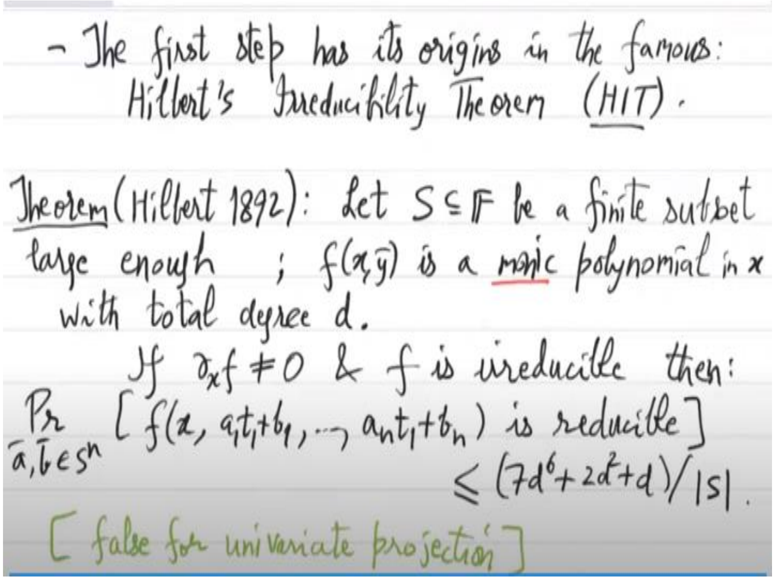
Computational Number Theory and Algebra

Prof. Nitin Saxena
Department of Computer Science and Engineering
Indian Institute of Technology-Kanpur

Lecture – 18
Multivariate Factoring - Hilbert's Irreducibility Theorem

So last time we started Hilbert’s irreducibility theorem.

(Refer Slide Time: 00:23)



- The first step has its origins in the famous: Hilbert's Irreducibility Theorem (HIT).

Theorem (Hilbert 1892): Let $S \subseteq \mathbb{F}$ be a finite subset large enough ; $f(x,\bar{y})$ is a monic polynomial in x with total degree d.

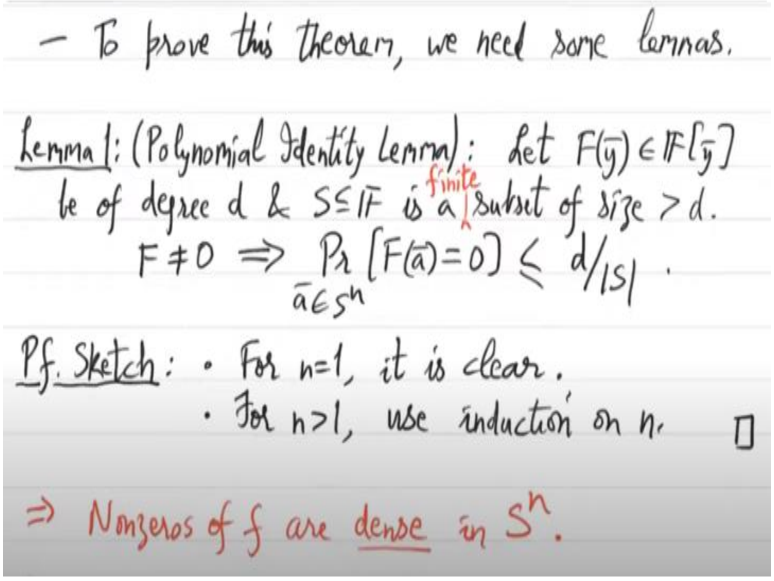
If $\partial_x f \neq 0$ & f is irreducible then:

$$\Pr_{\bar{a},\bar{b}\in S^n}[f(x, a_1t_1+b_1, \ldots, a_nt_1+b_n) \text{ is reducible}] \leq (7d^6+2d^2+d)/|S| .$$

[false for univariate projection]

Which states that if f is irreducible, then when you randomly project it to two variables, any irreducible n-variate polynomial, if you project to two variables in a random way then it will remain irreducible with high probability. So today we will prove this theorem.

(Refer Slide Time: 00:42)



- To prove this theorem, we need some lemmas.

Lemma 1: (Polynomial Identity Lemma): Let $F(\bar{y}) \in \mathbb{F}[\bar{y}]$ be of degree d & $S \subseteq \mathbb{F}$ is a finite subset of size $> d$.

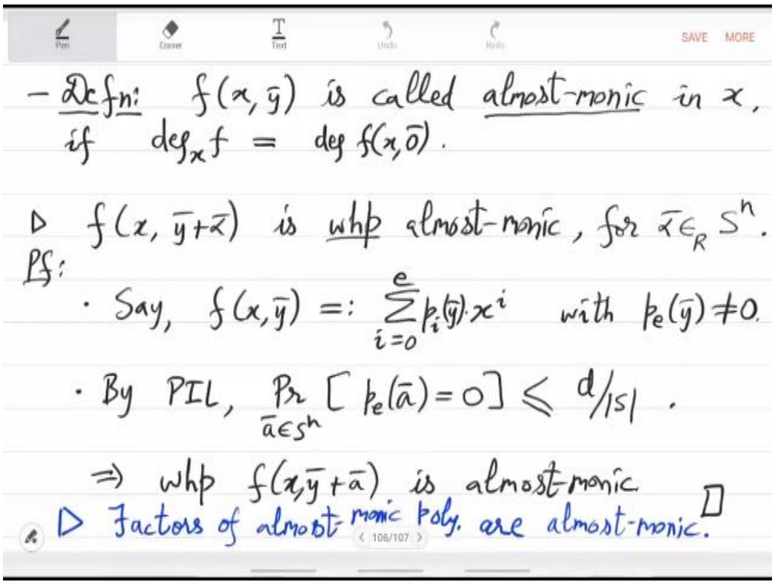
$$F \neq 0 \Rightarrow \Pr_{\bar{a}\in S^n}[F(\bar{a})=0] \leq d/|S| .$$

Pf. Sketch: • For $n=1$, it is clear.
• For $n>1$, use induction on n. □

⇒ Nonzeros of f are dense in S^n.

Recall that the first lemma which we will need is this polynomial identity lemma, which says that, if you have an n-variate polynomial which is nonzero, then on random evaluations, it the probability of it becoming zero is very low, okay? To be precise, it is the degree divided by the sample space. We skipped the proof. The proof is easy to give using induction on the number of variables.

(Refer Slide Time: 01:16)



- Defn: $f(x,\bar{y})$ is called almost-monic in x, if $\deg_x f = \deg f(x,\bar{0})$.

▷ $f(x,\bar{y}+\bar{\alpha})$ is whp almost-monic, for $\bar{\alpha} \in_R S^n$.

Pf:

· Say, $f(x,\bar{y}) =: \sum_{i=0}^{e} h_i(\bar{y})\cdot x^i$ with $h_e(\bar{y}) \neq 0$.

· By PIL, $\Pr_{\bar{a}\in S^n}[h_e(\bar{a})=0] \leqslant d/|S|$.

$\Rightarrow$ whp $f(x,\bar{y}+\bar{a})$ is almost-monic. □

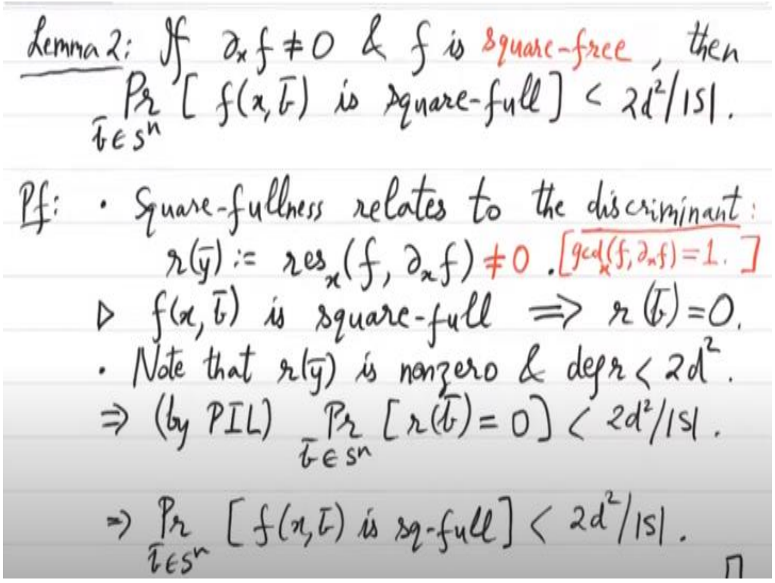
▷ Factors of almost-monic poly. are almost-monic.

Second thing we needed is we will assume that our multivariate polynomial has a key variable x. And n other variables, we will call them y 1 to y n. And we will assume that this is an almost monic polynomial, which means that if you look at it with respect to x, then the leading x monomial, its coefficient will be now a polynomial in y bar in the variables y 1 to y n.

And if you set them to zero the coefficient will not vanish. So the leading coefficient mod y 0 is nonzero. In other words, the degree of the polynomial f does not change when you set y 1 to y n to zero. This almost monic property can be ensured quite easily given any polynomial. So what you can do is if your polynomial is not almost monic then you can just shift the variables y 1 to y n by a random point and you can show by using this polynomial identity lemma that it will become almost monic.

Also we noted that factors of almost monic polynomials are themselves almost monic. So now gradually we will move towards the proof of Hilbert’s irreducibility theorem. So in that direction, the next lemma that we will do is as follows.

(Refer Slide Time: 02:57)



Lemma 2: If $\partial_x f \neq 0$ & f is square-free, then $\Pr_{\bar{b}\in S^n}[\, f(x,\bar{b})$ is square-full$\,] < 2d^2/|S|$.

Pf: • Square-fullness relates to the discriminant:

$r(\bar{y}) := res_x(f, \partial_x f) \neq 0$. $[\gcd_x(f,\partial_x f)=1.]$

▷ $f(x,\bar{b})$ is square-full $\Rightarrow r(\bar{b})=0$.

• Note that $r(\bar{y})$ is nonzero & $\deg r < 2d^2$.

$\Rightarrow$ (by PIL) $\Pr_{\bar{b}\in S^n}[r(\bar{b})=0] < 2d^2/|S|$.

$\Rightarrow \Pr_{\bar{b}\in S^n}[\, f(x,\bar{b})$ is sq-full$\,] < 2d^2/|S|$.

$\square$

So if the derivative of f is nonzero and f is irreducible then if you randomly evaluate f the probability that it is square-full, this probability is small. This is less than 2d square divided by the size of the sample space, okay. So assuming a non-vanishing derivative and irreducibility we can show that random fixing of y bar keeps the polynomial square-free. So the way we will show this is recall that square freeness or square fullness relates to the discriminant of f.

So what is the discriminant? Discriminant is defined as the resultant of f with the derivative with respect to x, okay. So when you do that, then x gets eliminated and you get a polynomial in y 1 to y n. That is called discriminant. So recall that by the properties of resultant recall that f with y bar fixed to b bar is square-full if and only if b bar is the root of the discriminant, okay.

So what this is saying is that the way to interpret it is that when you are fixing the variables y 1 to y n and if suppose your polynomial become square-full then this means that b bar that you have picked is a root of the discriminant r and now you can invoke the polynomial identity lemma which says that this is a very rare event, okay. So first note that the resultant is nonzero. Why is it nonzero?

It is nonzero because you have assumed that the derivative was nonzero, okay. So and f obviously is nonzero. So, then the resultant is nonzero. Both of them, f depends on x actually, and it is almost monic. So the discriminant is nonzero because of almost monic and derivative nonzero, okay. So because of these two properties, you can check that r will be nonzero.

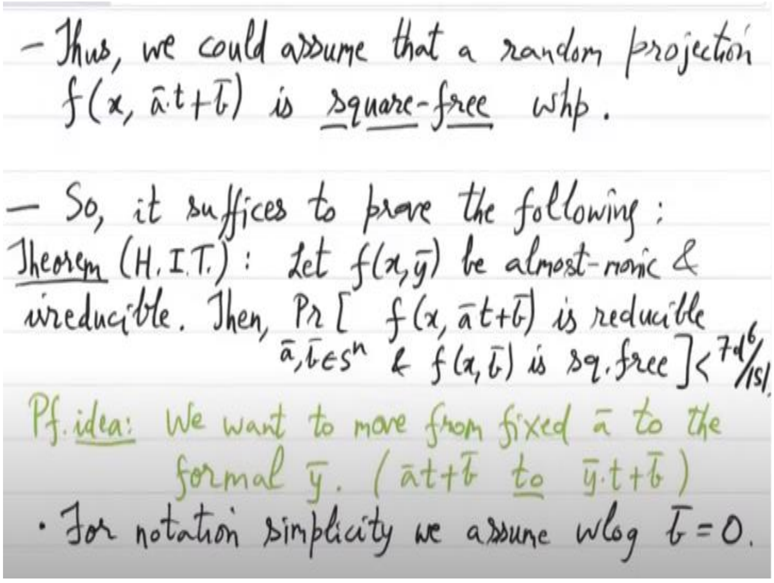
So r is a nonzero polynomial, r is nonzero and its degree is less than 2d square, right. That is again property of the resultant. It says below 2d square actually. So then by the polynomial identity lemma what you can deduce is probability, if you pick b bar from x to the n space, then r b bar being zero or b bar being a root of r, this is a low probability event. It is 2d square by s, okay.

But, so this is in particular also implies that this is the same as saying that the probability over b bar in s to the n space, f being square-full. This is low probability, 2d square by s, right? That is what you wanted to show. Note that we could have actually instead just assumed that f is square-free. You do not need, yes you do not need irreducibility. Actually square freeness is enough.

So where did we need? So r is nonzero, degree is less than 2d square. Okay, let me keep it. So in fact, we should have said that there is something stronger that we are using. Let me correct it. So the reason why this was nonzero is because the GCD of f and the derivative is 1 with respect to x, okay. This is true if you assume f to be square-free. So if f is a square-free with nonzero derivative, these two properties will give you the discriminant to be nonzero.

That is what we used here. So if you start with these two properties then at random fixing of y bar you will get with high probability. You will preserve the square freeness. Okay.

(Refer Slide Time: 11:18)



- Thus, we could assume that a random projection $f(x, \bar{a}\cdot t+\bar{b})$ is <u>square-free</u> whp.
- So, it suffices to prove the following:

<u>Theorem</u> (H.I.T.): Let $f(x,\bar{y})$ be almost-monic & irreducible. Then, $\Pr_{\bar{a},\bar{b}\in S^n}[\, f(x,\bar{a}t+\bar{b})$ is reducible & $f(x,\bar{b})$ is sq. free $] < 7d^6/|S|$

Pf. <u>idea:</u> We want to move from fixed $\bar{a}$ to the formal $\bar{y}$. ($\bar{a}t+\bar{b}$ <u>to</u> $\bar{y}\cdot t+\bar{b}$)

- For notation simplicity we assume wlog $\bar{b}=0$.

So thus from now on we will make the assumption that a random projection f x, a bar times one variable new variable t plus b bar is square-free with high probability, okay. This is because, you can if you even if you just look at t = 0 case x, b bar f x, b bar is square-free with high probability and so with the variability it will continue to be square-free.

So we can, since we are using random projections we can assume from now on that this f at x, a bar t plus b bar is indeed square-free. So let us then look at the version of irreducibility theorem that we will prove or that we need to prove. So it suffices to prove the following. So let f be almost monic and irreducible.

So in that case, when you randomly project, so a bar, b bar from the space s to the n, then f x, a bar t plus b bar, the chance that it is reducible, okay, chance that it is reducible and square-free, okay. So since you started with an irreducible polynomial you would expect that this probability will be low, okay. Probability is lower than something like this 7d 6 divided by the sample space size.

So if you take the sample space slightly bigger, let us say d to the 7, okay a 7 times d to the 7, then this probability is quite low. So when you randomly project to this univariate a bar t plus b bar your irreducible polynomial remains irreducible. In addition, actually this x, b bar remains square-free. Okay, you have both the properties. So let us try to show this now. It will immediately imply the Hilbert’s irreducibility theorem that was stated in the last class.

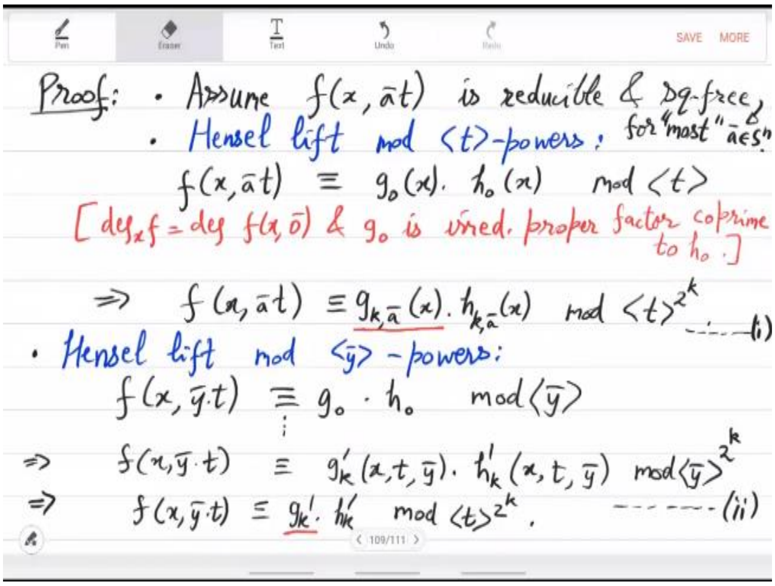
So this is a slightly technical proof in terms of notation. But, the idea will be that we will try to factorize f, projected f using Hensel lifting in two different ways, okay. So one way will be you look at this mod t. So mod t it is a univariate, there is a factorization and then you lift it to mod t square, t 4 and so on. The other way to start Hensel lifting will be that you replace a bar by f by the formal variables.

Okay y 1, instead of a bar you use y bar. And that you look at first mod y bar. Then the ideal mod y bar square and so on. Okay, so there will be two branches of Hensel lifting or two different ways of doing Hensel lifting. One is mod t powers and other is mod y bar powers. So this will be clear when we work, when we implement this idea.

So the idea is, so the idea is that this you have some information about this projection a bar t plus b bar that if say for example, assuming assume that f reduces. So from this information, how will you go to formal y bar, okay? So that jump from fixed a bar to formal y bar, that jump will happen through Hensel lifting in two different ways. So we will do that next. Okay. So also for simplicity, we will assume b bar to be 0.

We can assume without loss of generality that b prime is 0 just to make the notation a bit simpler that is all. Okay, so let us do this.

(Refer Slide Time: 19:13)



Proof: • Assume $f(x,\bar{a}t)$ is reducible & sq-free, for "most" $\bar{a} \in S^n$.

• Hensel lift mod $\langle t\rangle$-powers:

$$f(x,\bar{a}t) \equiv g_0(x) \cdot h_0(x) \mod \langle t\rangle$$

[$\deg_x f = \deg f(x,\bar{0})$ & g_0 is irred. proper factor coprime to h_0.]

$$\Rightarrow f(x,\bar{a}t) \equiv \underline{g_{k,\bar{a}}(x)} \cdot h_{k,\bar{a}}(x) \mod \langle t\rangle^{2^k} \quad \text{------ (i)}$$

• Hensel lift mod $\langle\bar{y}\rangle$-powers:

$$f(x,\bar{y}\cdot t) \equiv g_0 \cdot h_0 \mod \langle\bar{y}\rangle$$

$$\vdots$$

$$\Rightarrow f(x,\bar{y}\cdot t) \equiv g'_k(x,t,\bar{y}) \cdot h'_k(x,t,\bar{y}) \mod \langle\bar{y}\rangle^{2^k}$$

$$\Rightarrow f(x,\bar{y}\cdot t) \equiv \underline{g'_k} \cdot h'_k \mod \langle t\rangle^{2^k} . \quad \text{------ (ii)}$$

So assume that start with the assumption that f x, a bar t is reducible and square-free. Okay, so that is the basically the event which you want to claim, which we are claiming in the theorem statement to be rare, low probability event. So let us assume that event happens. So then we do Hensel lifting mod t powers. So do Hensel lifting. So when you do this, what is the first step?

First step is x, a bar t mod t factorizes into univariates in x. Let us say g 0 x, h 0 x mod t. Since we have assumed x, b bar which is x, 0 bar to be square-free that is a very important property because now you know that g 0 and h 0 are coprime, okay. So this is a coprime factorization and we can assume g 0 to be irreducible. So let us remember that. So degree of f is degree of f x, 0 bar. And g 0 bar is an irreducible proper factor coprime to h 0, right.

That is the starting point of the Hensel lifting, Hensel lifting number 1. So this will then imply that f x, a bar t after k times will give you g k x times h k x mod t to the 2 to the k. Okay, let us call this equation 1. So this is what you get starting from g 0 and then repeating this Hensel lifting k times. That is one way. Now let us do something different. So Hensel lift mod y bar powers, okay.

So what will that root give you? So f x, y bar t. What is it mod y bar? So the amazing thing here is that mod t, mod y bar is the same starting point. Okay, so mod t, you were looking at f x, 0 bar. And here in the new setting, also mod y bar you are looking at f x, 0 bar. So it is the same starting point. So you can use g 0 as before. And then when you do Hensel lifting what you will get is you will get let us say g k prime, which is a polynomial in everything, right?

So it is a polynomial in x in t and in y bar. And you will get h k prime polynomial in x, t, y bar modulo what? So this is modulo y bar to a large power 2 raised to k, right? That is your endpoint of the second type of Hensel lifting. Now we ask the question, what is the relationship between 1 and 2, right? So intuitively, second Hensel lifting should be the functional version of the first Hensel lifting, right?

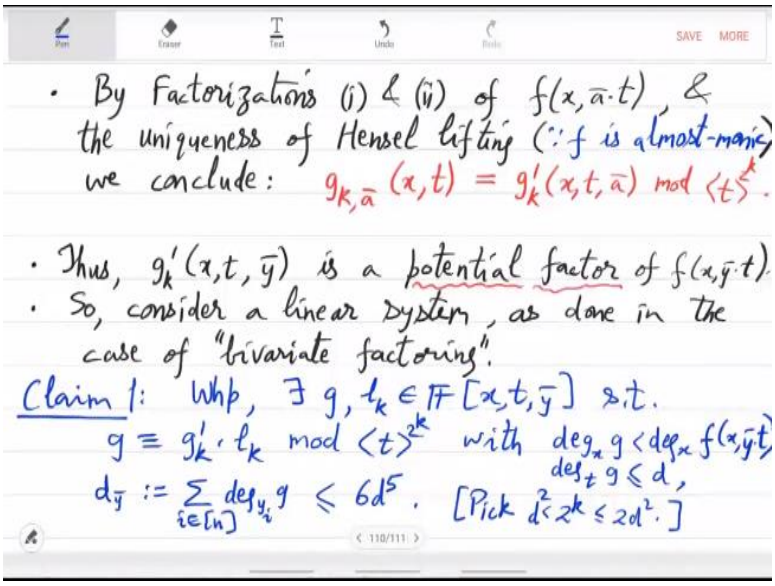
So in the second Hensel lifting you have this y bar hanging around. If you fix it to a bar, then intuitively it should give you equation number 1, factoring number the factorization number 1. But we do not know for sure, right. So we have to if this is true, we have to actually prove it, okay. So let us write one more equation, which is f x, y bar t factorizes as g k prime h k prime mod also t raised to 2 raised to k.

This also follows from the above factorization because note that y 1 to y n we are multiplying each of these variables with t, right. So if you set t raised to 2 raised to k to 0 that will be like setting this y bar to, monomials in y bar of degree 2 raised to k to 0. It is actually equivalent. Okay, so we actually have, now we have factorization 1 and factorization 2 in the same modulus, right.

We have mod t raised to 2 raised to k in both the moduli. In one we have g k h k. In one we have g k in the other we have g k prime. And in one we have a bar, in other we have y bar. Okay, that is the, that is how we read this. So what is the connection between g k and g k prime? So note that here we can invoke the uniqueness of Hensel lifting mod t raised to 2 raised to k, okay.

g k and g k prime both of them are almost monic and for almost monic factors there is a there is this strong uniqueness property of Hensel lifting factorization. So we can actually invoke that. So what will that give you?

(Refer Slide Time: 28:17)



- By Factorizations (i) & (ii) of $f(x, \bar{a}\cdot t)$, & the uniqueness of Hensel lifting ($\because f$ is almost-monic) we conclude: $g_{k,\bar{a}}(x,t) = g_k'(x,t,\bar{a}) \bmod \langle t\rangle^{2^k}$.

- Thus, $g_k'(x,t,\bar{y})$ is a potential factor of $f(x,\bar{y}\cdot t)$.
- So, consider a linear system, as done in the case of "bivariate factoring".

Claim 1: Whp, $\exists\, g, \ell_k \in \mathbb{F}[x,t,\bar{y}]$ s.t. $g \equiv g_k' \cdot \ell_k \bmod \langle t\rangle^{2^k}$ with $\deg_x g < \deg_x f(x,\bar{y}t)$, $\deg_t g \leq d$,

$d_{\bar{y}} := \sum_{i\in[n]} \deg_{y_i} g \leqslant 6d^5$. [Pick $d^2 < 2^k \leq 2d^2$.]

So by factorizations 1 and 2 of f x, a bar t and the uniqueness of Hensel lifting since f is almost monic we conclude. So what do we conclude? We conclude that, so let me change the notation slightly to include a bar here. So we will conclude that this g k a bar and g k prime, okay they are the same if you fix y bar. That is what we conclude. So g k a bar at x, t is equal to g k prime at a bar mod t raised to 2 raised to k.

Okay, that is the relationship. So this is the crux of the proof. This is what you should understand and remember that we factorized one in with a bar fixed mod t raised to 2 raised to k and other was with a bar with instead of a bar using the functional version which is y bar mod t raised to 2 raised to k.

We got this fixed and the functional type of factorization and then by uniqueness of Hensel lifting factorization for monic factors we deduce that they are equal for y bar equal to a bar, okay. So but still we are not really done right because this factorization or this g k prime is happening only mod t raised to 2 raised to k, right. What does it tell us about f?

So remember that in the original theorem statement we have to say something about f whether f projected being reducible implies that the original f is reducible, right. So we have to now move to original f. So for that let us just recall that g k prime x, t, y bar is a potential factor of f x, y bar t, right. But we do not know whether it actually divides f x, y bar t exactly.

So in these situations or in this situation we will do what we did before. So recall the case of bivariate factoring. So in bivariate factoring, we were in a similar situation. We had a potential factor mod ideal power and we wanted to deduce an actual factor. So what did we do? We solved a linear system. So consider a linear system as done in the case of bivariate factoring, okay. So let us move to that now.

So claim is that with high probability there exist polynomials g and l k in all these variables x, t, y bar such that g is a multiple of l k and g k, g k prime mod t raised to 2 raised to k with the degree restrictions, okay. So what is that? So for g the degree restriction is that degree of g with respect to x is smaller than that of f and degree of t is smaller than at most d, okay.

This is expected because or this is natural, it is intuitive, because we hope to just like in the case of bivariate factoring, we hope that this g k prime will be associated via multiplication by a product associated to a factor g of f x, y bar t. So the degree of it with respect to x should be strictly smaller. And if you look at the degree of g respect to t and also y bar actually, it should be it cannot exceed d, okay.

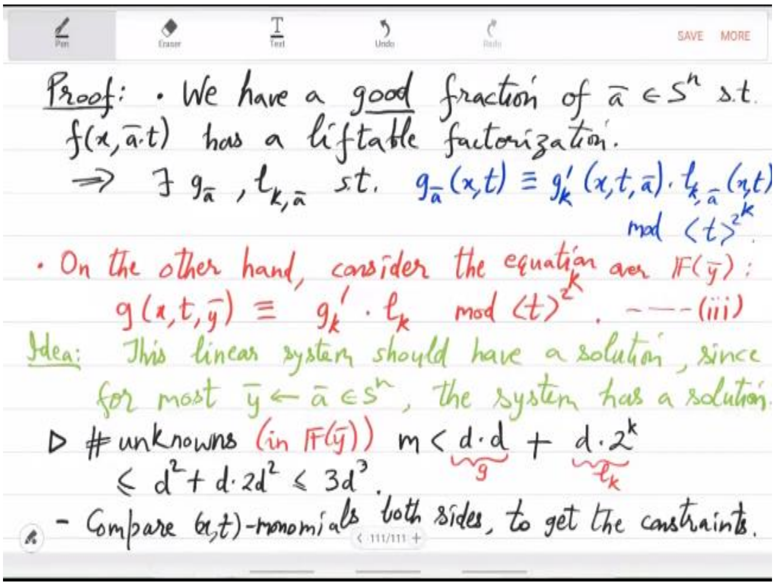
That is one thing. But for y bar, it is a bit more complicated because there are many variables, right. There are there is y 1 to y n. So let us write that down. So degree of g with respect to y bar is what? It is degree of so I am defining the degree of g. Yeah that is bad notation. Let me change it slightly. We will call it d prime. Let me call it d prime, which is actually degree of g with respect to y i for all i and just sum it up.

This, yeah the intuition of this is not clear, we will see in the calculation. So we will claim that this will be at most 6d 5, okay? So that is the claim we are making. We are saying that this g k prime itself may not be dividing f x, y bar t. But there is some multiple of it which can be found by solving a linear system where the degrees are like this. So degree with respect to x is strictly smaller than that of f.

Degree with respect to t is less than equal to that of f. And the individual degrees of g with respect to y i they sum up to this 6d 5. So actually, this g may not, this g may still not divided f. What we will do, once we have shown this claim is that we will actually take its GCD with f, like we did in the bivariate case, and we will show that the GCD will divide f, okay.

So this is a mysterious polynomial g. So let us prove this claim first. It is similar to slight it is similar to what we did in bivariate, but slightly more complicated because of n being arbitrary here.

(Refer Slide Time: 39:45)



<u>Proof:</u> • We have a <u>good</u> fraction of $\bar{a} \in S^n$ s.t. $f(x, \bar{a}\cdot t)$ has a liftable factorization.

$\Rightarrow \exists\, g_{\bar{a}}, \ell_{k,\bar{a}}$ s.t. $g_{\bar{a}}(x,t) \equiv g_k'(x,t,\bar{a}) \cdot \ell_{k,\bar{a}}(x,t) \mod \langle t \rangle^{2^k}$.

• On the other hand, consider the equation over $\mathbb{F}(\bar{y})$:

$$g(x,t,\bar{y}) \equiv g_k' \cdot \ell_k \mod \langle t \rangle^{2^k}. \quad \text{---(iii)}$$

<u>Idea:</u> This linear system should have a solution, since for most $\bar{y} \leftarrow \bar{a} \in S^n$, the system has a solution.

▷ # unknowns (in $\mathbb{F}(\bar{y})$) $m < \underbrace{d \cdot d}_{g} + \underbrace{d \cdot 2^k}_{\ell_k}$ $\leq d^2 + d \cdot 2d^2 \leq 3d^3$.

- Compare (x,t)-monomials both sides, to get the constraints.

So the first thing that we will do is use this random a bar property that we had before. So we know that we have a good fraction of a bar such that f x, a bar t has a liftable factorization. Actually why is that? Why is that fraction good? Let us go back. Just take a step back and try to understand this. So what we are actually assuming is the opposite of what we want to show that for most of the a bar b bar, f x, a bar t plus b bar is reducible, okay.

And then because it is reducible so you can and because x, b bar f x, b bar is square-free so you can Hensel lift. So that is what we are reading off. So that actually I should add here, is reducible and square-free greater for greater than equal to that much fraction for most a bars. Actually that is what our assumption, starting assumption. So we will actually use this part now.

That for most a bar whatever we have done is actually true. So which means that for a good fraction of a bars, x, a bar t has a liftable factorization which implies that there exist g a bar and l k, a bar such that g a bar x, t is g k prime x, t a bar times l k, a bar. So how is this happening? Well, this is just the same equation that we get by Hensel lifting say in the second way, right.

So in the second way you got this f x, y bar t factorizes as g k prime. And then you also then we also showed that g k prime in fact, when you fix y bar to a bar it is g k a bar. So that those properties which we have shown we are using them now. Okay, this red equation we are now using. It is true for most a bars. Okay and the remaining part we are just calling it l, right. It was g k prime times h k prime.

But that remaining thing we are calling now l. So this is just a reformulation. So and you can see easily that this degree of g a bar with respect to t varies at most d because this is actually a factor, univariate factor which we lifted. So the degree is bounded by d. Now on the other hand, let us make it now let us make a bar formal. Yeah, so on the other hand consider the equation g x, t, y bar g k prime x, t, y bar times.

So let us remove the variables. It is disturbing. g k prime times l k mod t raised to 2 raised to k. Consider this equation in red and consider the equation above in blue. So for the red equation, you know that if you fix y bar equal to a bar for many a bars for in fact most of the a bars, the linear system has a solution, right. So intuitively it should also have a solution without fixing y bar.

That is the key idea, okay. This is why we have been trying to connect y bar with a bar. So it should have a solution as or since for most y bar fixed to a bar the system has a solution, okay. This idea in green is the is the key thing that we wanted to get at. So we have these two linear systems. And the red one is the main one the functional one. For it to have a solution it takes actually enough if it is random fixings have a degree bounded solution.

So now all that remains is to formally prove this. So for that we will basically convert this linear system into a matrix and the proof will basically boil down, right. So let us just now implement this idea or show that this is what is actually happening. So this linear system how many unknowns are there? So number of unknowns, let me first specify here that we are thinking of unknowns as polynomials or functions in y bar, right.

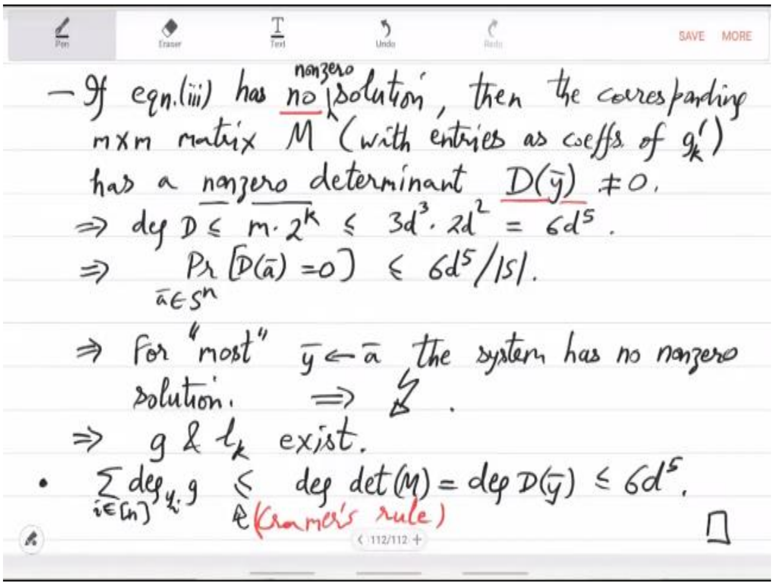
So g k prime is a polynomial in x, t and y bar. We want to find g and l k. So let us view them as bivariates. So x, t with the coefficients being functions or polynomials in y bar. So in that sense how many unknowns are there? So that number is easy to compute. So degree of x is what, at most d, right? And degree of t in this equation is also at most d. That is because of what you know about g k prime and the type of g and l that you are looking for.

Let me take that back now. So for g it is d times d, is d times d. For g, for l k degree of x is yeah it is at most d. But degree of t may go up to 2 raised to k – 1. Okay, that is the bound. So this is for g and this is for l k. So then the then we can estimate it like as follows. Okay, I did not tell you what k is, how big k should be? So let me add that. So I will be needing it to be between d square and 2d square, okay.

I am assuming k to be something like 2 log d, okay. So with that, it is d square plus d times 2d square which is so that is cannot exceed 3d cube. So number of unknowns in this bivariate system is at most 3d cube. So let us call this number of unknowns m. Okay. Yeah, and note that this red equation is actually a homogeneous equation, it is a homogeneous linear equation in these unknowns, right.

So you get kind of this m cross m matrix when you compare x t monomials both sides to get constraints. Yeah, but why would it have a nonzero solution, right. So for that we will rely on the random fixing of y bar. We know that if we randomly fix y bar then there is a solution always. So from that you can deduce that for formal y bar also there has to be a solution. Because if there is none then what happens?

(Refer Slide Time: 54:13)



– If eqn.(iii) has no nonzero solution, then the corresponding $m \times m$ matrix M (with entries as coeffs. of g_k') has a nonzero determinant $D(\bar{y}) \neq 0$.

$\Rightarrow \deg D \leq m \cdot 2^k \leq 3d^3 \cdot 2d^2 = 6d^5$.

$\Rightarrow \Pr_{\bar{a} \in S^n}[D(\bar{a}) = 0] \leq 6d^5/|S|$.

$\Rightarrow$ For "most" $\bar{y} \leftarrow \bar{a}$ the system has no nonzero solution. $\Rightarrow$ ↯.

$\Rightarrow$ g & l_k exist.

- $\sum_{i \in [n]} \deg_{y_i} g \leq \deg \det(M) = \deg D(\bar{y}) \leq 6d^5$.

(Cramer's rule)

□

So if equation 3 has no solution then the corresponding m, small m cross small m matrix M. So what are the entries of this matrix? Entries are coefficients of g k prime.

So then this corresponding matrix M has a nonzero determinant, right. It is a homogeneous equation. If it does not have a solution, nonzero solution, then this means that the matrix M is actually invertible.

So when you compute its determinant, let us call it so the matrix M has coefficients of g k prime right and those are all polynomials in y bar. So the determinant is also a polynomial in y bar. So that is nonzero. Its degree is given by the dimension which is m times each entries degree, which in turn depends on the degree of g k prime in y bar right, which is 2 raised to k at most.

So what is m? m is at most 3d cube and what is 2 raised to k? That is at most 2d square. So you get 6d 5. So d is nonzero and it has degree at most 6d 5. So the probability that it vanishes for a random fixing of y bar, that is quite small, right. So for random a bars, also the same property will then continue. So for random a bars also there will be no nonzero solution, which you know is not the case, right.

That is a contradiction. So this contradiction finally gives you that g and l k exist. Degrees restrictions or degree bounds which we were claiming in the statement of claim 1, degree of g with respect to x and t is clear. It is clear because here in this equation in blue, those are the g k prime x, t, a bar that you had, right. So both x and t the degree bounds you have we continue to have. About y bar you have to deduce.

So that you can deduce as follows. So sigma degree of g y i, i 1 to n this is what? So this will really depend on the degree of the determinant, okay. Because remember that you have a homogeneous linear system. So the solutions will actually, solutions of this linear system they will actually be given by ratio of determinants. So we can safely say that all this is at most degree of the determinant of M, degree of d y bar which is at most 6d 5 as shown above.

So this is by Cramer's rule, okay. So what we have shown is that claim 1 which says that g and l k will exist in this restricted degree. g and l k will exist and they will have restricted degree. And the hypothesis was that f is factoring for most of the y bars equal to a bar setting, right. That is what we started with. So if f x, a bar t factors for most a bar, then we have shown that Hensel lifting will give you this g k prime for most a and from that we have deduced that you will get a g k prime with formal y bar also.

And from that you will get a g. So next time what we will do is that, we will just take the GCD of g with f, okay and that will actually factor f. And factoring f means you get a contradiction, okay. That is our, you get a contradiction or you get that f is actually reducible, okay. So if f is reducible for most y bar equal to a bar setting then it is actually reducible. So reducibility implies reducibility. So let us do this in the next lecture.