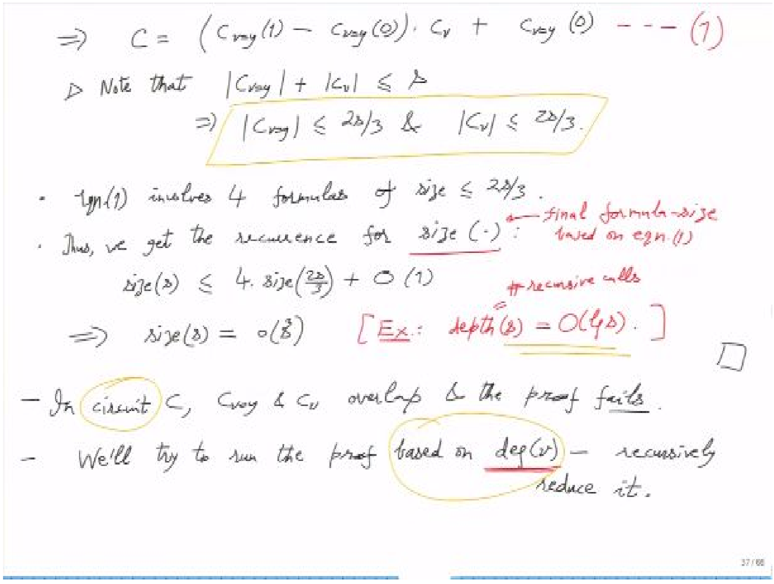
Arithmetic Circuit Complexity

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

Lecture - 08

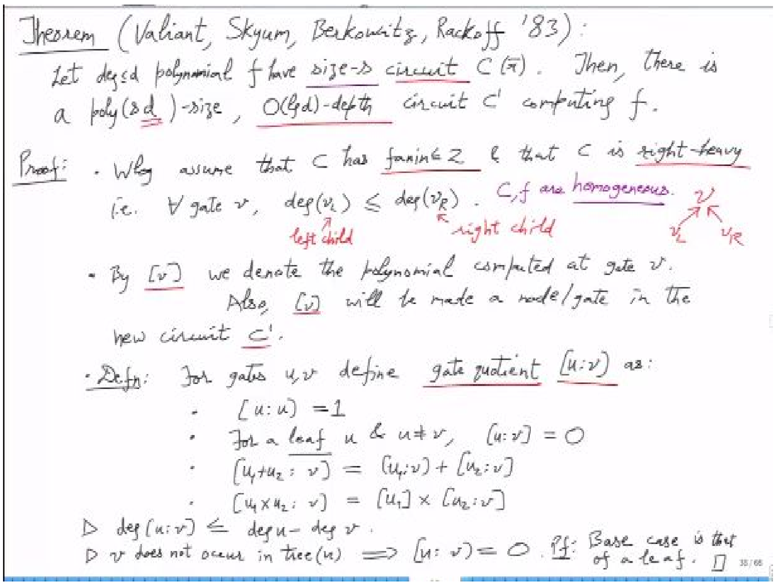
Okay, so last time we did Brent's proof for formula reduction of depth in the case of formulas.

(Refer Slide Time: 00:17)



So depth can be reduced to $\log s$ that was our result. And we noticed that for the case of circuits that proof will fail. So now we will give a different proof, a proof based on degree as a potential function instead of size.

(Refer Slide Time: 00:47)



So this is a theorem by VSBR. It is quite old already from 1983. They showed that if you have a degree d polynomial with size s circuit C. So let degree d polynomial f have a size s circuit C. Then, so although in the assumption in the hypothesis there is no mention of depth, which means that the depth can be as high as size. What we will show is we will give an algorithm a constructive way to reduce the depth to log d and size will not blow up by much.

So then there is a polynomial in s. Forget n because that is contained in s, $poly(s \log d)$ size and $O(\log d)$ depth, circuit $C`$ that also computes f. And proof will be mostly constructive. So degree d here can be arbitrary. It can be as high as s^s in the case of circuits. Like these are general circuits. But the depth will reduce to $\log d$ and accordingly the size will grow.

But the growth in the size will be dependent on only log d, not d okay. So this is actually applicable to also exponential degree polynomials. This is much stronger than the homogenization result. It is actually efficient for exponential degree polynomials also as long as there is a small circuit computing it.

This is very different from formula. And the proof will be long and technical, but the idea is to work with the degree as a potential function. So without loss of generality assume that C has fanin 2 and that C is right heavy. So right heavy will be defined as for every gate v in C

$$deg(v_L) \le deg(v_R)$$

where v_L, v_R are left and right children respectively.

Yes. So this is without loss of generality because we are assuming fanin to be 2 and if for any gate, for some gate if degree on the left is more than you just swap. So this you can do efficiently also. So we will assume that the circuit is right heavy. Heavy in terms of degree and not size. This proof exposition is not following VSBR. We will follow the exposition given in a survey by Ramprasad.

So that is available online. We are following that exposition. But the main idea is same as in [VSBR'83]. So by this notation $[v]$, we denote the polynomial computed at the node v, or at gate v. And so you should think of the proof as building circuit $C`$ step by step looking at C as you walk down from C from the root to the leaves.

And in $C`$ the nodes that we will put will exactly be the $[v]$ type. So this will also be a node simultaneously in $C`$. It will be made a node or a gate in the new circuit $C`$. So this $[v]$ has two interpretations. This is happening in parallel. $C`$ is being built as we are analyzing C.

So as we have seen in the previous proofs in derivatives and also in Brent's formula depth reduction, we had some notion of identifying a subtree v and removing it from the tree and replacing it by a new variable. So we now formalize it in terms of quotients, quotienting process. So for gates u, v define gate quotient $[u : v]$ as -

- [u:v] = 1
- For a leaf u & $u \neq v$, $[u : v] = 0$.

The idea would be that if v appears below u, below the gate u then the quotient should be the thing which intuitively you should get if you divided u by v , not the remainder but the quotient. So ignore the remainder and look at the quotient if you expand u in terms of v, like $Av + B$.

And you can do this arithmetic. If two gates are being added, then quotient by v should be defined as-

- $[u_1 + u_2] = [u_1 : v] + v$

So we are now inductively going upwards right. If you know u_1/v and u_2/v then the sum should just be the sum of the quotient. So this is the definition, inductive definition and also a property.

And finally, you might face a multiplication gate, so intuitively you should quotient only one of these, u_1 or u_2. It does not make sense to quotient both and multiply intuitively.

- $u_1 \times u_2 : v] = [u_1] \times [u_2 : v]$

$[u_1]$ is just u_1, whatever u_1 was computing. So u_1 is not changed, just u_2 is changed.

So this is essentially the definition of quotient for all the gates. It is an inductive definition, goes from leaves to the root level by level. So looking at this definition, what are the immediate properties? So first of all, this is a polynomial right? We are calling it a quotient, but this is not a fraction. It is always a polynomial.

Because base cases it is 1 or 0. And then when you are adding you obviously get a polynomial and the multiplication gate also gives you a polynomial. So this is always a polynomial. So you can talk about its degree. What is the degree of this polynomial $[u : v]$? I do not know it exactly but at least the upper bound is the difference right.

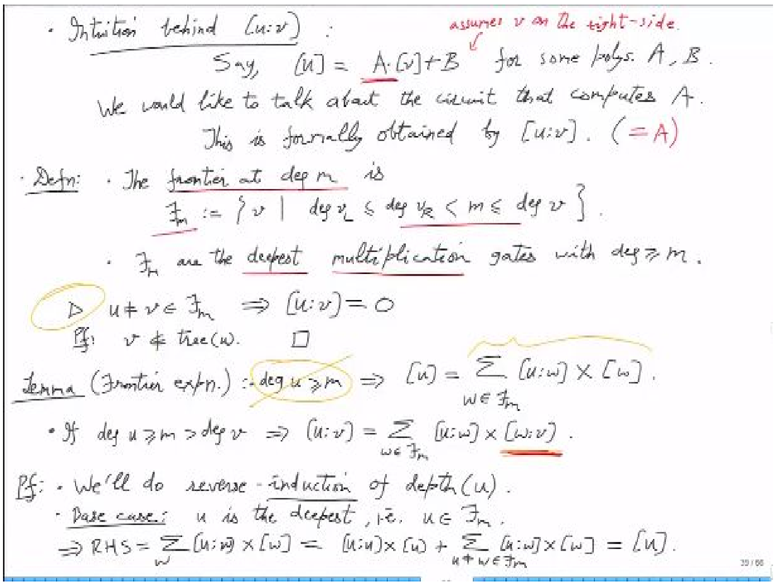
$$deg[u : v] \leq deg\, u - deg\, v.$$

This again follows just inductively from the axioms. **"Professor - student conversation starts"** But when you quotient you might quotient itself. Then deg u minus deg v is zero. Yeah, right **"Professor - student conversation ends".** That is consistent with our norms and it is also consistent with if the degree of v is strictly more than u then the RHS is a negative number. Left hand side also we can understand it to be a negative degree because u question v is 0. So 0 is somehow special, its degree is not 0 but negative, which makes sense.

The other simple observation is if v does not occur in the tree rooted at u, so you look at the sub tree under u and if v is not a gate there. Then $[u:v] = 0$. This is just an extension of this leaf property. So the proof sketch. In the induction base cases that of a leaf. So you will end up downwards starting from u and ultimately you will reach a leaf and you will still not have found v.

So you will get 0 and the 0 will just add and multiply. Giving you 0 at the top. Details are skipped, and can be filled easily.
These are the tools that we will use now a lot in the proof. The proof will really develop on this quotienting idea.

(Refer Slide Time: 15:12)



Let me write down again the intuition for the quotient. Say in the subtree of u, v appeared. So $[u] = A[v] + B$. The intuition behind the quotient definition is, $[u:v]$ should be so this is for some polynomials A, B. We would like to talk about the circuit that computes A. But in this tree computing u it is not immediately clear whether A was computed.

So maybe A and B and v were all computed together. So it was all mix and match. A may not have been separately computed. This is why we need a new notation to talk about A and that is exactly $[u : v]$. It is formally obtained by u quotient v. You can see that this actually equals A. Assuming that v is on the right because in the axioms of quotienting v, when we have a multiplication gate we are preferring the right side.

So v should appear in the tree of v as a right child of its parent. And then you can see inductively that the claim $[u : v] = A$ is correct. So this is the sole intuition behind the quotient operation. The circuit may not be computing A as an intermediate polynomial, but still we can refer to it by this operation. If you think of u as the root then what are the v's to look at.

v refers to all the gates in the circuit, so which of these v's are good for an algorithm to reduce depth. So those will again be Frontiers. We defined that frontier gate. The frontier at degree m is

$$F_m := \{v \mid deg\ v_L \leq m \leq deg\ v\}.$$

Simply put it is just those frontier at degree m are those gates, where the degree of the polynomial computed is at least m but the children it is smaller than m. That is naturally the frontier. Like the first time it crosses m or it falls. So v the first v is the gate where the first time it is crossing m as you go from leaf to root.

"Professor - student conversation starts" If we go from the leaf to root the degree would not change monotonically, right? Oh, but somewhere it has to increase. Yeah, but it could, on the same path it could increase and then decrease and then increase again, right? **"Professor - student conversation ends".** No, I am not sure we want to do all that. The definition of frontier stands as it is as written here.

Let F_m be the deepest multiplication gates with degree greater than equal to m. So put this in the definition. So F m will be the deepest ones.

So once degree m has been crossed, maybe later on it will fall. But we do not care about that for now. Let us see in the future if there is a problem we will redefine. And the other thing is that it has to be a multiplication gate. In the definition it was any gate v. But if the degree is increasing then it has to be, it has to be a multiplication gate, addition cannot increase degree.

So these are the deepest multiplication gates. So now if there are two gates in the frontier what can you say about the quotient?

$$u \neq v \in F_m \Rightarrow [u : v] = 0 \ .$$

Because v cannot be in the subtree of u, so that is 0. That is almost by definition. v is not in the tree rooted at u. That is what because if it was then u would not be the deepest. Now for the root u, we have these frontier gates.

So we want to expand the root using the frontier gates. So we will write something called the frontier expansion lemma. So suppose u is a node with degree at least m, then you can you have this identity using the frontiers.

$$deg\ u \geq m \Rightarrow [u] = \sum_{w \in F_m} [u : w] \times [w] \,.$$

Since u has degree, at least m somewhere in the tree at u, degree must have crossed m because at the leaves, the degree you start with is 1 or 0.

So somewhere there was a transit there was a jump and so that gives you at least one frontier gate w. With respect to this you can quotient. $[u : w]$ will be a nonzero polynomial. You multiply that with the w and take the sum. We want to show that this sum will come out to be u if you go over all the frontier gates. This is a slightly non trivial statement. So let us prove this.

Actually, I want to make more statements. So that is one thing. In the lemma we will also say that

$$deg\ u \geq m > deg\ v \Rightarrow [u : v] = \sum_{w \in F_m} [u : w] \times [w : v]$$

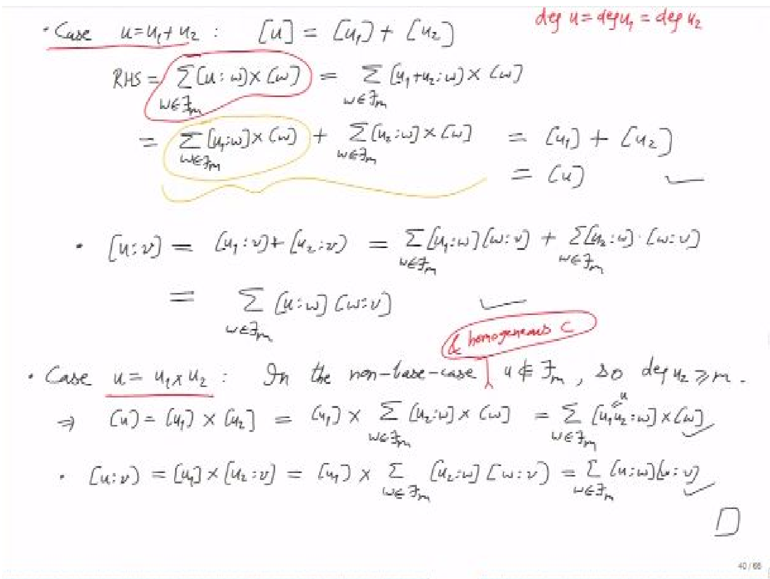
the quotient $[u:v]$ this will be consistent with the above formula in the way above. So we have the original formula of u and that we can also quotient by a v with a lower degree and this would be the change.

So we will prove these two things in the same way and obviously it will be inductive proof. So we will do reverse induction on depth, $depth(u)$. The base case is in the leaf, the deepest place. Which will be actually the frontier. So which means u itself is the place where the degree jumped from something smaller than m to m or more than m.

So u is the deepest which means that u is in F_m which would then mean that if you look at the RHS, so in the sum w can also be taken as u. So that will give you this plus the other w's. Now obviously the first summand is just u and what about the other summands? So since both u and w are frontiers, we have this observation here. So they are all 0. So this is equal to just u.

That was the base case. Now the induction step will be working with addition and multiplication gates.

(Refer Slide Time: 29:31)



So if you are adding up u's in addition gate. So in this case, u is the sum of its children and each of the children follow the identity. So let us write that down. What is the degree of u_1 ? Degree of u is at least m. But degree of u_1 may not be at least m, maybe something smaller like m_1 . But u_2 will have degree at least m. So here we can use F_m . So now what yeah I wanted to sum.

So is this LHS or was also, if it was the same w then I could have summed up. Otherwise I have this leftover portion. Maybe the idea of homogenization can work but homogenization can be expensive. So is there an easy fix here? If u_1 has less degree than u_2 , which is equal to the degree of u; in the lemma statement we are talking about frontiers smaller than.

Yeah so maybe antecedent is unnecessary. Maybe you just expand it by being dependent of u. We just in frontier expansion we use m as a parameter. Could try doing that. So you were saying that if the case when degree of u_1 is less than m. That is the bad case. Let us just expand u with respect to F_m .

Yeah m, u and m are given. Let us just think of frontier expansion lemma is expanding u with respect to F_m . Yeah, no so actually I have to yeah m has to be smaller. If I take m to be bigger than the degree then this RHS will just be 0. There has to be something below. So we have, let us look at the RHS, their summation.

So this is equal

$$RHS = \sum_{w \in \setminus F_m} [u_1 : w] + \sum_{w \in F_m} [u_2 : w][w] .$$

But then I have to show that this sum is u. So then I have to go back and change the theorem. Yeah otherwise I think I am stuck here. So then let me take back the big claims. Let us just be happy with $poly(sd)$ size. So if I am willing to spend $poly(sd)$ size then I can as well make my polynomial and circuit to be homogeneous.

So I look at homogeneous parts of f and I prove the theorem the depth reduction only for the homogeneous parts and which will then summing up will give you also low depth for the original f right. So let me add that assumption here. f is homogeneous and C is a homogeneous circuit. Let me go through the proof with this assumption then I mean if later on I find that there is a stronger proof I will tell you okay.

So for now let us just continue using homogeneity. So in the homogeneous case, the place where we were stuck yeah now it will be fine because you know that degree of u is the same as degree of u_1. Intuitively it should be possible, but let us proceed. There is no counter example for that. It is only in this proof where we are getting stuck. So anyways that homogeneity addition gate also has to be homogenous. So it will be adding up gates of the same degree.

In fact, u_1, u_2 are homogeneous of the same degree. So all these degrees are the same. The frontier expansion for u_1 will be with respect to F_m that is allowed and for u_2 also frontier expansion with respect to F_m is allowed. Okay both of them are allowed. And this then comes out to be u. Let me write the step.

$$RHS = \sum_{w \in \setminus F_m} [u_1 : w] + \sum_{w \in F_m} [u_2 : w][w] = [u_1] + [u_2] = [u]$$

So the first thing is by induction hypothesis u_1 and the second thing is u_2. So RHS equals u, this expression that we started with is in fact u. And in the same case what is $[u : v]$?

So the other identity in the lemma statement.

$$[u : v] = [u_1 : v] + [u_2 : v]$$

By the axiom of quotient A. And now individually you can use the induction hypothesis to get $[u_1 : w]$, $[w : v]$ plus the symmetric thing. And which you can again take the summation out, take the $[u : v]$ common and you will get this equality. So both the identities in the lemma statement are done in the user addition gate.

Then you cannot use the induction hypothesis. You cannot complete the proof because the RHS I mean this red part which I am calling RHS, this is then just equal to $u_2 : w] \times [w]$ sum which is equal to u_2. So you do not even get u then. You get only a part of u. Well which is also in a way it is intuitive because if you are using frontier gates whose degree is higher than u_1, then expanding with respect to them can never give you u_1.

So you will actually only be able to compute u_2. So it is a fundamental problem in this proof method, so I had to change the theorem statement. Let us prove the weaker version first. Second case is that of the multiplication gate.

So in the case when u is a multiplication gate since the degree of u was at least m you know that u_2 has degree at least m, because the circuit is right heavy. No that I cannot say. In the non-base case, u is not in F_m. So not being in the frontier means that the right child degree is at least m. This is not the first time that the degree crossed m.

Degree of u_2 is greater than equal to m. We will need this conclusion. So now since the degree of u_2 is at least m, we can intuitively when you use frontier gates from F_m they will be able to give you u_2. That would be enough in the induction step. So $[u] = [u_1] \times [u_2]$ which is? So u_2 now you can expand by the frontier that is allowed and can you bring u 1 inside?

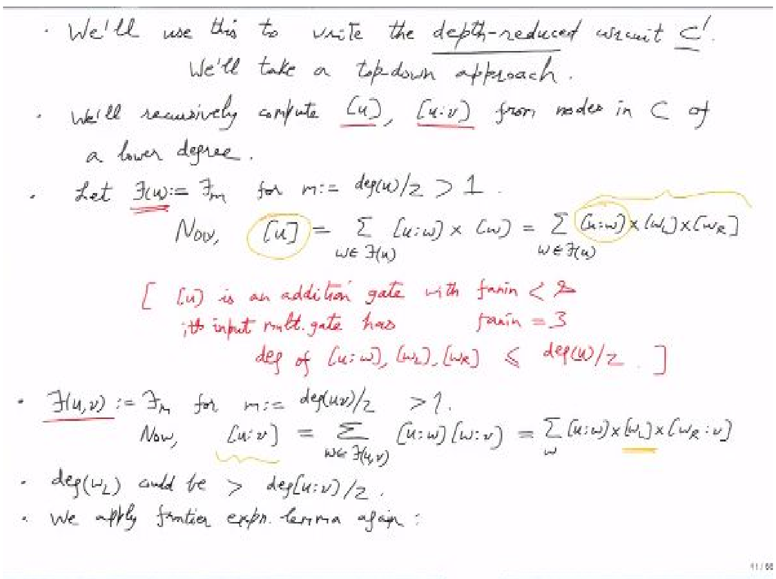
So if you bring u_1 inside you can multiply it with $[u_2 : w]$ and get $u_1 \cdot u_2$ which is u. That is again an axiom of quotienting. In the non-base case u is not a frontier but we are using homogeneity here as well and this is equal to u. So that is our first identity in the lemma statement and let us simultaneously prove the second identity. So in this case, when you take the quotient of $u_1 \cdot u_2$ you will divide u_2.

And now you can use the induction hypothesis. So that will give you with respect to frontiers and when you bring u_1 inside you will get the result. That is the form as claimed. So this completes the proof of frontier expansion lemma. The import of all these calculations is simply that a node u can be expanded by frontier gates of smaller degree, at smaller degree.

So just the frontier gates are enough, nothing else is required as long as you are doing this at a degree below or at most u. And you can also do the same thing with quotienting, $[u:v]$. So using this we will now see what the circuit $C`$ is, okay. So $C`$ will have these $[u]$ and $[u:v]$ as nodes and it will be using frontier expansion lemma to do things faster in terms of depth.

So in a way it will be faster because in the original circuit C, between u and the frontier gates, a lot of extra calculations may have been happening. All those will be now optimized by these frontier expansion lemma identities. So in one shot you will be jumping to high degree. Yeah, but still I mean it will have some technicalities. So we have to go through that. It is not straightforward.

(Refer Slide Time: 51:22)



So we will use this lemma to write the depth, reduced circuit C prime. So we will take a top down approach, which is what the frontier expansion lemma already suggests that expand u with respect to the frontiers come down and then proceed inductively. So we will recursively compute u and the quotient from nodes in C of a lower degree. But m is actually a parameter.

It is any number below the degree of u. So you now want to fix m. So let us fix m to be half of the degree of u. Because we are interested in optimizing the depth. Llet us look at the frontier which is exactly half degree or around half degree of u, expand with respect to that. So this frontier expansion lemma will in a way be doubling the degree.

Yeah, so let us fix m to be that. So let $F(u)$ be the new notation for frontier. So this is the frontier of u at $m = deg(u)/2$, so that is what we are defining that is $F(u)$. The degree of $u/2$ may also be half right and or it may also be 1. This will happen when you are looking at really things close to the leaves. So that part you handle separately; make that your base case.

So we can assume that $m = deg(u)/2 > 1$ so that doubling really happens. You are above 1 and then when you double you will get 2, and bigger integers. So m is an integer bigger than 1 or at least 1 and when you use frontier expansion lemma on u, you will get that identity, w frontier of u. And you know that the w is a multiplication gate, right. So let us further expand this.

$$[u] = \sum_{w \in F(u)} [u : w] \times [w] = \sum_{w \in F(u)} [u : w] \times [w_L] \times [w_R]$$

So u we have expanded as sum over the frontiers of u of these three gates, their product. So let us just write down what we have got here. So u we have written as an addition gate with a fan in less than s. In this summation the number of summands is equal to the number of frontier gates and that cannot exceed the size s. These multiplication gates which is this part its summand is a multiplication gate of fan in only 3.

And these input multiplication gates so these multiplication gates have what is the degree that you see here? So deg of $[u : w]$, $[w_L]$, $[w_R]$ What is the degree upper bound on these? Since we have taken m to be half the quotient has degree upper bounded by the difference. So that is half of the $deg(u)$ for w by since it is a frontier gate at m $deg(u)/2$.

Left and right both of them have. So w was a multiplication gate. Its children cannot have a degree more than that. So all of them have degree $deg(u)/2$. So this you should think of as something happening inside circuit $C`$. So there is a node $[u]$ which is an addition gate with lots of inputs, each corresponding to a w in $F(u)$ and each of these are actually multiplication gates with only three inputs.

And these three inputs are the lower $[u:w],[w_L],[w_R]$ gates. So we have developed this sigma product layer of $C`$ by one application of frontier expansion lemma. The input to this $\Sigma\Pi$ layer is of a low degree which at the output doubles. So this is exactly the progress that we wanted, doubling the degree. So does it mean we are done?

Right, so to complete this inductive proof we now have to so we have analyzed u. Now we have to do the analysis also for $[u:w]$ type of things, which appears here. So what is the equation frontier expansion lemma for that? So for that we will need a frontier of this type. Let me define frontier of u, v $F(u,v)$ to be F_m for, so this is the frontier for the frontier expansion lemma of $[u:v]$.

So you are given u and v. What should you fix your m as? So u in the tree of u, there is somewhere there is v and so the w should be in the middle because in the frontier expansion lemma you get u divided by w and w divided by v. So w is the average. So let us take m to be average. So average is just degree of u plus degree of v which is actually also degree of product half $m = deg(uv)/2$. And let us expand with respect to this.

So this is allowed, this is a legal expansion. So what you get is this. And just following the previous calculation above we want to now see a doubling of degree here. So this will be our snippet for $[u:v]$ in $C`$. So the gate $[u:v]$ how is that being computed? Again as two layers. One for the sigma gate and other for the multiplication layer.

So we can immediately write with respect to w_L, w_R because w is a multiplication gate, being a frontier. So that would mean w_L outside and $[w_R : v]$,. We get this, these three things.

$$[u : v] = \sum_{w \in F(u,v)} [u : w][w : v] = \sum_{w \in F(u,v)} [u : w] \times [w_L] \times [w_R : v]$$

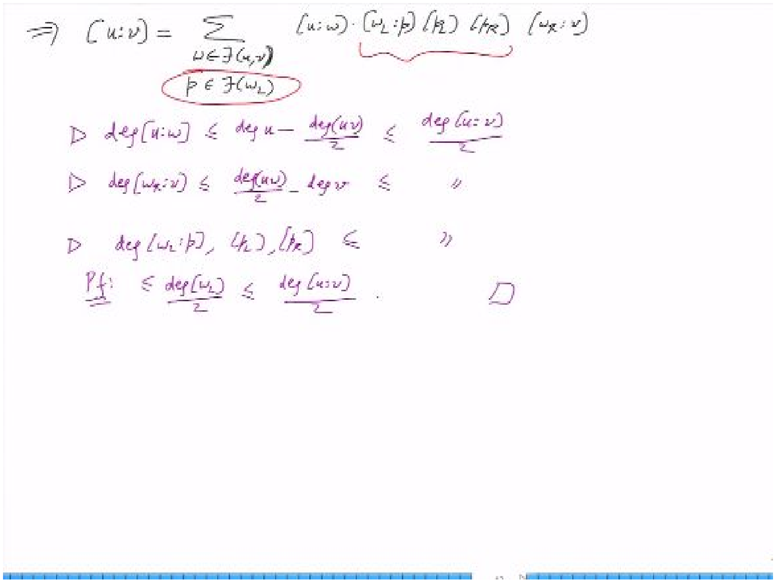
Now are these three things, is the degree less than half of degree $[u : v]$. So the problem is actually, if you look at this w_L what is the degree bound that you have, m right? Which is $(deg(u) + deg(v))/2$.

But that is more than the degree of u by v, right. So this is the gate which may have actually degree more half of the degree of this. So we cannot stop here, I mean we have to develop $C`$ more, so that this problem is corrected. So degree of w_L could be more than $deg([u : v])/2$. So what should we do? Yeah, it is negative.

So we have defined, we were at least forced to define m like that, it should be between u and v. So we picked exactly in between. But then the place where it hurts is, in the LHS you have u by v, which has degree as difference. So the difference may be smaller than the mean by 2, the difference can be small. This is well difference by 2 can be smaller than the mean, which actually usually it will be.

Whenever stuck in such a situation we will use the only thing we know which is frontier expansion lemma. So we will expand w_L by another application of frontier expansion. So we apply frontier expansion lemma again. So that will give us a big sum.

(Refer Slide Time: 1:05:26)



So u quotient v is now w we already had and for w_L look at the frontiers. So this will be you have $[u : w]$, you have now $[w_L : p]$, $[p_L]$, $[p_R]$ and $[w_R : v]$. So that is the thing which is new, the red thing that is the frontier expansion of the single node w_L. So now we have five things instead of three. And what can you say about their degrees?

So the degree of $[u : w]$ is upper bounded by $deg(u) - deg(w)$ which is the mean, which is half of what we are computing. That is fine. Degree of the $[w_R : v]$ is smaller than the mean minus $deg(v)$ which is again half of what we are computing. In the red part we want to claim the degree of the $[w_L : p]$ and $[p_L]$ and $[p_R]$ they are all smaller than this. So this we have to check. So why is that?

So remember that p is here. So what it is expected of degree of $[w_L : p]$ and $[p]$? So they are at most $deg(w_L)/2$ and the degree of w_L will be smaller than the degree of $[u : v]$. That will be the proof. Well w_L may not be half of the final thing, but it cannot exceed that degree. Not by 2, I am just saying that the degree of w_L is at most the degree of LHS. There is no half. So that is a simple demand, okay.

So as an exercise show that degree of $w_L \le deg([u : v])/2$. That is all. So since that is true, and on that w_L we are doing frontier expansion. So $[w_L : p]$ will now be bounded by degree $deg([w_L])/2$ which is then smaller than half of the final thing. So now we have a perfect case of I mean, we have this snippet, this part of $C`$, where there is a big sum the feeding which is in which you are feeding multiplication gates.

And these multiplication gates have fan in only 5. So this is the bound you get. You get that fanin of multiplication gates, is 5. Fan in of addition gates is unbounded and whenever multiplication happens, the degree at least doubles. So you get all these structural properties which imply the theorem.