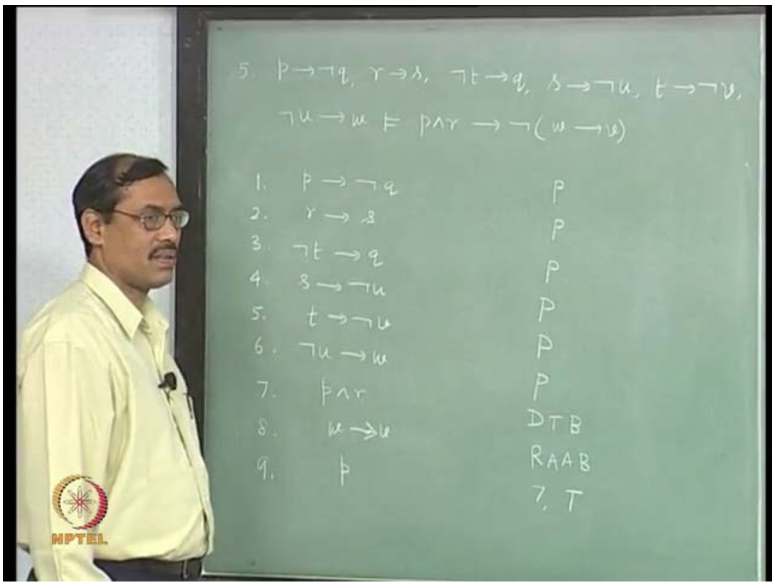
Mathematical Logic
Prof. Arindama Singh
Department of Mathematics
Indian Institute of Technology, Madras

Module - 1
Lecture - 8
More Informal Proofs

We had seen the calculations and how to introduce informal proofs, instead of the calculations. In calculations, we found a difficulty in, using the deduction theorem and reductio ad absurdum inside the proofs. So, they are to be put as sub-calculations inside a calculation; that is what we wanted to avoid, though this can be done. Then we introduced informal proofs, but informal proofs also have some limitations. Like, they go only for the consequence relation; they do not show equivalence directly. If you want to show p if and only of q then you have to show two consequences: p entails q and q entails p. None the less, let us use it.

So, the fifth one we were discussing last time; it is this. It is also customary to start one informal proof by first listing all the premises. Then whenever you want you use that, right? That is not always followed, but it is a custom. So, let us try with that.

(Refer Slide Time: 01:23)



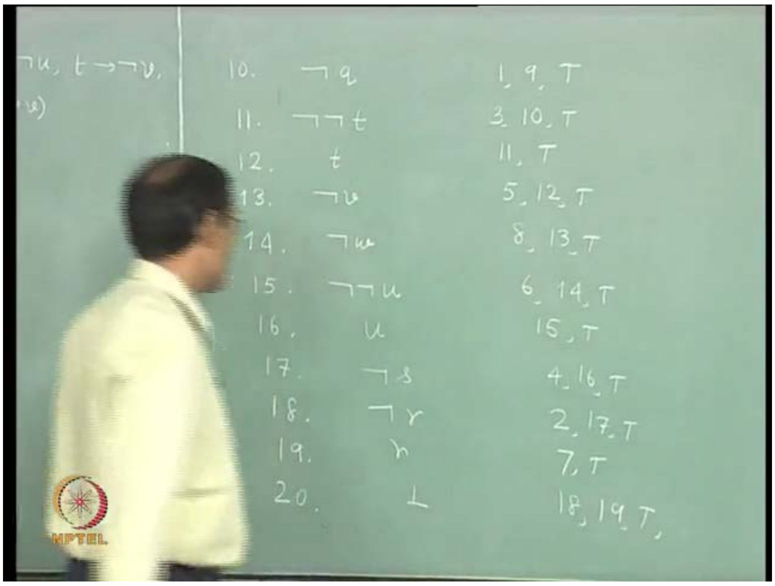
Say, we will have one informal proof in this manner; first, list all the premises, include `P' in the documentation part; so, these are all the premises. There ends our premises. Then you have to go to the conclusion. Now, when you see that the conclusion is in the form of an implication, we are going to use the deduction theorem. That means, we take its antecedent, this p and r as extra hypotheses or extra premises; and you document it as deduction theorem begins. We start with the seventh line as p and r, which we will be writing as deduction theorem begins.

Then our aim is to prove that not of w implies v; and there is a way here; we can start with reductio ad absurdum; because it is in the not form, which you are not going to use it. You may start with w implies v in the beginning as another extra premise. There is another alternative: you may think of proving this by first proving its equivalence, which is w and not v, not of w implies v is equivalent to w and not v. You may proceed by getting w and then not v, then bring it to w and not v; then not of w implies v. That is one alternative. Another is the reductio ad absurdum. We will start using reductio ad absurdum here. Because? We want to show how the nesting is done in the loops; an application of these meta theorems.

So, let us take the w implies v as the next extra premise. We say eight, which is w implies v; here, we have to write: reductio ad absurdum begins. Then, what is our strategy? How do you get a contradiction? It is starting from p, this is also starting from r and we have p and r. We start with concluding p from p and r, similarly r from p and r. Then apply these two premises and modus ponens. Let us take p, this follows from seven. You are using p and r entails p, that is your elimination, law of elimination. If you do not remember the laws, there is another alternative, but be aware of bluffing. There, you may just write `T' for tautology; you know that, this is already done. Only when you are experienced and you do not want to bluff, you can say: well, I know this as a theorem, I do not know what its name is. Then, just write `T'! It is really the law of elimination, p and r entails p, that is what you are using.

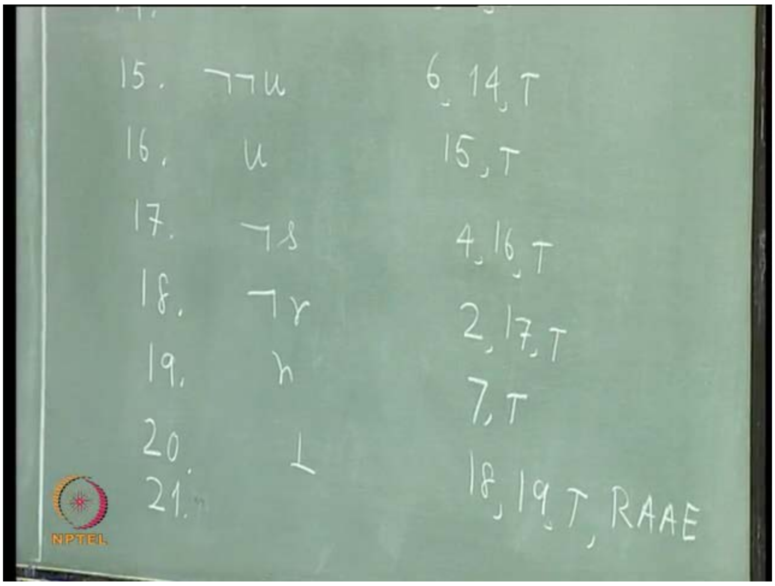
Then, our plan is to use this p along with p implies not q, and use modus ponens. That gives you not q from line 1, line 9 and modus ponens, even if you do not remember modus ponens, you are allowed to write `T'. Now then what we want to do? Try to see wherever q appears. It is in the third line, not t implies q, and you have not q. You can use modus tolens, and it will give not of not of t. So, that gives not not t by using line 3, T, again, modus talons. You do not remember the name, just write T. So, not not t, first bring it to t, using double negation. Now, you have a nice formula, double negation, you do not remember? So, write T; then what is our plan here? Here there is, modus ponens we can use.

(Refer Slide Time: 05:17)



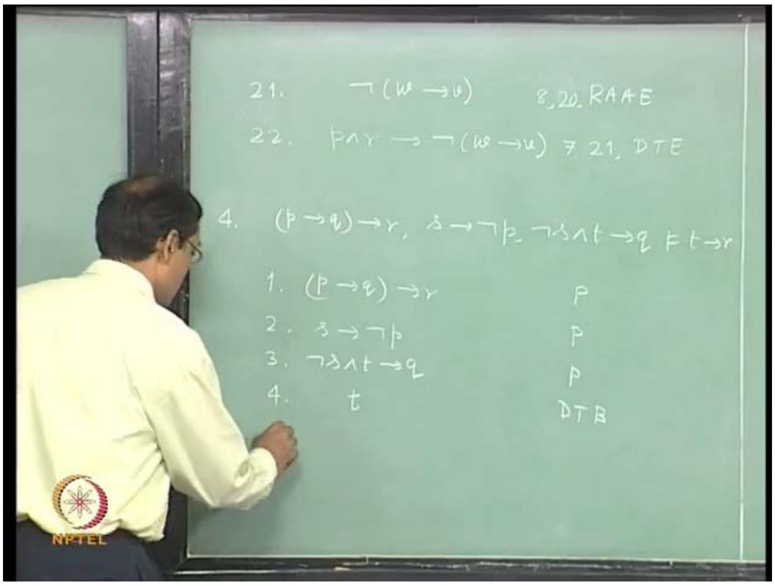
That will give us not v from line 5, 12, modus ponens. Next, how do use not v? Well, you can use here, again, modus talons. So, 14, gives not w and you are using from 13, modulus tolens, next, can go to this. That gives not not u, using 6,14, modus tolens. Let us bring it to better form, so u, double negation. Next? We have got u. So, again this is appearing here; so seventeen is not s, that comes from 4,16, modus talons. 2, that gives not r, same way; 2, 17, modus tolens, next, from 7, p and r will give us r. That would give us a contradiction. So, write 19, r, that comes from 7, elimination. We have got r we have got not r, therefore bottom.

(Refer Slide Time: 07:13)



Now, the problem is, this is not complete, because you have taken two extra assumptions one is p and r, another is w implies v. Where does that end? You have taken one extra assumption here, p and r, you have also taken another extra assumption w implies v, where do they end. Well, anywhere you could have ended; this requires your premise p and r, 7 is being there, beyond that there is no seven. So, there itself you could have stopped and till that p and r implies the other things, but it is easier to end it here itself. So, here you may say; which one to end first? This is the inside loop, so write RAAE; that ends here. When that ends here, what do you get? Let us write 21 over the other side. What we get that, when you end RAA, RAA starts with the premise w implies v. So, you will be writing w implies v, its negation, because assuming w implies v gives you a contradiction. So, its negation must be valid. So, you will be writing not of w implies v. There only, we have to write RAAE; not here, because that is what you are concluding. After you see that top is over, or bottom you have reached. It is unsatisfiable, by applying the RAA, you are obtaining that not of w implies v. So, documentation should not be here, documentation should be over there.

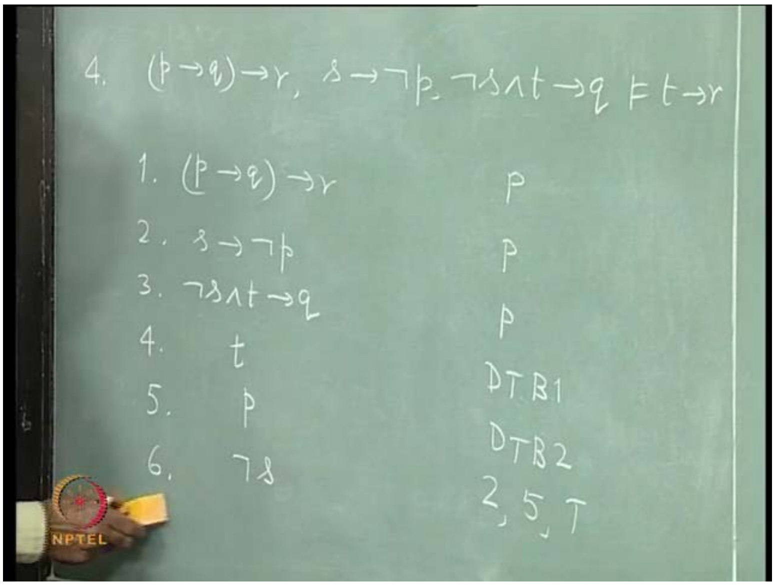
(Refer Slide Time: 10:36)



We should write RAAE over here, instead of on line 20. Once you come to RAAE, that means the conditionality of w implies v, that premise, is removed. Now, you do not have this assumption in the proof, that is what reductio ad absurdum says. Fine? But still there is another conditionality; it is p and r. By deduction theorem would conclude that w implies v has been obtained, its negation has been obtained by assuming p and r. So, p and r implies negation of that; is it clear? There you are using the deduction theorem. p and r implies not of w implies v; here ends the deduction theorem. And you can also documented the line numbers, like you are getting this RAA, due to seventh line, sorry eighth line, and nineteenth line. Here, you can document as eight, nineteen, RAA; 8 and 20, because on twentieth only you are getting a contradiction. Similarly for DTE, you will be getting twenty one, you are getting as a conclusion, and when it starts at seventh one. So, you documented it as 7, 20, DTE; 21. There ends the proof. Is it clear?

So, let us see the fourth problem; that should be easier. That problem says, we go from p implies q implies r, s implies not p, not s and t implies q; that should give us t implies r. Here again your strategy says if you use deduction theorem assume t, infer r. If you want to use reductio ad absurdum, you start with not of t implies r, that will give you t, that will also give you not r. That is same thing as telling entails t as an extra premises, concluding r, and after that using the reductio ad absurdum; t, then not r also, then introduce a, or infer one contradiction. But here it may be possible to get r directly without going to RAA, so let us see that. We start with the premises, first p implies q implies r is a premise, s implies not p is a premise, not s and t implies q is a premise. Now comes the extra premise, because of deduction theorem. We said t, deduction theorem begins. Our aim is to get r. So, how to get r? We can get if we prove p implies q, but how to prove p implies q? Use deduction theorem assume p infer q.

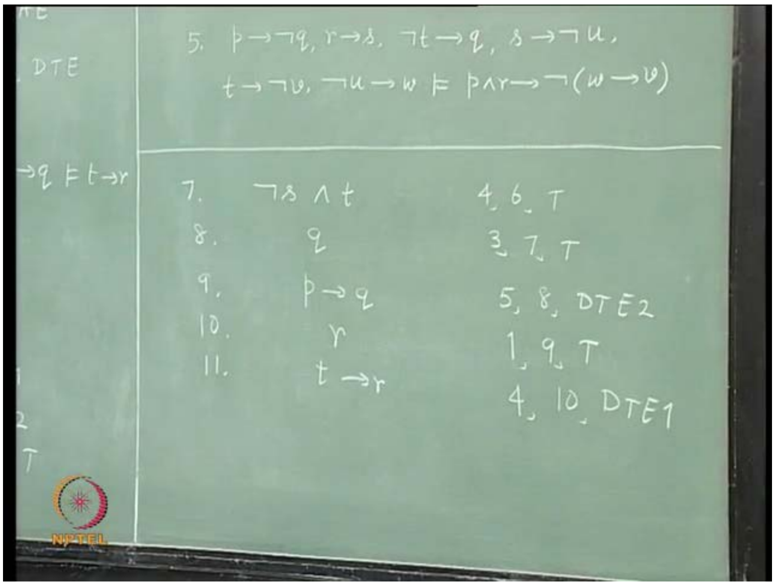
(Refer Slide Time: 14:20)



So, you take another extra hypothesis as p; you say deduction theorem begins, but then there is a problem. You took one here, two here. The loop for deduction theorem two should be inside that of one, that is our idea here. Now p is an extra premise, how do we proceed? How do we begin with p? You need to show r. Now, we have a premise, which says p implies q implies r. We can prove p implies q by one application of modus ponens, it is done.

Now, how to prove p implies q by deduction theorem? I can assume p and deduce q, that is what I am doing. So, it is a sub-proof inside the proof, now that is possible, because of this looping and nesting. Now, once you assume p what should we do next? Six gives not s because two, five, modus tolens. You have not s, you have t. We will write here, seventh line, gives us not s and t first, not q directly.

(Refer Slide Time: 17:18)



That is an introduction: if you have a premise as x, a premise as y, then we can infer x and y; that is introduction of and. We go for not s and t, and that is inferred from lines four and six, by the law of introduction. We are free to use T now. Yes? Any problem? Next, we, our plan was to use this, third one, so we get q from three, seven, and modus ponens. Our aim was to prove p implies q, we have assumed p in the fifth line, got q. First, lets go to p implies q there, deduction theorem, application or second application will end. So, write nine as p implies q, and document as, that premise was introduced in five, line five; so, five, eight, deduction theorem ends here, its second end; is that ok?

By writing this conditionality of p is removed, we have no more assumed p, because of deduction theorem. So, p implies q is deduced from our premises, and possibly, the extra assumption DTB1. We do not know that one, but now you can use all the premises anywhere. So, our plan was to use this. ten. That gives us r, that is, from line one, line nine, modus ponens. Is that right?

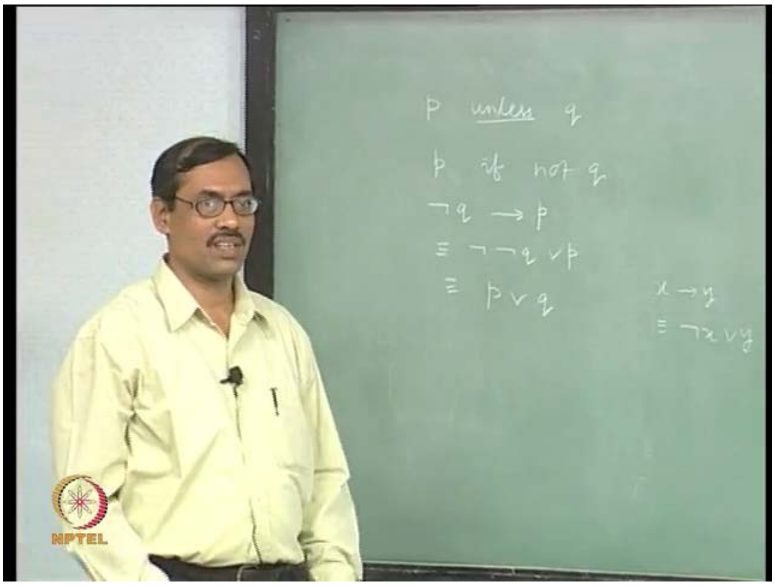
You have got r; still there is a conditionality, here, that has not ended. That assumption was t, therefore we get t implies r, which line was it? Fourth line. So write four, ten, and DTE1; is it clear? The advantage is, we can read the proof easily. What is happening inside the proof, that is very clear. You can see the construction also; how did we proceed thinking towards the proof. The whole process was decoded, or encoded here, while reading it you have to decode it. Is it clear?

This informal proofs and the equivalences or the calculations can be used for many other purposes, not only for proving. See, a usual practical problem, it does not come with symbolization, you have to understand and symbolize it. That requires something more, just like a mathematical modeling. Just by knowing some differential equations you may not be able to solve practical problems. You have to understand what is their meaning, how they are connected and how to model it. The same way, in propositional logic, we are concerned with the connectives, so you must know what are the meanings of connectives used in the natural languages. And is used as and, that is no problem, or is used as or, there is no problem, implies used as if then also; if something, then something; you have to write it as implies. Sometimes you will write q provided that p. So you know, it is p implies q. Some similar concerns will be required. But there are some connectives, which will be difficult to decode.

For example, unless, how do you go about it? You say p unless q. When you say p unless q, p if not q, p if not q, that is your first task; p if not q. Let us write it that way, p if not q; which is simply not q implies p. Now, what happens, if you use the equivalences not q implies p will be equivalent to not of not q or p. Because, you know x implies y is equivalent to not x or y. This is true when x is false or y is true, these are the only case when this becomes true. It is equivalent to not x or y. Now once you apply it, you get this, which is simply p or q. So, unless becomes simply or in our language of propositional logic.

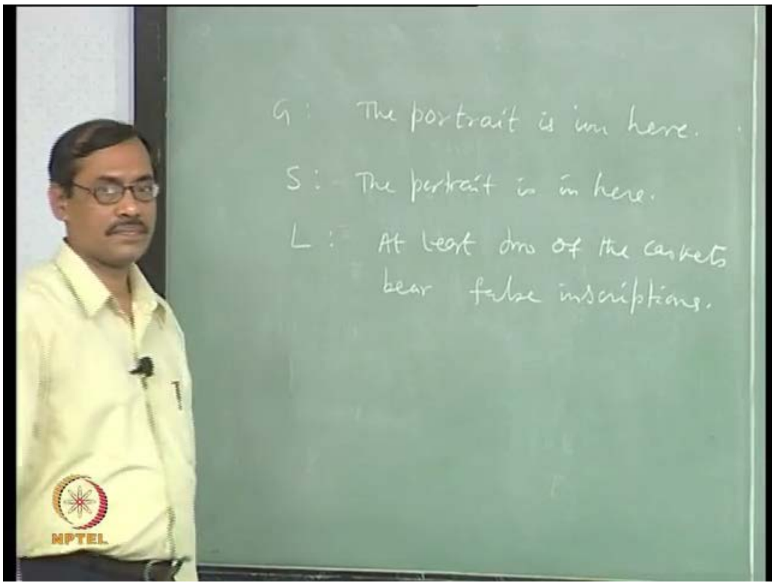
Now what about until? Until and unless, they are same, because there is no time in propositional logic. There is no concern for time in propositional logic. Time is simply omitted, and we cannot really correctly symbolize until, because we do not have the concept of time here. So, it will be simply interpreted as unless, and that is or. It will not be correct when you apply in the programming scenario. There you have to go for another logic propositional logic is not completely adequate there, but at best which can be done is, until will be translated as unless, which will again be symbolized as or, is it clear? Sometimes in natural languages problems do not come as problems. They will come as stories, then you have to decode it correctly.

(Refer Slide Time: 21:37)



For example if you have read merchant of Venice you would have got nice problems, have you read? So, its heroin Portia, she says, what she says, among all my suitors, I will choose the one who passes my test. The test is this, she takes three caskets, one gold casket, one silver casket, one lead casket. In one of the caskets only she put her portrait and then locks them. On each of the caskets she writes one sentence that she called an inscription. Now, she brings all these three boxes in front of the suitors. And then she declares that you read the inscriptions written on the caskets and I guarantee that it may not be true, the inscriptions may not be true. Now, from that you have to find out where the portrait is. She gives the boxes. On the gold box something is written. Let us say, the inscription is the portrait is here, and on the silver casket it is written the portrait is in here. Now, you see all of them cannot be true together. On the lead casket it is written at least two of the caskets bear false inscriptions.

(Refer Slide Time: 25:00)



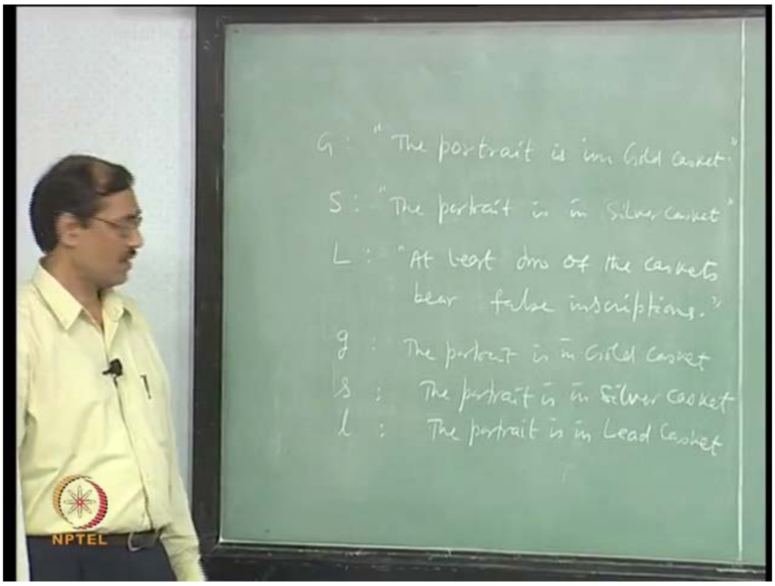
Now, it is a real logical task. Something, some solution will come. There may not be any suggestion, we do not know, she might have lied completely. Because she is fond of that. Informally, what you can do is, start looking at these caskets, where the portrait may be, is it consistent. So, if she puts in the lead casket, then what happens? Suppose the portrait is in the lead casket. So, this is false, this is false, at least two inscriptions are false. It is called consistent; it is a possible solution.

If you put inside the gold casket, what happens? G is true, S is false, what about L? It is true or false? If it is true then at least two of them should have been false, but two of them are becoming true, that will be definitely false. Right? If it is false, then what happens? At least two of them are false, is false. So, at most one of them can be false; this is already false, the other one cannot be, is that ok? It is not consistent in G, the same way in S also it will not be consistent. It does not matter, whether G or S, inscriptions are the same. So, it is in L, because that is the only consistent one we are finding; but this is the informal one. Now, how to formalize it? The problem is to formalize and prove really. Yes. She declared it, and not only at least one of them, it is in one of them.

Student: Best way to try is if it is in G, then it should be in S, because the inscriptions are the same.

Possible, but that is no formalization of that in propositional logic. That is what it is. Yeah, that is how you went to Lead.

(Refer Slide Time: 28:38)

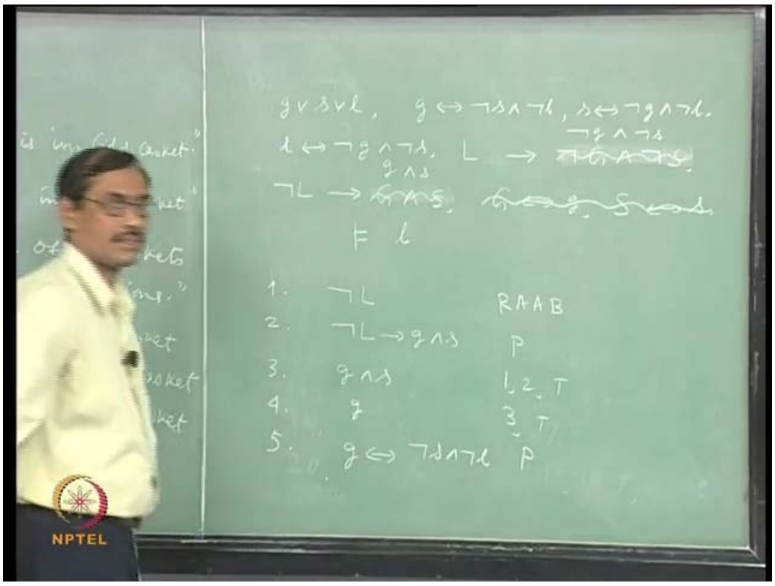


Let us try, let us try this way. Suppose I write G, capital G, for the inscription that is written on the gold casket. It is the inscription which is written on the gold casket. So, that means G will be `the portrait is in here', that sentence itself is G, as it is written. Then same way I write capital S for the inscription written on the silver casket, so it is this. In fact when you say `in here', here is really confusing. So, you have to change the inscription, this way, when you interpret. You say that the portrait is in the gold box casket. Not only here that is the inscription, that is the way we have to read G. So, G becomes the portrait is in gold casket. Similarly, S stands for, capital S stands for the portrait is in silver casket, capital L stands for the inscription on the lead, which is this itself, fine?

Let us introduce some more propositional variables: small g. What should be small g or something else? I am writing related to the gold casket. See one is the inscription that you are writing the portrait is in gold casket that is the inscription, but where is the portrait you do not know, that maybe true of false it is not given. So, let us write small g means the portrait is in gold casket, right? It is not the inscription, where is the portrait, for that we are symbolizing. So, this g is this inscription itself; you may write a quote for that. Now, small g will be the portrait is in gold casket. So, capital G is for the inscription written on the gold casket, small g is for the portrait is in the gold casket. Now, small s for the portrait is in silver casket; next small l for the portrait is in lead casket. Now, these are all propositional variables; not that the premises given. It is in one of the caskets, exactly one of the caskets.

Student: g or s or l, and of g, s.

(Refer Slide Time: 31:59)



g or s or l . If it is in one of them, it is not in the others. so g implies not s and not l. Similarly, s implies not g and not l is it? Next, l implies not g, not s. It is in exactly one of the caskets. Next, what are the other premises? Yeah, capital L implies not g. L, Capital L, if L is true, then at least two of them, we have false inscriptions that is true. That means g has to be false the other inscription g has to be false. The other inscription s has to be false, which says not g and not s. If L is false then? It says at most one of the inscriptions can be false. Already L is false therefore, other two must be true. G or S. Any other premise? Why implies, if and only if, yeah? Suppose the inscription, which is written on gold casket, is true. That means the portrait in here is true. So, small g is true and conversely. So, we have G if and only if small g, S if and only if small s. And our hypothesis is, our guess is, it should give us l. This is consistent, that is what we have found out, in the informal arguments.

Now, to show that really entails l. Portia is not irrational, is that ok? Now, how to go about it? How to prove this? There are so many, but so many may not be relevant. So, first thing is look at this, capital G small g, capital S small s. So, these two are premises; we do not need to consider all those capitals and smalls; is that ok?, for g and s. Instead of this capital G and S you could have taken small g and s also. That is your first observation, where else? Here, also you could have taken, but we are not able to think about L and small l.

We do not know, it does not say the portrait is in here. It is something else. Right? Those two you could do, because they are the same sentences. But for l, sentences are different. Let us do that first; once we do it, instead of this one, you would have gone for g and s. Then instead of this, you could have gone for not g and not s. You do not need the last one, now it is done. Now, how do you prove l from this? Where from should we start? Once you want to prove small l; where from it will follow; You have to check that. Where from it will follow? Small l. g and s will give what, not g and not s? Not of g and s is where? Here. That will give capital L, g or s? It is there. Can you get g or s? But g or s, see this is not of g or s. Demorgan. So, if you say g or s, then it will say not L. right, by contribution. So, you have to see that it does not happen.

Now, you go back, so once it is in l it is not in g and it is not in s, but if it is not in g, it is not in s. Then where is it? It is also in l. So, you should have? Is it ok? This is what you have missed; of course, it will follow from this, once you have this, that will also follow. Similar way you could have got your stronger premises. Now, to prove l you simply go for not g and not s, if you can show that, it is enough. Now, to give not g and not s? Somewhere hear or here? Where to show?

Student: we have an extra premise.

Which extra premise?

Student: not of capital L.

Not of L? So, suppose we start with not of L. Then, we get g and s. Then, g and s gives what?

Student: g and s both are true, that cannot be. g gives not s, so,...

No, his argument is, g and s is not possible.

Student: Yeah, g and s gives not s, and

Where it is not possible, we have shown?

Student: g implies not s, and not s.

No, you have g and s. He says it is not possible. That is clear from the context also. Does it follow from anywhere?

Student: g and s gives not l, small l.

g and s gives us g or s. By modus tolens, it gives us not l; this not l. Then?

Student: not g and not s gives not of g or s.

No, do not use that way. Go the other way. Not l gives g and s. g and s gives?

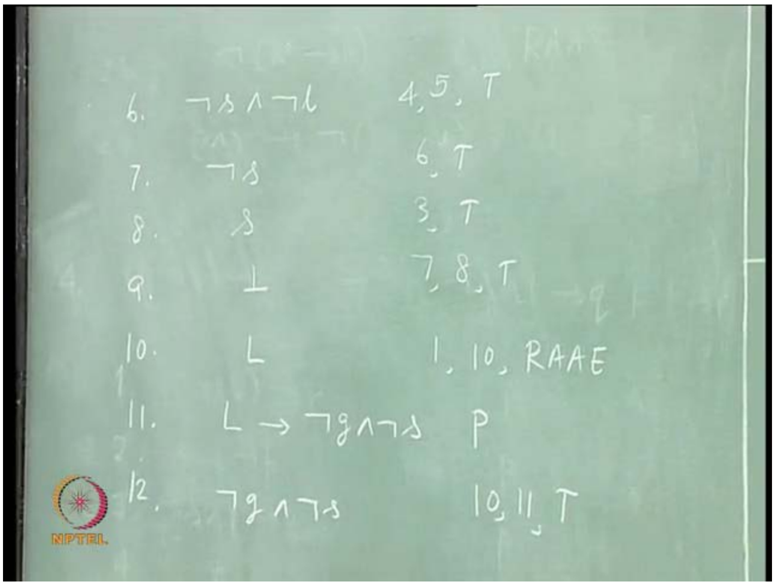
Student: g and s gives not s.

Not s? How?

Student: g imples not s and not l. so not s.

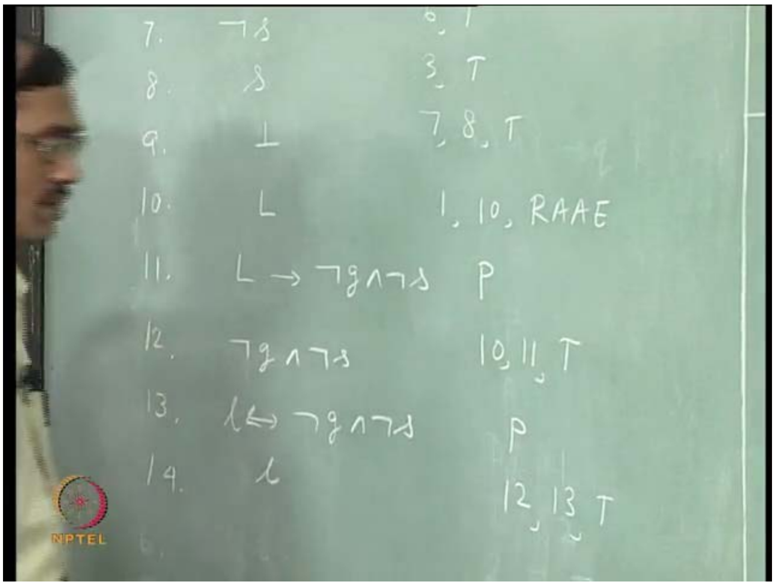
So? s and not s, that gives contradiction. Is it ok?

(Refer Slide Time: 42:05)



Now, where should we start? Not L. So, deduction theorem begins, or, you want to put RAA? Which one you want? RAA, you want? Let us try. So you have RAA begins. Next, we have to introduce the premise not L implies g and s, that is the premise, so you get g and s by modus ponens. Next? Use this. So, fourth one is, you need g from this, so three and tautology, which is elimination. Now, keep this, introduce that premise, g if and only if not s and not L, is a premise. You want to infer not s and not l, from line five, but not only line five, you have to use g also there. You write four also, that is really modus ponens, because g if and only if not is will give you g implies not s and not l. So, it is modus ponens. Now from this you get not s, elimination, then? This one gives g and s, that give s, so eight s, 3, elimination, that gives what? Bottom? 7, 8. This comes because of our extra assumption; therefore L, 1, you take 10, RAA ends, now you have L. Next you can utilize this. Let it be this, so eleven, l implies not g and not s, which is a premise. 12, not g and not s, from 10, 11, modus ponens.

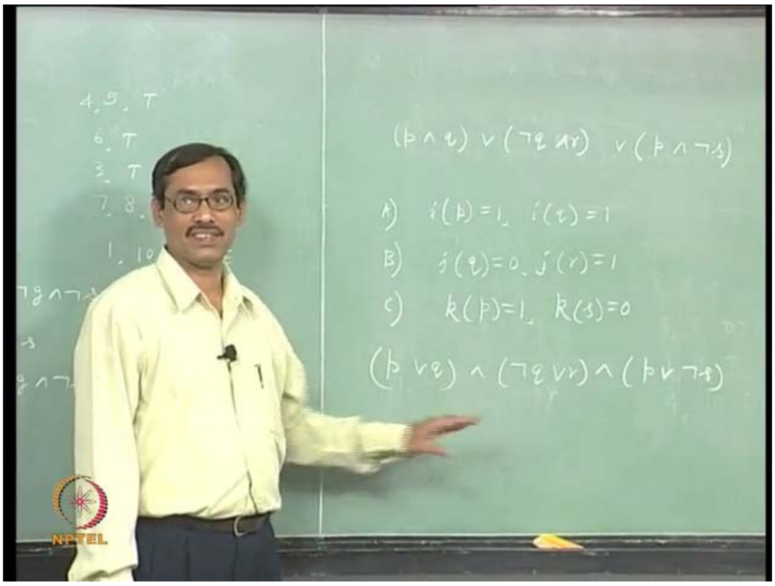
(Refer Slide Time: 44:01)



Next, that is a premise. Next, l, it is really modus ponens.

Fine, so, equivalence says can be used also for many other purposes. One of them, let us see, how to bring some propositions to nicer form, from where we can guess better things. Let us see one example, how does it go. Suppose, I write one proposition in this form. Suppose I take this proposition. Now, can you tell me what are its models? A model means you are searching for one interpretation, which makes the proposition true. It becomes one. It is an or proposition; it is or-ed together. This becomes one when anyone of them is one. One avenue will give you this as, one another possibility one, another possibility as this as one. Now, this is one and propositions it is a conjunction of many. So, this can be 1 and all of them are 1.

(Refer Slide Time: 44:44)



Now, we have three possibilities; one possibility says p must be 1 and q must be 1. In that case the proposition becomes 1; and the other possibility is, when not q is 1 r is 1. So, you say q is 0 and r is 1; and there is another possibility. When p is 1 and not s is 1. These are the three possibilities you get, looking at the proposition itself. There is no other possibility when it becomes 1, is that clear? Because, it is or.

Now, from this, of course, you can find out so many others. Like you have now four propositional variables involved, but you are considering only two propositional variables, so other two are free. Free means they can be either zero or one, does not matter, still this will be a model; so there will be four possibilities here. When you give r as 1 or 0, s as 1 or 0. Similarly here, there are again four possibilities, here also there are four possibilities. So, you get all the models directly looking at the preposition. This is certainly a nicer form to get?

Student: It does not give the number of models.

No, you have to go for that. You have to go for that finding out all the possibilities, that will give you the number of models. Now, suppose I change the or's and and's here. Now, I consider p or q, and not q or r, and p or not s; keep everything else as it is. The same way you can find the non-models of this. Just think about it.