Secure Computation: Part II

Prof. Ashish Choudhury
Department of Computer Science and Engineering
Indian Institute of Information Technology, Bangalore

Lecture - 34
Bivariate Polynomials Over Finite Fields: I

So, in the next few lectures we are going to discuss about Bivariate Polynomials Over Finite Fields and their properties which will be later useful for designing polynomial based verifiable secret sharing schemes.

(Refer Slide Time: 00:35)

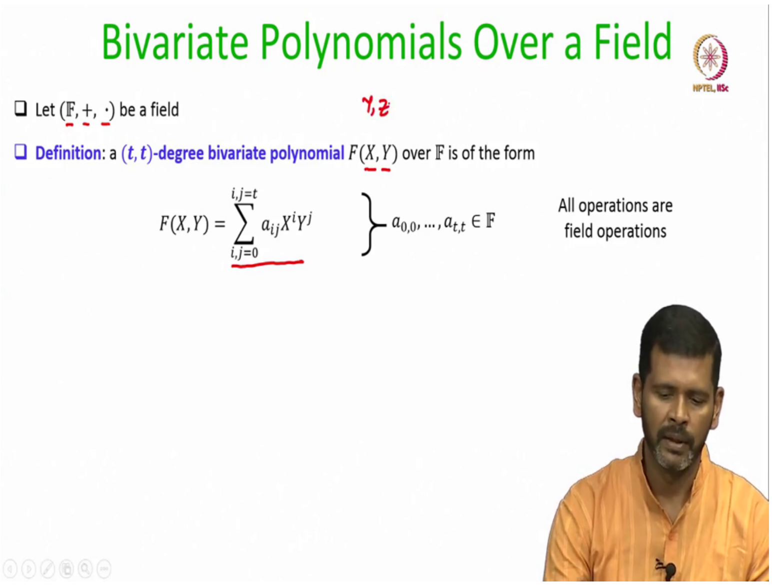
Lecture Overview

❑ Bivariate polynomials over a finite field

- ❖ Properties
- ❖ Lagrange's interpolation

So, in this lecture specifically, we will discuss about the Lagrange's interpolation in the context of bivariate polynomials over a finite field.

(Refer Slide Time: 00:45)



Bivariate Polynomials Over a Field

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

Y, Z

- ❑ **Definition:** a (t, t)**-degree bivariate polynomial** $F(X, Y)$ over $\mathbb{F}$ is of the form

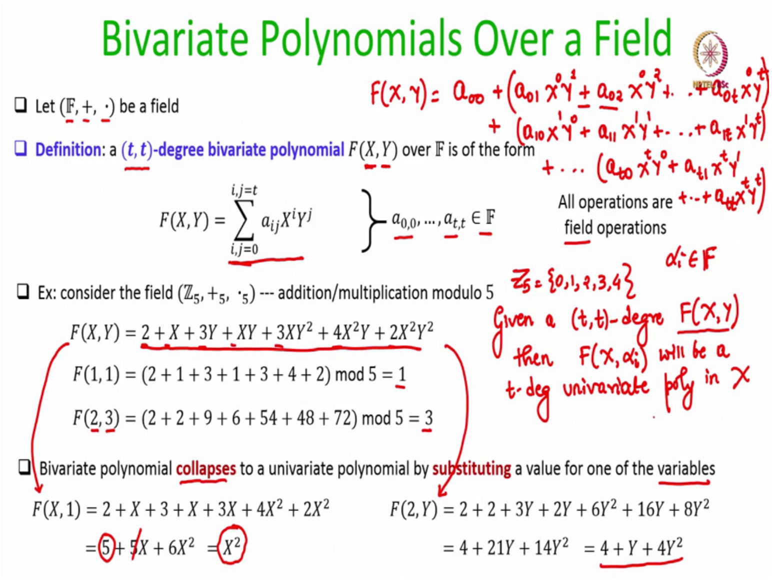
$$F(X,Y) = \sum_{i,j=0}^{i,j=t} a_{ij} X^i Y^j \quad \Big\} \; a_{0,0}, \dots, a_{t,t} \in \mathbb{F}$$

All operations are field operations

So, what are bivariate polynomials over a field? So, imagine you are given a field F with the plus and dot operations. Then a t, t degree bivariate polynomial over the field is of the following form ok. So, it is called bivariate because, it is a polynomial in two variables say X and Y. Well, they can be any two variables, you can call them Y and Z or any variables.

So, I am calling the two variables as the variable X and a variable Y. And, we will be specifically using a bivariate polynomial where the degree of the X variable will be t and the degree of the Y variable will be t in the overall bivariate polynomial. So, the expansion of this summation, you can interpret it as follows.

(Refer Slide Time: 01:53)



Bivariate Polynomials Over a Field

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

❑ **Definition**: a (t, t)-**degree bivariate polynomial** $F(X, Y)$ over $\mathbb{F}$ is of the form

$$F(X,Y) = \sum_{i,j=0}^{i,j=t} a_{ij} X^i Y^j \quad \Big\} \; a_{0,0}, \dots, a_{t,t} \in \mathbb{F}$$

All operations are field operations

$$F(X,Y) = a_{00} + (a_{01} X^0 Y^1 + a_{02} X^0 Y^2 + \dots + a_{0t} X^0 Y^t) + (a_{10} X^1 Y^0 + a_{11} X^1 Y^1 + \dots + a_{1t} X^1 Y^t) + \dots (a_{t0} X^t Y^0 + a_{t1} X^t Y^1 + \dots + a_{tt} X^t Y^t)$$

❑ Ex: consider the field $(\mathbb{Z}_5, +_5, \cdot_5)$ --- addition/multiplication modulo 5

$\mathbb{Z}_5 = \{0,1,2,3,4\}$

$\alpha_i \in \mathbb{F}$

$$F(X,Y) = 2 + X + 3Y + XY + 3XY^2 + 4X^2Y + 2X^2Y^2$$

$$F(1,1) = (2+1+3+1+3+4+2) \bmod 5 = 1$$

$$F(2,3) = (2+2+9+6+54+48+72) \bmod 5 = 3$$

Given a (t,t)-degree $F(X,Y)$ then $F(X, \alpha_i)$ will be a t-deg univariate poly in X

❑ Bivariate polynomial collapses to a univariate polynomial by substituting a value for one of the variables

$$F(X,1) = 2 + X + 3 + X + 3X + 4X^2 + 2X^2 = \boxed{5} + \cancel{5}X + 6X^2 = \boxed{X^2}$$

$$F(2,Y) = 2 + 2 + 3Y + 2Y + 6Y^2 + 16Y + 8Y^2 = 4 + 21Y + 14Y^2 = 4 + Y + 4Y^2$$

So, you will have the constant coefficient a00, then you will have a term for X power 0 Y power 1, its coefficient will be a01. Then, you will have a term with X power 0 Y power 2, its coefficient will be a02. And, like that you will have a term with X power 0 Y to the power t, its coefficient will be a0t. And, then you will have similarly terms like this.

And, then all the way to terms where you have X power t Y power 0, a term with X power t Y power 1 and a term with X power t Y power t ok. So, you can imagine it as a two-dimensional generalization of univariate polynomials. All of us are familiar with univariate polynomials in one variable of degree t.

Now, we are extending that concept to two-dimensional polynomials, where the two-dimensions are represented by two variables X and Y. And, all these coefficients a00, a01, up to att will be elements of finite fields. And, all the plus operations and the dot operations here in the expansion are your field plus and dot operations ok.

So, let us see some examples here. So, imagine you consider the field Z5. So, Z 5 will have the elements 0, 1, 2, 3 and 4 and where all the addition operation is addition modulo 5 and multiplication operation is multiplication modulo 5. Then, a bivariate, this is a bivariate polynomial where you have the coefficients 2 1 3 1 3 4 and 2 respectively ok.

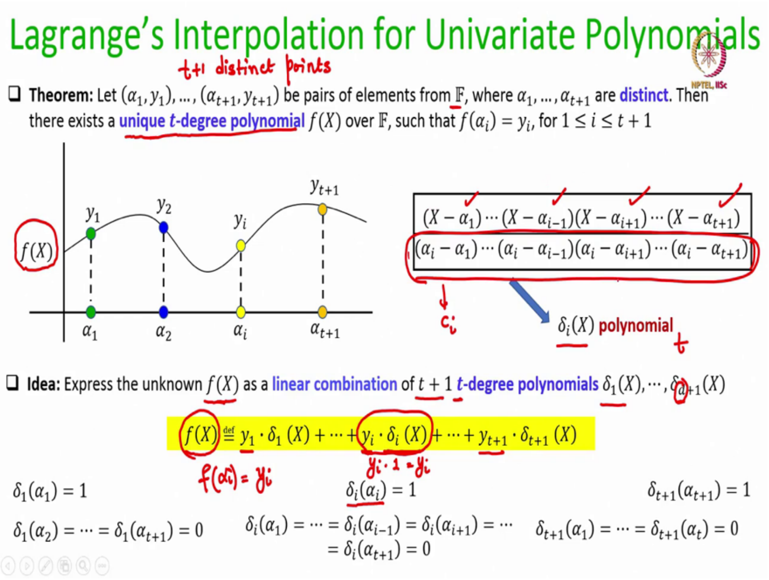
So, now if I want to find out the value of this polynomial, let us say at X equal to 1 and Y equal to 1, then I can substitute the value in this polynomial and, remember all the plus and multiplication operations are performed modulo 5, then the value of this bivariate polynomial at X equal to 1 and Y equal to 1 will be 1. If I want to evaluate or find the value of this bivariate polynomial at X equal to 2 and Y equal to 3, it will turn out to be 3 ok.

Now, imagine you are given a bivariate polynomial in two variables, as soon as I substitute the value for one of the variables; the bivariate polynomial collapses or reduces to a univariate polynomial. So, again for instance if I take the same example here, if I substitute Y is equal to 1 in this bivariate polynomial, then you can see that the resultant polynomial will be now a polynomial only in the variable X.

So, it is a univariate polynomial in X and since we are performing all the operations modulo 5, then in the field Z 5; element 5 is same as the element 0. So, that is why this 5 will vanish off, 5 times X also will vanish off and 6 will be 6 modulo 5 which is 1. So, the value of this bivariate polynomial at Y is equal to 1 will result in a univariate polynomial X square. On the other hand, if I take the same bivariate polynomial and evaluate it at X equal 2, then I will obtain a univariate polynomial in Y.

And, since we are performing all the operations modulo 5, the resultant polynomial will be this. So, in general if we are given a t, t degree bivariate polynomial say F(X, Y); then F(X, alpha i) will be a t degree univariate polynomial in X, where alpha i is some element from the field. In the same way, if I substitute X equal to alpha i in a t, t degree bivariate polynomial, then it collapses or reduces to a t degree univariate polynomial in Y ok.

(Refer Slide Time: 08: 16)



Lagrange's Interpolation for Univariate Polynomials

t+1 distinct points

❑ **Theorem:** Let $(\alpha_1, y_1), \ldots, (\alpha_{t+1}, y_{t+1})$ be pairs of elements from $\mathbb{F}$, where $\alpha_1, \ldots, \alpha_{t+1}$ are distinct. Then there exists a unique t-degree polynomial $f(X)$ over $\mathbb{F}$, such that $f(\alpha_i) = y_i$, for $1 \leq i \leq t+1$

$$\frac{(X-\alpha_1)\cdots(X-\alpha_{i-1})(X-\alpha_{i+1})\cdots(X-\alpha_{t+1})}{(\alpha_i-\alpha_1)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_{t+1})}$$

c_i

$\delta_i(X)$ polynomial

t

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

$$f(X) \overset{\text{def}}{=} y_1 \cdot \delta_1(X) + \cdots + \underbrace{y_i \cdot \delta_i(X)}_{y_i \cdot 1 = y_i} + \cdots + y_{t+1} \cdot \delta_{t+1}(X)$$

$f(\alpha_i) = y_i$

$\delta_1(\alpha_1) = 1$

$\delta_1(\alpha_2) = \cdots = \delta_1(\alpha_{t+1}) = 0$

$\delta_i(\alpha_i) = 1$

$\delta_i(\alpha_1) = \cdots = \delta_i(\alpha_{i-1}) = \delta_i(\alpha_{i+1}) = \cdots = \delta_i(\alpha_{t+1}) = 0$

$\delta_{t+1}(\alpha_{t+1}) = 1$

$\delta_{t+1}(\alpha_1) = \cdots = \delta_{t+1}(\alpha_t) = 0$

Now, we want to discuss the Lagrange's interpolation for bivariate polynomials, but before going into that let us quickly recall the Lagrange's interpolation in the context of univariate polynomials. So, we know that if we are given t plus 1 distinct points over a field, then I can always find I can always interpolate a unique t degree polynomial over the field passing through those given t plus 1 distinct points.

And, that unique polynomial can be obtained through several mechanisms, by solving a system of linear equations or by using this nice Lagrange's interpolation formula, where the idea is to express that unknown curve f(X) as a linear combination of several t degree polynomials.

So, the idea here is to express that unknown polynomial which you want to find out, which you want to pass through the given t + 1 points, as a linear combination of several t degree polynomials, to be more specific, t + 1 numbers of t degree polynomials, where the y components of the given points serve as the linear combiners.

And, these t degree polynomials $\delta_1(X), \cdots, \delta_{t+1}(X)$ have some special properties. So, for instance if I take the polynomial $\delta_1(X)$, then all the alpha components except alpha 1 will be the root of that polynomial whereas, at alpha 1 the polynomial $\delta_1(X)$ should give you the value 1.

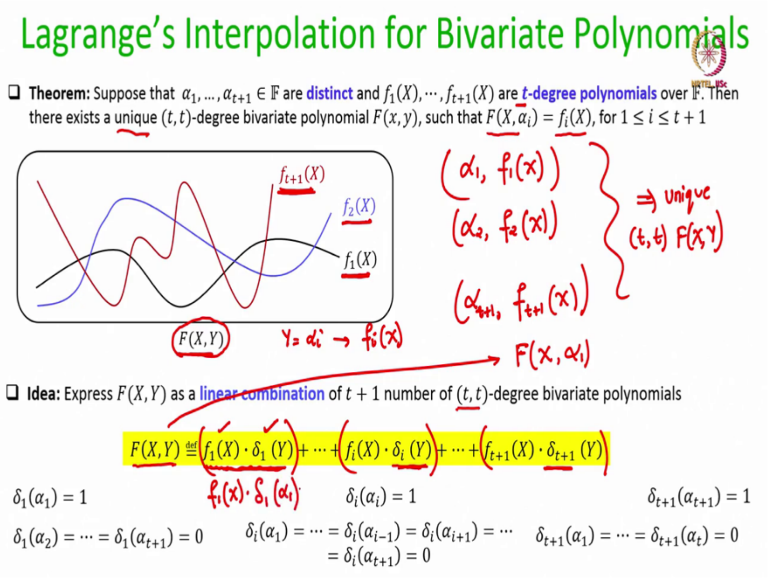
In general, if I take the ith delta polynomial then all the alpha components except alpha i should be the root and at alpha i this $\delta_i(X)$ polynomial should give the value 1. So, you can see that each of these delta polynomials have t roots, that is why it is a t degree polynomial. So, now, if we have these special delta polynomials, then it is easy to see that indeed f(X) is a t degree polynomial.

Why it is a t degree polynomial? Because, it is summation or a linear combination of several t degree polynomials and, indeed f(X) at alpha i will evaluate to y i, because all the delta polynomials $\delta_1(X), \cdots, \delta_{i-1}(X), \delta_{i+1}(X),$ except the ith delta polynomial $\delta_i(X)$ will vanish, will give the value 0 at X equal to alpha i. And, its only this ith term which will survive.

And, what will be the ith term if I substitute X equal to α_i? Well, it will give yi multiplied with 1 which will be same as yi ok. Now, what is the form of this $\delta_i(X)$ polynomial? We want that all the alpha components except α_i should be the root. So, α_1 is the root, α_2 is the root, α_{i-1} is the root, α_{i+1} is the root, α_{t+1} is the root. And, we also want that at α_i, it should give the value 1.

So, that is why in the denominator you have this term. I would like to stress that since this polynomial is over a field, you should not treat it as numerator over denominator. So, the denominator here will be a non-zero element from the field, say the denominator is ci. Then, the $\delta_i(X)$ polynomial is basically the numerator multiplied with inverse of ci ok.

(Refer Slide Time: 12:53)



Lagrange's Interpolation for Bivariate Polynomials

□ **Theorem:** Suppose that $\alpha_1, \ldots, \alpha_{t+1} \in \mathbb{F}$ are distinct and $f_1(X), \cdots, f_{t+1}(X)$ are t-degree polynomials over $\mathbb{F}$. Then there exists a unique (t, t)-degree bivariate polynomial $F(x, y)$, such that $F(X, \alpha_i) = f_i(X)$, for $1 \leq i \leq t+1$

$f_{t+1}(X)$
$f_2(X)$
$f_1(X)$
$F(X,Y)$

$Y = \alpha_i \rightarrow f_i(x)$

$(\alpha_1, f_1(x))$
$(\alpha_2, f_2(x))$
$(\alpha_{t+1}, f_{t+1}(x))$

$\Rightarrow$ unique (t,t) $F(X,Y)$

$F(x, \alpha_1)$

□ **Idea:** Express $F(X, Y)$ as a linear combination of $t+1$ number of (t, t)-degree bivariate polynomials

$$F(X,Y) \overset{\text{def}}{=} \left(f_1(X) \cdot \delta_1(Y)\right) + \cdots + \left(f_i(X) \cdot \delta_i(Y)\right) + \cdots + \left(f_{t+1}(X) \cdot \delta_{t+1}(Y)\right)$$

$f_1(x) \cdot \delta_1(\alpha_1)$

$\delta_1(\alpha_1) = 1$

$\delta_1(\alpha_2) = \cdots = \delta_1(\alpha_{t+1}) = 0$

$\delta_i(\alpha_i) = 1$

$\delta_i(\alpha_1) = \cdots = \delta_i(\alpha_{i-1}) = \delta_i(\alpha_{i+1}) = \cdots = \delta_i(\alpha_{t+1}) = 0$

$\delta_{t+1}(\alpha_{t+1}) = 1$

$\delta_{t+1}(\alpha_1) = \cdots = \delta_{t+1}(\alpha_t) = 0$

Now, we want to extend this Lagrange's interpolation for bivariate polynomials and in fact, we can extend, we can have a version of Lagrange's interpolation for in fact, polynomials in three variables, polynomials in four variables or polynomial in any number of variables. But, in the context of verifiable secret sharing, we will be dealing only with polynomials in two variables where, the degree of both the variables will be t.

So, what exactly the Lagrange's interpolation formula for bivariate polynomial state? So, there are two versions here. So, let us try to understand the first version. So, to understand this, again let us go back to the case of the univariate polynomials. In the case of univariate polynomials, we have seen that if you are given t + 1 distinct points, then you can always pass a unique t degree polynomial passing through those t + 1 distinct points ok.

Now, I am not giving you t+1 distinct points, but rather I am giving you t + 1 polynomials, where each polynomial has degree t and each of these polynomials is a polynomial in X variable. So, you are given t + 1 number of t degree univariate polynomials in X ok. If you are given such t degree univariate polynomials and the statement is that you can always find the unique bivariate polynomial of degree t in each variable which when evaluated at $\alpha_1, \cdots, \alpha_{t+1}$ would have given you those univariate polynomials.

That means, pictorially you can imagine that say I am giving you one t degree univariate polynomial, another t degree univariate polynomial. And, like that I am giving you t + 1 number of univariate polynomials. They may be same, they may be different, just they are arbitrary t degree univariate polynomials in the X variable.

Then, using this t plus 1 number of univariate polynomials, I can always form a unique bivariate polynomial of degree t in each variable, such that when I evaluate this bivariate polynomial at Y is equal to α_i, it will give me the ith univariate polynomial which I was given right.

So, on a very high level, it is a generalization of your Lagrange's interpolation formula in one variable right to two dimensions. So, in one dimension for the case of univariate polynomials the statement was if I give you t + 1 points, you can find one polynomial, one unique polynomial in one variable, passing through those points. Now, the points themselves are polynomials in X variable. So, you have one polynomial $f_1(X)$, another polynomial $f_2(X)$, another polynomial $f_{t+1}(X)$.

So, my statement is that through $(\alpha_1, f_1(X)), \cdots, (\alpha_{t+1}, f_{t+1}(X))$ I can find a unique bivariate polynomial F(X, Y) of degree t in both X and Y, that is the statement here. And, again the idea here is to express that bivariate polynomial which we want to interpolate as a linear combination of t + 1 number of bivariate polynomials of degree t in each variable, where somehow these univariate polynomials $f_1(X), \cdots, f_{t+1}(X)$ serve as the linear combiners right.

So, more specifically we want to express that unknown bivariate polynomial F(X, Y) in this form ok. And, here these delta polynomials will be some special polynomials, each of these delta polynomial will be a t degree polynomial and it will have some special properties. So, for instance if I take the first delta polynomial, then all the alpha components except alpha 1 should be the root of this delta 1 Y polynomial. And, this delta 1 polynomial evaluated at Y equal to alpha 1 should give me a value 1.

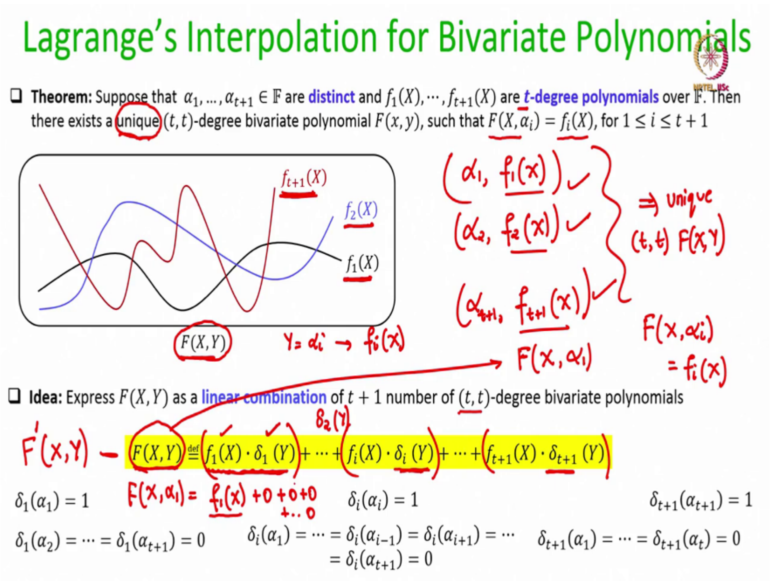
So, since this delta 1 polynomial has t number of roots that automatically implies that its degree will be t. In the same way, if I take the ith delta polynomial, it should have the property that when evaluated at alpha i, this polynomial should give me the value 1. And, all the remaining alpha values should serve as the root of this delta i polynomial.

So, again it has t number of roots; so, that is why its degree will be t. And, like that if I take the t + 1th Y polynomial, then it should give me the value 1 at the t + 1th evaluation point and all the remaining t evaluation point should be the root. So, that automatically implies that the degree of this t + 1th Y polynomial is also t. And, now you can see that each of these terms here is nothing but a bivariate polynomial of degree t in each variable.

Because, say for instance if I take this first term, then $f_1(X)$ has degree t and $\delta_1(Y)$ has also degree t. And, if I multiplied these 2 t-degree univariate polynomials in X and Y, that will actually result in a bivariate polynomial of degree t in each variable. So, each of these terms is actually a bivariate polynomial of degree t in both the variables.

And, that automatically implies that this F(X, Y) polynomial is also a bivariate polynomial of degree t in both the variables. Now, let us see what will be the value of this F(X, Y) polynomial whether this is the correct polynomial or not. So, if I evaluate it at say α_1, then the first term here will be $f_1(X)$ multiplied with $\delta_1(Y)$ evaluated at α_1. But, $\delta_1(Y)$ evaluated at α_1 is nothing but 1. Now, if I take the second term for this F(X, Y) it will vanish.

(Refer Slide Time: 20:44)



Lagrange's Interpolation for Bivariate Polynomials

❑ **Theorem:** Suppose that $\alpha_1, \dots, \alpha_{t+1} \in \mathbb{F}$ are distinct and $f_1(X), \cdots, f_{t+1}(X)$ are t-degree polynomials over $\mathbb{F}$. Then there exists a unique (t, t)-degree bivariate polynomial $F(x, y)$, such that $F(X, \alpha_i) = f_i(X)$, for $1 \le i \le t+1$

$Y = \alpha_i \rightarrow f_i(x)$

$(\alpha_1, f_1(x))$ ✓
$(\alpha_2, f_2(x))$ ✓
$(\alpha_{t+1}, f_{t+1}(x))$ ✓

$\Rightarrow$ unique (t,t) $F(x,Y)$

$F(x, \alpha_i) = f_i(x)$

$F(x, \alpha_1)$

❑ **Idea:** Express $F(X, Y)$ as a linear combination of $t+1$ number of (t, t)-degree bivariate polynomials

$$F'(x,Y) - F(X,Y) \overset{\text{def}}{=} \left(f_1(X) \cdot \overset{\checkmark}{\delta_1}(Y)\right) + \cdots + \overset{\delta_2(Y)}{\left(f_i(X) \cdot \delta_i(Y)\right)} + \cdots + \left(f_{t+1}(X) \cdot \delta_{t+1}(Y)\right)$$

$F(x, \alpha_1) = f_1(x) + 0 + 0 + 0 + \dots 0$

$\delta_1(\alpha_1) = 1$

$\delta_1(\alpha_2) = \cdots = \delta_1(\alpha_{t+1}) = 0$

$\delta_i(\alpha_i) = 1$

$\delta_i(\alpha_1) = \cdots = \delta_i(\alpha_{i-1}) = \delta_i(\alpha_{i+1}) = \cdots = \delta_i(\alpha_{t+1}) = 0$

$\delta_{t+1}(\alpha_{t+1}) = 1$

$\delta_{t+1}(\alpha_1) = \cdots = \delta_{t+1}(\alpha_t) = 0$

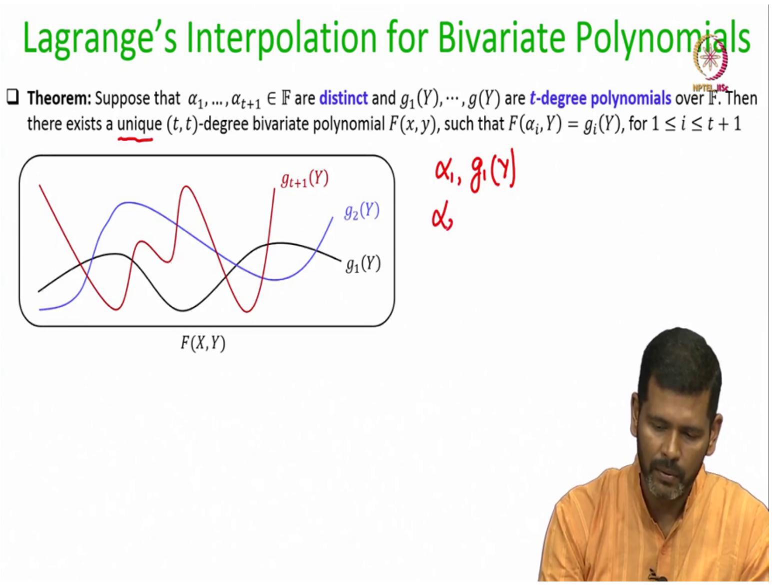
Because, in the second term there will be contribution of $\delta_2(Y)$ polynomial and $\delta_2(Y)$ evaluated at α_1 will give you the value 0. So, the second term will be 0, the third term will be 0, the fourth term will be 0. And, like that t + 1th term will be 0; that means, if I evaluate this polynomial at α_1, indeed I get $f_1(X)$ and all other terms simply give you the value 0. Like that you can verify that indeed this F(X, Y) is the correct polynomial.

Because, if I evaluate it at alpha i then it will give you the ith univariate polynomial which you are given. So, that shows that ok, this is definitely a bivariate polynomial of degree t in both the variables which satisfies the constraint that it passes through these univariate polynomials. But, the theorem statement also says that there is only one such unique bivariate polynomial in both the variables, passing through this given t + 1 univariate polynomials. We have shown definitely one such polynomial is there.

Now, to show the uniqueness part; that means, there is only one such F(X, Y) polynomial and you do not have any other polynomial F'(X, Y) which also passes through these univariate polynomials. Well, we can show the uniqueness part very easily. We can prove it by contradiction.

So, imagine that there is other polynomial as well, then it turns out that the difference of these two polynomials will be a 0 polynomial which automatically implies that F' polynomial is same as the F polynomial, that automatically implies that you have only one such unique polynomial possible. So, I am not going through the uniqueness part that is very easy to prove.

(Refer Slide Time: 22:53)



Lagrange's Interpolation for Bivariate Polynomials

❑ **Theorem:** Suppose that $\alpha_1, \ldots, \alpha_{t+1} \in \mathbb{F}$ are **distinct** and $g_1(Y), \cdots, g(Y)$ are ***t*-degree polynomials** over $\mathbb{F}$. Then there exists a unique (t, t)-degree bivariate polynomial $F(x, y)$, such that $F(\alpha_i, Y) = g_i(Y)$, for $1 \leq i \leq t+1$

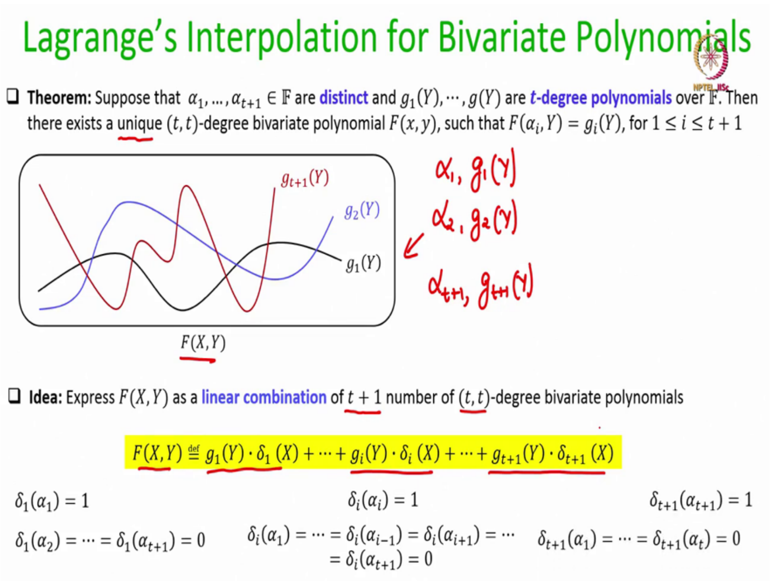
$\alpha_1, g_1(Y)$

α_2

So, now, what will be the form for these delta polynomials which have these properties? Well, we already now know what should be the form of the delta polynomials as per our requirement. So, the requirement from $\delta_i(X)$ polynomial was that α_i should not be the root and $\alpha_1, \cdots, \alpha_{i-1}, \alpha_{i+1, \cdots, \alpha_{t+1}}$ should be the roots.

That means, all the evaluation points among thes t + 1 evaluation points except the ith evaluation point should be the root. So, that is why in the numerator you will have these terms and we also want that at α_i, this $\delta_i(X)$ polynomial should give you the value 1. So, that is why in the denominator, we will have the product like this. And, since all the evaluation points are distinct; that means, the denominator is a non-zero element; that means, its inverse exists and that is why this is a valid polynomial.

(Refer Slide Time: 24:01)



Lagrange's Interpolation for Bivariate Polynomials

❑ **Theorem:** Suppose that $\alpha_1, \dots, \alpha_{t+1} \in \mathbb{F}$ are distinct and $g_1(Y), \cdots, g(Y)$ are t-degree polynomials over $\mathbb{F}$. Then there exists a unique (t, t)-degree bivariate polynomial $F(x, y)$, such that $F(\alpha_i, Y) = g_i(Y)$, for $1 \le i \le t+1$

❑ **Idea:** Express $F(X, Y)$ as a linear combination of $t+1$ number of (t, t)-degree bivariate polynomials

$$F(X,Y) \overset{\text{def}}{=} g_1(Y) \cdot \delta_1(X) + \cdots + g_i(Y) \cdot \delta_i(X) + \cdots + g_{t+1}(Y) \cdot \delta_{t+1}(X)$$

$\delta_1(\alpha_1) = 1$

$\delta_1(\alpha_2) = \cdots = \delta_1(\alpha_{t+1}) = 0$

$\delta_i(\alpha_i) = 1$

$\delta_i(\alpha_1) = \cdots = \delta_i(\alpha_{i-1}) = \delta_i(\alpha_{i+1}) = \cdots = \delta_i(\alpha_{t+1}) = 0$

$\delta_{t+1}(\alpha_{t+1}) = 1$

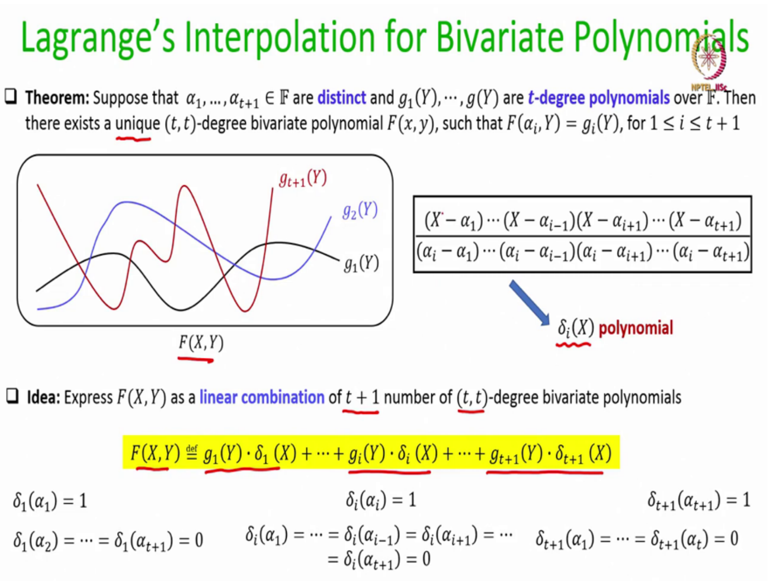
$\delta_{t+1}(\alpha_1) = \cdots = \delta_{t+1}(\alpha_t) = 0$

Now, let us see the other version of the Lagrange's interpolation for bivariate polynomials. Well, actually this is not a different statement, it is just a different way of interpreting the univariate polynomials. In the previous statement, we interpreted the given univariate polynomials as polynomials in X variable. Now, the statement is that imagine you are given t + 1 number of univariate polynomials in Y variable.

It is just a renaming of the variables, previously you were given t + 1 number of univariate polynomials in X variable. Since, its a variable I can interpret them as a polynomial in Y variable as well. Then, the statement says that I can always pass a unique bivariate polynomial of degree t in both the variables passing through these given univariate polynomials. Namely, passing through $(\alpha_1, g_1(Y)), \cdots, (\alpha_{t+1}, g_{t+1}(Y))$.

And, again the idea remains the same; we have to express that unknown polynomial as a linear combination or as a summation of several bivariate polynomials; to be more specific t + 1 number of bivariate polynomials which will have these forms. And, here if I take the ith delta polynomial in X, α_i should not be its root. So, at α_i it should give the value 1 and for all the remaining evaluation points, all the remaining evaluation points should be the root of this $g_i(Y)$ polynomial.

(Refer Slide Time: 25:58)



Lagrange's Interpolation for Bivariate Polynomials

❑ **Theorem:** Suppose that $\alpha_1, \ldots, \alpha_{t+1} \in \mathbb{F}$ are distinct and $g_1(Y), \cdots, g(Y)$ are t-degree polynomials over $\mathbb{F}$. Then there exists a unique (t,t)-degree bivariate polynomial $F(x,y)$, such that $F(\alpha_i, Y) = g_i(Y)$, for $1 \le i \le t+1$

$$\frac{(X-\alpha_1)\cdots(X-\alpha_{i-1})(X-\alpha_{i+1})\cdots(X-\alpha_{t+1})}{(\alpha_i-\alpha_1)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_{t+1})}$$

$\delta_i(X)$ polynomial

❑ **Idea:** Express $F(X,Y)$ as a linear combination of $t+1$ number of (t,t)-degree bivariate polynomials

$$F(X,Y) \overset{\text{def}}{=} g_1(Y)\cdot\delta_1(X) + \cdots + g_i(Y)\cdot\delta_i(X) + \cdots + g_{t+1}(Y)\cdot\delta_{t+1}(X)$$

$\delta_1(\alpha_1) = 1$

$\delta_1(\alpha_2) = \cdots = \delta_1(\alpha_{t+1}) = 0$

$\delta_i(\alpha_i) = 1$

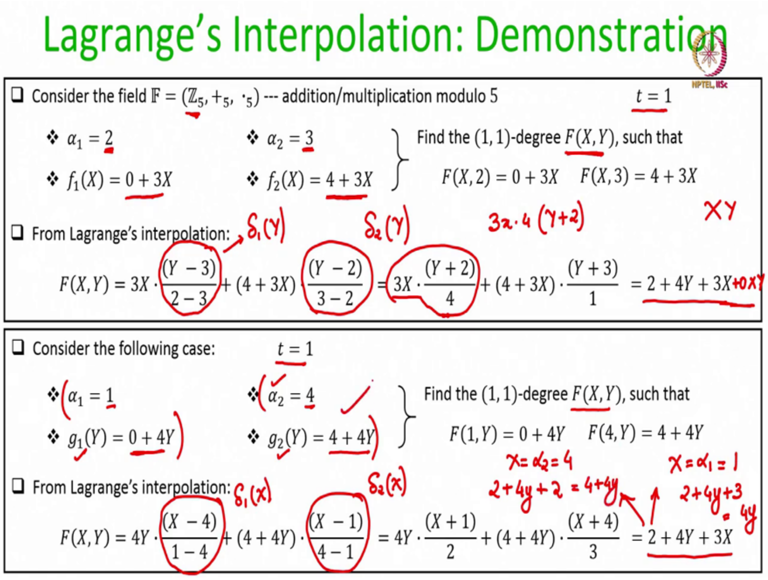
$\delta_i(\alpha_1) = \cdots = \delta_i(\alpha_{i-1}) = \delta_i(\alpha_{i+1}) = \cdots = \delta_i(\alpha_{t+1}) = 0$

$\delta_{t+1}(\alpha_{t+1}) = 1$

$\delta_{t+1}(\alpha_1) = \cdots = \delta_{t+1}(\alpha_t) = 0$

Now, what will be the form of the g i Y polynomial? Will it be the same as the form of the delta i X polynomial? It is same as the delta i X polynomial that we had seen in the previous slide except that now we have to interpret the X variable as the Y variable right.

(Refer Slide Time: 26:15)



Lagrange's Interpolation: Demonstration

❑ Consider the field $\mathbb{F} = (\mathbb{Z}_5, +_5, \cdot_5)$ --- addition/multiplication modulo 5 $t = 1$

❖ $\alpha_1 = 2$ ❖ $\alpha_2 = 3$

❖ $f_1(X) = 0 + 3X$ ❖ $f_2(X) = 4 + 3X$

Find the (1, 1)-degree $F(X,Y)$, such that $F(X,2) = 0 + 3X$ $F(X,3) = 4 + 3X$

❑ From Lagrange's interpolation: $\delta_1(Y)$ $\delta_2(Y)$ $3x \cdot 4\,(Y+2)$ XY

$$F(X,Y) = 3X\cdot\frac{(Y-3)}{2-3} + (4+3X)\cdot\frac{(Y-2)}{3-2} = 3X\cdot\frac{(Y+2)}{4} + (4+3X)\cdot\frac{(Y+3)}{1} = 2 + 4Y + 3X + 0XY$$

❑ Consider the following case: $t = 1$

❖ $\alpha_1 = 1$ ❖ $\alpha_2 = 4$

❖ $g_1(Y) = 0 + 4Y$ ❖ $g_2(Y) = 4 + 4Y$

Find the (1, 1)-degree $F(X,Y)$, such that $F(1,Y) = 0 + 4Y$ $F(4,Y) = 4 + 4Y$

❑ From Lagrange's interpolation: $\delta_1(x)$ $\delta_2(x)$

$x = \alpha_2 = 4$ $2 + 4y + 2 = 4 + 4y$ $x = \alpha_1 = 1$ $2 + 4y + 3 = 4y$

$$F(X,Y) = 4Y\cdot\frac{(X-4)}{1-4} + (4+4Y)\cdot\frac{(X-1)}{4-1} = 4Y\cdot\frac{(X+1)}{2} + (4+4Y)\cdot\frac{(X+4)}{3} = 2 + 4Y + 3X$$

So, now, let us see a demonstration for the Lagrange's interpolation. So, for the purpose of demonstration I choose this field and say t is equal to 1 ok. Now, suppose I take two evaluation points alpha 1 and alpha 2, those evaluation points are distinct non zero elements. So, I can take them to be any pair of distinct elements from the field. Suppose, I take them to

2 and 3 and suppose I am given two arbitrary univariate polynomials of degree 1, because t is equal to 1, in X variable.

Now, my goal is to find the unique bivariate polynomial of degree 1 in both the variables passing through these given univariate polynomials. Namely, that bivariate polynomial when evaluated at the first evaluation point alpha 1, should give me the first univariate polynomial. And, this bivariate polynomial when evaluated at second evaluation point alpha 2 should give me the second univariate polynomial.

So, what I will do? I will apply the Lagrange's interpolation. So, this is my $\delta_1(Y)$ polynomial and this is my $\delta_2(Y)$ polynomial. Since, I am performing all the operations over the field; now you can see in the denominator I have 2 minus 3, which is minus 1, and minus 1 over the field Z 5 is nothing but 5 minus 1 which is 4 ok. And, division by 4 is nothing but multiplying the numerator with the multiplicative inverse of 4.

So, what will be the multiplicative inverse of 4? The multiplicative inverse of 4 will be 4 because, 4 into 4 is 16, 16 modulo 5 is 1. So, basically this term is nothing but 3 X into 4 into Y plus 2 and so on. And, remember all the plus and multiplication operations are performed modulo 5. So, after solving this will be the resultant bivariate polynomials of degree 1 in both the variables.

So, you might be saying that how can it be a bivariate polynomial of degree 1 in both the variable, because we do not have a term like X times Y, namely X power 1 Y power 1. Well, we do have a term here whose with the coefficient 0 ok. In fact, we also have a term yeah so, yeah. So, this is the actual bivariate polynomial ok. Now, again let us take the same case, where we have t is equal to 1 and now suppose my evaluation points are 1 and 4.

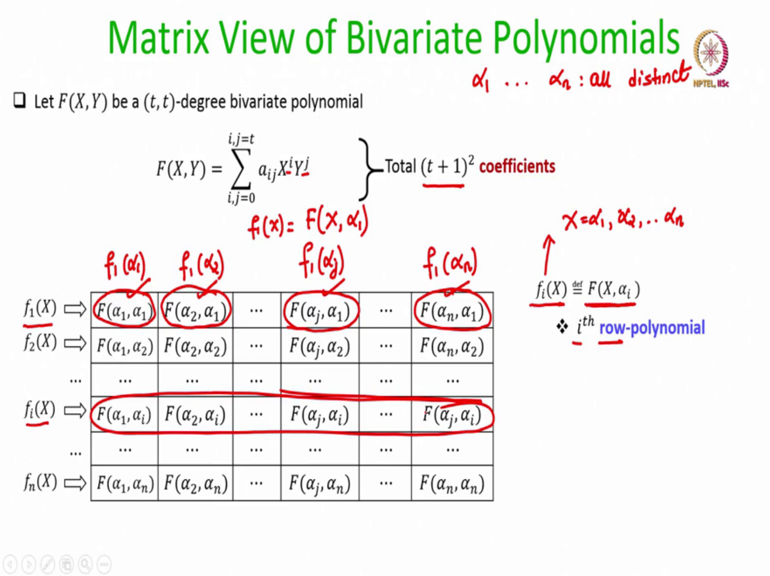
The first evaluation point is 1, the second evaluation point is 4 and you are given two arbitrary univariate polynomials in variable Y, both of degree 1. And, my goal is to find the unique bivariate polynomial of degree 1 in both the variables which when evaluated at the first evaluation point gives me the first given univariate polynomial.

And, when evaluated at the second evaluation point gives me the second univariate polynomial. Namely, I want to pass them through alpha 1 comma g 1 Y and alpha 2 g 2 Y. So, now, the Lagrange's interpolation will be this. So, this one polynomial will be your delta sub 1 X polynomial and this polynomial will be your delta sub 2 polynomial.

And, then if I solve further where all the operations are considered over the field Z 5, this will be the resultant bivariate polynomial. You can verify that, indeed if I evaluate this polynomial at X equal to alpha 1, if I evaluate it at X equal to alpha 1 and alpha 1 is 1; that means, I have to substitute X equal to 1 here.

So, it will give me 2 plus 4 Y plus 3 into 1 is 3 and 3 plus 2 is 5, 5 vanishes. So, what is left is 4 Y and 4 Y is nothing but 0 plus 4 Y. In the same way, if I evaluate this polynomial at the second evaluation point namely at X equal to alpha 2 and alpha 2 is equal to 4 in this case. That means, if I substitute the value of X equal to 4 here, then I will get 2 plus 4 Y plus 3 times 4 which is 12, 12 modulo 5 is 2. So, 2 plus 2 is 4, 4 plus 4 Y that is the requirement ok.

(Refer Slide Time: 31:49)



Matrix View of Bivariate Polynomials

$\alpha_1 \ldots \alpha_n$: all distinct

❑ Let $F(X,Y)$ be a (t,t)-degree bivariate polynomial

$$F(X,Y) = \sum_{i,j=0}^{i,j=t} a_{ij} X^i Y^j \quad \Big\} \text{Total } (t+1)^2 \text{ coefficients}$$

$f_1(x) = F(x, \alpha_1)$

$$\begin{array}{c|cccccc}
 & f_1(\alpha_1) & f_1(\alpha_2) & & f_1(\alpha_j) & & f_1(\alpha_n) \\
\hline
f_1(X) \Rightarrow & F(\alpha_1,\alpha_1) & F(\alpha_2,\alpha_1) & \cdots & F(\alpha_j,\alpha_1) & \cdots & F(\alpha_n,\alpha_1) \\
f_2(X) \Rightarrow & F(\alpha_1,\alpha_2) & F(\alpha_2,\alpha_2) & \cdots & F(\alpha_j,\alpha_2) & \cdots & F(\alpha_n,\alpha_2) \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
f_i(X) \Rightarrow & F(\alpha_1,\alpha_i) & F(\alpha_2,\alpha_i) & \cdots & F(\alpha_j,\alpha_i) & \cdots & F(\alpha_j,\alpha_i) \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
f_n(X) \Rightarrow & F(\alpha_1,\alpha_n) & F(\alpha_2,\alpha_n) & \cdots & F(\alpha_j,\alpha_n) & \cdots & F(\alpha_n,\alpha_n)
\end{array}$$

$X = \alpha_1, \alpha_2, \ldots \alpha_n$

$f_i(X) \overset{\text{def}}{=} F(X, \alpha_i)$

❖ i^{th} row-polynomial

Now, let us also consider another property of bivariate polynomials here. Namely, the matrix view of the bivariate polynomials which will later be useful when we will discuss the VSS schemes. So, imagine you are given a bivariate polynomial of degree t in both the variables. So, how many coefficients are there in this formula? There are total t plus 1 square coefficients ok; because, your i ranges from 0 to t and j ranges from 0 to t. Now, imagine you are given n distinct evaluation points alpha 1 to alpha n all distinct.

So, if I evaluate this bivariate polynomial by changing X from alpha 1 to alpha n and Y from alpha 1 to alpha n, basically I get a matrix of n cross n values. And, why I am calling it as a matrix, because if I focus on the value in the ith row here, then it has a special property.

It has a special property in the sense that, the values here among these n square values, if I focus on the values in the ith row then they basically lie on a univariate polynomial in X variable, namely the polynomial F(X, alpha i), which I denote by fi(X) polynomial.

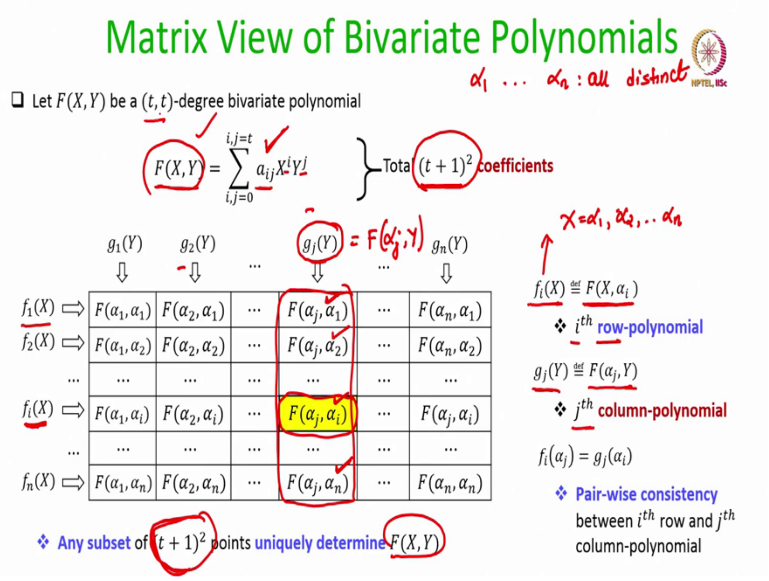
I will often call it as the ith row polynomial because, when I evaluate this polynomial fi(X) at X equal to alpha 1, alpha 2, alpha n, I get the values along the ith row in this matrix. Well, this is not a matrix in true sense, but we can imagine it as a matrix with n rows and n columns. And, what I am claiming here is that if I focus on the values along the ith row, then all of them lie on the univariate polynomial F(X, alpha i) which I denote as f sub i X.

So, for instance all these values F(alpha 1, alpha 1), F(alpha 2, alpha 1), F(alpha j, alpha 1), F(alpha n, alpha 1), all of them lie on f1(X).

Because, f 1 of X as per my definition is nothing but the bivariate polynomial evaluated at Y equal to alpha 1. And, remember as soon as I substitute the value of Y, then the bivariate polynomial collapses or reduces to a univariate polynomial of degree t in the X variable.

So, I am calling the univariate polynomial which I obtain by substituting Y equal to alpha i as the ith row polynomial. The term row signifies here that if I further evaluate that polynomial at X equal to alpha 1, alpha 2, alpha n, then basically I will obtain the values which are there along the ith row of this matrix.

(Refer Slide Time: 35:55)



Matrix View of Bivariate Polynomials

$\alpha_1 \ldots \alpha_n$: all distinct

❑ Let $F(X,Y)$ be a (t,t)-degree bivariate polynomial

$$F(X,Y) = \sum_{i,j=0}^{i,j=t} a_{ij} X^i Y^j \quad \Big\} \text{Total } (t+1)^2 \text{ coefficients}$$

$$g_j(Y) = F(\alpha_j, Y)$$

$$\begin{array}{c|cccccc}
 & g_1(Y) \Downarrow & g_2(Y) \Downarrow & \cdots & g_j(Y) \Downarrow & \cdots & g_n(Y) \Downarrow \\
\hline
f_1(X) \Rightarrow & F(\alpha_1,\alpha_1) & F(\alpha_2,\alpha_1) & \cdots & F(\alpha_j,\alpha_1) & \cdots & F(\alpha_n,\alpha_1) \\
f_2(X) \Rightarrow & F(\alpha_1,\alpha_2) & F(\alpha_2,\alpha_2) & \cdots & F(\alpha_j,\alpha_2) & \cdots & F(\alpha_n,\alpha_2) \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
f_i(X) \Rightarrow & F(\alpha_1,\alpha_i) & F(\alpha_2,\alpha_i) & \cdots & F(\alpha_j,\alpha_i) & \cdots & F(\alpha_j,\alpha_i) \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
f_n(X) \Rightarrow & F(\alpha_1,\alpha_n) & F(\alpha_2,\alpha_n) & \cdots & F(\alpha_j,\alpha_n) & \cdots & F(\alpha_n,\alpha_n)
\end{array}$$

$X = \alpha_1, \alpha_2, \ldots \alpha_n$

$f_i(X) \overset{\text{def}}{=} F(X, \alpha_i)$

❖ i^{th} row-polynomial

$g_j(Y) \overset{\text{def}}{=} F(\alpha_j, Y)$

❖ j^{th} column-polynomial

$f_i(\alpha_j) = g_j(\alpha_i)$

❖ Pair-wise consistency between i^{th} row and j^{th} column-polynomial

❖ Any subset of $(t+1)^2$ points uniquely determine $F(X,Y)$

And, in the same way what I can do is, I can have a column view as well; that means, if I now consider the jth column here, the jth column of the matrix; then those values also lie on some t degree polynomial. They basically lie on the univariate polynomial evaluated at X equal to alpha j. So, it will be a univariate polynomial of degree t in the Y variable, I call it as the jth column polynomial and represented by $g_j(Y)$ ok.

So, if this $g_j(Y)$ polynomial which is F(alpha j, Y), then when I further evaluate that polynomial at Y equal to alpha 1, I will get the first value along the jth column. If I evaluate at Y equal to alpha 2, then I get the second value along the jth column. If I evaluate at Y equal to alpha i, I obtain the ith value along the jth column. And, I evaluate it at Y equal to n then I obtain the nth value along the jth column ok.

So, this will be an important way of viewing the points on the bivariate polynomials. Now, it turns out that any subset of $(t + 1)^2$ points in this matrix uniquely determine the bivariate polynomial. It something similar to what we have for the univariate polynomials.

For the univariate polynomials, we know that if I give you t + 1 points on that univariate polynomial, then you can always find it out uniquely. You can always apply the Lagrange's interpolation formula and uniquely find it out or you can solve a system of linear equations.

Because, that unknown univariate polynomial will have t + 1 coefficients and the t + 1 points basically gives you t + 1 equations in t + 1 variables using which you can solve. In the same way, how many coefficients are there in this bivariate polynomial? We have $(t + 1)^2$ coefficients.

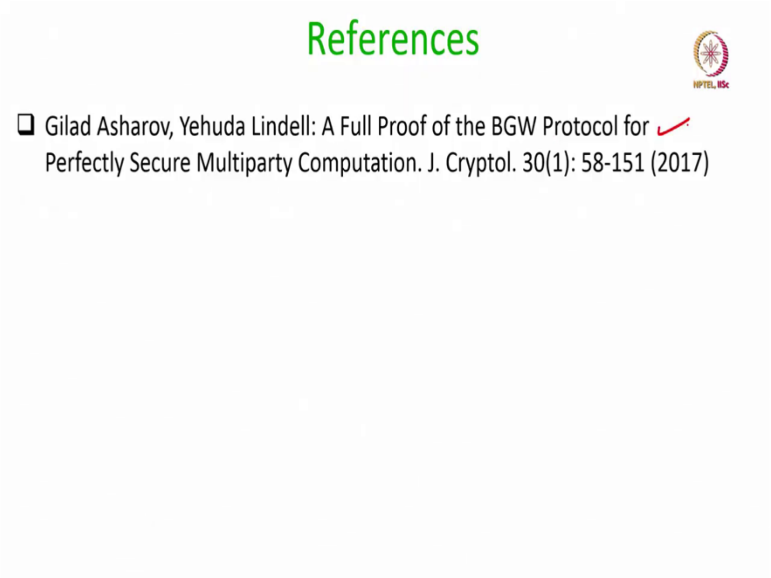
So, now, if I do not tell you the bivariate polynomial; that means, I do not tell you the value of the $(t + 1)^2$ coefficients, but instead I give you $(t + 1)^2$ points from this matrix. Any $(t + 1)^2$, they need not be the consecutive values, they need not lie on the same row, column etcetera.

They are just arbitrary subset of $(t + 1)^2$ distinct points from this matrix. The claim is that those points are sufficient to uniquely determine the bivariate polynomial, because using these $(t + 1)^2$ distinct points, you can form $(t + 1)^2$ equations in the $(t + 1)^2$ unknown coefficients which you have. And, then by solving a system of linear equations over the finite field, you can find out the value of each of these coefficients and hence the bivariate polynomial.

Another property which will be later useful in the context of verifiable secret sharing is this pair wise consistency property. You can see here that there is this highlighted value; it is a common value which appears both on the ith row polynomial as well as on the jth column polynomial.

That means, if I evaluate the ith row polynomial at X equal to alpha j, then I will get this highlighted value. And, at the same time if I take the jth column polynomial and evaluate it at alpha i, then also I will obtain this highlighted value ok. So, this is a property which holds for any bivariate polynomial of degree t in both the variables ok.

(Refer Slide Time: 39:58)



References

❑ Gilad Asharov, Yehuda Lindell: A Full Proof of the BGW Protocol for Perfectly Secure Multiparty Computation. J. Cryptol. 30(1): 58-151 (2017)

So, with that I end this lecture. So, there are some nice references from where you can find out the properties of bivariate polynomials. In fact, there are several other properties for bivariate polynomials, but we do not require all of them; in the context of VSS whatever we require, we have discussed some of them. And, in the follow up lecture, we will discuss more of those properties. So, all the properties which I have discussed in today's lecture, you can find in this paper ok.

Thank you.