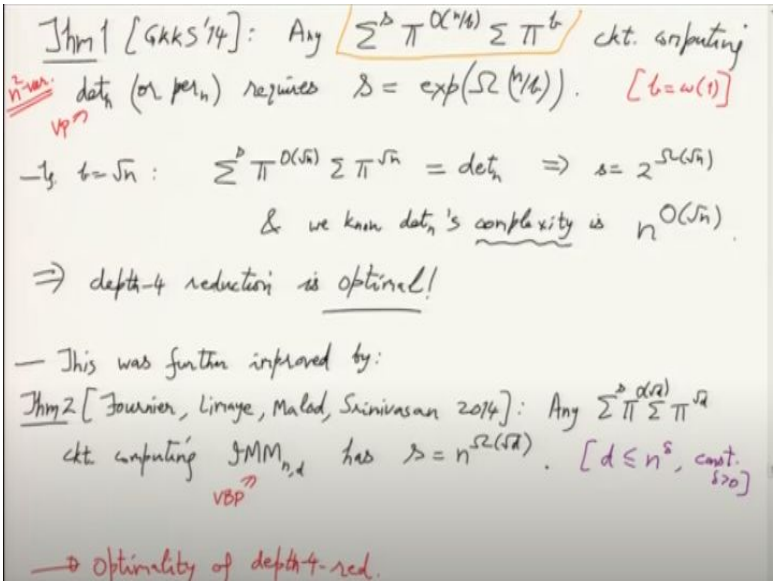
Arithmetic Circuit Complexity
Prof. Nitin Saxena
Department of Computer Science and Engineering
Indian Institute of Technology-Kanpur

Lecture - 21

So last time we proved this theorem by GKKS 2014.

(Refer Slide Time: 00:18)



Which is for the depth-4 model where both the product fanins are restricted. So the bottom product fanin is b and the top product fanin is n/b and we intend to produce a polynomial of degree n. And the number of variables will be n^2. So that it is an anomaly. So here the number of variables is actually different because this is for the determinant. So it is an n^2 variate degree and model. Product fanins are restricted.

So with these assumptions, we showed that the size required or even the product gates required in the top this is $2^{n/b}$, okay. So if you take b to be $\sqrt{n}$ and the balanced version, then you get $2^{\sqrt{n}}$ and you know a construction $n^{\sqrt{n}}$. So this is nearly an optimal lower bound and hence the depth-4 reduction is also optimal.

So this requires the new tool of shifted partials. The result was followed by many others in particular so this was further improved by a result where the polynomial was

changed. So instead of determinant they use something else which is basically iterated matrix multiplication. Determinant is also in VP, right? It is a VP polynomial.

So what this result is showing is that a VP polynomial which is hard for this model, right. So this is still away from the original goal of VP versus VNP. So we are already starting with a kind of easy polynomial, a VP polynomial. And the same thing in this result also but it will be iterated matrix multiplication, it is again in VP. So theorem 1, theorem 2 is by Fournier, Limaye, Malod and Srinivasan.

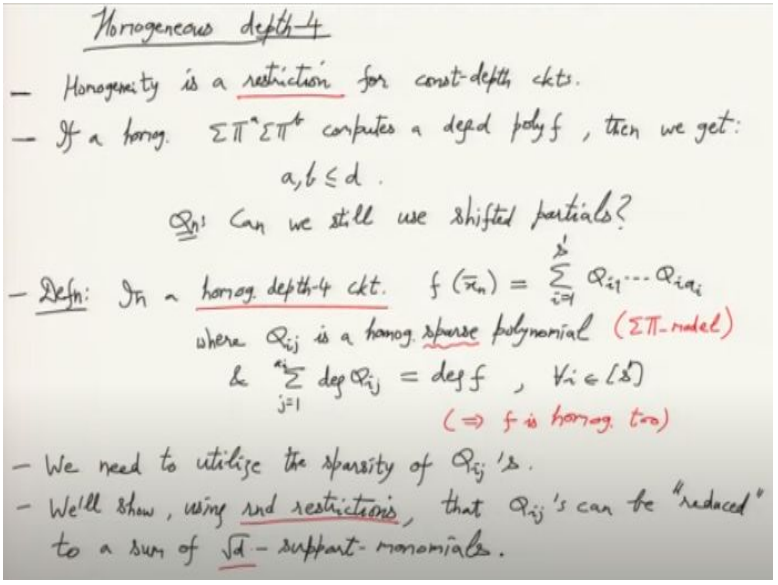
So any $\Sigma^s\Pi^{O(\sqrt{d})}\Sigma\Pi^{\sqrt{d}}$ circuit computing $IMM_{n,d}$. So n by n matrices and d many. So degree is d of the polynomial. Number of variables is n^2d. So for this polynomial the size s= $n^{\Omega(\sqrt{d})}$. So improvement is in the base. So instead of $2^{\Omega(\sqrt{d})}$ now you are getting $n^{\Omega(\sqrt{d})}$ which is truly optimal.

So you can actually write an iterated matrix multiplication as $\Sigma\Pi\Sigma\Pi$ model in $n^{O(\sqrt{d})}$ and you cannot do any better. So depth-4 reduction is truly optimal. That is what you get. Because this is in VBP. So it is an even simpler polynomial. So this is a stronger result. The technique the same? Yes. You have to prove a lower bound for IMM. That needs more specialized analysis. There is some assumption on d.

So d is assumed to be n^{δ} for small δ. So these δ will be chosen accordingly in the proof. So ultimately d will be some n to the some fraction. That is not very important. The result you will get will be $n^{\Omega(\sqrt{d})}$ and you also have a circuit of this size. Any questions? So that shows the optimality.

So I will not prove this because this will again be a very specialized analysis just like what we did with the shifted partials of determinant. Here you have to do it on IMM. We will skip this, but it can be read. Yeah that is s, s is the top fanin in this because the proof method is like that. In the upper bound you get s $\times$ something, s is the top fanin. Okay, so now we will move to another result which will require us to change the measure a bit.

(Refer Slide Time: 06:58)



So this will be homogeneous depth-4 model. So using these techniques, there have been many results, cover all of them of course, but see the representative ones. So homogeneous depth-4 is by itself also an interesting model and it is a restriction. So when you are looking at constant depth, then it is a restriction. If you look at unrestricted depth, then it is not a restriction.

Because in unrestricted depth you can separate the homogeneous parts by Strassen's homogenization theorem. In constant depth you will not be able to do that.

Student Professor conversation starts: Sorry. **Student:** We just proved that in constant depth we cannot. **Professor:** No, there is an absence of proof. How do you do? Yes, so in that, in the way you extract the homogeneous parts. **Student:** In that circuit, you look at the original circuit and build up at each node, computing the homogeneous parts, computed at each node. It is like, depth is almost like, copy the circuit, but little bit different. **Professor:** So you are saying that the depth does not change? **Student:** I mean, yeah. If it does not change, it definitely does not increase. **Professor:** By how much? **Student:** We have to prove that it will increase and so we can not depth reduce. **Professor:** No, but can you reduce depth-4 circuit to a homogenous depth-4 circuit? **Student:** Maybe homogeneous depth 8 or something. **Professor:** Exactly. **Student:** Depth 4 is quite compact.

Student Professor conversation ends.

Homogeneity is a restriction. So depth will slightly increase. Homogeneity is a restriction for constant depth. But not for general circuits. So this is a, this is then a different model. It will need a new proof. This result will not follow from the previous result. Because in the previous result we have said that a and b are bounded. I mean a and b are upper bounded by a function that we had fixed.

By homogeneity, you do not get that automatically. So the method has to be different. So if a homogeneous $\Sigma\Pi^a\Sigma\Pi^b$ computes degree a d polynomial f, then we get, so all we can deduce is that $a,\ b \leq d$. We cannot do we cannot claim anything better, right. Because in some product gate, it can be 1 and b is d. In some other product gate it can be the opposite, a is d and b is 1.

So you cannot claim anything better than this. So this is then a and b are kind of very high. So the question is can we still use shifted partials? So the problem with shifted partials is that in its lemma 1 which was the upper bound, you will get a trivial upper bound if you take a b to be d. So that will not see anything special about the model. That has to change. Yeah, just to remind, I think let us define the model properly.

So in a homogeneous depth-4 circuit take it as a definition. In a homogeneous depth-4 circuit $f(\overline{x_n})$ being computed like this $(= \sum_{i=1}^{s} Q_{i1} \cdots Q_{i\,a_i})$ where Q_{ij} is a homogeneous sparse polynomial. I am using the word sparse, but it just, this is just to signify that all the monomials in Q_{ij} will be counted. So whatever monomials appear, they will count. The monomials that do not appear will not be counted.

So the actual support will be counted in the overall size of the model. So Q_{ij} 's are explicitly given, then you multiply them and add them. Okay that computes f, equals f. And the degree of Q_{ij} for a fixed i, this is equal to the degree of f for every i. f also is homogeneous. So that is the definition.

We will take the it is a depth-4 circuit where every factor is homogeneous and in our products, the sum of the degrees of the factors is the degree of the polynomial being computed if. So the addition gates will also be adding up equidegree monomials. So that is our model and you want to get a lower bound for this. There is no previous lower bound; a b is d. Both a and b are d. So right now we have nothing for this model. It seems to be a hard model.

Could you explain why we expect these Q_{ij} to be homogeneous polynomials? Sparse. What do you mean expect? No, this is a definition. There is no expectation. But why sparse, why sparsity is coming? Well sparse just means that if the size is t then there are only t monomials. Sparsity just signifies the fact that the size will include each and every monomial that appears. And do not, we do not count monomials that do not appear. So when we also count them, then sometimes we call that dense polynomial.

Sparse polynomial is basically $\Sigma\Pi$. So formally, we can also think of this as a $\Sigma\Pi$ model. So it is a sum of products and as many products you have that is the size of Q_{ij}. The Q_{ij}'s are depth-2 and then you multiply them and add them so you get depth-4. So those are the things in the definition. And so since we do not have anything about a and b, I mean in general in depth-4 a and b could have been arbitrarily large.

So at least that has been restricted. It is not, it cannot be more than d. But still d is quite large as far as our measure is concerned or measure fields at that regime, in that region. So one thing that we will use in the proof is that Q_{ij}'s have few monomials. That will be used. Yeah so I think I should at this point not use s for the top fanin because s will really be total size in our proof from now on. Let us call it s'.

So now what we will do is if the total size is s, which will also include how many monomials appeared in Q_{ij}. We have to use that fact. We have to use the fact that Q_{ij} has few monomials and then try to do something. Basically in the end we will use

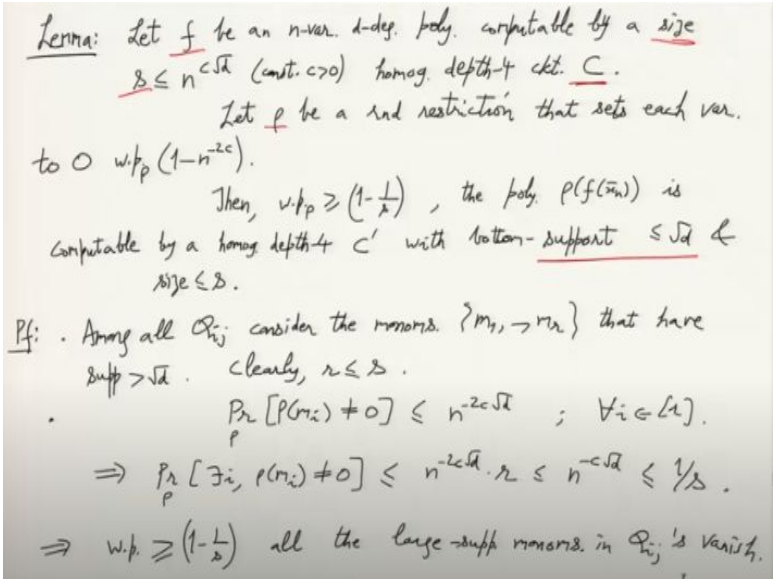
shifted partials after doing some transformations. Since the set of monomials we are assuming is small the union of the support. So we need to utilize the sparsity of Q_{ij} 's.

So for example, there may be a monomial like $x_1 \cdots x_d$. So this is a degree d monomial and it has maximum possible support and this is the reason why b could be d, b could be as high as d. So can you think of a way to reduce b by applying a transformation? When you look at the monomial $x_1 \cdots x_d$, which is making b equal to d, can you think of a transformation that reduces the associated parameter b below d.

We apply the transformation on $x_1 \cdots x_d$ and well essentially some of the variables get killed. So variable restriction, right. So if you try the idea of restricting the variables to constants, then potentially these high supported monomials will become low supported and that will reduce b. So we will try the random restrictions.

So we will show using random restrictions that Q_{ij} 's can be reduced to a sum of $\sqrt{d}$ support monomials. We are basically killing some variables and the advantage will be b will come down to $\sqrt{d}$. And then we can use shifted partials as before. So let us prove that lemma formally.

(Refer Slide Time: 19:56)



First state it. So this is: let f be an n-variate d-degree polynomial computable by a size $s \leq n^{c\sqrt{d}}$ c some constant yet to be fixed and assume that f is a polynomial that is computable in size $s \leq n^{c\sqrt{d}}$ homogeneous depth-4 circuit C. Let ρ be a random restriction that sets each variable to zero with probability $1 - n^{-2c}$ point being that it is a high probability.

So ρ is a random restriction which will set a variable to zero with probability, very close to 1. No, no randomization is just on the bits that ρ uses. When you give x_1 to ρ, it will flip coins to decide whether to set it to zero or leave it free. It is just the biasness of its coins. Not variables. It is over its own randomness. It has nothing to do with the variable. It depends on what it has in its mind. It is not external to it.

So use this process rho on all the variables. So $\rho\, x_1,\ \rho\, x_2,\ \cdots, \rho\, x_n$. The motivating case is again a monomial. So a monomial that has a lot of variables that has an extremely high chance of being set to zero and a monomial that has very few variables will be able to escape from becoming zero. So then with probability greater than equal to $1 - 1/s$. The polynomial $\rho(f(\overline{x_n})$, what is $\rho(f(\overline{x_n})$?

Well ρ of f is just apply a ρ on each variable. So this polynomial is computable by a homogeneous depth-4 C' with bottom product fanin less than equal to $\sqrt{d}$ and size less than equal to s. Okay, so note that now we are talking about size and not just the top fanin. So we are counting the monomials also. So there were overall s monomials that you can see in the circuit C.

And when you apply this transformation ρ then random transformation rho then, with probability $1 - 1/s$ only those monomials will survive that have support $\sqrt{d}$. Actually, this should be not just product fanin but support. It is a stronger thing. So bound on the support of these monomials that you see. That is a weaker thing. Yeah. So support is small, but the individual degrees may still be high.

Yeah, we still have not gotten to b less than equal to $\sqrt{d}$. So b can still be high. We have just reduced the support with this, right. So this is believable. Probabilistically this should happen. Of course, the parameters we have to carefully see , why are we getting $\sqrt{d}$ here? So that is a short proof. Is the statement clear? No. Yes. Okay.

"Professor - student conversation starts" This lemma kind of allows us, it is a large number of polynomials. Then, you can by the fanin restrictions we have smaller most sparse polynomials. But like we have modeled it the sparsity is like almost given for free. **Professor:** What do you mean given for free? **Student:** It is told that the Q_{ij} 's are homogenous sparse polynomials. **Professor:** Right. **Student:** So why are we doing it? **Professor:** I do not understand that. The sum of the sparsity is s. The definition of s is sum of the sparsity of all the Q_{ij} 's is s. And we are working with s. That is our size parameter. And the probabilities here are all with respect to the process rho. **"Professor - student conversation ends".**

So once we have proven this lemma, then probabilistically we can think of the model being somehow weakened. But it is still not clear whether b if we can say that b is less than equal to $\sqrt{d}$.

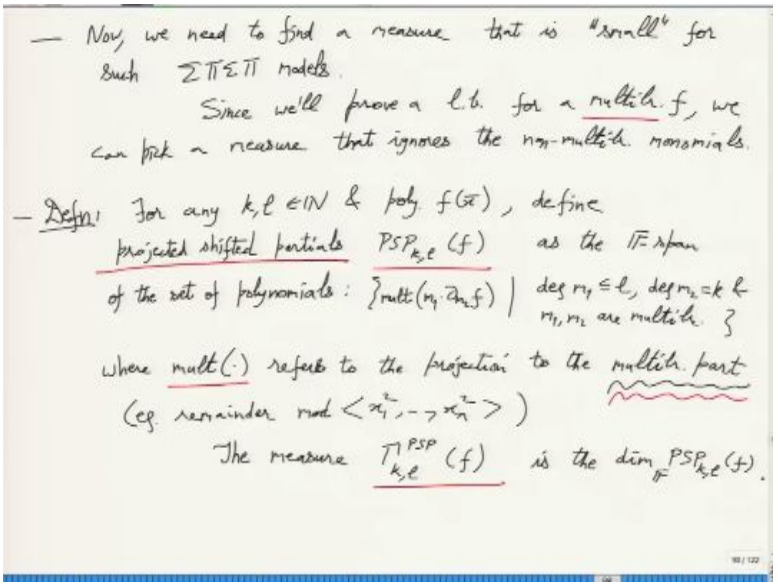
So it is still not clear how will we use the upper bound of shifted partials. But anyways, we will see how to do that next. Let us first do the proof. The proof of this is so among all these Q_{ij} 's collect the bad monomials. So among all Q_{ij} 's consider the monomials m_1 to m_r that have support greater than $\sqrt{d}$. How big can r be? This s is everything. So r is less than equal to s.

So now for one monomial m_i what is the chance of non-vanishing? So m_i is a monomial that has more than $\sqrt{d}$ variables. So what is the probability of this being not set to zero? Every variable should be left free, right and that happens with probability n^{-2c}. So you multiply those probabilities. So you get this and this is for every $i \in [r]$. Is that clear? So now what is the probability that there exists an i?

There is an m_i, which was not set to zero by ρ and is badt. So that is less than equal to this probability, times r, that is the union bound. r is at most s, which is at most $n^{-c\sqrt{d}}$. So this is less than equal to $n^{-c\sqrt{d}}$ which is smaller than 1 by s. So the probability that some bad monomial survives ρ is smaller than $1/s$.

So hence we have shown that with probability greater than $1 - 1/s$ all the large support monomials vanish. Monomials in Q_{ij}'s vanish. Yeah, so this is a simple argument. Now the monomials that remain are low support $\sqrt{d}$ support. But we are still not in a position to use the upper bound for shifted partials, because the b is not small. So we will slightly change that measure.

(Refer Slide Time: 30:48)



So now we need to find or define a measure that is small for such ΣΠΣΠ models. Yes so any ideas how do we modify shifted partials so that it works for support and not degree. Well, what is the difference between low support and low degree? Why does the degree increase? Because of individual degree greater than 1. So why not just force the monomials to be multilinear.

Then the support and degree will be the same. So that is all. That is what we will do. So since we will prove a lower bound for a multilinear f. Anyways, I mean our goal or our objective polynomial is already multilinear. So we will if we impose

multilinearity also on the monomials then the support becomes the degree, right. So this is not in conflict with our final application.

So we can pick a measure that ignores the non-multilinear monomials or ignores the squareful monomials. So let us just give the definition of the measure in full.

"Professor - student conversation starts" So if this kind of computes the derivative with respect to each variable and if you set it to zero and if it is if it becomes zero. No so I will now give the definition of the measure, a measure that works for any polynomial. Polynomial will not be restricted. It will be a modification of shifted partial. **"Professor - student conversation ends".**

So for any k, l and polynomial $f(\bar{x})$ so what the author has defined is called projected shifted partials. Who are the authors? This will be KLSS 2014. So Kayal Limaye Saha Saptarishi. You saw all of them, did you not? Yeah, Limaye was not there. You saw three of them. So okay. Projected shifted partials $PSP_{k,l}(f)$. It is called projected because even when you are looking at a squareful monomial like x_1^2 you project it down to x_1 .

When basically you go modulo the ideal $x_1^2 - x_1$. So you project x_1^2 to x_1 . So the exponent is just made 1 if it was not 0. If the exponent was 0 then you do not do anything. So it is this type of a projection that we want to use. So the result will definitely be multilinear. So this is the F span of the set of polynomials where so we will do similar thing. We will first differentiate f and then we will multiply it by a monomial.

And then whatever we get, we will make it we will project it down to multilinear. So multilinear projection. So this is the action on shifted partials. So degree of m_1 is l. In this case, we are taking it exactly l. I am not sure whether, let us make it less than equal to like before. And degree of m_2 is k, k order derivatives. And there is no point taking m_1, m_2 squareful because we are going to project.

So we will take m_1, m_2 to be multilinear. Yeah that also we have taken multilinear. It is work. Yeah sure. Yeah there are these objections, but it will work. I think it does not matter. Okay. So where this multilinear projection operator mult(.) this refers to the projection mod $< {x_1}^2 - x_1 \cdots, {x_n}^2 - x_n >$ that is just a projection or a restriction to this ideal. Oh no, that is not what it is. It is actually the multilinear part.

So squareful will be sent to 0. It refers to the projection to the multilinear part. So this is exactly. So remainder modulo $< {x_1}^2, \cdots, {x_n}^2 >$. It is slightly different. So ${x_1}^2$ will actually be sent to 0. You have to ignore the squareful monomials. So this is really extracting the multilinear part. Also taking m_2 multilinear is justified because your f ,target f is multilinear.

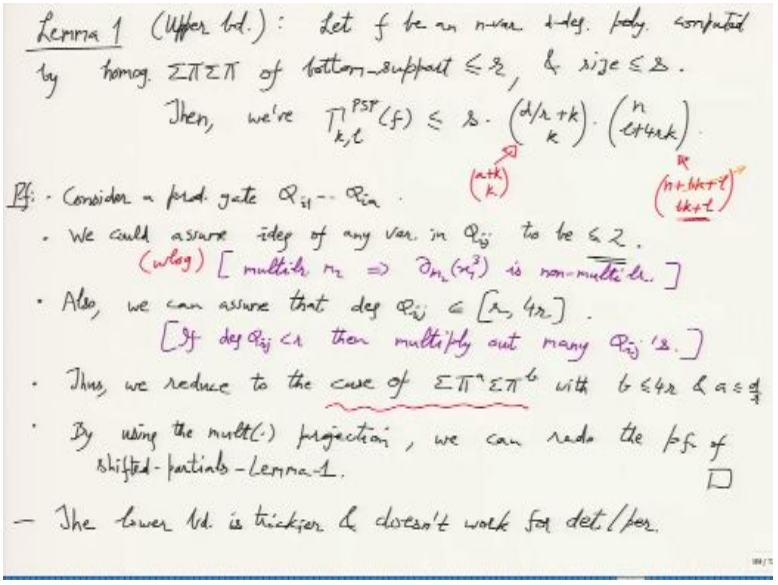
So if you will differentiate determinant by ${x_1}^2$, you will anyways get 0. So you do not get mileage on the lower bound size, side. So there is no point using anything else as m_2. Here m_1 is different. There is an advantage if you had taken m_1 non-multilinear or general, but then since here we are using this mult operator if you multiply by ${x_1}^2$ again this will not contribute, mult will kill it to zero.

So here both the things are justified. So finally the measure will be dimension of this space. So the measure gamma projected shifted partials with parameters k, l of a polynomial f: $\Gamma^{PSP}{}_{k,l}(f)$. This gamma measure is the dimension of $PSP_{k,l}(f)$ space over the base field F. Dimension of this vector space. Is this clear?

This is the modification on shifted partials and its motivation is the previous lemma where we randomly restrict the variables. So it is good for proving an upper bound, because in any Q_{ij}, if you have ${x_1}^2$ appearing it will not contribute anything to the measure. So the upper bound will come out to be small, which is the correct thing to have.

And on the side of the lower bound, since you are working with determinant taking m_1, m_2 multilinear would be enough. So lower bound you cannot really jack up in a by taking more m_1 or more m_2. So that is the rough motivation. Let us quantitatively do this. Let us do the upper bound.

(Refer Slide Time: 42:01)



What expression do you get? So let f be an n-variate d-degree polynomial computed by homogeneous $\Sigma\Pi\Sigma\Pi$ of bottom support $\leq r$. So all the Q_{ij}'s we are assuming monomials of support at most r and total size is s of the circuit. So then the upper bound is so $\Gamma^{PSP}{}_{k,l}(f)$,s for the upper bound on the number of product gates, top product gates.

And each product gate will essentially give you the same thing that you got for shifted partials with minor changes here and there. So if you remember this was with $\binom{a+k}{k}$. So that a we have replaced by d/r which, I mean, a is not actually bounded by d/r but in the proof we will see that the measure will still have this expression instead of a. And the second expression was that was something like $\binom{n+bk+l}{n}$.

So which is also bk, which is also this bk + l. Yeah so how will that change to this? So this will basically be because of the fact that we are now only looking at multilinear monomials. In shifted partials we were looking at more general monomials whose

degree could become $n + bk + l$. But now the degree would not matter. So now actually the top part will remain n. This $bk + l$ will go away.

And this $bk + l$ will continue to be there with b replaced by r. So we are getting $rk + l$ essentially. So those are the changes. So it is a similar expression. This is again expected to be large. This is again expected to be I mean it is exponentially large, but still in relation to the lower bound for determinant this will be small. It is similar, the comparison will be very similar to what we did in the previous proof for depth-4.

That is the idea. So let us just complete this. So consider a product gate $Q_{i1} \cdots Q_{ia}$. We could assume the individual degree of any variable or every variable in Q_{ij} to be less than equal to 2. Why is that? What if you have a ${x_1}^3$ sitting in Q_{ij} ? Sorry. But that is also true for ${x_1}^2$. So why I am keeping ${x_1}^3$. So just a small point is that ${x_1}^2$ when you differentiate by x_1, you get x_1.

So that x_1 will contribute. But ${x_1}^3$ when you differentiate by x_1 you will get ${x_1}^2$ which will not contribute. So this is why we keep 2 but nothing beyond. So this is without loss of generality. So let us also let me write down the point. The point is that for a multilinear m_2, when you differentiate ${x_1}^3$ you get something non-multilinear.

And since you get something non-multilinear when you apply the mult operator you get zero. So such things have no contribution whatsoever to the measure. And remember we are proving an upper bound right. So we have to be careful about counting everything. So up to beyond 2 we are fine in ignoring, but 2 we cannot ignore. Also we can assume without loss of generality that degree of Q_{ij} is at least r and at most 4r.

So why is that? So why is the degree of Q_{ij} at most 4r? No in Q_{ij} look at the monomials. So how can you say that each monomial has degree at most 4r? Well because of bottom support r. We can take 2r right? Yeah, so why am I taking 4r? Yeah, I am not sure. So this should be 2r I think okay. And no I think it will yeah, that

4r would probably come. So for the other side how can you say that the degree of Q_{ij} is at least r?

No. If it is less than r, then you just multiply Q_{ij} with the next one. You keep multiplying them till you get to degree r, till you cross degree r. But when you do this process now what is the upper bound? 3r. Yeah, it could be more than 2r. But then 4r is also possible. Yeah so let us just keep it simple and go back to 4r. It is because of this process. So I want simultaneously the degree of Q_{ij} to be [r,4r].

And that can be achieved by just multiplying out things if needed. If the degree is too low, then you just multiply things. So now we have these bounds on the degree of Q_{ij} which is really now the bound on b, right. So with this we know that b is at most 4r, but we also know that b is at least r. So since b is at least r and this is a homogeneous model right. So what could a be?

To compute degree-d monomial a could at most be d/r. So that is a bound on both. To the case of $\Sigma\Pi^{a}\Sigma\Pi^{b}$ with b less than equal to 4r and a less than equal to d by r. Is that clear? So now we are in this r and d/r product fanin. So we can just repeat the proof of shifted partial's upper bound. No a, b I have defined here. It is now defined here, where a is less than equal to d/r and b is less than equal to 4r.

This we get because of the measure definition. So for the purposes of proving upper bound we get these assumptions. Originally the product finance could have been arbitrary. So in a way only those product gates contribute that are well behaved. Other product gates we just ignore. Because they will not contribute to the measure. So finally, by using the multilinearity projection, we so by using the multilinearity projection, we can redo the proof of shifted partials upper bound.

So shifted partials lemma 1. So when you do that you will get this bound. a is d/r and b is 4r and moreover this n + bk + l goes away, just n remains. Is that clear? So that is the upper bound. Now for the lower bound, you have to show that under these

projections ρ, Γ should come out to be large. So that for some reasons is not has not been done for determinant.

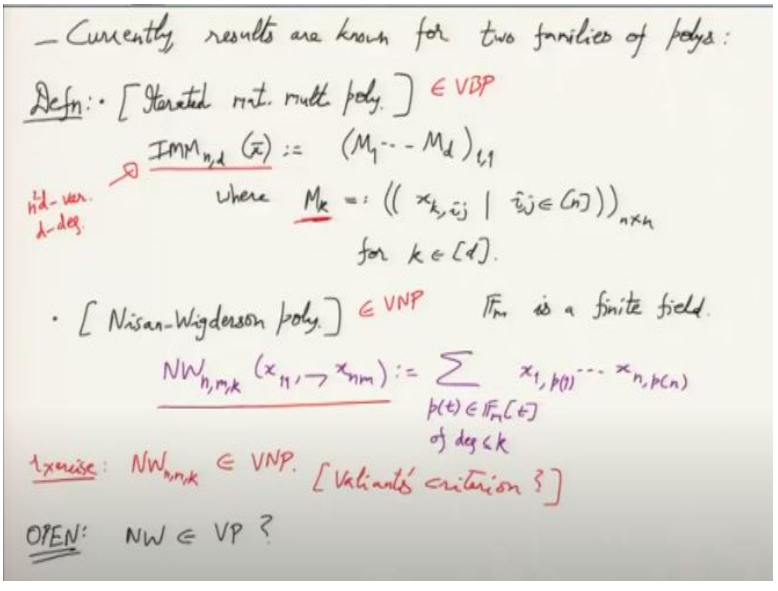
So polynomials that are more complicated were used. So if you do random restriction on determinant then I think it vanishes. Because if you just kill a row then it is gone. **"Professor - student conversation starts"** What is the, there was this parameter c, right. So roughly what. No c is a constant. Just that the size is smaller than $n^{-c\sqrt{d}}$. But then what is the, the constant will matter, because it is the exponent.

The probability of killing a determinant so it sort of depends on c, right. Yes but the probability was very high. It was nearly 1 offsetting something to 0. **"Professor - student conversation ends".**

So with such a high probability you I think usually would just kill a rho. And once you have killed a rho you are done. So the determinant is too sensitive and permanent also is too sensitive to this measure, to this variable restriction.

So other polynomials will be used that are not so sensitive. So the lower bound is trickier and does not work for determinant permanent. So some new polynomials are invented.

(Refer Slide Time: 56:32)



So currently results are known for two families of polynomials. So one is the iterated matrix multiplication because that clearly is completely insensitive to the variable restrictions, because you are multiplying these n cross n matrices, even if you kill many rows or many columns. It does not change iterated matrix multiplication much. Right? It still survives and you can talk about its shifted partials.

The iterated matrix multiplication polynomial. So what is that? That is just multiply d matrices and look at the corner, 1, 1 entry that is a polynomial. So where M_k is the matrix $x_{k,ij} \quad i,j \in [n]$. So each M_k k from 1 to d is a matrix n $\times$ n matrix where you can identify the variables as $x_{k,ij}$. So you multiply them. So this is n^2d-variate and d-degree.

There is another polynomial which has been used in this sequence of results, which is called the Nisan-Wigderson polynomial. So the thing is that this is the first polynomial is better because this is in VBP. Not just in VP but in VBP right? So very I mean the hierarchy of things, it is a very easy polynomial. The Nisan-Wigderson polynomial is more like permanent, it generalizes permanent.

So all we could say is that this will be in VNP. So it will be a much harder polynomial. So when you prove a lower bound for IMM versus when you prove it for Nisan-Wigderson there is a difference in the quality. So IMM results are more interesting because it is an easier polynomial and you are proving a lower bound. Nisan-Wigderson polynomial anyways seems quite hard.

But initial results were proof for this because the lower bound techniques are nicer here to analyze. So the way this is defined is there are three parameters n, m, k and there are n, m variables. So think of it as an n $\times$ m matrix and like permanent it is a sum of a huge number of monomials. So $x_{1,p(1)}x_{2,p(2)}\cdots x_{n,p(n)}$. So in the case of permanent p is a permutation. In here p will be a polynomial, it is a polynomial map.

So you in fact go over all the polynomials. And what is F_m ? F m F_m is a finite field. So over F_m is a finite field of size m. So $p(t)$ of degree k. So once you restrict the degree of p since you are over the finite field, there are finitely many polynomials. Use all of them and some of these permanent kind of monomials. So that is the Nisan-Wigderson function.

Now where can you put it? What is an algebraic complexity class that contains this? Why is VNP obvious? No it is not obvious. If it is obvious then you are making a mistake. So it is worthy of an exercise. Yes, maybe next. I think I forgot to give or state this Valiant's criterion. If a polynomial's coefficient is $\#P/\text{poly}$ computable then it is in VNP. I did not state it.

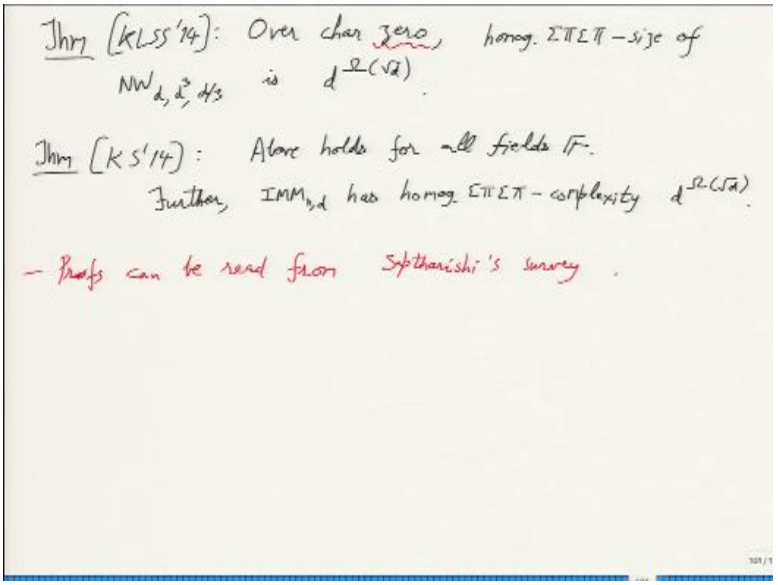
So that should also be that should be an assignment. So using that you get this immediately. It follows from Valiant's criterion. I do not know how you will get it otherwise actually. Yeah, so if you are given a sum of monomials where the where there is an easy way to extract coefficients given a monomial where easy is actually defined in a very relaxed way. It is not a polynomial time algorithm it is $\#P/\text{poly}$.

So in particular, you can use permanent and other very hard algorithm. So using those hard algorithms, NP hard algorithms, if you can extract a coefficient of a given monomial then that polynomial is in VNP. So it is a pretty useful criterion in particular this. It will immediately follow that NW is in VNP. And it is an open question whether anything better holds.

So is NW in VP? That is an open question. Like n m is the number of variables. It is a family. We never talk about a single polynomial in VNP. It is an infinite family of polynomials. So for these polynomials what are the results known. Upper bound you have seen, now for the lower bound, you have to really work with the special properties of these polynomials. So those things I am completely skipping.

That will take several lectures. So I think at this point you know the techniques and you can just go and read if you want to read the proof from Ramprasad's survey.

(Refer Slide Time: 1:05:41)



So I will just finish off with the final theorem statements. Showing you all those calculations I think will not serve much purpose and also with the risk of making your bored. So over characteristic zero homogeneous ΣΠΣ complexity of Nisan-Wigderson polynomial with parameters $NW_{d,d^3,d/3}$. So these are the n, m, k. They are comparable to $d^{\Omega(\sqrt{d})}$.

So what is the degree of this? That is d, right? It is a degree-d polynomial on d^4 variables. And for that you are getting $d^{\sqrt{d}}$ which is good. Right? So it is a result comparable to what you got for $\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$ model. It is a comparable result. And then this was improved by KS'14. So this KS is Kumar and Saraf. So here characteristic zero is needed because the lower bound goes through some real analysis.

So Kumar Saraf then proved it for all fields. So above holds for all fields F. So no restriction on the characteristic. Further they proved it for a better polynomial. So this IMM this complexity is $d^{\Omega(\sqrt{d})}$. So IMM is a polynomial of degree-d and you are getting and n will be assumed to be poly(d). So the number of variables is also d^3 or d^4 whatever. So again $d^{\Omega(\sqrt{d})}$ is a good bound.

So yeah these are the results which you will get ultimately. So proofs are being left. Proofs can be read from Ramprasad's survey. Any other questions? Okay.