i, y_i), \dots, (x_t, y_t)\}$ arbitrary values from \mathbb{F} :
 $x_i \neq \dots \neq x_t \neq 0$ $f(x_i) = y_i$ $g(x_i) = y_i$
- For any given $s \in \mathbb{F}$, there is a **unique** polynomial from $\mathcal{P}^{s,t}$ passing through $(0, s), (x_1, y_1), \dots, (x_t, y_t)$

So, let us see an example here. Imagine my $t = 2$; my field is \mathbb{Z}_3 ; \mathbb{Z}_3 means, my elements could be 0, 1 and 2. And my plus operation here is addition modulo 3, and my multiplication operation here is multiplication modulo 3. And imagine my $s = 1$. So, now, if I want to list down all possible polynomials of degree-2, where the coefficients could be either 0, 1 or 2, and whose constant term is 1; then that collection of polynomials as per my notation is this.

And you can see that now I have, how many? $9 \mathbb{F}^2$ number of polynomials. And \mathbb{F} cardinality is basically here 3, because I have 3 elements in my field. So, 3 square, which is 9 possible polynomials. You can see. This is a polynomial of degree-2. You might be wondering that there is no term like X and X^2 . But that is fine, I can always imagine that I have a term like $0X$ and $0X^2$.

So, overall this will be treated as a polynomial of degree-2 whose constant term is 1. This is a polynomial of degree-2 whose constant term is 1; another polynomial. So, all the polynomials have their constant term as 1, and the maximum degree could be 2, and number of such polynomials is 9. Now, another property which we can derive based on whatever we have discussed till now is the following:

Imagine you are given t pairs, t x, y pairs. Pictorially you are given t number of distinct points in the x, y -coordinate, where this all x and y elements are elements of the field. And these x -coordinates are different, which ensures that these points are distinct points. Now, if I take an element s from the field, that s , element s could be any element from the field; my question is,

how many possible polynomials can be there whose constant term is s and where this x, y pairs also constitute the points on that polynomial?

Basically, how many polynomials from this set; so, this is the bigger set, this is the set of all possible t -degree polynomials whose constant term can be s . I am asking that from this collection, namely from \mathbb{F}^t number of polynomials, how many possible polynomials can be there whose constant term is s ; namely, the point $(0, s)$ lies on that polynomial as well as the remaining t distinct points which are given to you also lie on that polynomial?

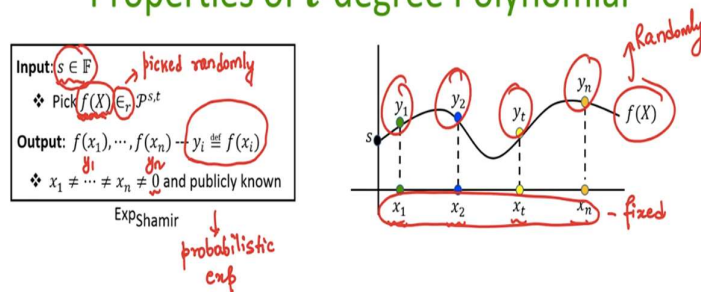
And it turns out that there is only 1 possible polynomial from this set. You cannot have more than 1 polynomial from this set satisfying this property. This is because, you are already given t number of pairs, x, y pairs, t number of points, and you also want that $(0, s)$ should also lie on that polynomial. So, overall, you have now $t + 1$ points. And through $t + 1$ points, you can have only 1 polynomial of degree- t passing through all $t + 1$ of them.

You cannot have multiple, you cannot have a polynomial $f(X)$ belonging to this set $\mathcal{P}^{s,t}$, as well as $g(X)$ also belonging to $\mathcal{P}^{s,t}$ such that your $f(x_1) = y_1$ and $g(x_1) = y_1$ And like that, $f(x_t) = y_t$ and $g(x_t) = y_t$. That is not possible, because that means, anyhow since both $f(X)$ polynomial and $g(X)$ polynomial has their constant term s ; you also have the condition that $f(0) = s, g(0) = s$.

And hence, you get that f and g polynomials, even though they are different polynomials of degree- t , but they have $t + 1$ common values; that is not possible. So, that means, there can be only 1 $f(X)$ polynomial, whose constant term is s and whose degree is t , and which can pass through these given t distinct points; cannot have another $g(X)$ polynomial possible.

(Refer Slide Time: 44:56)

Properties of t -degree Polynomial



So, now, let us see another important property of t -degree polynomial. So, this property, for demand stating, I will consider a random experiment here. So, in this experiment, I call this experiment as experiment Shamir attributed to Adi Shamir, who gave this experiment. So, what is this experiment. So, the input to this experiment is some element s from the field \mathbb{F} . Now, the experiment does the following:

It randomly picks a t -degree polynomial, call it $f(X)$, whose constant term is s . So, this notation \in_r , belongs to and subscript r , that means, this picked randomly, uniformly at random. Remember, there are many possible t -degree polynomials whose constant term could be s . I am just randomly picking one of them. And output of this experiment is the value of this randomly chosen polynomial at n publicly known distinct values.

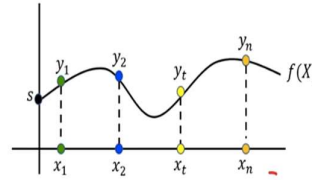
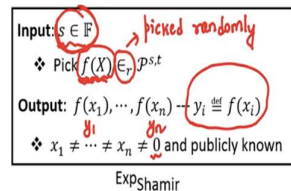
So, the outputs are $f(x_1), f(x_2), \dots, f(x_i), \dots, f(x_n)$; all of which are elements from the field; none of them is 0, and all of them are distinct. So, let me call the value of $f(x_i)$ as y_i . So, your outputs are y_1, y_2, \dots, y_n . A very simple experiment. So, now, you can see that if I run this experiment different times, my output could be different. First time I run this experiment with the input s .

The polynomial $f(X)$ that I might choose might be different from the polynomial which I pick when I run the same experiment with the input s , because, every time I am picking the polynomial randomly. I am not fixing the polynomial $f(X)$; that is important. That is why this is a probabilistic experiment. That means, even though the x values, x_1, x_2, \dots, x_n , they will be

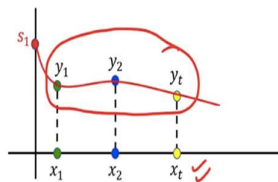
fixed for each instance of the experiment; fixed. Since my polynomial $f(X)$ is randomly chosen, my outputs y_1, y_2, \dots, y_n can take different values with different probability.

(Refer Slide Time: 47:38)

Properties of t -degree Polynomial



□ How much information about the input s is learnt through any subset of t output values?



Now, I want to capture, measure the following: Given this experiment, where the input s is not known to you; I will not be telling you the input s ; how much information about this input s is learnt if I just give you any set of t output values? So, I will not give you the full set of n output values, but I just gave you any set of t output values which I obtain by running this experiment. It is like saying the following:

I am a kind of a person; I want to challenge you. I run this experiment with some input s which is known only to me, and I generate the n outputs, and I give you any t of the n outputs that I have generated. And I challenge you, what was my input s ? how much information about the input s you learn? So, let us assume for simplicity that I give you the first t output values.

But whatever I am discussing here, it holds even if I give you t output values which are not the consecutive t y output values. So, I may give you, say y_1 . And then, I do not give you y_2 , but I give you y_3 . And then I do not give you y_4 , and I give you y_5 and y_6 and so on. But overall, I gave you t number of y output values. x output values are anyhow known to you. I challenge you, how much information about s you learn? The thing is, from your viewpoint, you do not know what was the curve $f(X)$ that I have chosen.

(Refer Slide Time: 49:24)

Properties of t -degree Polynomial

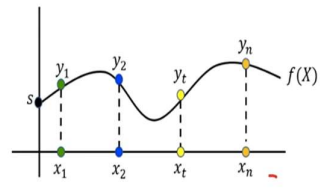
Input: $s \in \mathbb{F}$ picked randomly s'

❖ Pick $f(X) \in_r \mathcal{P}^{s,t}$

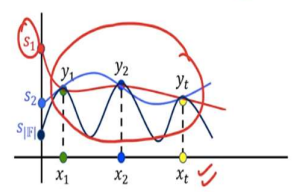
Output: $f(x_1), \dots, f(x_n) \rightarrow y_i \equiv f(x_i)$

❖ $x_1 \neq \dots \neq x_n \neq 0$ and publicly known

ExpShamir



□ How much information about the input s is learnt through any subset of t output values? Take any y_1, y_2, \dots, y_t from \mathbb{F}



$$\Pr_{f(X) \in_r \mathcal{P}^{s,t}} [(f(x_1) = y_1) \wedge \dots \wedge (f(x_t) = y_t)]$$

$$\Pr_{g(X) \in_r \mathcal{P}^{s',t}} [(g(x_1) = y_1) \wedge \dots \wedge (g(x_t) = y_t)]$$

You only know that in the experiment I have chosen the curve $f(X)$ uniformly at random. But that $f(X)$ curve could be such that its constant term could be say an element s_1 from the field. Or it could be also the case that the curve that I have chosen was such that its constant term was s_2 . That means, my input in the experiment was s_2 , and the polynomial that I evaluated, when evaluated at x_1, x_2, \dots, x_t , gives you the values, gives the output y_1, \dots, y_t .

Or it could be the case that my input in the experiment was say the third element from the field, because I have chosen a t -degree polynomial whose constant term was the third element from the field and so on. So, just based on the knowledge of t output values that I give you from this experiment, you cannot pinpoint what was the curve that I had chosen. And hence, from your viewpoint, it could be any element from the field which was my input in the experiment.

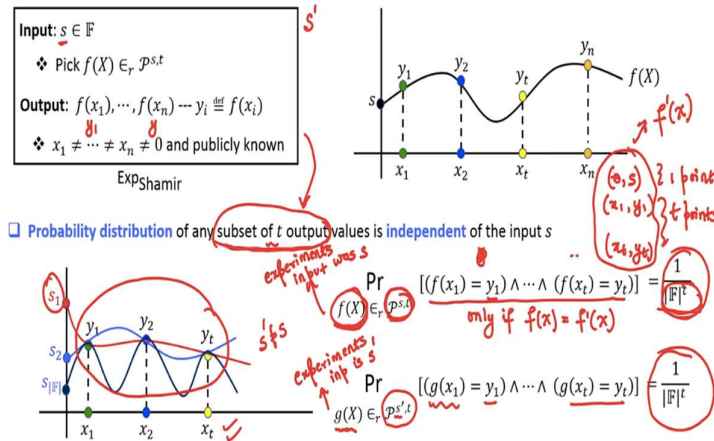
More formally, what we can prove here is the following: You take any y_1, y_2, \dots, y_t from \mathbb{F} . The probability that the y_1, \dots, y_t that I am giving to you, and which are elements from the field, they are generated as an outcome of the experiment where a polynomial $f(X)$ was chosen, whose constant term was s , is the same as the probability that the same y_1, y_2, \dots, y_t would have been generated, if in the experiment I would have chosen a polynomial $g(X)$ whose constant term would have been s' .

That means, I am now going to show you, it does not matter whether my input is s or whether my input in the experiment is s' ; if I just focus on any subset of t output values generated in the experiment, with equal probability, those t output values could have been generated from the input s or could have been generated from the input s' . You cannot pinpoint just based on

the t output y values, whether you are just seeing the output corresponding to the experiment run with input s or you are seeing the output for an experiment which was executed with the input s' . So, let us formally prove this. So, let us consider the first probability here.

(Refer Slide Time: 52:06)

Properties of t -degree Polynomial



I want to compute the following: What is the probability that in the experiment the $f(X)$ polynomial is chosen randomly from this set? That means, basically I am asking here, experiments input was s . Because, if the polynomial is chosen from this set, that means, the input was s . And given this, you see the first t outcomes to be y_1, \dots, y_t . That means, that randomly chosen polynomial evaluated at x_1, x_2, \dots, x_t , gives you the values y_1, \dots, y_t .

My claim is that this probability is 1 over the cardinality of the number of t -degree polynomials whose constant term is s . This is because $y_1, \dots, y_t; (x_1, y_1), \dots, (x_t, y_t)$, they are t points. And now, if you add $(0, s)$ also, you basically get 1 more point. Through this $t + 1$ points, there can be only 1 t -degree polynomial; call it $f'(X)$, passing through all $t + 1$ of them.

There cannot be multiple polynomials whose constant term could be s and satisfying or lying, passing through $(x_1, y_1), \dots, (x_t, y_t)$. There can be only 1 t -degree polynomial. But I am choosing the polynomial $f(X)$ randomly. So, my sample space here is the set of all possible t -degree polynomials whose constant term could be s . So, that is the cardinality of the sample space.

But out of all, out of these many number of t -degree polynomials whose constant term could be s , there could be only 1 t -degree polynomial which satisfies the condition that $f(x_1) =$

$y_1, f(x_2) = y_2, \dots, f(x_t) = y_t$. That means, this condition will be true only if the $f(X)$ polynomial which I am randomly choosing here is actually $f'(X)$. But since $f(X)$ is randomly chosen, the probability that $f(X) = f'(X)$ becomes overall this.

In the same way, the second probability expression here, tries to capture the following. Your experiments input is s' because you are picking now polynomials from the set of polynomials whose constant term is s' , where s' is different from s . But still you want to measure the probability of the event that randomly chosen t -degree polynomial whose constant term is s' , when evaluated at x_1 , gives you y_1 ; evaluated at x_2 , gives you y_2 ; evaluated at x_t , gives you y_t .

Again, because of the same reasoning that we have given just now, the probability of this event is also the same, whatever was the probability of the above event. That means, what we have formally proved here is that, in this experiment, if I just give you any subset of t output values, I do not give you the full vector of n output values, I run the experiment with some private input, but I give you only a partial subset of the output, namely, I just give you; you tell me which t output values you want, I will give you those t output values.

My claim is, from your viewpoint, those t output values could have been generated with equal probability both for input s as well as input s' . And hence, you do not learn any information about my input for the experiment.

(Refer Slide Time: 56:20)

Properties of t -degree Polynomial

Input: $s \in \mathbb{F}$ $s = 13$

❖ Pick $f(X) \in_r \mathcal{P}^{s,t}$ $13 + 10X + 2X^2$

Output: $f(x_1), \dots, f(x_n) \dots y_i \stackrel{\text{def}}{=} f(x_i)$

❖ $x_1 \neq \dots \neq x_n \neq 0$ and publicly known

Ex: $n = 5, t = 2, \mathbb{F} = (\mathbb{Z}_{17})_{+17, \cdot 17}$ and $s = 13$

$x_1 = 1, x_2 = 2, x_3 = 3, x_4 = 4, x_5 = 5$ $f(X) = 13 + 10X + 2X^2$

$y_1 = 8$ $y_2 = 7$ $y_3 = 10$ $y_4 = 0$ $y_5 = 11$

Can $y_1 = 8$ and $y_3 = 10$ occur as the output for every candidate $s \in \mathbb{Z}_{17}$, apart from $s = 13$?

Candidate s	Candidate $f(X)$	y_1	y_3
0	$16X + 9X^2$	8	10
1	$1 + 9X + 15X^2$	8	10
2	$2 + 2X + 4X^2$	8	10
3	$3 + 12X + 10X^2$	8	10
4	$4 + 5X + 16X^2$	8	10
5	$5 + 15X + 5X^2$	8	10
6	$6 + 8X + 11X^2$	8	10
7	$7 + X$	8	10

Candidate s	Candidate $f(X)$	y_1	y_3
8	$8 + 11X + 6X^2$	8	10
9	$9 + 4X + 12X^2$	8	10
10	$10 + 14X + X^2$	8	10
11	$11 + 7X + 7X^2$	8	10
12	$12 + 13X^2$	8	10
14	$14 + 3X + 8X^2$	8	10
15	$15 + 13X + 14X^2$	8	10
16	$16 + 6X + 3X^2$	8	10

So, let me demonstrate this property with this example, where I take the field to be \mathbb{Z}_{17} , and my input in the experiment is 13. And I am fixing my evaluation points to be 1, 2, 3, 4, 5. That means, suppose in the experiment here, my input was 13, I could have chosen any 2-degree polynomial whose constant term is 13. I am picking them randomly. So, imagine that I pick this polynomial; this is my polynomial which I have chosen.

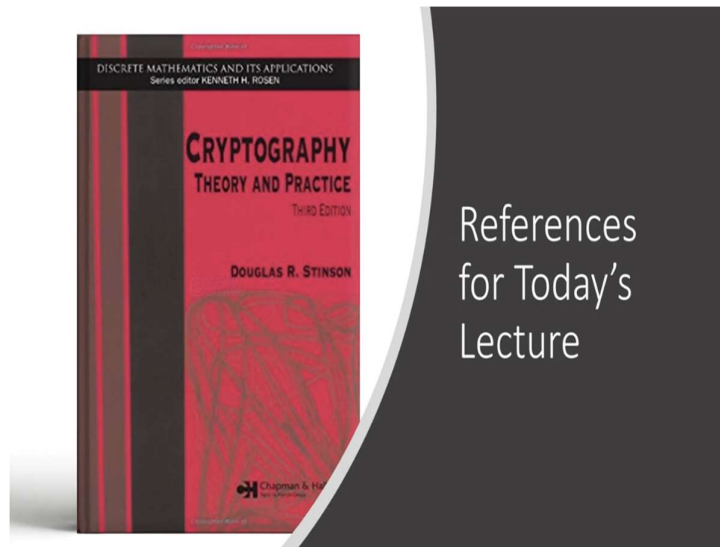
But I am not telling you this; I am running this experiment myself. And if I evaluate this polynomial at 1, 2, 3, 4, 5, I get these y values. Now, you come to me and ask for any 2 of the 5 y values. Suppose I give you the first two y values, not the first two; you ask for, say the first and the third y value. So, I gave you $y_1 = 8$ and $y_3 = 10$. And now I ask you, can you tell me what was my input? was it 1? was it 2? was it 0? was it 5? which element from \mathbb{Z}_{17} I have used as my input in the experiment?

And now you can see. What I am doing here is; you can do the following: You can ask yourself in the mind. Is it the case that my input in the experiment was 0, and you got outputs $y_1 = 8$ and $y_3 = 10$? Well, that is quite possible if in the experiment I would have chosen this 2-degree polynomial, because indeed, this 2-degree polynomial has its constant term 0, and when evaluated at $x = 1$ gives you 8, and when evaluated at $x = 3$ gives you 10.

Or if you ask in your mind that is it the case that my input was 1 in the experiment; well, that is quite possible if in the experiment, I would have chosen this 2-degree polynomial and indeed this 2-degree polynomial when evaluated at $x_1 = 1$ gives you 8 and when evaluated at $x_3 = 3$ gives you 10. And now, like that, if you ask, if you analyse in your mind that whether this output $y_1 = 8$ and $y_3 = 10$ can come from different candidate s values, each of the candidate s value is equiprobable from your viewpoint.

You cannot pinpoint what was my input in the experiment. It could have been any input from the field \mathbb{Z}_{17} which would have given you the output $y_1 = 8$ and $y_3 = 10$. And hence, each possible input is equiprobable.

(Refer Slide Time: 59:18)



So, with that, I end today's lecture. Thank you.