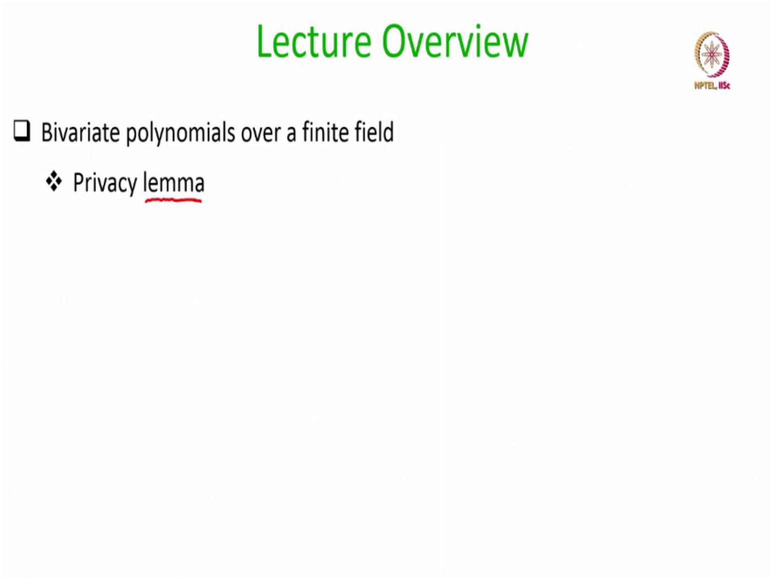
Secure Computation: Part II
Prof. Ashish Choudhury
Department of Computer Science and Engineering
Indian Institute of Information Technology, Bangalore

Lecture - 35
Bivariate Polynomials Over Finite Fields: II

Hello everyone, welcome to this lecture. So, in this lecture we will continue our discussion regarding Bivariate Polynomials Over Finite Fields.

(Refer Slide Time: 00:32)

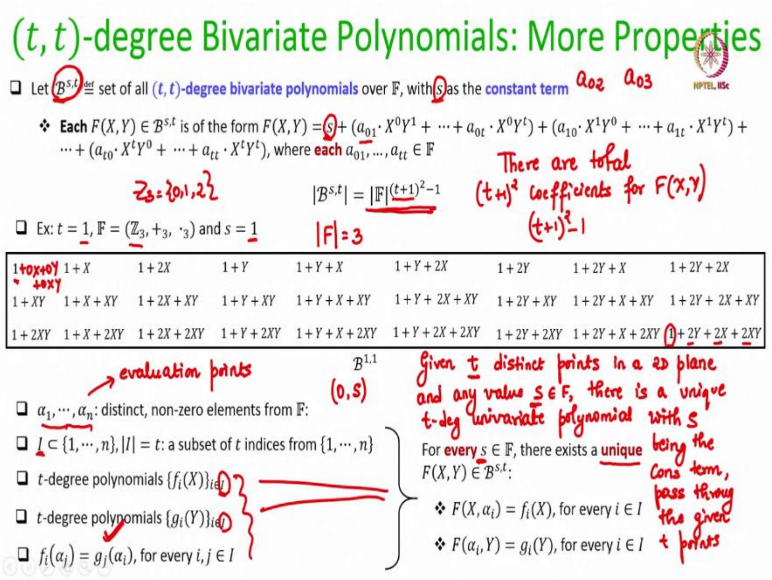


Lecture Overview

- ❑ Bivariate polynomials over a finite field
    - ❖ Privacy lemma

Namely, we will prove a lemma which I call as the privacy lemma which will be later useful when we will design verifiable secret sharing schemes based on bivariate polynomials.

(Refer Slide Time: 00:42)



(t, t)-degree Bivariate Polynomials: More Properties

NPTEL, IISc

- ❑ Let $\mathcal{B}^{s,t} \overset{\text{def}}{=}$ set of all (t, t)-degree bivariate polynomials over $\mathbb{F}$, with s as the constant term a_{02} a_{03}
  - ❖ Each $F(X, Y) \in \mathcal{B}^{s,t}$ is of the form $F(X, Y) = s + (a_{01} \cdot X^0Y^1 + \cdots + a_{0t} \cdot X^0Y^t) + (a_{10} \cdot X^1Y^0 + \cdots + a_{1t} \cdot X^1Y^t) + \cdots + (a_{t0} \cdot X^tY^0 + \cdots + a_{tt} \cdot X^tY^t)$, where each $a_{01}, \ldots, a_{tt} \in \mathbb{F}$

$\mathbb{Z}_3 = \{0, 1, 2\}$

$$|\mathcal{B}^{s,t}| = |\mathbb{F}|^{(t+1)^2 - 1}$$

There are total $(t+1)^2$ coefficients for $F(x, y)$

$(t+1)^2 - 1$

- ❑ Ex: $t = 1$, $\mathbb{F} = (\mathbb{Z}_3, +_3, \cdot_3)$ and $s = 1$

$|F| = 3$

$1 + 0X + 0Y + 0XY$	$1 + X$	$1 + 2X$	$1 + Y$	$1 + Y + X$	$1 + Y + 2X$	$1 + 2Y$	$1 + 2Y + X$	$1 + 2Y + 2X$
$1 + XY$	$1 + X + XY$	$1 + 2X + XY$	$1 + Y + XY$	$1 + Y + X + XY$	$1 + Y + 2X + XY$	$1 + 2Y + XY$	$1 + 2Y + X + XY$	$1 + 2Y + 2X + XY$
$1 + 2XY$	$1 + X + 2XY$	$1 + 2X + 2XY$	$1 + Y + 2XY$	$1 + Y + X + 2XY$	$1 + Y + 2X + 2XY$	$1 + 2Y + 2XY$	$1 + 2Y + X + 2XY$	$1 + 2Y + 2X + 2XY$

$\mathcal{B}^{1,1}$

evaluation points

$(0, s)$

Given t distinct points in a 2D plane and any value $s \in F$, there is a unique t-deg univariate polynomial with s being the cons term, pass throug the given t points

- ❑ $\alpha_1, \cdots, \alpha_n$: distinct, non-zero elements from $\mathbb{F}$:
- ❑ $I \subset \{1, \cdots, n\}, |I| = t$: a subset of t indices from $\{1, \cdots, n\}$
- ❑ t-degree polynomials $\{f_i(X)\}_{i \in I}$
- ❑ t-degree polynomials $\{g_i(Y)\}_{i \in I}$
- ❑ $f_i(\alpha_j) = g_j(\alpha_i)$, for every $i, j \in I$

For every $s \in \mathbb{F}$, there exists a unique $F(X, Y) \in \mathcal{B}^{s,t}$:

- ❖ $F(X, \alpha_i) = f_i(X)$, for every $i \in I$
- ❖ $F(\alpha_i, Y) = g_i(Y)$, for every $i \in I$

So, imagine you are given a field and I take a value s. I want to find out all bivariate polynomials of degree t in variable X and Y where there is no restriction on the coefficients except that the constant term should be this value s.

So, I am fixing the value s it should be the constant term of the bivariate polynomial remaining all other terms could be remaining all other coefficients could be any element from the field. So, there will be several such polynomials in fact, each polynomial will have the following form there is no restriction on the coefficient of $X^0Y^1, \ldots, X^0Y^t, \ldots., X^tY^t$ and so, on.

The only restriction is that the coefficient of X^0Y^0 is set to be s. So, all such polynomials will be constituting a set I denote that set as this set $\mathcal{B}$ and in the superscript we have s, t. So, this set will denote a set of all bivariate polynomials and from now onwards I will not be saying that the degree is t in both the variables or degree t in X and degrees t in y.

I will just say that the degrees of both X and Y variable is t. So, the set of all bivariate polynomials of degree t with constant coefficient being s will be denoted by this set and how many polynomials will be belonging to this set? Well, there will be these many polynomials the $|\mathbb{F}|^{(t+1)^2-1}$ this is because there is a total of $(t + 1)^2$ coefficients.

For $F(X, Y)$ if I do not put any restriction on any of these coefficients, then for the first coefficient I can choose any element from the field as the first coefficient second coefficient again I can choose any element from the field and like that, but the constant coefficient here is fixed to be s apart from that for each of the coefficients here I have field size number of options. I can take any element from the field to be the coefficient a_{01}

And independent of that I can take any element from the field as the coefficient a_{02} and independent of that I can take any element from the field as the coefficient a_{03}. So, except the constant coefficient all other coefficients have field size number of options and if I ignore the constant coefficient, then I am left with these many number of coefficients namely $(t+1)^2-1$.

And for each of those coefficients I have field size number of options that is why the total number of polynomials in this set namely the number of bivariate polynomials with s being the constant term and degree being t in both the variables will be this.

So, let me demonstrate this with an example suppose I take t is equal to 1, my field is $\mathbb{Z}_3$, $\mathbb{Z}_3$ means it will have the elements 0 1 and 2 all the operations are addition modulo 3 and multiplication modulo 3 and suppose I fixed the constant to 1, then there will be how many bivariate polynomials? Well, the field size here is 3.

So, I will have 27 possible bivariate polynomials of degree 1 in both the X and Y variable and where the constant coefficient constant term is 1 those polynomials are listed down here. So, you can see here this is a bivariate polynomial where all the coefficients are 0 here $0 \cdot X + 0 \cdot Y + 0 \cdot XY$. Whereas this polynomial also has the constant term 1 where the coefficient of X^0Y^1 is 2, the coefficient of X^1Y^0 is 2 and the coefficient of X^1Y^1 is 2.

Now imagine that I choose n distinct nonzero evaluation points from the field I call them as evaluation points why I call them evaluation points? It will be clear very soon and among these n evaluation points I focus on a subset of t evaluation points. So, they can be any t evaluation points the exact indices corresponding to those t evaluation points which I am denoting by the set I, and now suppose I give you t number of univariate polynomials in X variable and t number of univariate polynomials in Y variable corresponding to the indices in this index set I.

And those X and Y polynomials have the property that they are pairwise consistent. They are pairwise consistent in the sense that if I evaluate the ith X polynomial and evaluate it at $X = \alpha_j$ then that value will be same as the jth Y polynomial evaluated at $Y = \alpha_i$. If this condition is if these three conditions are satisfied namely you are given t number of X univariate polynomials t number of Y univariate polynomials the only condition is that they should correspond to the same indices within the index set I.

And they should be pairwise consistent then for every element for every value from the field I can find a unique bivariate polynomial of degree t with s being the constant term which passes through this given X univariate polynomials and Y univariate polynomials. So, it might look very confusing on the first look, but let me try to explain it in a simpler term.

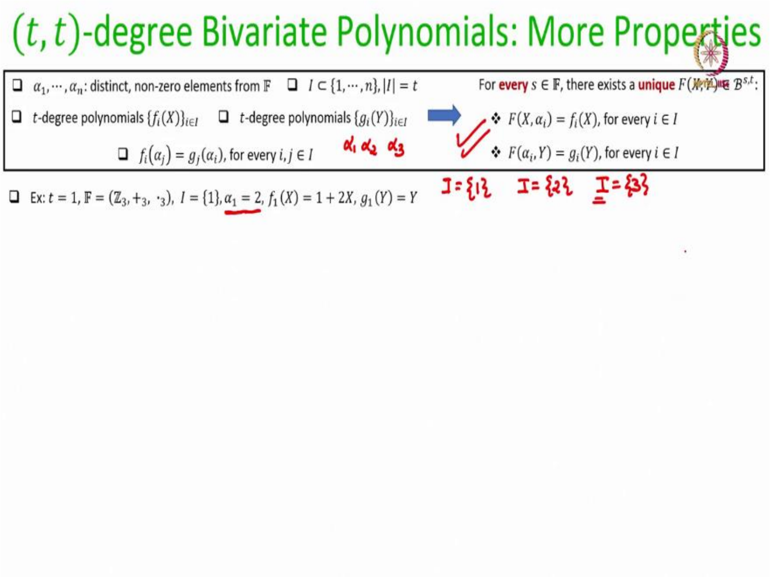
We know that for the univariate world we have seen the following property. Given t distinct points given t distinct points in a 2 D plane over where the points are over the field and any value s from the field there is a unique t degree univariate polynomial, there is a unique t degree univariate polynomial with s being the constant term passing through the given t points that is well known we have proved that in the context of univariate polynomials.

I give you t points in the two dimensional plane and any value s then I can always find a unique t degree univariate polynomial whose constant term will be s and which passes through those given t distinct points because when I say that its constant term will be s namely, I am fixing the point $(0, s)$ on the curve and anyhow they have to pass through the remaining t given points.

So, together they constitute $t + 1$ distinct points and through $t + 1$ distinct points I can find a unique univariate polynomial. Now I am just trying to extend that concept that property in the context of bivariate polynomial. So, I am fixing a value s that has to be the constant term of the bivariate polynomial which I want to find out and I am asking that I am also fixing t pairs of X univariate polynomials and Y univariate polynomials which are pairwise consistent.

So, I am now given two criteria. The constant term of the bivariate polynomial should be the given value s and they should pass through the t number of X univariate polynomials and t number of Y univariate polynomials which are pairwise consistent. The claim is you can find only one such univariate only one such bivariate polynomial you cannot find multiple bivariate polynomials.

(Refer Slide Time: 11:46)



(t, t)-degree Bivariate Polynomials: More Properties

□ $\alpha_1, \cdots, \alpha_n$: distinct, non-zero elements from $\mathbb{F}$ □ $I \subset \{1, \cdots, n\}, |I| = t$

□ t-degree polynomials $\{f_i(X)\}_{i \in I}$ □ t-degree polynomials $\{g_i(Y)\}_{i \in I}$

□ $f_i(\alpha_j) = g_j(\alpha_i)$, for every $i, j \in I$ α_1 α_2 α_3

For **every** $s \in \mathbb{F}$, there exists a **unique** $F(X, Y) \in \mathcal{B}^{s,t}$:

✓

❖ $F(X, \alpha_i) = f_i(X)$, for every $i \in I$

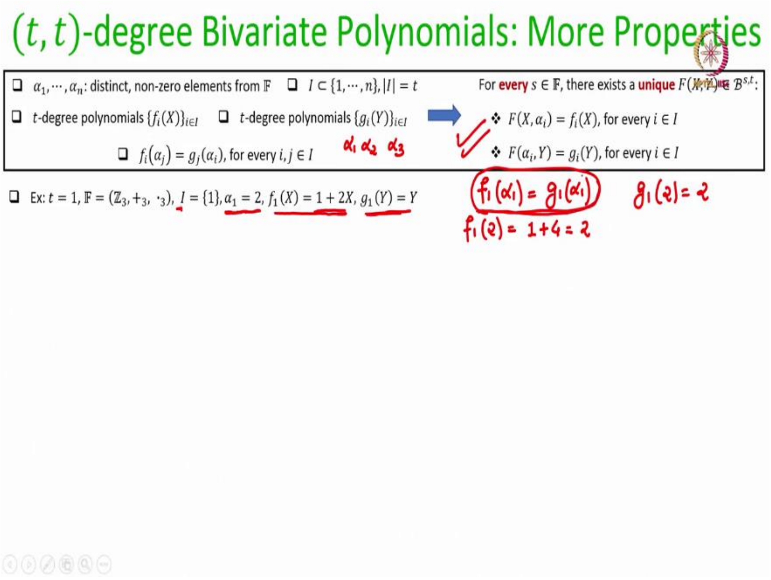
❖ $F(\alpha_i, Y) = g_i(Y)$, for every $i \in I$

□ Ex: $t = 1$, $\mathbb{F} = (\mathbb{Z}_3, +_3, \cdot_3)$, $I = \{1\}$, $\underline{\alpha_1 = 2}$, $f_1(X) = 1 + 2X$, $g_1(Y) = Y$ $I = \{1\}$ $I = \{2\}$ $\underline{I} = \{3\}$

So, let me first demonstrate this property and then we will prove it formally. So, this is what we want to claim to understand a statement again let us take the field $\mathbb{Z}_3$ and suppose I fix the index set to be 1 and evaluation point corresponding to that index set is 2; that means, there would have been multiple evaluation points $\alpha_1, \alpha_2, \alpha_3$ well since this field has only 3 elements I can choose 3 distinct evaluation points.

Then my I could be either the first evaluation point or my I could be the second evaluation point or the third evaluation point because the set I corresponds to t evaluation points and t is equal to 1 here. So, I am taking the case where I is equal to 1; that means, I am focusing on the first evaluation point and suppose my first evaluation point is 2, I am given here one X polynomial and one Y polynomial.

(Refer Slide Time: 13:12)



(t,t)-degree Bivariate Polynomials: More Properties

- □ $\alpha_1, \cdots, \alpha_n$: distinct, non-zero elements from $\mathbb{F}$ □ $I \subset \{1, \cdots, n\}, |I| = t$
- □ t-degree polynomials $\{f_i(X)\}_{i \in I}$ □ t-degree polynomials $\{g_i(Y)\}_{i \in I}$
- □ $f_i(\alpha_j) = g_j(\alpha_i)$, for every $i, j \in I$

α_1 α_2 α_3

For **every** $s \in \mathbb{F}$, there exists a **unique** $F(X,Y) \in \mathcal{B}^{s,t}$:

- ❖ $F(X, \alpha_i) = f_i(X)$, for every $i \in I$
- ❖ $F(\alpha_i, Y) = g_i(Y)$, for every $i \in I$

□ Ex: $t = 1, \mathbb{F} = (\mathbb{Z}_3, +_3, \cdot_3)$, $I = \{1\}$, $\underline{\alpha_1 = 2}$, $\underline{f_1(X) = 1 + 2X}$, $\underline{g_1(Y) = Y}$

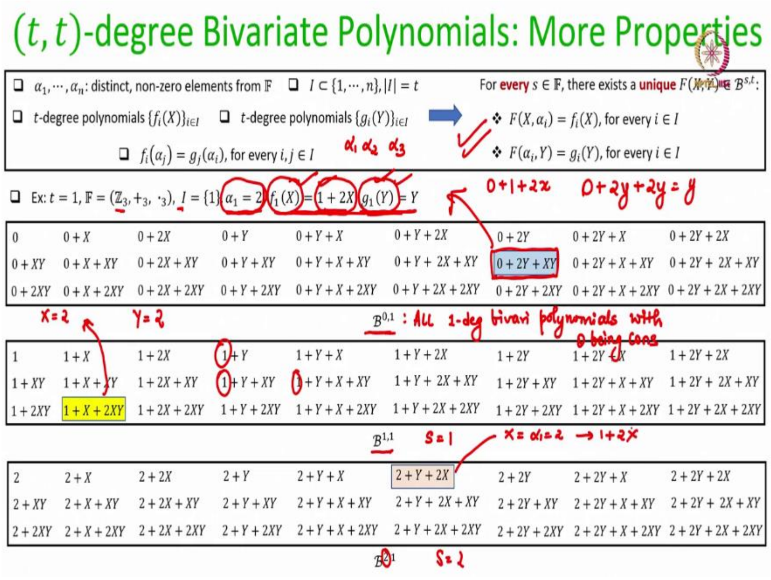
$\boxed{f_1(\alpha_1) = g_1(\alpha_1)}$ $g_1(2) = 2$

$f_1(2) = 1 + 4 = 2$

And you can see that this X polynomial and this Y polynomial they are pairwise consistent namely f 1 evaluated at α_1 is same as g 1 evaluated at α_1. So, what will be f_1 evaluated at α_1? α_1 is 2. So, f_1 evaluated at 2 will be $(1 + 2 \cdot 2 + 1)$ modulo 3 is 2 and what will be g_1 evaluated at α_1? g 1 evaluated at α_1 will be g_1 evaluated at 2 which will be 2.

So, the pairwise consistency is guaranteed here, and we do not have more indices in this index set alpha. So, we just want to have this condition being satisfied which is holding here. So, now, what I will show is, you take any value from this field $\mathbb{Z}_3$ corresponding to that value there will be 1 and 1 only one bivariate polynomial of degree 1 whose constant term will be the value which you want to fix. And that bivariate polynomial when evaluated at this evaluation point α_1 being 2 will give you these two univariate polynomials.

(Refer Slide Time: 14:29)



(t, t)-degree Bivariate Polynomials: More Properties

□ $\alpha_1, \cdots, \alpha_n$: distinct, non-zero elements from $\mathbb{F}$ □ $I \subset \{1, \cdots, n\}, |I| = t$

□ t-degree polynomials $\{f_i(X)\}_{i \in I}$ □ t-degree polynomials $\{g_i(Y)\}_{i \in I}$

□ $f_i(\alpha_j) = g_j(\alpha_i)$, for every $i, j \in I$

For **every** $s \in \mathbb{F}$, there exists a **unique** $F(X, Y) \in \mathcal{B}^{s,t}$:

❖ $F(X, \alpha_i) = f_i(X)$, for every $i \in I$

❖ $F(\alpha_i, Y) = g_i(Y)$, for every $i \in I$

α_1 α_2 α_3

□ Ex: $t = 1$, $\mathbb{F} = (\mathbb{Z}_3, +_3, \cdot_3)$, $I = \{1\}$, $\alpha_1 = 2$, $f_1(X) = 1 + 2X$, $g_1(Y) = Y$

$0+1+2x$ $0+2y+2y=y$

0	$0+X$	$0+2X$	$0+Y$	$0+Y+X$	$0+Y+2X$	$0+2Y$	$0+2Y+X$	$0+2Y+2X$
$0+XY$	$0+X+XY$	$0+2X+XY$	$0+Y+XY$	$0+Y+X+XY$	$0+Y+2X+XY$	$0+2Y+XY$	$0+2Y+X+XY$	$0+2Y+2X+XY$
$0+2XY$	$0+X+2XY$	$0+2X+2XY$	$0+Y+2XY$	$0+Y+X+2XY$	$0+Y+2X+2XY$	$0+2Y+2XY$	$0+2Y+X+2XY$	$0+2Y+2X+2XY$

$X=2$ $Y=2$

$\mathcal{B}^{0,1}$: All 1-deg bivari polynomials with 0 being cons

1	$1+X$	$1+2X$	$1+Y$	$1+Y+X$	$1+Y+2X$	$1+2Y$	$1+2Y+X$	$1+2Y+2X$
$1+XY$	$1+X+XY$	$1+2X+XY$	$1+Y+XY$	$1+Y+X+XY$	$1+Y+2X+XY$	$1+2Y+XY$	$1+2Y+X+XY$	$1+2Y+2X+XY$
$1+2XY$	$1+X+2XY$	$1+2X+2XY$	$1+Y+2XY$	$1+Y+X+2XY$	$1+Y+2X+2XY$	$1+2Y+2XY$	$1+2Y+X+2XY$	$1+2Y+2X+2XY$

$\mathcal{B}^{1,1}$ $s=1$ $X=\alpha_1=2 \rightarrow 1+2X$

2	$2+X$	$2+2X$	$2+Y$	$2+Y+X$	$2+Y+2X$	$2+2Y$	$2+2Y+X$	$2+2Y+2X$
$2+XY$	$2+X+XY$	$2+2X+XY$	$2+Y+XY$	$2+Y+X+XY$	$2+Y+2X+XY$	$2+2Y+XY$	$2+2Y+X+XY$	$2+2Y+2X+XY$
$2+2XY$	$2+X+2XY$	$2+2X+2XY$	$2+Y+2XY$	$2+Y+X+2XY$	$2+Y+2X+2XY$	$2+2Y+2XY$	$2+2Y+X+2XY$	$2+2Y+2X+2XY$

$\mathcal{B}^{2,1}$ $s=2$

So, there are several ways. So, this is the set of all 1-degree bivariate polynomial all 1-degree bivariate polynomials with 0 being the constant. In the same way this is the set of all bivariate polynomials of degree 1 with 1 being the constant term.

And this is the set of all bivariate polynomials of degree 1 with 2 being the constant term. Now you have fixed your evaluation point $(\alpha_1, 2)$ and you are fixing these two univariate polynomials which are pairwise consistent. Now among all the bivariate polynomials whose constant term is 0, there is 1 and only one bivariate polynomial namely this highlighted bivariate polynomial which when evaluated at $X = \alpha_1$ and which when evaluated at Y equal to alpha 1 would have produced these two univariate polynomials. You can verify that.

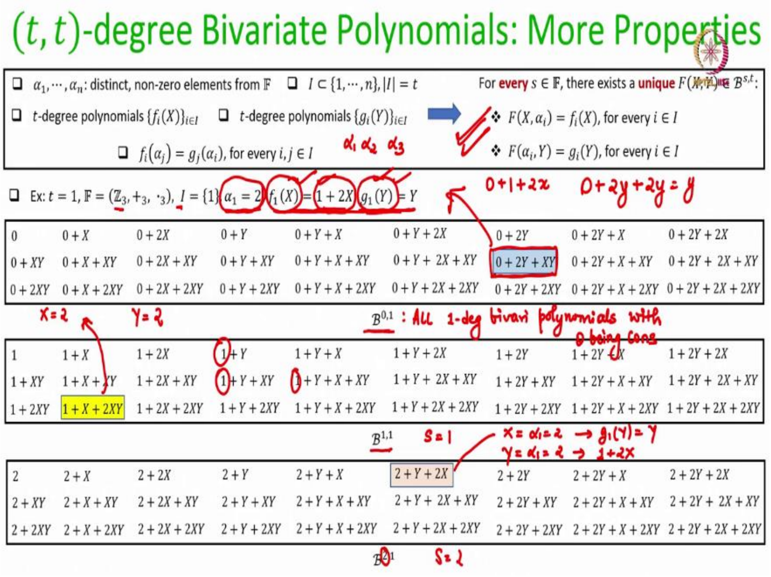
So, $0 + 2Y + XY$ when I evaluate it at $X = \alpha_1$ and α_1 is 2 here. So, let us substitute $X = 2$. So, it will become $0 + 2Y + 2Y = 0 + 4Y$ which in the field $\mathbb{Z}_3$ turns out to be y only because 4 becomes 4 modulo 3. So, indeed this polynomial evaluated at $X = \alpha_1$ gives you this Y univariate polynomial.

And now let us evaluate this bivariate polynomial at $Y = \alpha_1$ namely Y equal to 2. So, at Y equal to 2 it will be $0 + 2 \cdot 2 + 2X = 2X + 1$. Now, let us fix s being 1. Now there are several bivariate polynomials of degree 1 whose constant term is 1. In fact, here you have 27 such polynomials.

Now, among those 27 polynomials it is only this highlighted polynomial which when evaluated at $X = 2$ and when evaluated at $Y = 2$ would have produced this $f_1(X)$ polynomial and $g_1(Y)$ polynomial and in the same way let us set s equal to 2. There are 27 possible bivariate polynomials whose constant term is 2 and where the degree of X and Y is 1.

Among all those 27 polynomials there is only one bivariate polynomial which

(Refer Slide Time: 18:10)



(t, t)-degree Bivariate Polynomials: More Properties

□ $\alpha_1, \cdots, \alpha_n$: distinct, non-zero elements from $\mathbb{F}$ □ $I \subset \{1, \cdots, n\}, |I| = t$

□ t-degree polynomials $\{f_i(X)\}_{i \in I}$ □ t-degree polynomials $\{g_i(Y)\}_{i \in I}$

□ $f_i(\alpha_j) = g_j(\alpha_i)$, for every $i, j \in I$

α_1 α_2 α_3

For **every** $s \in \mathbb{F}$, there exists a **unique** $F(X, Y) \in \mathcal{B}^{s,t}$:

❖ $F(X, \alpha_i) = f_i(X)$, for every $i \in I$

❖ $F(\alpha_i, Y) = g_i(Y)$, for every $i \in I$

□ Ex: $t = 1$, $\mathbb{F} = (\mathbb{Z}_3, +_3, \cdot_3)$, $I = \{1\}$ $\alpha_1 = 2$ $f_1(X) = 1 + 2X$ $g_1(Y) = Y$

$0+1+2x$ $0+2y+2y=y$

0	$0+X$	$0+2X$	$0+Y$	$0+Y+X$	$0+Y+2X$	$0+2Y$	$0+2Y+X$	$0+2Y+2X$
$0+XY$	$0+X+XY$	$0+2X+XY$	$0+Y+XY$	$0+Y+X+XY$	$0+Y+2X+XY$	$0+2Y+XY$	$0+2Y+X+XY$	$0+2Y+2X+XY$
$0+2XY$	$0+X+2XY$	$0+2X+2XY$	$0+Y+2XY$	$0+Y+X+2XY$	$0+Y+2X+2XY$	$0+2Y+2XY$	$0+2Y+X+2XY$	$0+2Y+2X+2XY$

$X=2$ $Y=2$

$\mathcal{B}^{0,1}$: All 1-deg bivari polynomials with 0 being cons

1	$1+X$	$1+2X$	$1+Y$	$1+Y+X$	$1+Y+2X$	$1+2Y$	$1+2Y+X$	$1+2Y+2X$
$1+XY$	$1+X+XY$	$1+2X+XY$	$1+Y+XY$	$1+Y+X+XY$	$1+Y+2X+XY$	$1+2Y+XY$	$1+2Y+X+XY$	$1+2Y+2X+XY$
$1+2XY$	$1+X+2XY$	$1+2X+2XY$	$1+Y+2XY$	$1+Y+X+2XY$	$1+Y+2X+2XY$	$1+2Y+2XY$	$1+2Y+X+2XY$	$1+2Y+2X+2XY$

$\mathcal{B}^{1,1}$ $s=1$

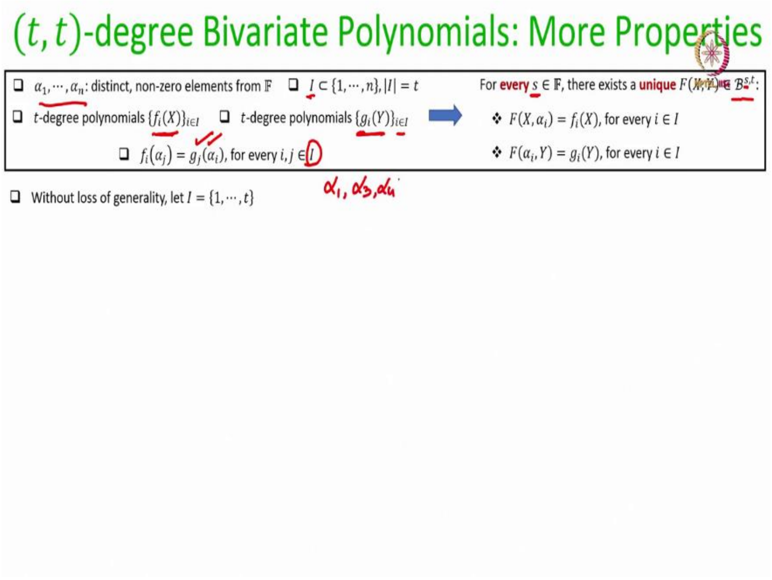
$X=\alpha_1=2 \rightarrow g_1(Y)=Y$
$Y=\alpha_1=2 \rightarrow 1+2X$

2	$2+X$	$2+2X$	$2+Y$	$2+Y+X$	$2+Y+2X$	$2+2Y$	$2+2Y+X$	$2+2Y+2X$
$2+XY$	$2+X+XY$	$2+2X+XY$	$2+Y+XY$	$2+Y+X+XY$	$2+Y+2X+XY$	$2+2Y+XY$	$2+2Y+X+XY$	$2+2Y+2X+XY$
$2+2XY$	$2+X+2XY$	$2+2X+2XY$	$2+Y+2XY$	$2+Y+X+2XY$	$2+Y+2X+2XY$	$2+2Y+2XY$	$2+2Y+X+2XY$	$2+2Y+2X+2XY$

$\mathcal{B}^{2,1}$ $s=2$

will produce $g_1(Y)$ namely Y and when evaluated at $Y = \alpha_1$ which is 2 will produce the polynomial $1 + 2X$. So, at least through demonstration it seems that this property is correct, but just because it works for one example one case this property need not hold for other cases or in general we have to prove it. That this holds in general always.

(Refer Slide Time: 18:40)



(t, t)-degree Bivariate Polynomials: More Properties

- ❑ $\alpha_1, \cdots, \alpha_n$: distinct, non-zero elements from $\mathbb{F}$ ❑ $I \subset \{1, \cdots, n\}, |I| = t$
- ❑ t-degree polynomials $\{f_i(X)\}_{i \in I}$ ❑ t-degree polynomials $\{g_i(Y)\}_{i \in I}$
- ❑ $f_i(\alpha_j) = g_j(\alpha_i)$, for every $i, j \in I$

➡ For **every** $s \in \mathbb{F}$, there exists a **unique** $F(X, Y) \in \mathcal{B}^{s,t}$:

- ❖ $F(X, \alpha_i) = f_i(X)$, for every $i \in I$
- ❖ $F(\alpha_i, Y) = g_i(Y)$, for every $i \in I$

$\alpha_1, \alpha_3, \alpha_4$

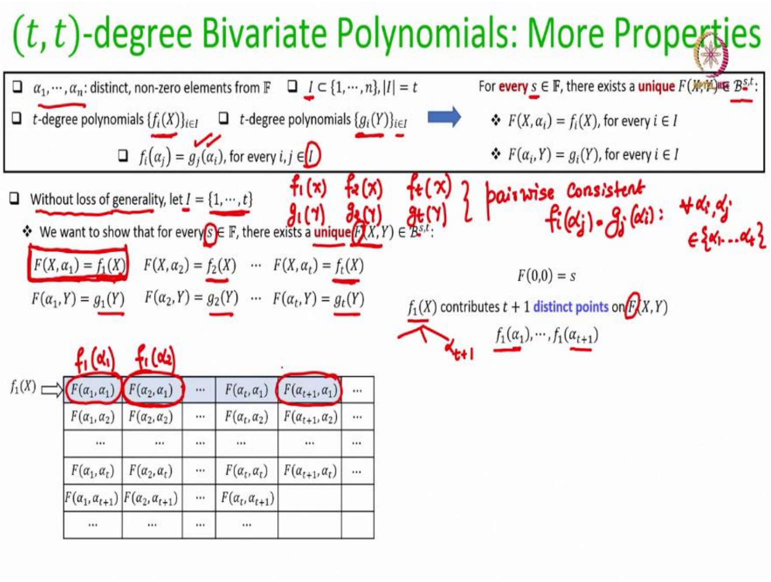
- ❑ Without loss of generality, let $I = \{1, \cdots, t\}$

So, what is the statement? You are given n distinct nonzero evaluation points among those n distinct non zero evaluation points you are fixed you are focusing only a subset of t evaluation points. Now corresponding to those t evaluation points you are given t number of univariate polynomials in X and Y of course, of degree t which are pairwise consistent corresponding to those indices in the index set which you are focusing on.

Then the claim is that for every element from the field there is one and only one bivariate polynomial of degree t in both the variables with that s being the constant term and which passes through the X and Y univariate polynomials corresponding to the indices in your index set I. So, as I said that this index set I could include any of the t evaluation points from $\alpha_1, \dots, \alpha_n$.

It could be the first t evaluation points it could be the last t evaluation points it could be say for instance $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ and so, on.

(Refer Slide Time: 20:24)



(t,t)-degree Bivariate Polynomials: More Properties

❑ $\alpha_1, \cdots, \alpha_n$: distinct, non-zero elements from $\mathbb{F}$ ❑ $I \subset \{1, \cdots, n\}, |I| = t$

❑ t-degree polynomials $\{f_i(X)\}_{i \in I}$ ❑ t-degree polynomials $\{g_i(Y)\}_{i \in I}$

❑ $f_i(\alpha_j) = g_j(\alpha_i)$, for every $i, j \in I$

➡ For **every** $s \in \mathbb{F}$, there exists a **unique** $F(X,Y) \in \mathcal{B}^{s,t}$:

❖ $F(X, \alpha_i) = f_i(X)$, for every $i \in I$

❖ $F(\alpha_i, Y) = g_i(Y)$, for every $i \in I$

❑ Without loss of generality, let $I = \{1, \cdots, t\}$

$f_1(x)$ $f_2(x)$ $f_t(x)$ } pairwise Consistent

$g_1(Y)$ $g_2(Y)$ $g_t(Y)$ } $f_i(\alpha_j) = g_j(\alpha_i)$: $\forall \alpha_i, \alpha_j \in \{\alpha_1 \dots \alpha_t\}$

❖ We want to show that for every $s \in \mathbb{F}$, there exists a **unique** $F(X,Y) \in \mathcal{B}^{s,t}$:

$\boxed{F(X, \alpha_1) = f_1(X)}$ $F(X, \alpha_2) = f_2(X)$ $\cdots$ $F(X, \alpha_t) = f_t(X)$

$F(\alpha_1, Y) = g_1(Y)$ $F(\alpha_2, Y) = g_2(Y)$ $\cdots$ $F(\alpha_t, Y) = g_t(Y)$

$F(0,0) = s$

$f_1(X)$ contributes $t+1$ **distinct points** on $F(X,Y)$

α_{t+1}

$f_1(\alpha_1), \cdots, f_1(\alpha_{t+1})$

$f_1(\alpha_1)$ $f_1(\alpha_2)$

$f_1(X) \Rightarrow$

$F(\alpha_1, \alpha_1)$	$F(\alpha_2, \alpha_1)$	$\cdots$	$F(\alpha_t, \alpha_1)$	$F(\alpha_{t+1}, \alpha_1)$	$\cdots$
$F(\alpha_1, \alpha_2)$	$F(\alpha_2, \alpha_2)$	$\cdots$	$F(\alpha_t, \alpha_2)$	$F(\alpha_{t+1}, \alpha_2)$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$F(\alpha_1, \alpha_t)$	$F(\alpha_2, \alpha_t)$	$\cdots$	$F(\alpha_t, \alpha_t)$	$F(\alpha_{t+1}, \alpha_t)$	$\cdots$
$F(\alpha_1, \alpha_{t+1})$	$F(\alpha_2, \alpha_{t+1})$	$\cdots$	$F(\alpha_t, \alpha_{t+1})$		
$\cdots$	$\cdots$	$\cdots$	$\cdots$		

So, we can prove the theorem for any index set of size t, but for simplicity and to avoid the complication of notations, let me prove it for the simpler case when the t evaluation points are the first t evaluation points, but I stress that this is without loss of generality.

Whatever I am explaining here that holds even if those t evaluation points are not the first t consecutive evaluation points. What we want to show here? We want to show that you take any value from the field for s corresponding to that you can find one and only one bivariate polynomial of degree t in both the variables and whose constant term is s which passes through the first X univariate polynomial the second X univariate polynomial and the tth X univariate polynomials.

From where you get this t univariate polynomials? Well, we are getting them because I am assuming that the index set of size t which we are considering as the first t evaluation points. So, corresponding to these two evaluation points you will be given $f_1(X), f_2(X), \dots, f_t(X)$ you are given that you are given those t arbitrary X polynomials and you are given also t arbitrary Y polynomials.

Of course, all the degrees are here t when I do not say explicitly you have to assume here that the degrees are t here if it is univariate polynomial, then the degree is t in that variable if the bivariate then the degrees t in both the variables. So, you are given t number of X polynomials, t number of Y polynomials and they are pairwise consistent. Pairwise consistent means that f_i at α_j is given to be g_j polynomial evaluated at α_i for all α_i, α_j belonging to $\alpha_1 \dots, \alpha_t$.

Why $\alpha_1 \dots, \alpha_t$? Because I am fixing my I to be the subset of first t evaluation points.

So, we want to show that for every s from the field you can find a unique bivariate polynomial of degree t with that s being the constant term and which passes through the given t X univariate polynomials and Y univariate polynomials when I say passes; that means, $(f_1(X), \alpha_1)$ constitutes or lie on this bivariate polynomial $(f_2(X), \alpha_2)$ lie on that bivariate polynomial $(f_t(X), \alpha_t)$ lie on the bivariate polynomial I means when I evaluate this bivariate polynomial at $Y = \alpha_1, Y = \alpha_2, \dots, Y = \alpha_t$ I should get $f_1(X), f_2(X), \dots, f_t(X)$.

In the same way $(\alpha_1, g_1(Y)), \big(\alpha_2, g_2(Y)\big), \dots, (\alpha_t, g_t(Y))$ should also lie on that bivariate polynomial lie in the sense that when I evaluate this bivariate polynomial at $X = \alpha_1, X = \alpha_2, \dots, X = \alpha_t$ I should get $g_1(Y), g_2(Y), \dots, g_t(Y)$respectively. So, let us prove this. So, how many points on the bivariate polynomial? That bivariate polynomial $F(X, Y)$ which you want to find out you are fixing.

Well, you are fixing it is constant term because you want that the constant term of that bivariate polynomial should be s; that means, you are fixing the point $F(0,0)$ and now you want that bivariate polynomial $F(X, Y)$ when evaluated at α_1 should give you $f_1(X)$. Now if I evaluate this polynomial $f_1(X)$ further at $X = \alpha_1, X = \alpha_2, \dots, X = \alpha_{t+1}$ then they contribute basically $2t + 1$ distinct points on that unknown bivariate polynomial.

So, you have already fixed one point on that unknown bivariate polynomial, but by putting this constraint by putting the constraint that that bivariate polynomial when evaluated at $Y = \ \alpha_1$ should give you $f_1(X)$ you are actually fixing $t + 1$ more points on that bivariate polynomial because when I evaluate this bivariate when I evaluate this f_1 polynomial at $X = \alpha_1$ that is nothing but the point F evaluated at (α_1, α_1).

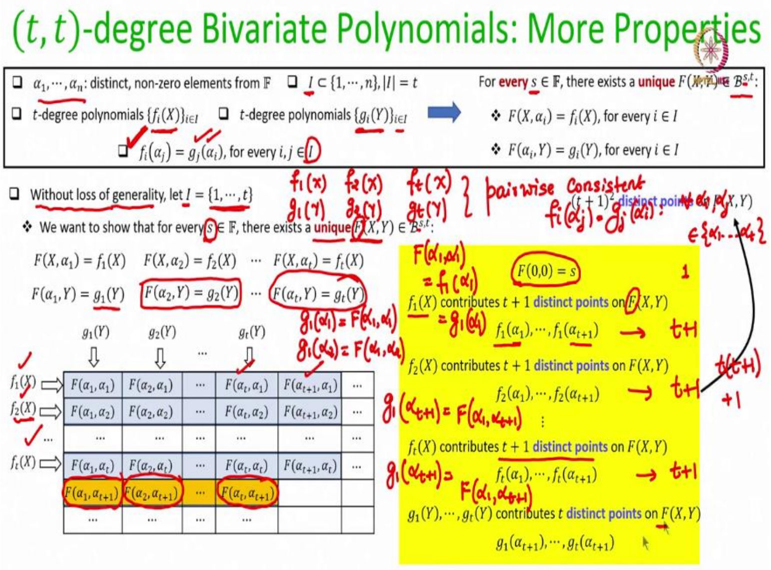
So, this is nothing but the point f_1 evaluated at $X = \alpha_1$ in the same way when I evaluate the when I evaluate the univariate polynomial f_1 at $X = \alpha_2$ that is nothing but one more distinct point on that unknown bivariate polynomial and like that when I evaluate this f_1

polynomial at $X = \alpha_{t+1}$ that basically gives me one more distinct point on that unknown bivariate polynomial.

So, by setting this constraint that that unknown bivariate polynomial when evaluated at y equal to α_1 should give me $f_1(X)$ polynomial I am basically fixing $t + 1$ distinct points on that unknown bivariate polynomial ok I am setting this constraint. I am basically setting the constraint that you are anyhow given $f_1(X)$ and if you are given $f_1(X)$ then basically all the points which I have highlighted here you are given those points.

You are given those points and you are basically fixing those points to lie on the unknown bivariate polynomial.

(Refer Slide Time: 27:24)



(t, t)-degree Bivariate Polynomials: More Properties

□ $\alpha_1, \cdots, \alpha_n$: distinct, non-zero elements from $\mathbb{F}$ □ $I \subset \{1, \cdots, n\}, |I| = t$

□ t-degree polynomials $\{f_i(X)\}_{i \in I}$ □ t-degree polynomials $\{g_i(Y)\}_{i \in I}$

□ $f_i(\alpha_j) = g_j(\alpha_i)$, for every $i, j \in I$

For **every** $s \in \mathbb{F}$, there exists a **unique** $F(X, Y) \in \mathcal{B}^{s,t}$:

- ❖ $F(X, \alpha_i) = f_i(X)$, for every $i \in I$
- ❖ $F(\alpha_i, Y) = g_i(Y)$, for every $i \in I$

□ Without loss of generality, let $I = \{1, \cdots, t\}$

- ❖ We want to show that for every $s \in \mathbb{F}$, there exists a unique $F(X, Y) \in \mathcal{B}^{s,t}$:

$F(X, \alpha_1) = f_1(X)$ $F(X, \alpha_2) = f_2(X)$ $\cdots$ $F(X, \alpha_t) = f_t(X)$

$F(\alpha_1, Y) = g_1(Y)$ $F(\alpha_2, Y) = g_2(Y)$ $\cdots$ $F(\alpha_t, Y) = g_t(Y)$

	$g_1(Y)$ ⇩	$g_2(Y)$ ⇩	$\cdots$	$g_t(Y)$ ⇩		
$f_1(X)$ ⇨	$F(\alpha_1, \alpha_1)$	$F(\alpha_2, \alpha_1)$	$\cdots$	$F(\alpha_t, \alpha_1)$	$F(\alpha_{t+1}, \alpha_1)$	$\cdots$
$f_2(X)$ ⇨	$F(\alpha_1, \alpha_2)$	$F(\alpha_2, \alpha_2)$	$\cdots$	$F(\alpha_t, \alpha_2)$	$F(\alpha_{t+1}, \alpha_2)$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$f_t(X)$ ⇨	$F(\alpha_1, \alpha_t)$	$F(\alpha_2, \alpha_t)$	$\cdots$	$F(\alpha_t, \alpha_t)$	$F(\alpha_{t+1}, \alpha_t)$	$\cdots$
	$F(\alpha_1, \alpha_{t+1})$	$F(\alpha_2, \alpha_{t+1})$	$\cdots$	$F(\alpha_t, \alpha_{t+1})$		
	$\cdots$	$\cdots$	$\cdots$	$\cdots$		

$(t+1)^2$ distinct points on $F(X, Y)$

$F(0,0) = s$ 1

$f_1(X)$ contributes $t + 1$ distinct points on $F(X, Y)$

$f_1(\alpha_1), \cdots, f_1(\alpha_{t+1})$ → $t+1$

$f_2(X)$ contributes $t + 1$ distinct points on $F(X, Y)$

$f_2(\alpha_1), \cdots, f_2(\alpha_{t+1})$ → $t+1$

$\vdots$

$f_t(X)$ contributes $t + 1$ distinct points on $F(X, Y)$

$f_t(\alpha_1), \cdots, f_t(\alpha_{t+1})$ → $t+1$

$g_1(Y), \cdots, g_t(Y)$ contributes t distinct points on $F(X, Y)$

$g_1(\alpha_{t+1}), \cdots, g_t(\alpha_{t+1})$

$f_1(x)$ $f_2(x)$ $f_t(x)$
$g_1(Y)$ $g_2(Y)$ $g_t(Y)$ } pairwise Consistent

$f_i(\alpha_j) = g_j(\alpha_i)$! $\alpha_i, \alpha_j \in \{\alpha_1 \ldots \alpha_t\}$

$F(\alpha_1, \alpha_1) = f_1(\alpha_1) = g_1(\alpha_1)$

$g_1(\alpha_1) = F(\alpha_1, \alpha_1)$

$g_1(\alpha_2) = F(\alpha_1, \alpha_2)$

$g_1(\alpha_{t+1}) = F(\alpha_1, \alpha_{t+1})$

$g_1(\alpha_{t+1}) = F(\alpha_1, \alpha_{t+1})$

$t(t+1)$ $+1$

In the same way you want that unknown bivariate polynomial to pass through $(f_2(X), \alpha_2)$ namely you want that unknown bivariate polynomial when evaluated at $Y = \alpha_2$ should give you $f_2(X)$. Now $f_2(X)$ is given to you and if $f_2(X)$ is given to you then you are basically given the second highlighted row here right.

Because you can evaluate f_2 at $X = \alpha_1, X = \alpha_2, \ldots, X = \alpha_{t+1}$ and now because of the second constraint you are basically fixing $t + 1$ new points on the unknown bivariate polynomial why they are new points? Because these points are different from the $t + 1$ points which you have fixed due to the first constraint namely the points which are there in the first row.

So, basically what I am trying to do here is I am trying to find out how many points on that unknown bivariate polynomial you are fixing because of the various constraint. We have fixed the constant term because of this constraint that $f_1(X)$ should lie on that unknown bivariate polynomial we have set the first row of this matrix consisting of $t+1$ points like that.

Because of the second constraint that $(f_2(X), \alpha_2)$ also should lie on the unknown bivariate polynomial we have set or we have fixed $t+1$ new distinct points on the bivariate polynomial and like that you have the tth constraint due to this X polynomial the tth constraint is that that unknown bivariate polynomial when evaluated at $Y = \alpha_t$ should give you the tth X univariate polynomial which is given to you and that tth univariate X polynomial.

If you evaluated at $X = \alpha_1, X = \alpha_2, \dots, X = \alpha_{t+1}$ basically gives you $t+1$ distinct points on that unknown bivariate polynomial. Why distinct? Because they will be different from all the points which you have fixed till now. So, what is the summary? So, till now we have fixed how many points? The constant is fixed 1 point through $f_1(X)$ we have fixed $t+1$ points through f sub 2 x we have fixed $t+1$ points and through the tth X polynomial we have fixed $t+1$ points.

So, $t \cdot (t+1)$ these many points on the unknown bivariate polynomial are fixed 1 because of the constraint on the constant term and because of the constraint at that unknown bivariate polynomial passes through $(f_1(X), \alpha_1), (f_2(X), \alpha_2), \dots, (f_t(X), \alpha_t)$. Now you see you also have constraints on that unknown bivariate polynomial in terms of the Y univariate polynomials.

They also have to satisfy, or they have to also these Y univariate polynomials also should lie on the same unknown bivariate polynomial. So, now, the interesting part here is that each of this t Y univariate polynomials they basically contribute to t distinct points on that unknown bivariate polynomial why so? because when I say that the first Y univariate polynomial should lie on that unknown bivariate polynomial then; that means, that $g_1(\alpha_1)$ is nothing but that unknown unknow bivariate at (α_1, α_1).

$g_1(\alpha_2)$ is nothing but that unknown bivariate at (α_1, α_2) and like that $g_1(\alpha_{t+1})$ is same as that unknown bivariate polynomial at (α_1, α_{t+1}), but I have already fixed the first t points in this column because of the constraint because of the constraints imposed by the X polynomials. I have already fixed them because I use the constraint that $f_1(X)$ lies on that bivariate polynomial.

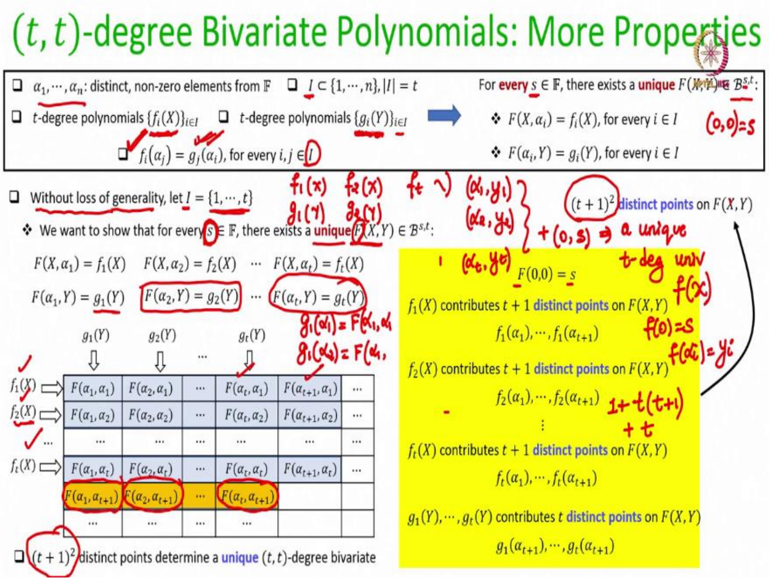
That means I have already set $F(\alpha_1, \alpha_1)$ to be whatever f_1 polynomial evaluates at α_1 and f_1 polynomial evaluates it to alpha 1 is given to be g_1 polynomial evaluated at α_1 because of this pairwise consistency condition. In the same way the second point along this first column have been already fixed because the second point on the first column is nothing but f_2 polynomial evaluated at α_1.

And that is given to be same as g_1 polynomial evaluated at α_2 due to this pairwise consistency; that means, when I am using this constraint on that bivariate polynomial unknown bivariate polynomial because of that I am now getting only one new point on the unknown bivariate polynomial namely the g_1 univariate polynomial evaluated at α_{t+1} which I can find out is given to be same as the unknown bivariate polynomial evaluated at (α_1, α_{t+1}),.

In the same way if I use the second constraint imposed by the g_2 univariate polynomial that gives me that fixes one more distinct point on the bivariate polynomial and like that when I use the tth constraint here it fixes the tth point highlighted here. So, now, let us see how many points total we have fixed on that unknown bivariate polynomial and whether those points imply a unique bivariate polynomial of degree t or many more bivariate polynomials more than 1.

So, it turns out that through all these constraints. So, we have three different types of constraints 1 constraint imposed by the constant term namely we want the constant term of that unknown bivariate polynomial to be the value s.

(Refer Slide Time: 35:22)



(t,t)-degree Bivariate Polynomials: More Properties

- ❑ $\alpha_1, \cdots, \alpha_n$: distinct, non-zero elements from $\mathbb{F}$ ❑ $I \subset \{1, \cdots, n\}, |I| = t$
- ❑ t-degree polynomials $\{f_i(X)\}_{i \in I}$ ❑ t-degree polynomials $\{g_i(Y)\}_{i \in I}$
- ❑ $f_i(\alpha_j) = g_j(\alpha_i)$, for every $i, j \in I$

For every $s \in \mathbb{F}$, there exists a unique $F(X,Y) \in \mathcal{B}^{s,t}$:

- ❖ $F(X, \alpha_i) = f_i(X)$, for every $i \in I$
- ❖ $F(\alpha_i, Y) = g_i(Y)$, for every $i \in I$

❑ Without loss of generality, let $I = \{1, \cdots, t\}$

❖ We want to show that for every $s \in \mathbb{F}$, there exists a unique $F(X,Y) \in \mathcal{B}^{s,t}$:

$F(X,\alpha_1) = f_1(X)$ $F(X,\alpha_2) = f_2(X)$ $\cdots$ $F(X,\alpha_t) = f_t(X)$

$F(\alpha_1,Y) = g_1(Y)$ $F(\alpha_2,Y) = g_2(Y)$ $\cdots$ $F(\alpha_t,Y) = g_t(Y)$

	$g_1(Y)$ ⇩	$g_2(Y)$ ⇩	$\cdots$	$g_t(Y)$ ⇩		
$f_1(X)$ ⇨	$F(\alpha_1,\alpha_1)$	$F(\alpha_2,\alpha_1)$	$\cdots$	$F(\alpha_t,\alpha_1)$	$F(\alpha_{t+1},\alpha_1)$	$\cdots$
$f_2(X)$ ⇨	$F(\alpha_1,\alpha_2)$	$F(\alpha_2,\alpha_2)$	$\cdots$	$F(\alpha_t,\alpha_2)$	$F(\alpha_{t+1},\alpha_2)$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$f_t(X)$ ⇨	$F(\alpha_1,\alpha_t)$	$F(\alpha_2,\alpha_t)$	$\cdots$	$F(\alpha_t,\alpha_t)$	$F(\alpha_{t+1},\alpha_t)$	$\cdots$
	$F(\alpha_1,\alpha_{t+1})$	$F(\alpha_2,\alpha_{t+1})$	$\cdots$	$F(\alpha_t,\alpha_{t+1})$		
	$\cdots$	$\cdots$	$\cdots$	$\cdots$		

❑ $(t+1)^2$ distinct points determine a unique (t,t)-degree bivariate

$(t+1)^2$ distinct points on $F(X,Y)$

$F(0,0) = s$

$f_1(X)$ contributes $t+1$ distinct points on $F(X,Y)$

$f_1(\alpha_1), \cdots, f_1(\alpha_{t+1})$

$f_2(X)$ contributes $t+1$ distinct points on $F(X,Y)$

$f_2(\alpha_1), \cdots, f_2(\alpha_{t+1})$

$\vdots$

$f_t(X)$ contributes $t+1$ distinct points on $F(X,Y)$

$f_t(\alpha_1), \cdots, f_t(\alpha_{t+1})$

$g_1(Y), \cdots, g_t(Y)$ contributes t distinct points on $F(X,Y)$

$g_1(\alpha_{t+1}), \cdots, g_t(\alpha_{t+1})$

And because of the constraints imposed by the X univariate polynomials we have $t \cdot (t+1)$ distinct points and now because of the constraints imposed by the Y univariate polynomials.

We are fixing t more distinct points on the bivariate polynomials. So, all together they contribute to $(t+1)^2$ distinct points on the unknown bivariate polynomial. Now what is the degree of that unknown bivariate polynomial its degree is t in both the variable X and both variable Y and recall that in the last lecture we had discussed that if I give you $(t+1)^2$ distant points on an unknown bivariate polynomial using them you can uniquely determine it.

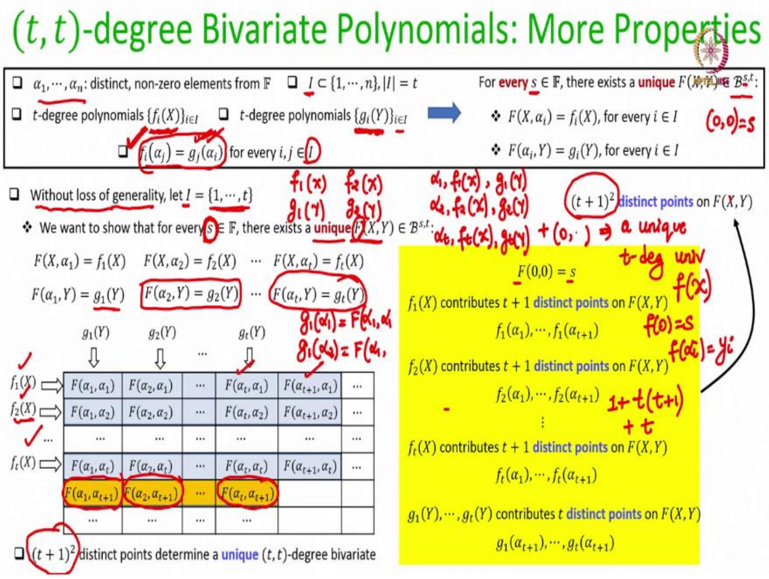
That means, through the given $(t+1)^2$ distinct points you cannot interpolate multiple bivariate polynomials of degree t in both the variables that is simply not possible; that means, once I fix the constant term s that constant term along with this t number of X univariate polynomials and t number of Y univariate polynomials which are guaranteed to be pairwise consistency implies a unique bivariate polynomial it does not imply multiple bivariate polynomials.

So, that is one of the properties which we will use later to prove some more interesting properties and as I said earlier this is nothing but a generalization of the property which we had proved earlier in the context of univariate polynomials in the context of univariate polynomials we have proved that if I give you the points say $(\alpha_1, y_1), (\alpha_2, y_2), \dots, (\alpha_t, y_t)$

then these t distinct points plus the point $(0, s)$ implies a unique t degree univariate f of X polynomial.

Such that $f(0)$ is s and $f(\alpha_i)$ is y_i. For the two-dimensional case the generalization is well the constant term is s; that means, the $(0,0)$ point is s and you are given t number of X univariate polynomials t number of Y univariate polynomials; that means, you are now, given t pairs of X univariate polynomials namely $(f_1(X), \alpha_1), \ldots, (f_t(X), \alpha_t)$.

(Refer Slide Time: 38:22)



(t, t)-degree Bivariate Polynomials: More Properties

❑ $\alpha_1, \cdots, \alpha_n$: distinct, non-zero elements from $\mathbb{F}$ ❑ $I \subset \{1, \cdots, n\}, |I| = t$

❑ t-degree polynomials $\{f_i(X)\}_{i \in I}$ ❑ t-degree polynomials $\{g_i(Y)\}_{i \in I}$

❑ $f_i(\alpha_j) = g_j(\alpha_i)$ for every $i, j \in I$

For **every** $s \in \mathbb{F}$, there exists a **unique** $F(X, Y) \in \mathcal{B}^{s,t}$:

❖ $F(X, \alpha_i) = f_i(X)$, for every $i \in I$

❖ $F(\alpha_i, Y) = g_i(Y)$, for every $i \in I$

$(0,0)=s$

❑ Without loss of generality, let $I = \{1, \cdots, t\}$

❖ We want to show that for every $s \in \mathbb{F}$, there exists a unique $F(X, Y) \in \mathcal{B}^{s,t}$:

$F(X, \alpha_1) = f_1(X)$ $F(X, \alpha_2) = f_2(X)$ $\cdots$ $F(X, \alpha_t) = f_t(X)$

$F(\alpha_1, Y) = g_1(Y)$ $F(\alpha_2, Y) = g_2(Y)$ $\cdots$ $F(\alpha_t, Y) = g_t(Y)$

$f_1(x)$ $f_2(x)$

$g_1(Y)$ $g_2(Y)$

$\alpha_1, f_1(x), g_1(Y)$

$\alpha_2, f_2(x), g_2(Y)$

$\alpha_t, f_t(x), g_t(Y)$ $+ (0, \cdot) \Rightarrow$ a unique t-deg univ $f(x)$

$f(0)=s$

$f(\alpha_i)=y_i$

$g_1(\alpha_1) = F(\alpha_1, \alpha_1$

$g_1(\alpha_2) = F(\alpha_1,$

	$g_1(Y)$ ⇩	$g_2(Y)$ ⇩	$\cdots$	$g_t(Y)$ ⇩		
$f_1(X)$ ⇨	$F(\alpha_1, \alpha_1)$	$F(\alpha_2, \alpha_1)$	$\cdots$	$F(\alpha_t, \alpha_1)$	$F(\alpha_{t+1}, \alpha_1)$	$\cdots$
$f_2(X)$ ⇨	$F(\alpha_1, \alpha_2)$	$F(\alpha_2, \alpha_2)$	$\cdots$	$F(\alpha_t, \alpha_2)$	$F(\alpha_{t+1}, \alpha_2)$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$f_t(X)$ ⇨	$F(\alpha_1, \alpha_t)$	$F(\alpha_2, \alpha_t)$	$\cdots$	$F(\alpha_t, \alpha_t)$	$F(\alpha_{t+1}, \alpha_t)$	$\cdots$
	$F(\alpha_1, \alpha_{t+1})$	$F(\alpha_2, \alpha_{t+1})$	$\cdots$	$F(\alpha_t, \alpha_{t+1})$		
	$\cdots$	$\cdots$	$\cdots$	$\cdots$		

❑ $(t+1)^2$ distinct points determine a **unique** (t, t)-degree bivariate

$(t+1)^2$ distinct points on $F(X, Y)$

$F(0,0) = s$

$f_1(X)$ contributes $t+1$ distinct points on $F(X, Y)$

$f_1(\alpha_1), \cdots, f_1(\alpha_{t+1})$

$f_2(X)$ contributes $t+1$ distinct points on $F(X, Y)$

$f_2(\alpha_1), \cdots, f_2(\alpha_{t+1})$

$\vdots$

$f_t(X)$ contributes $t+1$ distinct points on $F(X, Y)$

$f_t(\alpha_1), \cdots, f_t(\alpha_{t+1})$

$g_1(Y), \cdots, g_t(Y)$ contributes t distinct points on $F(X, Y)$

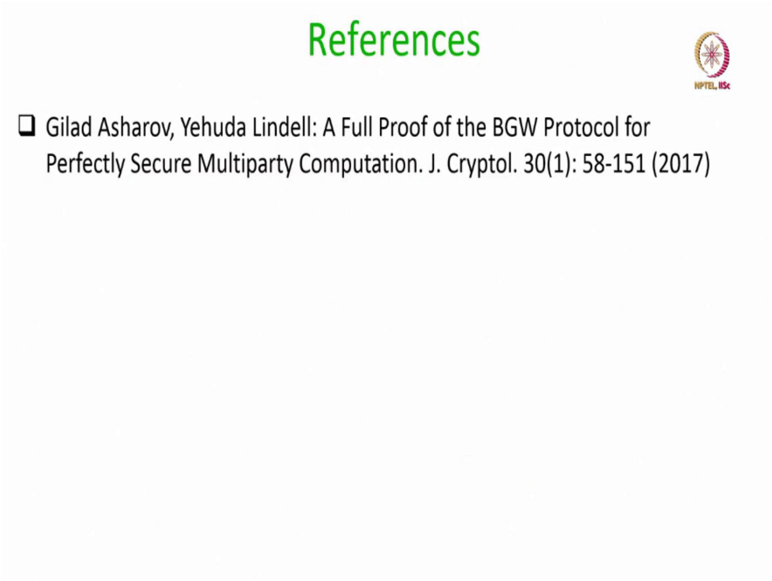
$g_1(\alpha_{t+1}), \cdots, g_t(\alpha_{t+1})$

$1 + t(t+1)$
$+ t$

And corresponding to the same alpha indices you are also given the Y polynomials$g_1(Y), g_2(Y), \ldots, g_t(Y)$, but they are not arbitrary X and Y polynomials they are pairwise consistent X and Y polynomials. Now you might be wondering why this pair wise consistency is imposed. If the pair wise consistency is not imposed, then this whatever argument we have given here does not hold.

So, now the claim is that these t pairs of X and Y polynomials along with the fact that the point along with the fact that the bivariate polynomial at $(0,0)$ gives s implies a unique bivariate polynomial of degree t in both the variables passing through s means the constant term being s and passing through this $f_1(X), f_2(X), \ldots, f_t(X)$ and $g_1(Y), g_2(Y), \ldots, g_t(Y)$ respectively.

(Refer Slide Time: 39:48)



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 again, I use this paper to discuss the properties for today’s lecture.

Thank you.