Mathematical Logic
Prof. Arindama Singh
Department of Mathematics
Indian Institute of Technology, Madras

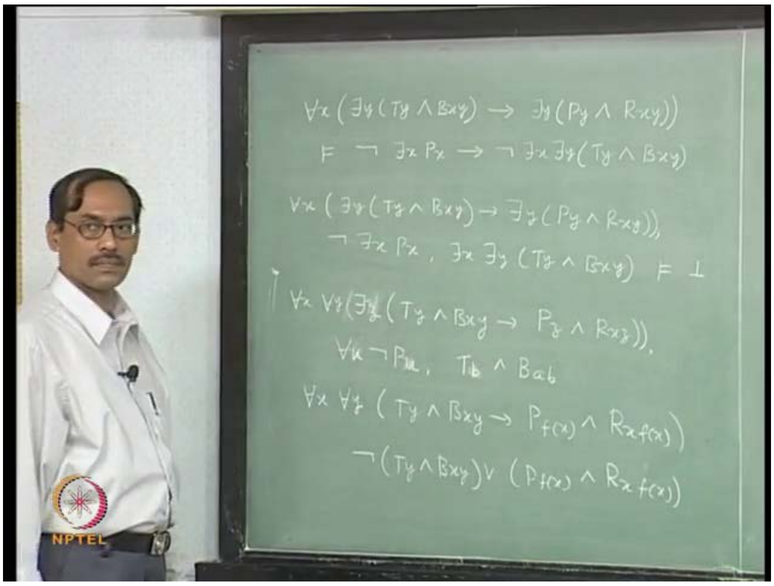
Lecture - 38
Resolution Examples

So, we had simply formulated the resolution rules. We had four rules in the resolution for first order logic; one was, here, binary resolution, which is just like resolution in propositional logic, but along with most general unifier. Now then, the other rule was the factor rule which unifies a sub-clause of the clause, then takes or applies that most general unifier on the whole clause; that will be considered as deduced from the original clause. Then, you have the paramodulant. So, this is specially for the equality predicates, there, if you have two clauses, one is having some equality literal, like say, t equal to u, and then the other one is having some formula where s occurs, s is another term, then, you take most general unifier of s and t call it sigma; now delete t equal to u, delete X of s add X of u; and then take the union of those two clauses; and then apply your most general unifier sigma; that was the paramodulant. Then, we have another equality axiom which we wrote as a rule; that is, anywhere you can introduce t equal to t.

These are the four rules of resolution. Then we wanted to discuss one example. So, the earlier example which says everyone who buys a ticket receives a prize. Therefore, if there are no prices nobody buys a ticket. That was the example we were considering. Let us write it in first order logic. We start with everyone who buys a ticket. There is a ticket which x buys, then that person x receives a prize. So, there is a prize which x receives that was our only premise. Therefore if there are no prizes, then nobody buys a ticket. This is the consequence we wanted to prove by resolution.

First thing is, we have to use deduction theorem or RAA, whatever, then bring it to the clausal form. We will use both deduction theorem and RAA. First, this one will be taken to the premises, next this one will be taken with negation sign, so double negation we are using. We will just omit it; that is, we have for each x there is y T y and B x y implies there is y P y and R x y; along with that we have not there is x P x. Then, we use RAA. We have the other one: there is x there is y T y and B x y; this should entail bottom due to deduction theorem and reductio ad absurdum; sigma prime.

(Refer Slide Time: 02:00)



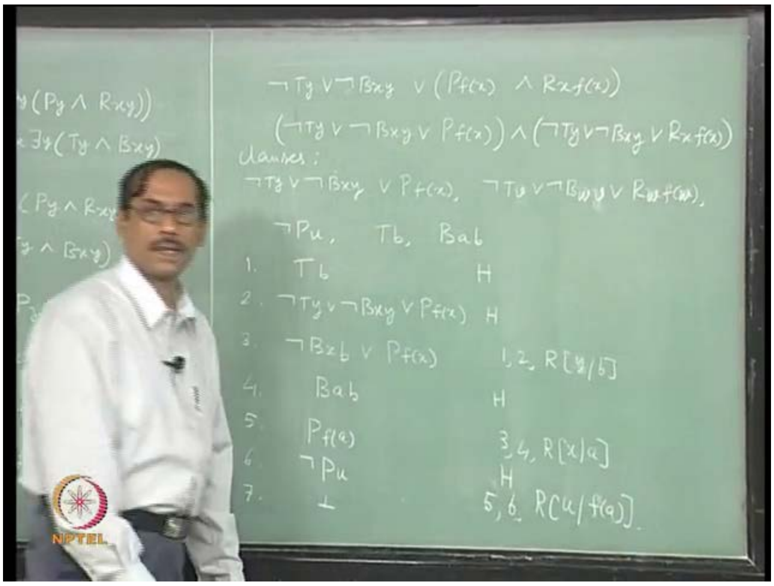
Next, we take them into clausal form without sharing a variable; clauses should not share variables; that we have to take care. So, first is, from this one, first one says, for each x, this becomes for each y when goes out; so that is, the other one comes here. We rename this. There is z, this y becomes z, now T y and B x y implies P z and R x z. Let us write the same way. Next, the other one is almost in the form: z gives for each x not P x we are going to omit the universal quantifiers. So, better to keep it in that form. Next, but x is already used; let us write it as u. Next, we have two existential quantifiers. There is no "far all" before it; they will be simply replaced by some constants, Skolem constants, which will be new to the, all the constants, everything, they should be new.

You write T a and b. Let us, b here, a, b, it is not necessary. But, let us write that. So, this is the set of clauses. But it is not a clause, first one; let us bring it to that form. There, we have, for each x, for each x for each y there is z; we have to use skolemization. With skolemization, z might depend on x and y, but z occurs only with x in a predicate. With y It does not occur; z will be replaced by some function of x, say, f of x; y is not important there. So, we get T y, B x y implies P f of x and R x f of x; the first one. Then, of course this will be omitted, all these. But then, we need clausal form. This is implication; we have to bring it to c n f. This will give not of T y and B x y or P f x and R x f of x. Now, you have started omitting this.

That will give what? Not T y or not B x y or P f of x; due to De Morgan, and R x f x. Yes, any problem? Let us we distribute; because we want c n f. This gives not T y or not B x y or P f x and not P y or not B x y or R x f x. Now, we have the clauses. As this is one clause: not P y or not B x y. Let us write the clauses: or P f x, one more: not P y or not B x y or R x f of x. Next, from this not P u, next T b, next B a v.

But before applying the resolution, we need to see that they do not share a variable. Still these two clauses, they share a variable, right? We should rename the variables before applying resolution. Here, we have y repeated, x is also repeated, fine? Those two we have to rename. Let us rename here itself. We get T b, y is x, let us say w. So, this is the set of clauses from which we have to get bottom by resolution. We should have a resolution refutation of this set of clauses. These are the clauses. Now, how do you go about?

(Refer Slide Time: 07:00)

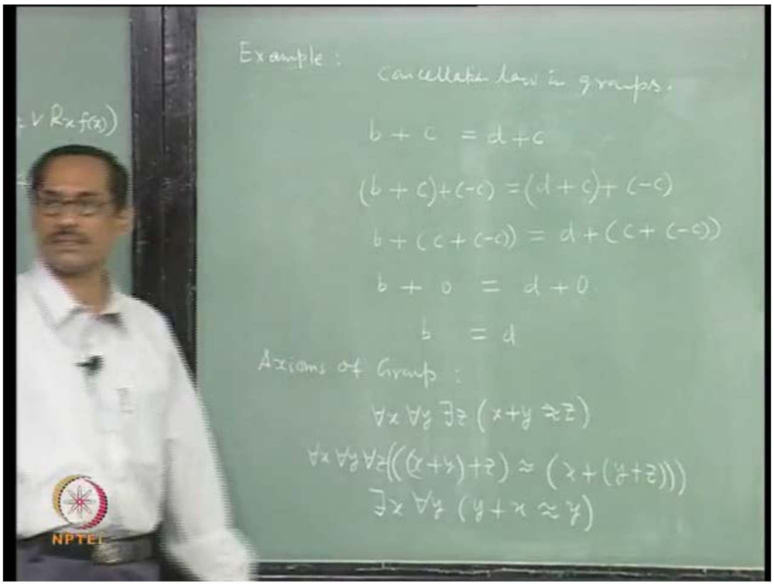


We should have a strategy; say, T b and this might resolve quickly. Let us start with T b it is a hypothesis, second we introduce not t y or not B x y or P f of x, now use the resolution. T b, not T b, not T y. They unify with y as b; that is the most general unifier; so you substitute y with b here; forget those two, take the others. So, resolution gives not B x b or P f of x; 1, 2, resolution with x as y. Next, we have B a b. Let us introduce that B a b, a hypothesis. Again we resolve. So, x should be replaced by a, that is the most general unifier of not of B a b, B x v; you get P f of a.

This comes from 3, 4, resolution with x substituted by a. Now not P is there, so they will resolve; not P u, hypothesis and 7 is bottom. Not of this unifies with u substituted by f of a. So, 5, 6 resolution with u substituted by f of a; that is it. We had never used this; fine. That is how our resolution will proceed.

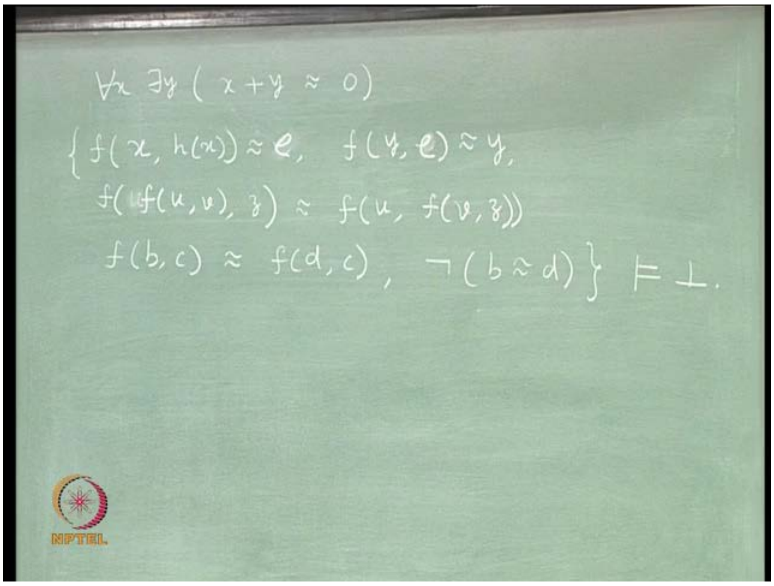
Let us take one more example. Suppose, you have some b plus c equal to d plus c. Next, how do you proceed proving that b equal to d? That is your cancellation law in schools. So, what you do is, take b plus c plus minus c on both the sides; minus c is the inverse of c; then you use associativity, so it was like this earlier. Then, you use associativity to get b plus c plus minus c equal to d plus c plus minus c. Then you use identity element; it gives b plus 0, d plus 0; that is definition of inverse itself. Next, property of identity element. So, b equal to d. That is how you proceed by informal arguments.

(Refer Slide Time: 11:41)



What have we used? Existence of inverse element, property of the inverse element, that becomes 0, and associativity. Then, property of the identity element. These are the things we are using. Let us see what are the axioms of the group itself. The group axioms you are using is what are available. One is a closure rule: for every x and y there is z such that x plus y is equal to z. For each x for each y there is z such that x plus y equal to z, that is your closure of the addition. Next, we use say, associativity. It says, for every x for every y for every z, x plus y plus z equal, let us write equal to this way, x plus y plus z. Next, identity element; identity says, there exists something which behaves like your identity; is that so? That is, for any x. So, you say there is x for every y such that y plus x equal to y; that is what you had used here on the right side. Only left side, we are not taking. Now, one more bracket will be there. No? Yeah, it ranges over everything, in associativity. Next, you have the inverse element which says, for each x there is y such that x plus y equal to that 0; 0 element which is the identity. Here, we are telling, call this as x; there is x for every y, call this as 0, so you can include directly as 0; does not matter, a constant, you can use that constant. Let us simplify it; it will be easy for us. There exists says that, x is called 0, we just take it; now it is combined, so then we say: for every x there is y such that x plus y is equal to 0; y is the inverse of that x. These are the four axioms of a group.

(Refer Slide Time: 15:09)



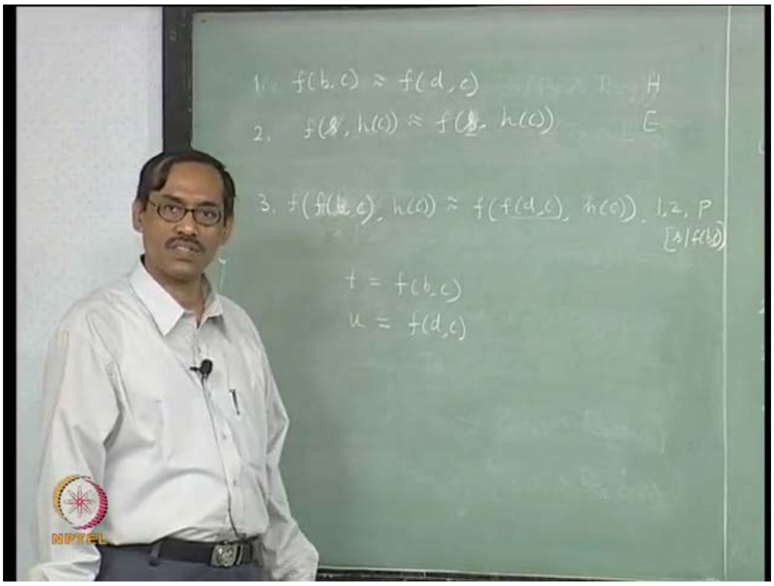
Now, when you write in clausal form, how will they look? First thing is, you cannot write this plus symbol; that is a function, of? It is a binary function, two-ary function, say f of x y, right, equal to this. Anyway, 0 we will introduce as it is. One more is this one: for every x, there is y; then you skolemize; then you say x plus some h of x equal to 0; when you skolemize this, this y will depend on x automatically. That means x plus some h of x equal to 0, so that will be our clause, directly.

So, let us write this in clause form. It will look like f of, we start from this f of x comma h of x equal to 0, equal to some constant, which constant we take? We can write 0, or let us write c in our language. Just omit it in clausal form. In clausal form every free variable is universally quantified, so we directly write them as clauses. Next, for every y, y plus 0 equal to c, that is, f of y comma c equal to y. This one. Next, this one, how do you write? For every x for every y there is z, x plus y equal to z. This is really f of x plus y, so, f of x plus y exists for every x y, that is what it will say; we assume that implicitly. We do not have to worry. Or, you can say this z becomes some x and y, so we write z equal to some function; this is already f of x y, so f of x y equal to g of x y, that is what it will say. Let us go to next one, associativity. That, you can write as f of, let us not use x and y, say u v, and z. Already two clauses are there. So, let us write u, again f, f of u v comma z, z we can use, equal to f of u comma f of v comma z. Abelian? Abelian group is not required here, we are just taking a group.

Next, we wanted to prove the cancellation law. Now, there is a premise; the given premise is b plus c equal to d plus c. From there this c is canceled, you get b and d; that is all, fine?

Now, yeah? We have already used c. Let us change something; say, let us write as e. Now something is given: f of b comma c equal to f of b comma c; from which we want to see that this entails b equal d, fine. That should be our conclusion. This entails b equal to d. So, we also assume not of b equal to d; and try a refutation of this. This is the formulation. Now we have to go for the resolution proof.

(Refer Slide Time: 20:56)



b plus c equal to d plus c. We start from there. That says, f of c equal to f of d c; hypothesis. Next, what we are doing? B plus c; we are adding with minus, so that means f of whatever is given comma h of c inverse, that is our inverse now; comma h of c. How do you do that? From this, we want to see that f of f b c comma h c equal to f f of d c comma; we want this to follow; which rule will allow you to do that? It is the closure rule that is allowing us. This rule is allowing us, whatever x y you take you can add them to get an element. That is assumed because f of any term will be another term, and terms can always be interpreted. It is implicitly there in the semantics. Fine?

Once it is a function, its semantics allows that there an element, but then within resolution how to infer it? That is the problem. So, f of, take some p, does not matter, call it a variable. Now, p, h of c equal to f of p h of c, equality that p, if you want you write s, first time you are using, so let us write s instead of p; s there; so, that is your X. Now this X of s when you write, it is not necessary that every s will be substituted; it is not a variable to be substituted by a term. Any occurrence you can specify. That occurrence will be substituted; everything need not be substituted; that is the freedom we have with paramodulant. So here, suppose we take this s and unify this t; this is your u with t and you delete that plus t equal to u, delete X s and introduce X of u; in place of s you are using some u. Let us write here. This s, I am replacing by u; it is there. The other s, I do not have to replace; it is kept as it is.

Now, what happens? If that is my s, this is my X, where s is there; X s will give me X of u. So, here it should have been s. That is your X of u, is that ok? u is f of d c, t is f of b c, so t equal to u is deleted, in X of s, one s or many s's, we can substitute by that u. That is what I have done on u, other one is left out. the left. So one step is ok. This is the third one which is obtained from 1 and 2 by paramodulation. In fact with the sigma s t, remember, if that is your s and this is your t, then on s u, you have to apply sigma, right? What is your sigma here? m g u of? m g u of s and t; two terms s and t; s is a variable here t is f of b c. So, their m g u is s by f of b c, right? So, this paramodulant sigma would have s by f of b c, so this s will be f of b c, is that clear now? It follows by paramodulation.

So, what I do? I take t equal to f of b c, u equal to f of d c. I have one clause t equal to u, another clause X of s, so what is my X of s? This s, I forget this. In that formula, this s, I am concentrating on; that is X of s. Now I have to delete t equal to u, delete X of s, introduce X of u. So, X of u means, this s will be replaced by u; so here it is s, here it is u, from this, that is my X of u, where s is here. But then, paramodulation says on X of u apply sigma; sigma is the most general unifier of s and t. So, s is here, t is here, their most general unifier is s by f of b c; that when applied on h of u x of u, s is replaced by f of b c; so directly this comes.

Student: I thinks we can replace only part, not everything.

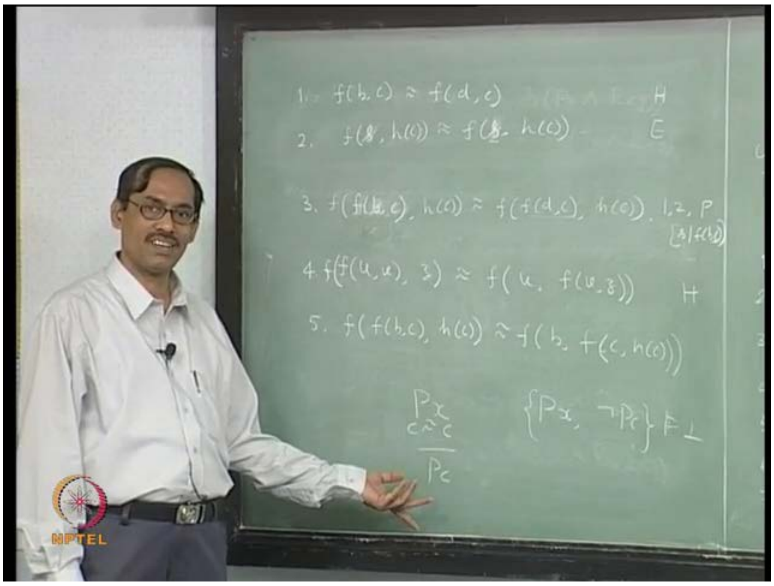
It allows to take X of s as part of one, that is what paramodulation says, we do not have to replace all the things. If we replace everything, then there no meaning of taking most general unifier. If one or many instances of s can be seen you can identify them as X of s; so there is some non determinism there. Suppose, there are many occurrences of s, I can take only one occurrence, I say this is my X of s; everything in X that is, I will be substituting. I can identify three or four, even all of them will be substituted at a time, the other one s will be remaining. I can introduce everything also s, suppose everything s, then it becomes f of d c h c, f of d c h c, that is all. So this require some practice, of paramodulation.

Student: Basically some instances of s we can replace by u and some as t.

Yes, that is what, because t equal to u, that is what paramodulation means, since t equal to u wherever s occurs. Some of the s, I can replace by t some of them I can replace by u, paramodulation allows it. That is what we really need. In this argument we are doing like that; some of them I replace by b plus c. Some of them I replace by d plus c. Clear? Now let us go further.

What is the next step? We have done associativity, we have used associativity on both the sides. Now, associativity, we have one clause for that; use that; f of, what is your clause? In terms of u b z; u b z equal to f of u comma f of b z right; this is our hypothesis. It is available with us as a clause. Now, what we want here is, this z should be h c, this f of b c, u should be b, b should be c. Then, one side of that will come. But what you get here is, f of b c, h c will be giving f of b comma f of c h c. So two steps will be required. At a time you cannot do here. What we want here is that from this and this we should get f of f of h c comma h of c equal to f of b comma f of c comma h of c. This would follow; one side of it. That is again paramodulation? Yes, with what? Paramodulation with what? We thought we will be taking that paramodulation.

(Refer Slide Time: 28:49)

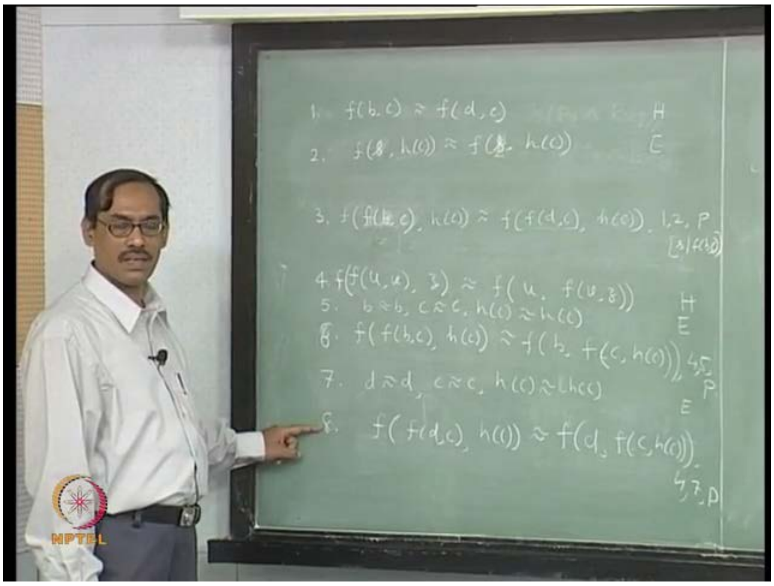


Suppose you take t equal to u here; this is my t this is my u. Then this is my X of s, s is say, z or something; now what would you do? z should be replaced by something; which thing will we replace? z will be replaced by h c, then? But u will introduce d again. If you take t equal to u, then when you take X of t, it will introduce the whole thing here. Do you see? See the problem or not? First, you have to realize the problem. See, from these two, you want to infer this; how do you infer? With associativity. But you say u should be substituted by b, v by c, z by h c; but that is, which rule allows that? Which rule allows that from this it will follow?

Well, let us see, say, temporarily; you have P x you have to infer P c from it; how you do it? You cannot do it here, in resolution. There is no rule to do it. How to do it in resolution? You can write it as a derived rule, once you do it. Before it, you cannot do. You have to do it through resolution only. So, how to do it in resolution? From P x, how to infer P c? Well, this inference we can do twice, say, P x and not P c and that entails bottom. In resolution therefore, P x entails P c, but this becomes a derived rule now. If you have X of x 1 to x n and then you can infer X of t 1 to t n; that becomes a derived rule; but directly it does not come. It comes as a meta theorem. you can use that as a meta theorem and get it done; not just by resolution. But paramodulation also can do it. For example, with P x, I introduce c equal to c, equality. Why? This is my t, this is my u, this is s; so t equal to u gone, X s gone; X of u. I get this. s is s, that is replaced by u, u is c, and t equal to u. So, most general unifier is f t, empty substitution, right? sigma is equal to empty substitution itself, because t equal to u. Now, t equal to s, when you take, substituted by c, from t and s you want, most general unifier you want; not t u. So, that is x by c, but once you replace this, this becomes P c, there is no X; so even if you applly, it does not matter; same P c remains. So, by paramodulation this follows.

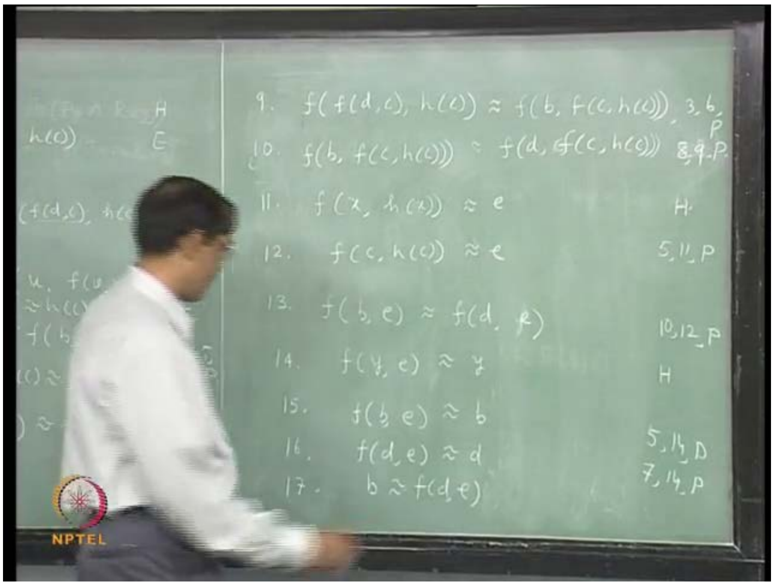
You do not have go to resolution again; by paramodulation inside the proof, you can do. Then here, similarly if you do, you have to do really three steps: b equal to b, then get b v z as it is; then c equal to c get v by c as it is, then z equal to h c equal to h c, then z h c will unify, you will get this. So three steps it we will take.

(Refer Slide Time: 34:54)



So, what we do, we will make a shortcut here. We will write five parts b equal to b, c equal to c, h of c equal to h of c, we will write equal to it; then three times using paramodulation, you will get this. So, by paramodulation. Ok? Clear, how this step is going? Next, similarly this is sixth step. Then seventh, what we do from this side? You have to do something from the other. c h c, d equal to d, c equal to c, h of c equal to h of c. If you do step by step, this will not be necessary, because they are already introduced somewhere; c equal to c is another line, h c equal to h c another line. So, you can again use these two. You do not have to write. But this is a better mnemonic for us that we are using these things, then eighth will be f of f of d, c h c equal to f of d f of c h c. This is 6, not 6, 7 and 4, 7 paramodulation; that we have got f of b h c equal to c f of d c, h c equal to f d, f c, h c.

(Refer Slide Time: 37:50)



From these two, you wanted to conclude these two are equal, it is like x equal to y and then what else we have x equal to y then y equal to z. Then, x equal to w then z equal to w; three things will be used; 3, 6 and 8. See, f of b c h c, f of d c, h c, now f of d c h c equal to f of b h c h c. Therefore, these two will be equal. Write down the other side to conclude that step. Now, from three, see this one from 3 and 6, from these two you wanted to conclude f of f of b c, b c, c is on the left side. This one, these two will be coming; f of b comma f of c h c equal to f of f of d c h c. Look at three and six. This is one, say, alpha; first one is alpha, alpha equal to beta, alpha equal to gamma, you want beta equal to gamma. You wrote as gamma equal to beta.

Now, how do you get it? Let us take in that form: alpha equal to beta. Then we have alpha equal to gamma equal to beta; this is how it should come. Does it follow from paramodulation? Let us take alpha equal to beta as t equal to u, finally you have something; beta is there; so this is t, this is u. Now, s is what? alpha. Then we identify this as alpha. This as alpha something; one of them I have to take as s. Then what happens, s will be, s will be replced, this will be going; this will also be going; you have to take X of u. Suppose I take alpha as s, then this will become beta; beta equal to gamma will follow. Is that right? Let us write that way. beta equal to gamma; that will follow if I take this as t, this as u, this is my t, this is u, and this is s. So, this is my X s; finally, x of u equal to whatever it is, X of u is beta equal to gamma. And, s, t their most general unifier is empty, because that is same here. Right? So it will follow; beta equal to gamma.

Fine? So, let us write them in that form. Instead of this form, we get f of f of d c comma h c equal to the other one f of b, f of c h c. This follows by 3, 6 paramodulation. You have empty substitution as the most general unifier. Next, you want to use what? 3 and 8. Similarly, if you use 3 and 8, f b c h c that is your alpha, now that common thing, and one of them is beta, and the other one is gamma; so which side you take does not matter. This will be equal to this. You have already f of c h c. So, you can write that. We can write there is, f of b, f of c, h c equal to f of d, c, h c; this is again 3, 8 paramodulation.

We want really one of these. We do not need both of them; any one of them should have done, right? Is it not? See, this c and h c, you want to combine. So, they are combined here; this c f c we want to combine; they are combined here. So what we want is, we should have b f c h c and d f c h c; that is what we have got. Then to get it you have to use what? 3 and 8? Does 8 give? f c s c is this b of f c s c; so these two are combined; these two will be same; then you get b c, not this. If you use that, 3, 8 you would get in this form: f b c h c. In this form. Yaah. That is what. That is what we wanted, in this form. You want the other format. If you use 3, you will be getting this form only.

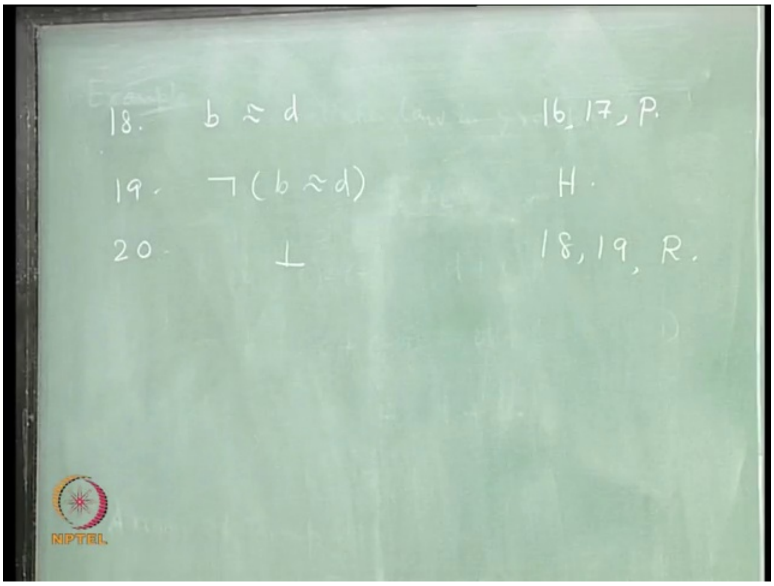
Student: We can use 8 and 9.

Yes, if we use 8 and 9, we will get the required one. So you really wanted this one: f of b f of c h c, so you have to use 8, 9, paramodulation. This is only the trickiest part in the resolution method. Because, it depends on which one you want; that is how will be choosing the premises and getting the conclusion.

Now, once this is done, we have come up to this stage of our argument. This does. Really? We have to go for c plus c minus c equal to 0; that is to be done. That means c h c should be replaced by 0. Which premise gives that? X, x equal to e, f of x h x equal to e; that is a hypothesis. Now, with this you want to substitute, get c, and x equal to b? No. f of c h c you want. Next c equal to c required; it is already introduced somewhere; 5, there. Let us forget it; this is only for our reference; it is already there, in fact, this 5 will be, 5 prime, 5 double prime; two stages are there. That is already there; so then, we say 12^{th}. That gives f of c h c equal to e, that is from, 5, 11, paramodulation. These heuristic rules will really help. Once we know one equality is there, it will follow like that. If P x, then P c will follow. How? by introducing c equal to c. Then similarly, 13, we want d equal to d, that is in 7, so you get f of d. No, that is not required; we do not require this; from this we can go. Now, 13, what you will get here? This is your t, this is your u, this is your s. Complete it. Ok? So replace them; you get f of b comma u which is e, so it will come in f of b e equal to f of d; you can take this s also, simultaneously, many s's you can take at the same time. So, this, we will write as e; this gives 10, 12, paramodulation. X of u, so you can identify both the s; and then replace.

You are at this stage, now d plus 0 equal to d plus 0. Next you need a premise, which one? f of y equal to f of y, so 14, f of y e equal to y, that is a hypothesis. Again we need here is what? 5 is b equal to b, so take here. So 5, 14 would give f of b e be equal to b, right? You need b equal to b there; that is a 5, 5, 14 paramodulation. 16 will be f of d e equal to d, similarly, but that is in 7 now; 7, 14 paramodulation. Then, from this 13, 17 is 13 and 15; 15, 16, then you need 13. Let us say, 13, and 15. 13, 15 would give b equal to f d; so, 13, 15 paramodulation.

(Refer Slide Time: 48:22)



Next, you need one more: 18, that gives 16, 17, b equal to d. Next, it is not over; hypothesis, 18, 19, resolution. So, that is how you have to proceed using paramodulation. But recall the heuristics we have used; those things will be really helpful.