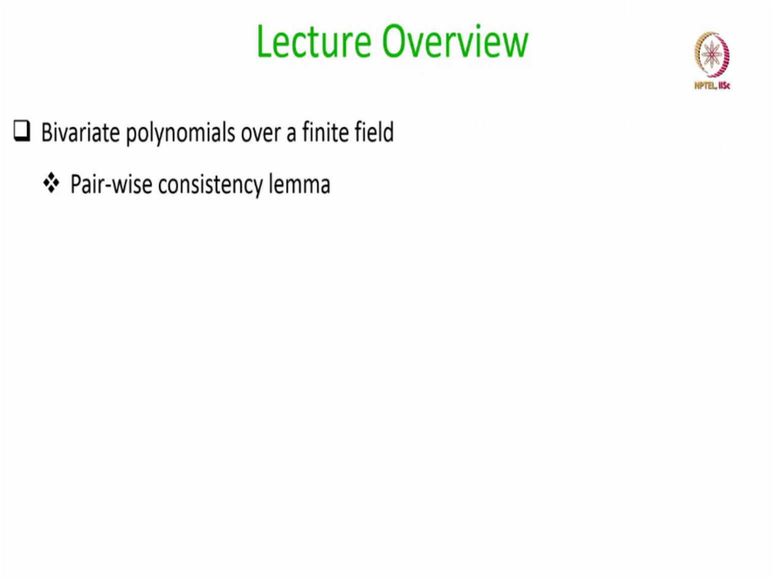
Secure Computation: Part II
Prof. Ashish Choudhury
Department of Computer Science and Engineering
Indian Institute of Science, Bengaluru

Lecture - 37
Bivariate Polynomials over Finite Fields IV

Hello, everyone. Welcome to this lecture.

(Refer Slide Time: 00:23)



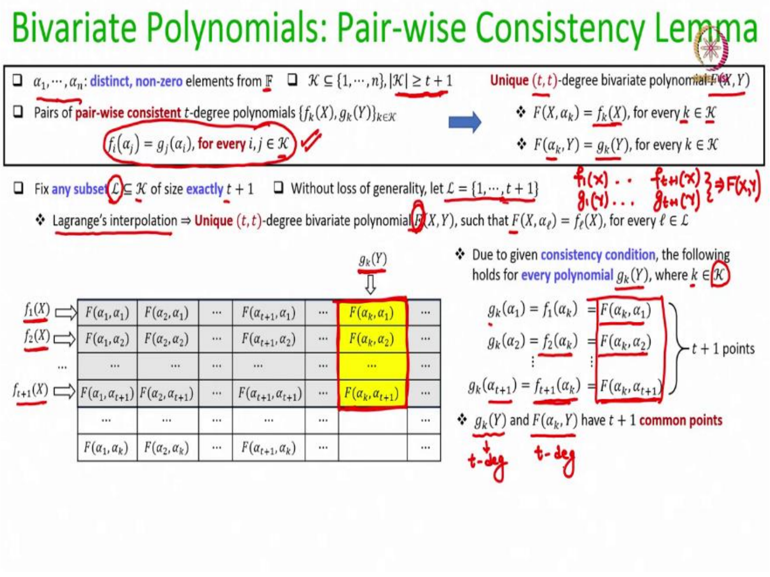
Lecture Overview

❑ Bivariate polynomials over a finite field

- ❖ Pair-wise consistency lemma

So, in this lecture, we will continue our discussion regarding Bivariate Polynomials over a Finite Field. In the last lecture, we had proved the privacy lemma; in this lecture, we will prove another important lemma namely the pair-wise consistency lemma and this also will be later useful when we design verifiable secret sharing schemes based on bivariate polynomials.

(Refer Slide Time: 00:46)



Bivariate Polynomials: Pair-wise Consistency Lemma

- ❑ $\alpha_1, \cdots, \alpha_n$: distinct, non-zero elements from $\mathbb{F}$ ❑ $\mathcal{K} \subseteq \{1, \cdots, n\}, |\mathcal{K}| \geq t+1$
- ❑ Pairs of pair-wise consistent t-degree polynomials $\{f_k(X), g_k(Y)\}_{k \in \mathcal{K}}$

$f_i(\alpha_j) = g_j(\alpha_i)$, for every $i, j \in \mathcal{K}$ ✓

⇒ Unique (t, t)-degree bivariate polynomial $F(X, Y)$

- ❖ $F(X, \alpha_k) = f_k(X)$, for every $k \in \mathcal{K}$
- ❖ $F(\alpha_k, Y) = g_k(Y)$, for every $k \in \mathcal{K}$

- ❑ Fix any subset $\mathcal{L} \subseteq \mathcal{K}$ of size exactly $t+1$ ❑ Without loss of generality, let $\mathcal{L} = \{1, \cdots, t+1\}$

$\left.\begin{matrix} f_1(X) \cdot\cdot & f_{t+1}(X) \\ g_1(Y) \cdots & g_{t+1}(Y) \end{matrix}\right\} \Rightarrow F(X,Y)$

- ❖ Lagrange's interpolation ⇒ Unique (t, t)-degree bivariate polynomial $F(X, Y)$, such that $F(X, \alpha_\ell) = f_\ell(X)$, for every $\ell \in \mathcal{L}$

						$g_k(Y)$ ⇩	
$f_1(X)$ ⇨	$F(\alpha_1, \alpha_1)$	$F(\alpha_2, \alpha_1)$	⋯	$F(\alpha_{t+1}, \alpha_1)$	⋯	$F(\alpha_k, \alpha_1)$	⋯
$f_2(X)$ ⇨	$F(\alpha_1, \alpha_2)$	$F(\alpha_2, \alpha_2)$	⋯	$F(\alpha_{t+1}, \alpha_2)$	⋯	$F(\alpha_k, \alpha_2)$	⋯
⋯	⋯	⋯	⋯	⋯	⋯	⋯	⋯
$f_{t+1}(X)$ ⇨	$F(\alpha_1, \alpha_{t+1})$	$F(\alpha_2, \alpha_{t+1})$	⋯	$F(\alpha_{t+1}, \alpha_{t+1})$	⋯	$F(\alpha_k, \alpha_{t+1})$	⋯
	⋯	⋯	⋯	⋯	⋯		⋯
	$F(\alpha_1, \alpha_k)$	$F(\alpha_2, \alpha_k)$	⋯	$F(\alpha_{t+1}, \alpha_k)$	⋯		⋯

- ❖ Due to given consistency condition, the following holds for every polynomial $g_k(Y)$, where $k \in \mathcal{K}$

$$\left.\begin{matrix} g_k(\alpha_1) = f_1(\alpha_k) & = F(\alpha_k, \alpha_1) \\ g_k(\alpha_2) = f_2(\alpha_k) & = F(\alpha_k, \alpha_2) \\ \vdots & \vdots \\ g_k(\alpha_{t+1}) = f_{t+1}(\alpha_k) & = F(\alpha_k, \alpha_{t+1}) \end{matrix}\right\} t+1 \text{ points}$$

- ❖ $\underset{t\text{-deg}}{g_k(Y)}$ and $\underset{t\text{-deg}}{F(\alpha_k, Y)}$ have $t+1$ common points

So, what exactly is a pair-wise consistency lemma statement? So, again our setting is the same we have a finite field we are given n distinct, non-zero evaluation points $\alpha_1, \ldots, \alpha_n$. And, you are given a subset of n indices $\mathcal{K}$ where the size of $\mathcal{K}$ is at least $t+1$. So, you are focusing on a subset of at least $t+1$ or more number of indices and you are given pair-wise consistent t degree polynomials corresponding to those indices.

So, you are given X univariate polynomials and Y univariate polynomials corresponding to the indices in $\mathcal{K}$ and they are given to be pair-wise consistent. What does that mean? That means that if you focus on any pair of indices (i, j) in this subset $\mathcal{K}$, then the X univariate polynomial evaluated at alpha j gives you the same value as the jth Y univariate polynomial evaluated at α_i.

If this is the case then the claim is the following. The claim is that there exist a unique t degree bivariate polynomial over the field which would have resulted in the following when that bivariate polynomial evaluated at $Y = \alpha_k$ would have given you the kth X univariate polynomial and the same bivariate polynomial when evaluated at $X = \alpha_k$ would have resulted in the kth Y univariate polynomial for every index small k in this $\mathcal{K}$. What does that mean?

So, on a very high level what we are trying to say here is the following. We know that for the case of univariate polynomials if I give you $t+1$ distinct points any $t+1$ arbitrary points pair of points who are distinct. So, which are distinct namely their X components are distinct then I can always pass a unique t degree univariate polynomial through those $t+1$ points.

Now, we are trying to generalize it for the bivariate polynomials. So, always remember that in the context of bivariate polynomials the points can be treated as the X univariate polynomials or the Y univariate polynomials. So, you are given $t+1$ or more number of pairs of X and Y univariate polynomials which are guaranteed to be pair-wise consistent among themselves that is important. Even though they are $t+1$ pairs of arbitrary univariate polynomials, they have to be pair-wise consistent then only this uniqueness property will hold.

So, if they are pair-wise consistent then basically what we are arguing here is that there exist a unique t degree bivariate polynomial passing through those $t+1$ or a greater number of pair-wise consistent univariate polynomials. You cannot have multiple bivariate polynomials passing through those given $t+1$ or a greater number of pair-wise consistent polynomials, that is the statement here. So, we will prove this and then later we will demonstrate it.

So, you are given $t+1$ or a greater number of pair-wise consistent X and Y univariate polynomials, right. So, focus first on any $t+1$ of them. So, remember the number of pair-wise consistent bivariate polynomials could be more than $t+1$, if it is more than $t+1$ focus on any $t+1$ of them any $t+1$ pairs of those pair-wise consistent X and Y univariate polynomials.

So, the indices corresponding to those $t+1$ univariate polynomials and denoting as $\mathcal{L}$ and again without loss of generality and for simplicity assume that those $t+1$ pair-wise consistent X and Y univariate polynomials correspond to the first $t+1$ indices. Now, first what we will do is the following.

We will show that if you are given the pair-wise consistent $f_1(X)$ up to $f_{t+1}(X)$ and $g_1(Y), \ldots, g_{t+1}(Y)$ and if they are pair-wise consistent, then through this $t+1$ pair-wise consistent X and Y univariate polynomials I can always pass a unique t degree bivariate polynomial. This is what first we will prove.

So, first what we will do is we will take the X univariate polynomials, the $t+1$ X univariate polynomials and apply the Lagrange's interpolation for the bivariate polynomial and get a unique t degree bivariate polynomial passing through those $t + 1$ X univariate polynomials. We have not yet touched the $t + 1$ Y univariate polynomials. We have just touched the polynomials $f_1(X), f_2(X), \dots, f_{t+1}(X)$ and through them we have interpolated a t degree bivariate polynomial $F(X, Y)$.

What we will end up eventually showing is that all other remaining polynomials which are given here in this system which are pair-wise consistent etcetera also will be lying on this bivariate polynomial $F(X, Y)$. But right now we have just used the first $t + 1$ given X univariate polynomials to fit a t degree bivariate polynomial $F(X, Y)$. So, this is what pictorially we have done.

Now, what you are given? You are given that if I take any Y univariate polynomial $g_k(Y)$ where k is one of the indices in this set $\mathcal{K}$ right, then it is pair-wise consistent with the first $t + 1$ univariate X polynomials. Why first $t + 1$ because I am assuming for simplicity that the set $\mathcal{L}$ consists of the first $t + 1$ indices.

That means, if I consider this polynomial $g_k(Y)$, then because of the pair-wise consistency fact we have this equality namely the kth Y univariate polynomial when evaluated at α_1 is same as the first X univariate polynomial evaluated at α_k. I am just triggering the pair-wise consistency condition. It is also given that the same kth Y univariate polynomial evaluated at α_2 will give you the same value as the second X univariate polynomial.

So, this kth Y univariate polynomial at α_2 and the second X univariate polynomial at α_k have the same values, right. And, like that the kth Y univariate polynomial at the $t + 1$th evaluation point is given to is given to give you the same it is given that it gives you the same it is value is same as the $t + 1$th X univariate polynomial evaluated at the kth evaluation point.

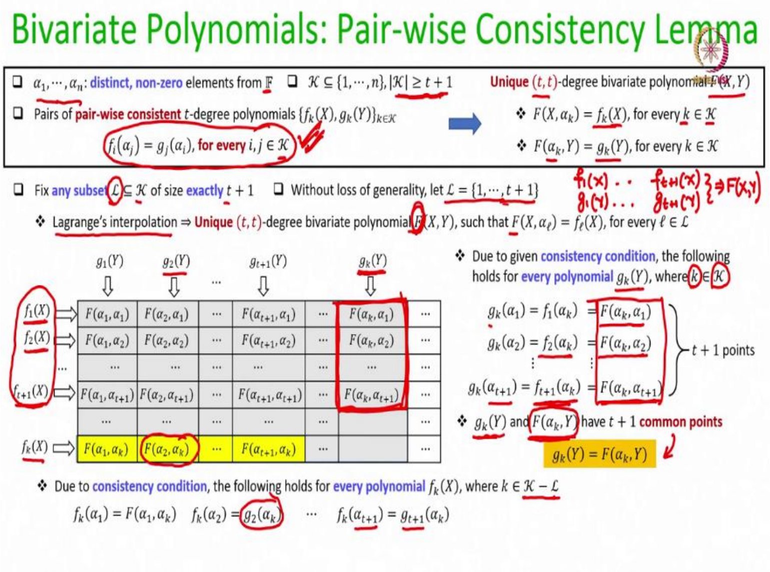
Now, we also know that this first X univariate polynomial is nothing but the first-row polynomial on my bivariate polynomial which I have interpolated. So, if I evaluate this $f_1(X)$ polynomial at α_k then that is nothing but this particular point on my bivariate polynomial. In the same way I have interpolated my bivariate polynomial $F(X, Y)$ using $f_2(X)$.

So, $f_2(X)$ is nothing but the second-row polynomial on my bivariate polynomial and because of that this point $f_2(\alpha_k)$is nothing but this particular point on my bivariate polynomial. And, like that my $t + 1$th X polynomial also lie on my bivariate polynomial it is specifically the $t + 1$th row polynomial and that row polynomial evaluated at α_k is nothing but this specific point on my bivariate polynomial.

Now, what I have shown here? I have shown that there are $t + 1$ points on my bivariate polynomial which are this highlighted point here in the kth column of my matrix. These are the. So, these are the $t + 1$ highlighted points in the matrix, they also lie on my $g_k(Y)$ polynomial and what is the degree of $g_k(Y)$ polynomial? The degree of $g_k(Y)$ polynomial is nothing but t degree. It is a t degree univariate polynomial and what are these highlighted points?

These highlighted points are nothing but points on another t degree univariate polynomial in Y namely the kth column polynomial of my bivariate polynomial $F(X, Y)$; that means, what I have shown here is the kth Y univariate polynomial which is given to me and the kth column polynomial of the interpolated bivariate polynomial they have $t + 1$ common points and their degrees are t.

(Refer Slide Time: 12:14)



Bivariate Polynomials: Pair-wise Consistency Lemma

- ❑ $\alpha_1, \cdots, \alpha_n$: distinct, non-zero elements from $\mathbb{F}$ ❑ $\mathcal{K} \subseteq \{1, \cdots, n\}, |\mathcal{K}| \geq t + 1$
- ❑ Pairs of pair-wise consistent t-degree polynomials $\{f_k(X), g_k(Y)\}_{k \in \mathcal{K}}$

$f_i(\alpha_j) = g_j(\alpha_i)$, for every $i, j \in \mathcal{K}$ ✓

Unique (t, t)-degree bivariate polynomial $F(X, Y)$

❖ $F(X, \alpha_k) = f_k(X)$, for every $k \in \mathcal{K}$

❖ $F(\alpha_k, Y) = g_k(Y)$, for every $k \in \mathcal{K}$

- ❑ Fix any subset $\mathcal{L} \subseteq \mathcal{K}$ of size exactly $t + 1$ ❑ Without loss of generality, let $\mathcal{L} = \{1, \cdots, t + 1\}$

$\left.\begin{matrix} f_1(x) \cdots f_{t+1}(x) \\ g_1(Y) \cdots g_{t+1}(Y) \end{matrix}\right\} \Rightarrow F(X,Y)$

❖ Lagrange's interpolation ⇒ Unique (t, t)-degree bivariate polynomial $F(X, Y)$, such that $F(X, \alpha_\ell) = f_\ell(X)$, for every $\ell \in \mathcal{L}$

$$\begin{array}{c|cccccccc}
 & g_1(Y) & g_2(Y) & \cdots & g_{t+1}(Y) & & g_k(Y) & \\
 & \Downarrow & \Downarrow & & \Downarrow & & \Downarrow & \\
\hline
f_1(X) \Rightarrow & F(\alpha_1, \alpha_1) & F(\alpha_2, \alpha_1) & \cdots & F(\alpha_{t+1}, \alpha_1) & \cdots & F(\alpha_k, \alpha_1) & \cdots \\
f_2(X) \Rightarrow & F(\alpha_1, \alpha_2) & F(\alpha_2, \alpha_2) & \cdots & F(\alpha_{t+1}, \alpha_2) & \cdots & F(\alpha_k, \alpha_2) & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
f_{t+1}(X) \Rightarrow & F(\alpha_1, \alpha_{t+1}) & F(\alpha_2, \alpha_{t+1}) & \cdots & F(\alpha_{t+1}, \alpha_{t+1}) & \cdots & F(\alpha_k, \alpha_{t+1}) & \cdots \\
 & \cdots & \cdots & \cdots & \cdots & \cdots & & \cdots \\
f_k(X) \Rightarrow & F(\alpha_1, \alpha_k) & F(\alpha_2, \alpha_k) & \cdots & F(\alpha_{t+1}, \alpha_k) & \cdots & & \cdots
\end{array}$$

❖ Due to given consistency condition, the following holds for every polynomial $g_k(Y)$, where $k \in \mathcal{K}$

$$\left.\begin{aligned} g_k(\alpha_1) &= f_1(\alpha_k) = F(\alpha_k, \alpha_1) \\ g_k(\alpha_2) &= f_2(\alpha_k) = F(\alpha_k, \alpha_2) \\ &\vdots \\ g_k(\alpha_{t+1}) &= f_{t+1}(\alpha_k) = F(\alpha_k, \alpha_{t+1}) \end{aligned}\right\} t + 1 \text{ points}$$

❖ $g_k(Y)$ and $F(\alpha_k, Y)$ have $t + 1$ common points

$g_k(Y) = F(\alpha_k, Y)$

❖ Due to consistency condition, the following holds for every polynomial $f_k(X)$, where $k \in \mathcal{K} - \mathcal{L}$

$f_k(\alpha_1) = F(\alpha_1, \alpha_k)$ $f_k(\alpha_2) = g_2(\alpha_k)$ $\cdots$ $f_k(\alpha_{t+1}) = g_{t+1}(\alpha_k)$

So, we know that if two t degree polynomials have $t + 1$ or more number of common points then they are the same polynomials. So, we have two different univariate polynomials here – the $g_k(Y)$ univariate polynomial which is given to us and the kth univariate polynomial in the kth column polynomial also in Y whose degree is also t and there are $t + 1$ points namely the highlighted points here which lie on the kth column polynomial of the bivariate as well as on the $g_k(Y)$ polynomial, then it automatically implies that kth Y univariate polynomial which was given to me is nothing but the kth column polynomial lying on the interpolated bivariate.

And, here k is any index from my set $\mathcal{K}$ that automatically shows that whatever I have argued for $g_k(Y)$ holds for $g_1(Y), g_2(Y), \ldots, g_{t+1}(Y)$ and so on. That means what I have shown here now is that all the g polynomials which are given to me. So, I have I was given $t + 1$ or more number of pair-wise consistent X and Y univariate polynomials. I have used the first $t + 1$ X univariate polynomials interpolated the bivariate.

And, now, I have shown that all the Y univariate polynomials not just the first $t + 1$ all the Y univariate polynomials they also lie on that interpolated bivariate polynomials. Now, what is left? It is left to show that all the remaining X univariate polynomials remaining means which were there in the set whose indices are in the set $\mathcal{K}$, but not in the index set $\mathcal{L}$, they also lie on this interpolated bivariate polynomial $F(X, Y)$.

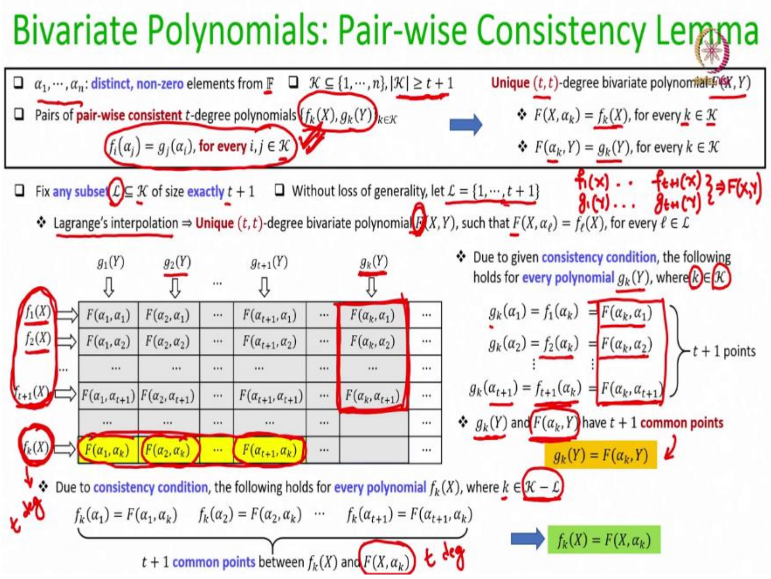
And, again to prove that we will trigger this pair-wise consistency statement. So, consider any X univariate polynomial outside I outside the first $t + 1$ X univariate polynomial different from the first $t + 1$ X univariate polynomial. Now, what we are given, what we know about such X univariate polynomials? So, we are given that this kth X univariate polynomial evaluated at α_1 gives you the same value as the first Y univariate polynomial evaluated at α_k because of this pair-wise consistency.

In the same way this kth X univariate polynomial at α_2 is given to be same as the second Y univariate polynomial evaluated at α_k and like that this kth X univariate polynomial evaluated at alpha $t + 1$ is given to be same as the $t + 1$th Y univariate polynomial evaluated at the kth evaluation point.

Now, what can I say about g 1 evaluated at α_k? Well, g_1 evaluated at α_k is nothing but a point on the bivariate polynomial namely it is this point $F(\alpha_1, \alpha_k)$ so; that means, we have I can rewrite this equality like this. In the same way what is $g_2(\alpha_k)$? g_2 polynomial evaluated at α_k is the second point here in this highlighted group and which is a point on my interpolated bivariate polynomial $F(X, Y)$.

That means, I can rewrite this equality as this and in the same way if I take the $t + 1$th Y univariate polynomial and evaluated at α_k then that will give me this highlighted point; that means, now I can rewrite this equation this equality as this, right.

(Refer Slide Time: 16:27)



Bivariate Polynomials: Pair-wise Consistency Lemma

❑ $\alpha_1, \cdots, \alpha_n$: distinct, non-zero elements from $\mathbb{F}$ ❑ $\mathcal{K} \subseteq \{1, \cdots, n\}, |\mathcal{K}| \geq t + 1$

❑ Pairs of pair-wise consistent t-degree polynomials $\{f_k(X), g_k(Y)\}_{k \in \mathcal{K}}$

$f_i(\alpha_j) = g_j(\alpha_i)$, for every $i, j \in \mathcal{K}$

Unique (t, t)-degree bivariate polynomial $F(X, Y)$

- ❖ $F(X, \alpha_k) = f_k(X)$, for every $k \in \mathcal{K}$
- ❖ $F(\alpha_k, Y) = g_k(Y)$, for every $k \in \mathcal{K}$

❑ Fix any subset $\mathcal{L} \subseteq \mathcal{K}$ of size exactly $t + 1$ ❑ Without loss of generality, let $\mathcal{L} = \{1, \cdots, t + 1\}$

$$\left.\begin{matrix} f_1(x) \cdots & f_{t+1}(x) \\ g_1(Y) \cdots & g_{t+1}(Y) \end{matrix}\right\} \Rightarrow F(X,Y)$$

❖ Lagrange's interpolation ⇒ Unique (t, t)-degree bivariate polynomial $F(X, Y)$, such that $F(X, \alpha_\ell) = f_\ell(X)$, for every $\ell \in \mathcal{L}$

	$g_1(Y)$	$g_2(Y)$	⋯	$g_{t+1}(Y)$		$g_k(Y)$	
$f_1(X)$	$F(\alpha_1, \alpha_1)$	$F(\alpha_2, \alpha_1)$	⋯	$F(\alpha_{t+1}, \alpha_1)$	⋯	$F(\alpha_k, \alpha_1)$	⋯
$f_2(X)$	$F(\alpha_1, \alpha_2)$	$F(\alpha_2, \alpha_2)$	⋯	$F(\alpha_{t+1}, \alpha_2)$	⋯	$F(\alpha_k, \alpha_2)$	⋯
⋯	⋯	⋯	⋯	⋯	⋯	⋯	⋯
$f_{t+1}(X)$	$F(\alpha_1, \alpha_{t+1})$	$F(\alpha_2, \alpha_{t+1})$	⋯	$F(\alpha_{t+1}, \alpha_{t+1})$	⋯	$F(\alpha_k, \alpha_{t+1})$	⋯
	⋯	⋯	⋯	⋯	⋯		⋯
$f_k(X)$	$F(\alpha_1, \alpha_k)$	$F(\alpha_2, \alpha_k)$	⋯	$F(\alpha_{t+1}, \alpha_k)$	⋯		⋯

❖ Due to given consistency condition, the following holds for every polynomial $g_k(Y)$, where $k \in \mathcal{K}$

$$\left.\begin{matrix} g_k(\alpha_1) = f_1(\alpha_k) = F(\alpha_k, \alpha_1) \\ g_k(\alpha_2) = f_2(\alpha_k) = F(\alpha_k, \alpha_2) \\ \vdots \\ g_k(\alpha_{t+1}) = f_{t+1}(\alpha_k) = F(\alpha_k, \alpha_{t+1}) \end{matrix}\right\} t + 1 \text{ points}$$

❖ $g_k(Y)$ and $F(\alpha_k, Y)$ have $t + 1$ common points

$g_k(Y) = F(\alpha_k, Y)$

t deg

❖ Due to consistency condition, the following holds for every polynomial $f_k(X)$, where $k \in \mathcal{K} - \mathcal{L}$

$$\underbrace{f_k(\alpha_1) = F(\alpha_1, \alpha_k) \quad f_k(\alpha_2) = F(\alpha_2, \alpha_k) \quad \cdots \quad f_k(\alpha_{t+1}) = F(\alpha_{t+1}, \alpha_k)}_{t + 1 \text{ common points between } f_k(X) \text{ and } F(X, \alpha_k)}$$

t deg

$f_k(X) = F(X, \alpha_k)$

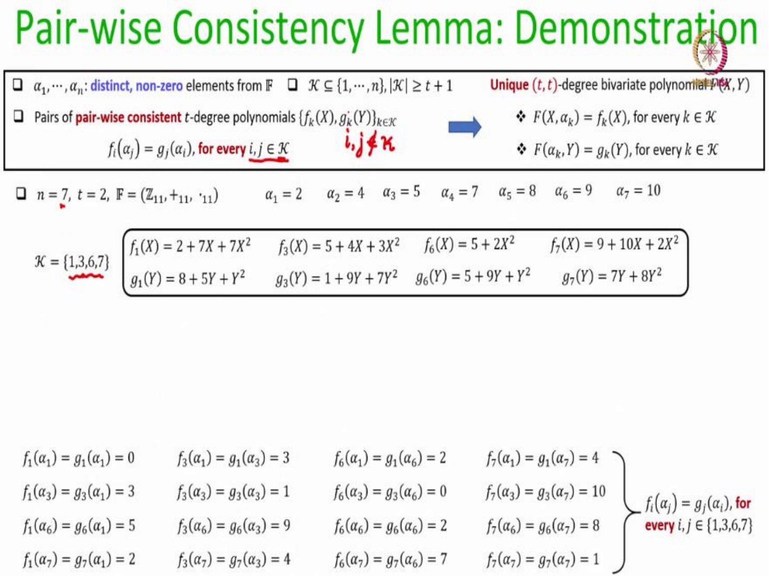
Now, what is the degree of $f_k(X)$ polynomial? It is a t degree polynomial and these points is highlighted points here actually lie on a t degree polynomial t degree univariate polynomial in X that polynomial is F of X of alpha k namely they are the points on the supposedly kth row polynomial of this bivariate, its degree is also t. So, $f_k(X)$ is a t degree polynomial and the supposedly kth row polynomial of the bivariate polynomial is also have its degree is also t.

And, we have shown that the kth X univariate polynomial it has $t + 1$ points which also lie on the kth row polynomial of my interpolated bivariate polynomial. So, again we can use the fact that if you have two t degree polynomials with $t + 1$ common points then basically both the polynomials are the same; that means, this kth X univariate polynomial is nothing but the kth row polynomial of my bivariate polynomial.

And, this k could be any k different from the first $t + 1$ X univariate polynomials and lying or belonging to the set of pair-wise consistent X univariate polynomial. So, you were given many pair-wise consistent X univariate polynomials may be more than $t + 1$ you have utilized the first $t + 1$ to interpolate the bivariate and now, I have shown is that if I use the remaining if I focus on the remaining pair-wise consistent X univariate polynomials I have shown that well they also lie on this interpolated bivariate polynomial $F(X, Y)$.

So, all in all what we have shown is that all this pair-wise consistent X and Y univariate polynomials lie on a single bivariate polynomial of degree t. We do not care what exactly is the constant term of that bivariate polynomial. What we have shown is that if they are pair-wise consistent and if we have $t + 1$ at least $t + 1$ such pairs of pair-wise consistent univariate polynomials then they lie on a unique bivariate polynomial.

(Refer Slide Time: 19:44)



Pair-wise Consistency Lemma: Demonstration

❑ $\alpha_1, \cdots, \alpha_n$: **distinct, non-zero** elements from $\mathbb{F}$ ❑ $\mathcal{K} \subseteq \{1, \cdots, n\}, |\mathcal{K}| \geq t + 1$

❑ Pairs of **pair-wise consistent** t-degree polynomials $\{f_k(X), g_k(Y)\}_{k \in \mathcal{K}}$

$f_i(\alpha_j) = g_j(\alpha_i)$, **for every** $\underline{i, j \in \mathcal{K}}$ $\quad i, j \notin \mathcal{K}$

$\Rightarrow$ **Unique** (t, t)-degree bivariate polynomial $F(X, Y)$

❖ $F(X, \alpha_k) = f_k(X)$, for every $k \in \mathcal{K}$

❖ $F(\alpha_k, Y) = g_k(Y)$, for every $k \in \mathcal{K}$

❑ $n = 7$, $t = 2$, $\mathbb{F} = (\mathbb{Z}_{11}, +_{11}, \cdot_{11})$ $\quad \alpha_1 = 2 \quad \alpha_2 = 4 \quad \alpha_3 = 5 \quad \alpha_4 = 7 \quad \alpha_5 = 8 \quad \alpha_6 = 9 \quad \alpha_7 = 10$

$\mathcal{K} = \{1,3,6,7\}$

$f_1(X) = 2 + 7X + 7X^2$	$f_3(X) = 5 + 4X + 3X^2$	$f_6(X) = 5 + 2X^2$	$f_7(X) = 9 + 10X + 2X^2$
$g_1(Y) = 8 + 5Y + Y^2$	$g_3(Y) = 1 + 9Y + 7Y^2$	$g_6(Y) = 5 + 9Y + Y^2$	$g_7(Y) = 7Y + 8Y^2$

$f_1(\alpha_1) = g_1(\alpha_1) = 0$	$f_3(\alpha_1) = g_1(\alpha_3) = 3$	$f_6(\alpha_1) = g_1(\alpha_6) = 2$	$f_7(\alpha_1) = g_1(\alpha_7) = 4$
$f_1(\alpha_3) = g_3(\alpha_1) = 3$	$f_3(\alpha_3) = g_3(\alpha_3) = 1$	$f_6(\alpha_3) = g_3(\alpha_6) = 0$	$f_7(\alpha_3) = g_3(\alpha_7) = 10$
$f_1(\alpha_6) = g_6(\alpha_1) = 5$	$f_3(\alpha_6) = g_6(\alpha_3) = 9$	$f_6(\alpha_6) = g_6(\alpha_6) = 2$	$f_7(\alpha_6) = g_6(\alpha_7) = 8$
$f_1(\alpha_7) = g_7(\alpha_1) = 2$	$f_3(\alpha_7) = g_7(\alpha_3) = 4$	$f_6(\alpha_7) = g_7(\alpha_6) = 7$	$f_7(\alpha_7) = g_7(\alpha_7) = 1$

$f_i(\alpha_j) = g_j(\alpha_i)$, **for every** $i, j \in \{1,3,6,7\}$

So, let me demonstrate it for demonstration I take n to be 7 and t to be 2 and I will be performing all the operations over this field $\mathbb{Z}_{11}$. And, since I need seven evaluation points, I have chosen my evaluation points to be 2, 4, 5, 7, 8, 9 and 10. So, you can now see that unlike previous examples where all my evaluation points were continuous that mean they were means one of they were the consecutive evaluation points from the field.

Now, my evaluation points are not consecutive. So, first evaluation point is not 1, not the element 1 it is the element 2 and then I am not taking 3 as one of my evaluation points, but rather I am taking 4 as my evaluation points. But, irrespective of what exactly are my evaluation points the pair-wise consistency lemma always hold.

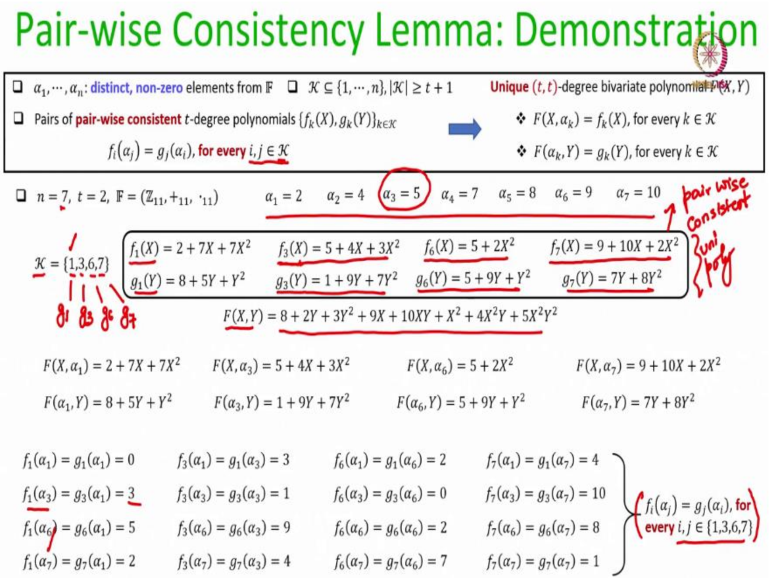
So, these are my seven evaluation points and suppose I take a proper subset of these evaluation points namely, I take this subset of size 4 and I give you four pairs of X and Y

univariate polynomials corresponding to these indices. Now, you can verify that these four pairs of X and Y univariate polynomials they are pair-wise consistent corresponding to the indices in $\mathcal{K}$.

So, I would like to stress when I say they are pair-wise consistent they are supposed to they are know they can be pair-wise consistent only within the indices in the set $\mathcal{K}$. If there is some (i, j) outside the set $\mathcal{K}$ then it is not necessary that the corresponding X and the Y univariate polynomials they are pair-wise consistent, that is not necessary. The condition of pair-wise consistent the pair-wise consistency is given only for every pair of indices within the set $\mathcal{K}$.

So, for instance in this example my set $\mathcal{K}$ has the indices 1, 3, 6, 7; so, that means, when I take the first X polynomial first means is $f_1(X)$ and then if I evaluate it at $\alpha_1, \alpha_3, \alpha_6, \alpha_7$; why $\alpha_1, \alpha_3, \alpha_6, \alpha_7$? Because I have the indices 1, 3, 6, 7.

(Refer Slide Time: 22:42)



Pair-wise Consistency Lemma: Demonstration

❑ $\alpha_1, \cdots, \alpha_n$: distinct, non-zero elements from $\mathbb{F}$ ❑ $\mathcal{K} \subseteq \{1, \cdots, n\}, |\mathcal{K}| \geq t+1$

❑ Pairs of pair-wise consistent t-degree polynomials $\{f_k(X), g_k(Y)\}_{k \in \mathcal{K}}$

$f_i(\alpha_j) = g_j(\alpha_i)$, for every $i, j \in \mathcal{K}$

Unique (t, t)-degree bivariate polynomial $F(X, Y)$

❖ $F(X, \alpha_k) = f_k(X)$, for every $k \in \mathcal{K}$

❖ $F(\alpha_k, Y) = g_k(Y)$, for every $k \in \mathcal{K}$

❑ $n = 7$, $t = 2$, $\mathbb{F} = (\mathbb{Z}_{11}, +_{11}, \cdot_{11})$ $\alpha_1 = 2$ $\alpha_2 = 4$ $\alpha_3 = 5$ $\alpha_4 = 7$ $\alpha_5 = 8$ $\alpha_6 = 9$ $\alpha_7 = 10$

pair wise consistent

$\mathcal{K} = \{1,3,6,7\}$

$f_1(X) = 2 + 7X + 7X^2$ $f_3(X) = 5 + 4X + 3X^2$ $f_6(X) = 5 + 2X^2$ $f_7(X) = 9 + 10X + 2X^2$

$g_1(Y) = 8 + 5Y + Y^2$ $g_3(Y) = 1 + 9Y + 7Y^2$ $g_6(Y) = 5 + 9Y + Y^2$ $g_7(Y) = 7Y + 8Y^2$

uni poly

g_1 g_3 g_6 g_7

$F(X, Y) = 8 + 2Y + 3Y^2 + 9X + 10XY + X^2 + 4X^2Y + 5X^2Y^2$

$F(X, \alpha_1) = 2 + 7X + 7X^2$ $F(X, \alpha_3) = 5 + 4X + 3X^2$ $F(X, \alpha_6) = 5 + 2X^2$ $F(X, \alpha_7) = 9 + 10X + 2X^2$

$F(\alpha_1, Y) = 8 + 5Y + Y^2$ $F(\alpha_3, Y) = 1 + 9Y + 7Y^2$ $F(\alpha_6, Y) = 5 + 9Y + Y^2$ $F(\alpha_7, Y) = 7Y + 8Y^2$

$f_1(\alpha_1) = g_1(\alpha_1) = 0$ $f_3(\alpha_1) = g_1(\alpha_3) = 3$ $f_6(\alpha_1) = g_1(\alpha_6) = 2$ $f_7(\alpha_1) = g_1(\alpha_7) = 4$

$f_1(\alpha_3) = g_3(\alpha_1) = 3$ $f_3(\alpha_3) = g_3(\alpha_3) = 1$ $f_6(\alpha_3) = g_3(\alpha_6) = 0$ $f_7(\alpha_3) = g_3(\alpha_7) = 10$

$f_1(\alpha_6) = g_6(\alpha_1) = 5$ $f_3(\alpha_6) = g_6(\alpha_3) = 9$ $f_6(\alpha_6) = g_6(\alpha_6) = 2$ $f_7(\alpha_6) = g_6(\alpha_7) = 8$

$f_1(\alpha_7) = g_7(\alpha_1) = 2$ $f_3(\alpha_7) = g_7(\alpha_3) = 4$ $f_6(\alpha_7) = g_7(\alpha_6) = 7$ $f_7(\alpha_7) = g_7(\alpha_7) = 1$

$f_i(\alpha_j) = g_j(\alpha_i)$, for every $i, j \in \{1,3,6,7\}$

They should give me the same value as the 1st Y polynomial and the 3rd Y 1 polynomial and the 6th Y polynomial and the 7th Y polynomial evaluated at α_1 and indeed it turns out that this is the case. So, for instance, if I take the first X polynomial this is my first X polynomial and if I evaluate it at alpha 3, alpha 3 is 5; that means, this particular polynomial if I evaluate it at alpha 5 is given to be same as the Y univariate polynomial corresponding to the index 3.

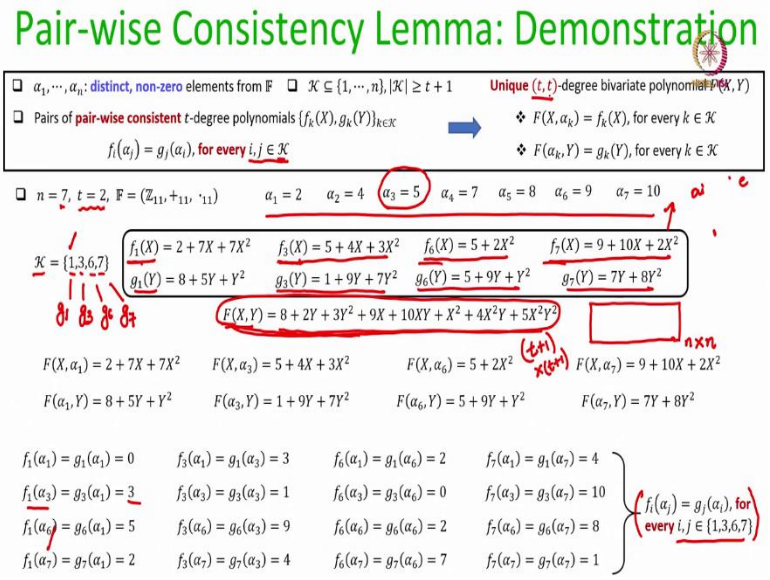
The Y univariate polynomial corresponding to the index 3 is this polynomial and this polynomial evaluated at the first evaluation point namely 2, both these values will turn out to be 3 and we can verify, right. So, I am not going through the calculation here, but you can verify here that $f_i(\alpha_j)$ and $g_j(\alpha_i)$ will be the same values for every (i, j) pair in the set 1, 3, 6, 7 where my evaluation points are 2, 4, 5, 7, 8, 9 and 10. Now using so, these are my pair-wise consistent. These are my pair-wise consistent univariate polynomials and now, we can show that there is a 2-degree bivariate polynomial.

So, this is my 2 degree bivariate polynomial whose first row will be $f_1(X)$ the given $f_1(X)$ and whose first column will be the given $g_1(Y)$ whose third row will be this $f_3(X)$ polynomial and whose third column will be this $g_3(Y)$ polynomial; whose sixth row will be this $f_6(X)$ polynomial and whose sixth column polynomial is this Y univariate polynomial and whose seventh row polynomial is this X univariate polynomial and whose seventh column is this Y univariate polynomial.

You can again verify that I am not going through the whole calculation. So, what we have shown here is that if I. So, by the way I am giving you more than $t + 1$ pairs of pair-wise consistent polynomials here, right. So, I am I have given you four pairs of pair-wise consistent X and Y univariate polynomials, then passing through them I can interpolate a unique bivariate polynomial.

By the way I am not saying anything regarding what will be the second and what will be the fourth and what will be the fifth-row polynomials of this bivariate polynomials because we are not given them we are not given that. We are only given the first, third, sixth and seventh row and column polynomials which are pair-wise consistent.

(Refer Slide Time: 26:33)



Pair-wise Consistency Lemma: Demonstration

- □ $\alpha_1, \cdots, \alpha_n$: **distinct, non-zero** elements from $\mathbb{F}$ □ $\mathcal{K} \subseteq \{1, \cdots, n\}, |\mathcal{K}| \geq t+1$
- □ Pairs of **pair-wise consistent** t-degree polynomials $\{f_k(X), g_k(Y)\}_{k \in \mathcal{K}}$

$f_i(\alpha_j) = g_j(\alpha_i)$, **for every** $i, j \in \mathcal{K}$

→ **Unique** (t,t)-degree bivariate polynomial $F(X,Y)$

- ❖ $F(X, \alpha_k) = f_k(X)$, for every $k \in \mathcal{K}$
- ❖ $F(\alpha_k, Y) = g_k(Y)$, for every $k \in \mathcal{K}$

□ $n = 7$, $t = 2$, $\mathbb{F} = (\mathbb{Z}_{11}, +_{11}, \cdot_{11})$ $\alpha_1 = 2$ $\alpha_2 = 4$ $\alpha_3 = 5$ $\alpha_4 = 7$ $\alpha_5 = 8$ $\alpha_6 = 9$ $\alpha_7 = 10$ α_i

$\mathcal{K} = \{1,3,6,7\}$ g_1 g_3 g_6 g_7

$f_1(X) = 2 + 7X + 7X^2$	$f_3(X) = 5 + 4X + 3X^2$	$f_6(X) = 5 + 2X^2$	$f_7(X) = 9 + 10X + 2X^2$
$g_1(Y) = 8 + 5Y + Y^2$	$g_3(Y) = 1 + 9Y + 7Y^2$	$g_6(Y) = 5 + 9Y + Y^2$	$g_7(Y) = 7Y + 8Y^2$

$F(X,Y) = 8 + 2Y + 3Y^2 + 9X + 10XY + X^2 + 4X^2Y + 5X^2Y^2$

$n \times n$

$(t+1) \times (t+1)$

$F(X, \alpha_1) = 2 + 7X + 7X^2$	$F(X, \alpha_3) = 5 + 4X + 3X^2$	$F(X, \alpha_6) = 5 + 2X^2$	$F(X, \alpha_7) = 9 + 10X + 2X^2$
$F(\alpha_1, Y) = 8 + 5Y + Y^2$	$F(\alpha_3, Y) = 1 + 9Y + 7Y^2$	$F(\alpha_6, Y) = 5 + 9Y + Y^2$	$F(\alpha_7, Y) = 7Y + 8Y^2$

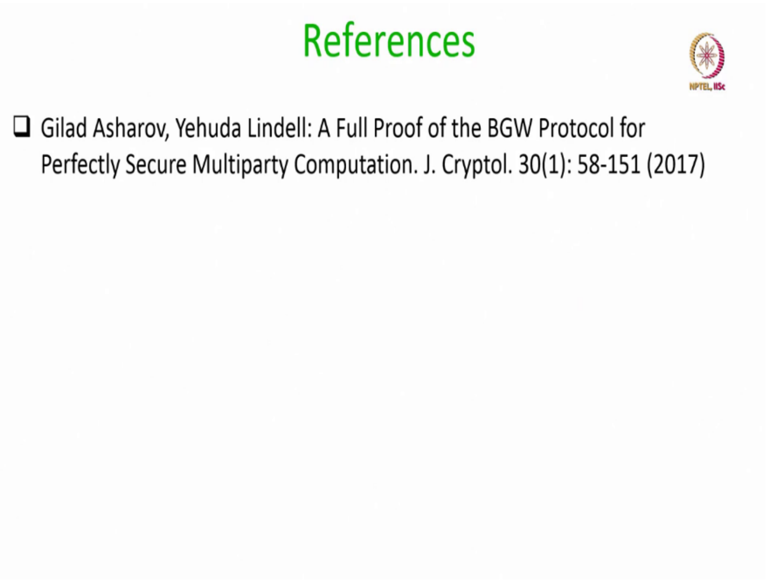
$f_1(\alpha_1) = g_1(\alpha_1) = 0$	$f_3(\alpha_1) = g_1(\alpha_3) = 3$	$f_6(\alpha_1) = g_1(\alpha_6) = 2$	$f_7(\alpha_1) = g_1(\alpha_7) = 4$
$f_1(\alpha_3) = g_3(\alpha_1) = 3$	$f_3(\alpha_3) = g_3(\alpha_3) = 1$	$f_6(\alpha_3) = g_3(\alpha_6) = 0$	$f_7(\alpha_3) = g_3(\alpha_7) = 10$
$f_1(\alpha_6) = g_6(\alpha_1) = 5$	$f_3(\alpha_6) = g_6(\alpha_3) = 9$	$f_6(\alpha_6) = g_6(\alpha_6) = 2$	$f_7(\alpha_6) = g_6(\alpha_7) = 8$
$f_1(\alpha_7) = g_7(\alpha_1) = 2$	$f_3(\alpha_7) = g_7(\alpha_3) = 4$	$f_6(\alpha_7) = g_7(\alpha_6) = 7$	$f_7(\alpha_7) = g_7(\alpha_7) = 1$

$f_i(\alpha_j) = g_j(\alpha_i)$, **for every** $i, j \in \{1,3,6,7\}$

So, intuitively what you can imagine here is that your $F(X,Y)$ is an unknown polynomial and there would have been a matrix of $n \times n$ values on that bivariate polynomial. What I am doing here is I am just focusing on a subset of $(t+1) \times (t+1)$ or more points among this $n \times n$ points which are lying on that unknown bivariate polynomial through this pair-wise consistent row and column polynomials.

And, arguing that also is sufficient to interpolate a unique or define a unique t degree bivariate polynomial.

(Refer Slide Time: 27:17)



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, for this pair-wise consistency lemma I have used this reference.

Thank you.