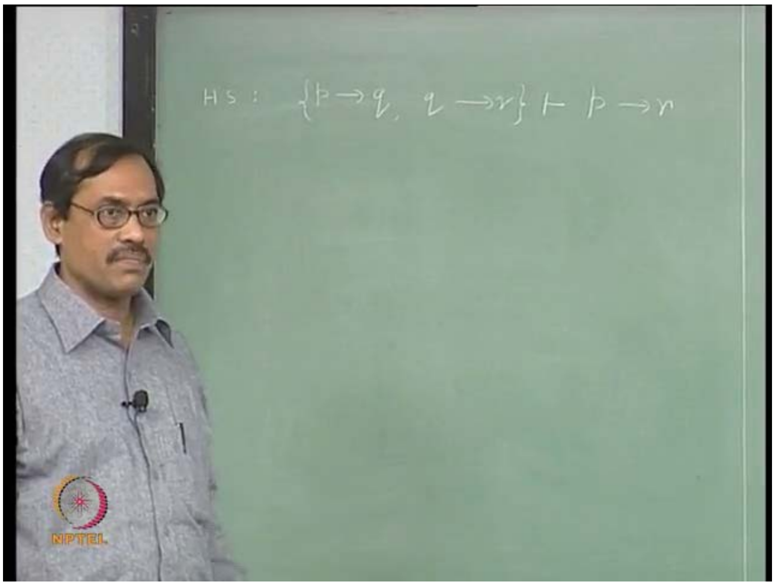
Mathematical Logic

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

Lecture - 16
Some Results about PC

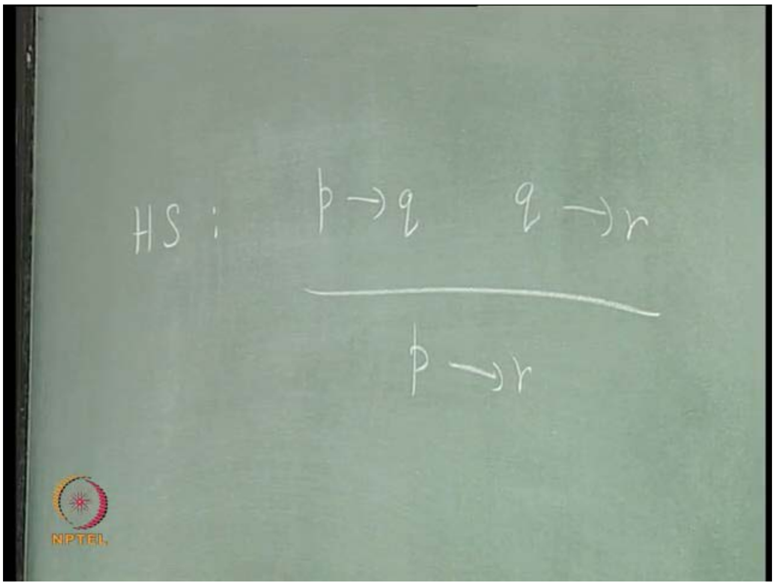
So, defined in the system, what the proof is, what the theorem is, what the derivation is and how a consequence is validated, it is not really valid, it is proved rather. How the theorems are proved, and how consequences are proved? Then on the way, we have given some comments like each axiom is an axiom scheme, each rule of inference is a rule of inference scheme, and then each theorem is also a theorem scheme, which can be used are axioms later. Similarly, each consequence becomes a consequence scheme. For example, we have proved HS in the last lecture.

(Refer Slide Time: 00:54)



HS says, HS says that p implies q, q implies r entails p implies r. This is what hypothetical syllogism says. We have proved this consequence. Now, once you see that this is a consequence scheme, that means you substitute any other propositions in place of p, q, r, whatever you get, that is also provable. This is what it says. In that case, it says that if you have p implies q, you have q implies r. Then you can deduce from it, p implies r, This is what it is telling. You can derive p implies r.

(Refer Slide Time: 01:46)

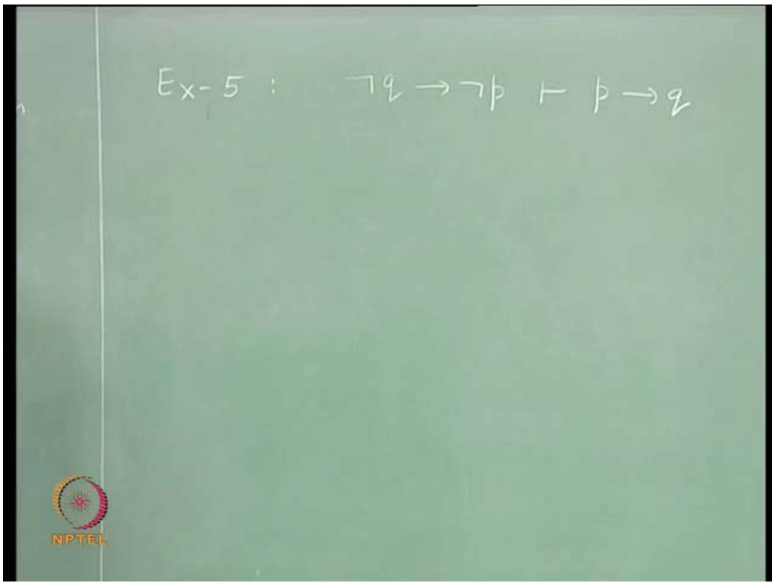


Then, you can write it as the inference rule, which says that, we will note it down as hypothetical syllogism, which says p implies q, q implies r, then you derive p implies r. Each consequence, in fact, gives raise to such an inference rule, which is, say, a derived inference rule. Just like theorems are termed as derived axioms, same way you can say consequence as derived inference rules. These inference rules can be used to prove something else. So, can be used means what?

Once you use it, that means you take some instance of these HS, where you have substituted p for something else, q for something else and r for something else probably. Suppose x, y, z are substituted instead of p, q, r; it means you will be really duplicating a proof of that instance of HS with x, y, z instead of p, q, r. Because it has a proof, the same proof can be duplicated and inserted there wherever you want to prove. That is the meaning of derived inference rules. Let us try to prove something using this HS as a derived inference rule.

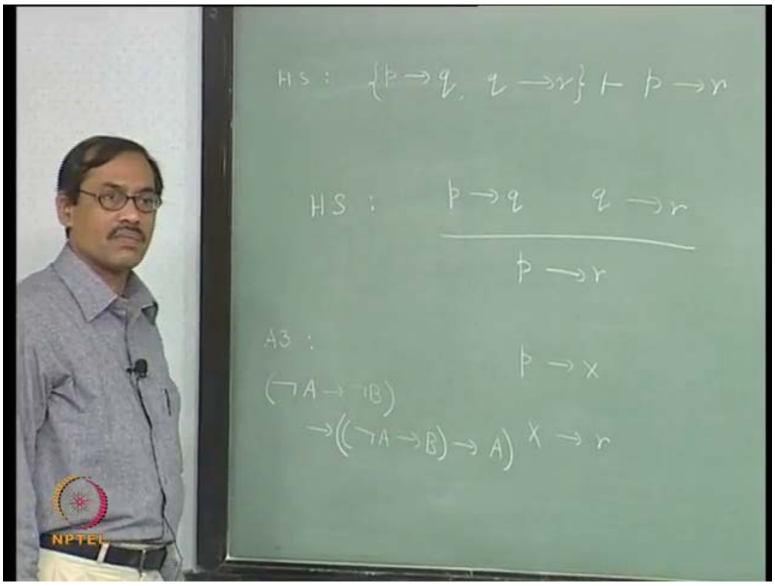
Suppose we give this: not q implies not v implies p implies q. Let us try a proof of this probably using HS. If you want to illustrate, our HS is used. We want to conclude p implies q later. If HS is used that means p implies something, say, x and x implies r. This is how it should be going. Is it clear? You want to derive this using HS.

(Refer Slide Time: 03:02)



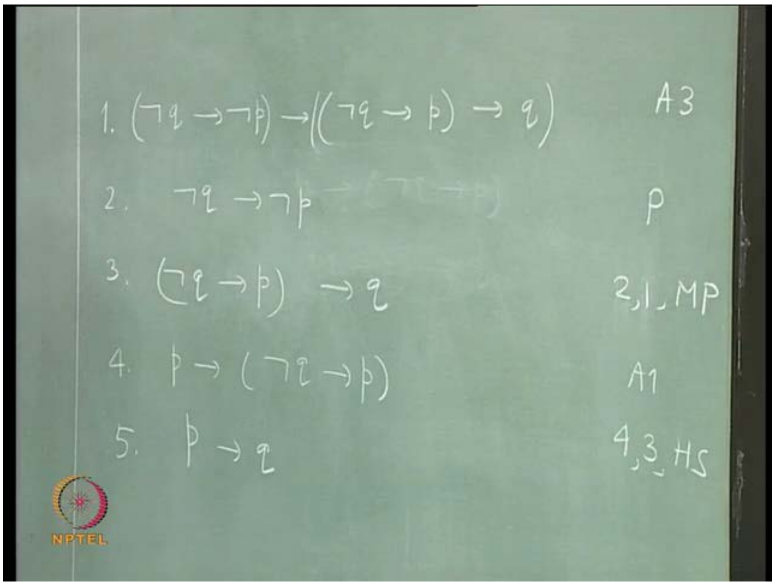
That means before that step somewhere, we would be obtaining p implies x, then x implies r. You use HS and conclude p implies r. Now, the question is what could be this x? If you can fill in this gap, then it will develop to a proof. We see; from axiom one, I can take x to be anything implies p, but for what thing is, I do not know. This is the mystery here. I see that not symbol is involved. I have only one axiom where not is involved that is axiom three.

(Refer Slide Time: 03:43)



So, axiom three looks like not A implies not B implies not A implies B implies A. This is how axiom three looks. If you have not A implies not B, then you can conclude not A implies B implies A by modus ponens, from this. Now, in this case, it looks, we have not q implies not B. So, I can take A and B as not q implies not q and not p. If we start with that, then we would get not q implies p implies q. Now, how to go about it? What this x would be? You should try. This is not the way, we are trying it and see whether something works or not. So, suppose I start from axiom three.

(Refer Slide Time: 05:36)

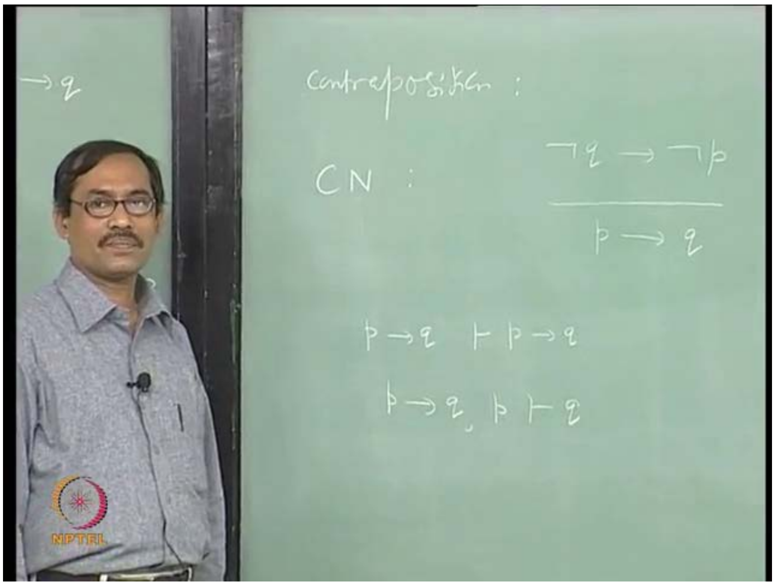


I would start this way; not q implies not p implies not q implies p implies q. I must start like this. Then I have already not q implies not p. So, I will get not q implies p implies q, because I have got it, not q implies p implies q, but I want to get p implies q. I want to use HS. Can I say p implies this? As another missing premise here, suppose I take p implies not q implies p. Now, you can see if I use HS, p implies r, r implies q, therefore p implies here, and it will follow.

Now, how to justify this? It is axiom one. So, proof is done. Yes, is it right? So, all that you have to do is start with this axiom three, use this as a premise, conclude the third line here, then introduce axiom one, then use HS. Let us write the proof. We will start with these, that is first one, which is axiom three. Next, second one will be not q implies not p, which is a premise. Then by modus ponens, we conclude not q implies p implies q. In fact, we should write 2, 1. That is the way it is being applied. It will increase.

Then, what should I do? We have to introduce axiom one. You say, p implies not q implies p, this is axiom one. Next, we would get p implies q by using HS in the order four and three. Is it clear? If we want another proof without using HS, all that you have to do is, insert the proof of HS here starting from these, and then go on using this, finally concluding this. Is it clear? Now, once you get that this consequence is provable, and then you can say another inference rule from this.

(Refer Slide Time: 08:33)

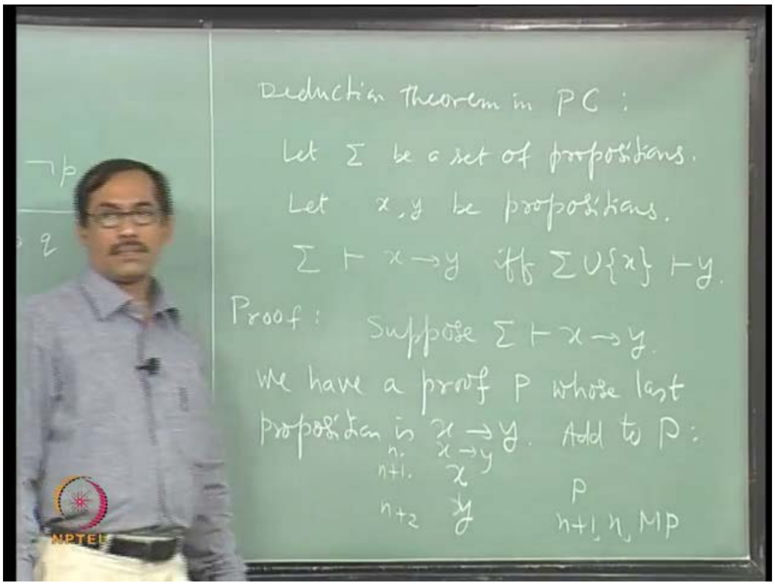


Let us write this as contraposition, CN, this is not q implies not p, therefore p implies q. Later you can use this as a rule also, if you need, fine. But let us not go on deriving so many things. We have to study this system also. Let us do some statements or some results about the system. Then we come back to the examples.

Once set, remember statements about your five results in the propositional logic PL? If you remember there, monotonicity, deduction theorem, reductio ad absurdum, then two substitution laws: uniform substitution and equivalence substitution. Out of this, let us try to prove something. Whether that is possible in this system or not? It looks possible because you see p implies q entails p implies q. Is it fine?

It does not need anything. That is it, one line proof because p implies q is a premise. That can be used as a, in a proof, so just one line proof is sufficient. Is that okay? But, then correspondingly, we also have this and see how, it is modus ponens. You can just develop three line proof, take p implies q as a premise, take p as another premise, apply modus ponens to conclude q. It gives that deduction theorem. See that p from this side has come to this side. Can we prove deduction theorem in PC? Let us state it first, how will it look like, if it holds.

(Refer Slide Time: 10:55)



Let sigma be a set of propositions. So I mean, it is a set of propositions. These propositions are in PC. That means we use only the symbols not and implies; or and if and only if, these are not used here. Now then, let x and y be propositions. What we conjecture is that sigma entails x implies y if and only if sigma union x entails y. This is how it should look like, but we cannot give a proof of this by using semantics taking interpretations and models, we cannot do that.

The meanings of these are fixed. This means there is a proof where possibly premises of sigma are used and x implies y is the last line of that proof. That is what it says. On the other side, it says, there is again another proof where last line is y, possibly x is used. We do not know. Along with premise with sigma, possibly x is also used. Now, how to say these two is the same thing? If there is a proof here, there is also a proof for that and converse of it; this we were going to see here. It is on the existence of proofs now. Yes?

Student: Then put x.

Suppose this is the proof for x implies y. Take this as a proof, introduce x, conclude y. That becomes a proof of this. That is the `only if' part. Let us write that. First you suggested that suppose sigma entails x implies y. That means we have a proof P whose last line is, whose last proposition is, x implies y, where possibly premises from sigma are used. Then add to P, the following two lines. So, what are the two lines? x and then y. That is all.

If you want to document it, then you have to say that p has n lines and then you start from n plus 1 here, n plus 2 here, n-th line is x implies y. Then we will be telling x as a premise from sigma union x. Earlier it was from sigma. Now, it is from sigma union x. Next, use this as n plus 1, n, MP. Now, this is a proof of sigma union x entails y. Therefore, one part is proved. What about the converse? For the converse, what you have? Let us take a start. We have a proof where possibly x has been used and then you have y. If x has not been used in that proof.

Student: In this proof, sigma entails x.

No, suppose x has not been used at all in the proof.

Student: Yes, sigma entails then y.

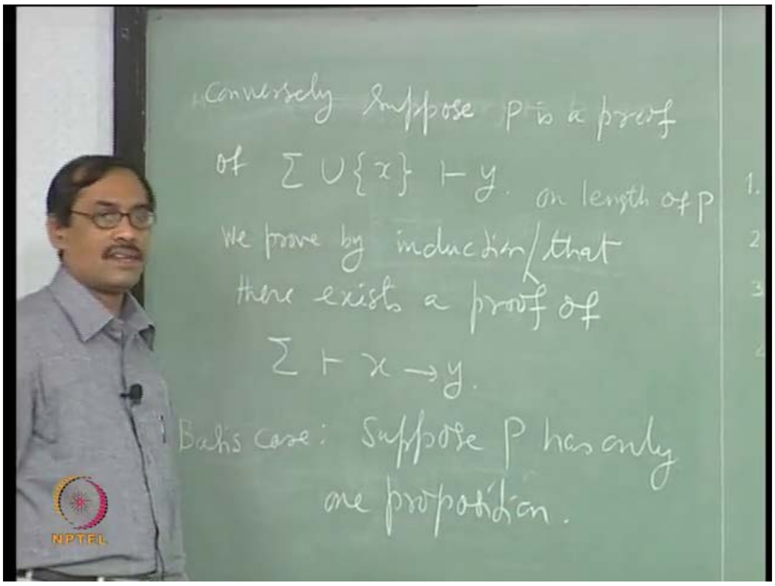
Then, for any x, sigma entails y.

We are doing a proof. Let us say axiom one. You have y as the last line. You will have axiom one, y implies x implies y, then x implies y. That is also a proof, in using premises from sigma. So, sigma entails x implies y. Is it clear? That is your first case. Now, the second case is what? Suppose x has been actually used. Then what to do? You have a proof where premises from sigma are used. We do not know whether or not, but it does not matter. What we say that x has been used in the proof and the last line is y.

Now, how to eliminate that x line and produce a proof where x implies y with the last line, this is the job. Is that right? This is not very straight forward like earlier cases. We will do it by induction on the length of the proofs because we have proofs as the objects. We take the length of the proofs as a parameter and use induction on that. It is not difficult. We will see.

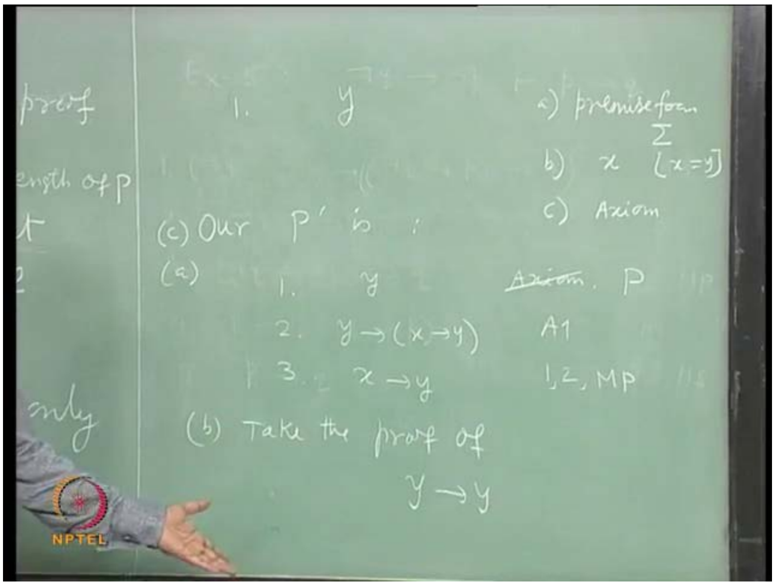
So, conversely suppose P is a proof of sigma union x entails y. See our aim is to construct the proofs of sigma entails x implies y. Now, we prove by induction that there exist a proof of sigma entails x implies y. This is what our plan is, so induction on what, induction on the length of P. Let us write that on length of P, what is length means, number of proposition occurring in P.

(Refer Slide Time: 16:50)



It is a finite sequence of propositions. So, its length will be defined as number of propositions occurring in P. We are doing the induction on that. Suppose basis case; what is the basis case? Suppose P has only one proposition. There is no zero here. It is a proof. In that case, how P will look? See, last line of P is fixed. There is only one line. That line will look like y. Now, problem is here. Why? Why y is there? You said it is a proof, it is a premise, premise from where, sigma union x. So, let us demarcate some cases there, premise from sigma. B, it can be x because you are taking premise from sigma union x.

(Refer Slide Time: 18:43)



It may be from sigma, it may be from x. Any other guess? It can be an axiom. In proof, it is an axiom. You cannot use any inference rule. In any proof, you can use axiom anywhere. It could be an axiom. We do not know what is the nature of this y.

Suppose it is an axiom. Then what is that you want? You want to construct the proof of sigma in terms of x implies y. How to construct sigma entails x implies y? x implies y we want, y implies x implies y is the axiom, y, y can be axiom, y is already an axiom, y will get a premise here in modus ponens. So, that will be our proof of sigma entails x implies y. Call that as P prime, call proof of sigma entails x implies y as P prime. Now, we want the proof of sigma entails x implies y. In order to construct P, in this case, P prime, our P prime would look like this. What is it? First line, y axiom, so we are taking this case C first. It is easier to see.

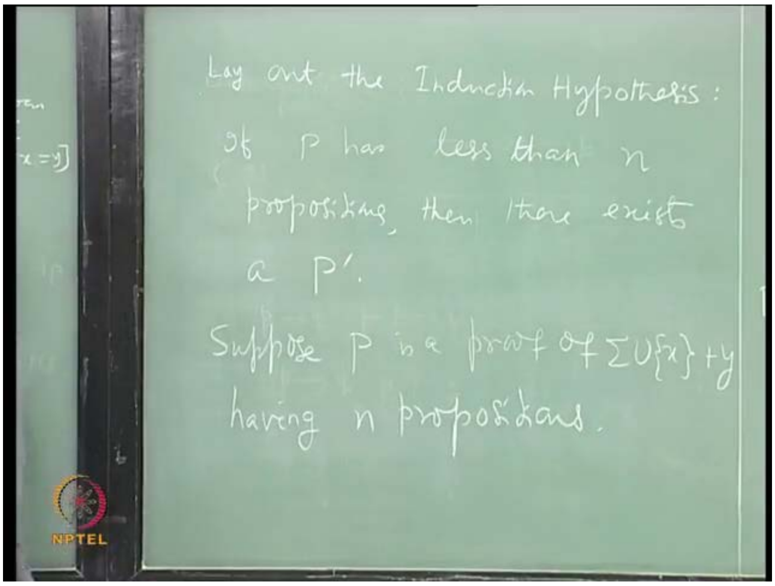
Second is y implies x implies y, axiom one. Third line is, x implies y, 1, 2 modus ponens. So, P prime will look like this, which proves that sigma entails x implies y. Nothing of sigma has been used. It does not matter, but it is not using any premise outside sigma. So, it is a proof of sigma entails x implies y. Is it clear?

Once you understand this case, you can also understand A, because in case of A, you would have written as P. It is a premise. It is a premise from sigma. It is a premise from sigma, same thing goes. So, sigma entails x implies y. Is that clear? So, B case; A case is also over.

Next, come to B. How can you write x here? Because x is equal to y. In this case, you should have taken, x must be equal to y, that is the assertion now. If y can be written as x; and it is a one line proof, that means it is a premise, which is equal to x. So, y is equal to x; no other way it can be justified. If x is equal to y, that means, x equal to y, it gives a proof of p implies p or P prime will be that. In this case, we take the proof of y implies y, that uses no premise. We have already seen it. So, that proves in this case, that is, our basis case is clear. Now, come to the induction step.

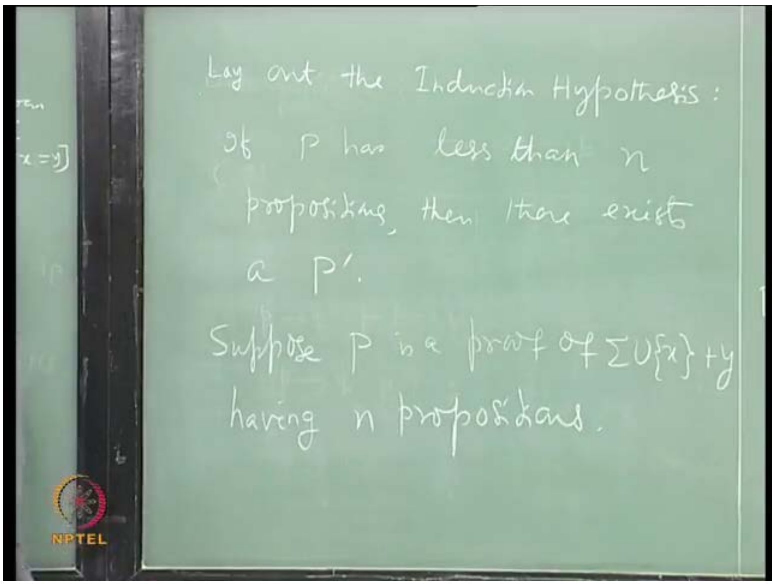
In the induction step, first we have to assume something. What is our induction hypothesis here? P, P. If P has less than, let us say, less than n propositions, then there exists a P prime. Here we are not writing everything. It means, there exists a proof of, P stands for a proof of sigma union x entails y, whose length is less than n. Then there exists a proof of sigma entails x implies y. That is what P prime is. Is that clear?

(Refer Slide Time: 23:26)



Now, what happens? Suppose we have got another proof of sigma entails, sigma union x entails y, having more than n number of or exactly n propositions, let us say. Suppose P is a proof of sigma union x entails y having n propositions. Our aim is to construct P prime, construct P prime, which should be a proof of sigma entails x implies y. That is what we want. Now, how to construct? Well, what could be this P?

(Refer Slide Time: 25:30)



That is how it looks. Now, there are n lines in this proof P, whose last line should be y because it is sigma union x entails y and the premises used here should be from sigma union

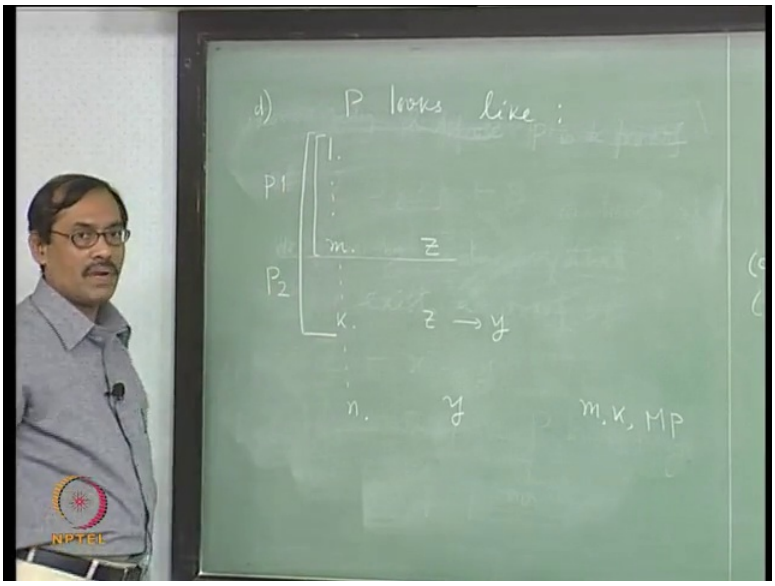
x. Now, what could be this y again? How did you reach at y? Well, all those cases are possible. y can be an axiom, y can be a premise in sigma, y can be x or it might have been derived by modus ponens, modus ponens. That is what the proof is here. The proof of a consequence means it has to be derived from these premises. Derivation is only possible through modus ponens, nothing else. So, there are really four cases for this y. Yes?

Student: There is an axiom y, is there y is there in n steps.

We do not know. We just have something there; y can be an axiom and n can be anything. It may be 1, it may be 2. It is still a proof. Isn't it? You may not want to write it at hundredth step, an axiom and say that this is the proof of those axioms. It can be in one step, but there is nothing wrong in writing there. It is still a proof. Is that clear? So, it is a vacuous case, but it does not matter. It is a possibility. We have to consider all those possibilities.

Here, y can be an axiom. Second, y is a premise in sigma. Third, y is equal to x. Fourth, y is derived by an application of MP. These are the all cases possible. Now, these three cases are similar to the basis step. All those three cases; just the same proof you give, that proof sigma entails x implies y. We are not using any premise or anything. That takes care of your case as if it is one line. Even if trivially somebody has done it, it does not matter. Still we allow and we get away with it. Is that clear?

(Refer Slide Time: 28:58)

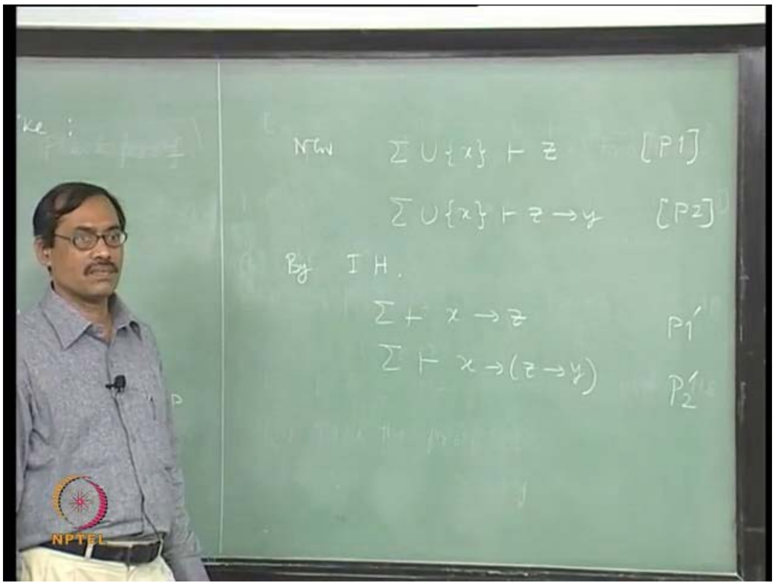


See for example, y is an axiom. Then I will construct my P prime as y implies x implies y. Apply MP, get x implies y. In that proof, nothing is used, no premise is used. So, sigma entails x implies y. Similarly, all these three cases are done. Now, the only interesting is this one, fourth case. Let us see that.

So, the fourth case is case D, that, now imagine how the fourth case can come. y is derived by an application of MP. MP says that earlier there should be some two propositions on which you eliminate its first part, get y, right? That means for some k and some m, which are less than n such that k-th line will be some z, we do not know x or what, some z, and m-th line will be z implies y. Then n-th line is y. Earlier somewhere it will be occurring.

P would look like this. This m and k can be interchanged, which one comes first, it does not matter, but if you write m, k, then m should be in this form, otherwise you have to write k, m. So, you follow this. Now, what happens? Consider this portion as your proof P1, this much. Consider this portion as your proof P2. Apply induction hypothesis.

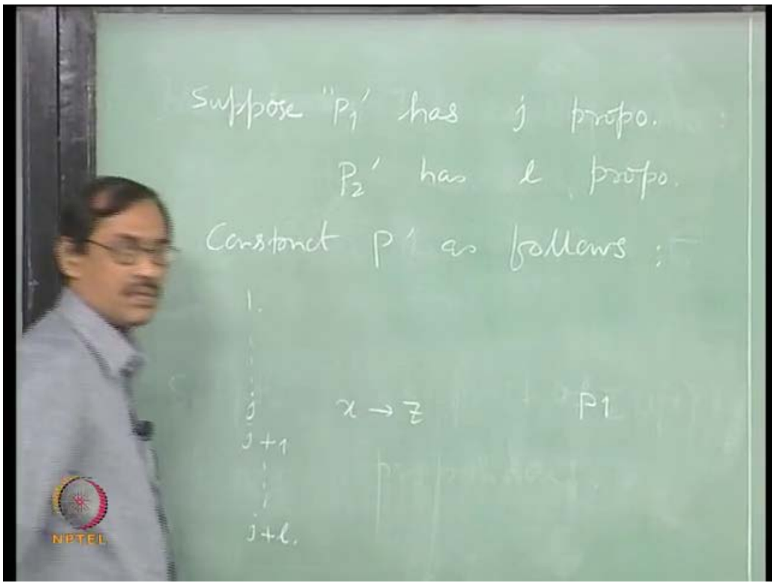
(Refer Slide Time: 30:45)



Considering P1, we say that sigma union x entails z, P1 proves it. So, I am considering a portion of this proof, which is line number 1 to line number m that is my P1. That is also a proof. That proves sigma union x entails z because possibly x could be used there. I do not know. For safe thing, I keep x still. Similarly up to P2 if I take, I get sigma union x entails z implies y. The proof is in P2.

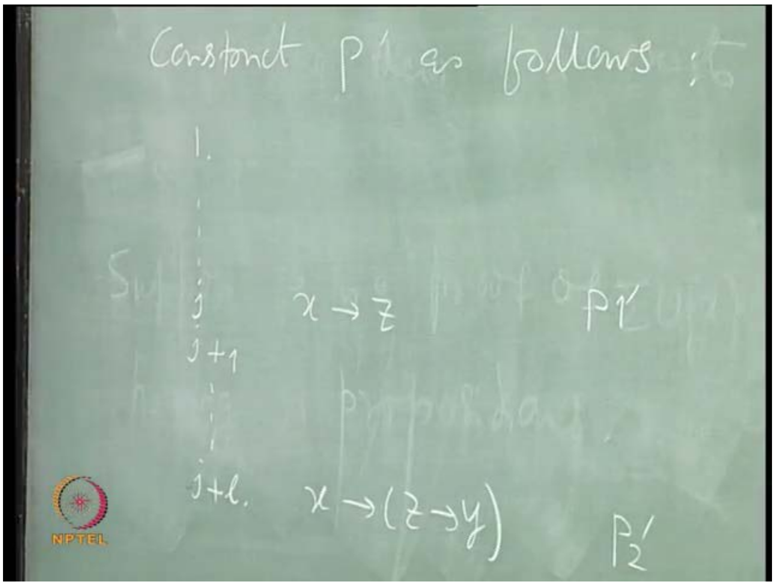
Now P1 and P2 are of length less than n, so use induction hypothesis. What do I get? Sigma entails x implies z and sigma entails x implies z implies y. That means, there are proofs; call it P1 prime, which proves it, and this one, P2 prime, which proves this.

(Refer Slide Time: 32:40)



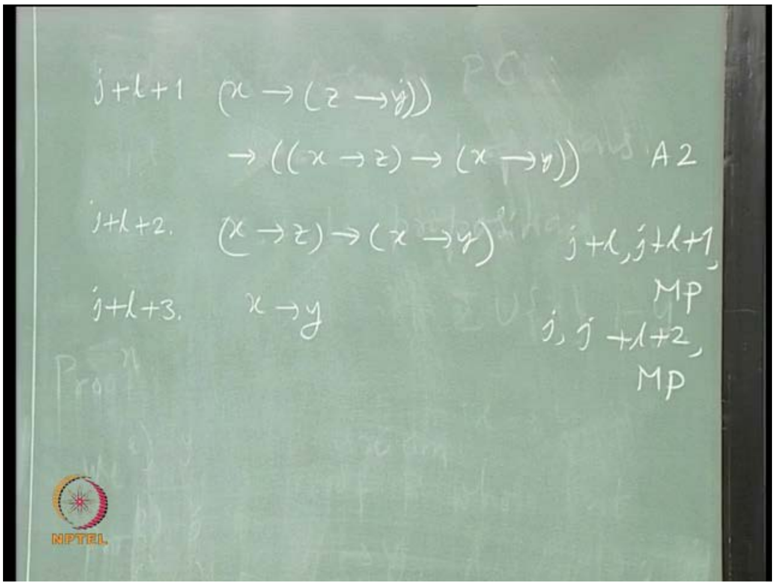
The induction hypothesis says there are proofs. So, you take those two proofs. Now, we will construct P prime using this two proofs. How many propositions are there in P1 prime, in P2 prime? We have no idea, how many exactly, we do not know.

(Refer Slide Time: 33:49)



Suppose, just to write it, we need that number. Suppose, P1 prime has j propositions and P2 prime has, say, some another l propositions. Now, construct P prime as follows. Take P1 first up to j. Next, take P2. P1 will prove x implies z. Here, it is really P1, up to this it is P1 prime. Next, you take first line of P2 prime here and continue up to l lines. That last line will be x implies z implies y. This portion is P2 prime. This much is guaranteed. I just add those two proofs. Now, after adding, I have to get what? That is what we want: x implies y. Now, what to do? Axiom one, we have used; axiom two, we have not used. Let us use it here.

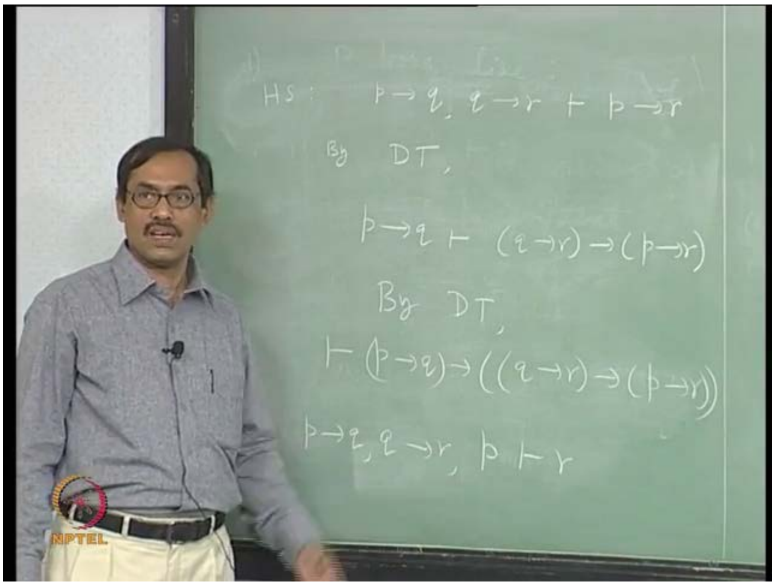
(Refer Slide Time: 34:24)



I continue the proof j plus l plus one-th step, which says x implies z implies y implies x implies z implies x implies y, axiom two. Next, you should be clear now, what I am doing. I get x implies z implies x implies y by modus ponens from j plus l, j plus l plus 1. Is it okay? Next, j plus l plus 3, will be x implies y. Why? I used j here and j plus l plus 2 here and modus ponens. Job is done. Yeah, clear?

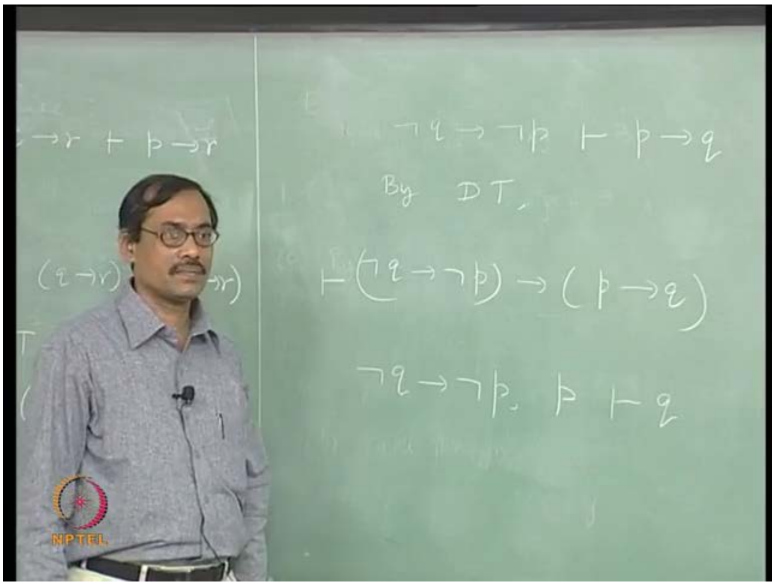
It says how to construct a proof from x implies z, z implies y to x implies y. That is used in only one step. See there are many such steps of application of MP using the premise x, then it is not easy to give the proof immediately, but every line has to be inserted and then carried over slowly. It becomes difficult, but it is possible. That is what it says and we are concerned with provability now. We are talking about the system PC. The theorem is proved. Then you can use deduction theorem anywhere. For example, you take HS.

(Refer Slide Time: 36:22)



HS says p implies q, q implies r entails p implies r. By deduction theorem, we can say p implies q entails q implies r implies p implies r, though you have not proved it. But, it is some theorem, it says that if this is provable, then this is also provable. Again, another application of deduction theorem says this is a theorem. Is it okay? Now, for proving this, we can give also simpler proofs, we go back, another step, the other direction. This says this one, this is provable if p implies q, q implies r, p entails r.

(Refer Slide Time: 38:29)



Now, you can have a nice proof of this without thinking, yes? Because you have p, you have p implies q by modus ponens q, you have q, q implies r by modus ponens r. You want to do such things later. That is why we are doing these metatheorems like deduction theorem. They are really talking about our PC, which theorems are provable, which statements can be considered as theorems and so on. This will help in this way.

For the contraposition, we can similarly write a theorem instead of the consequence, say you have not q implies not p this entails p implies q. Now, you can write it as by deduction theorem that not q implies not p implies p implies q is a theorem. Is it clear? But, then if we go one step here, what will it give, the other direction. That would say not q implies not p p, therefore q. That is also proved along with contraposition. This is another consequence.

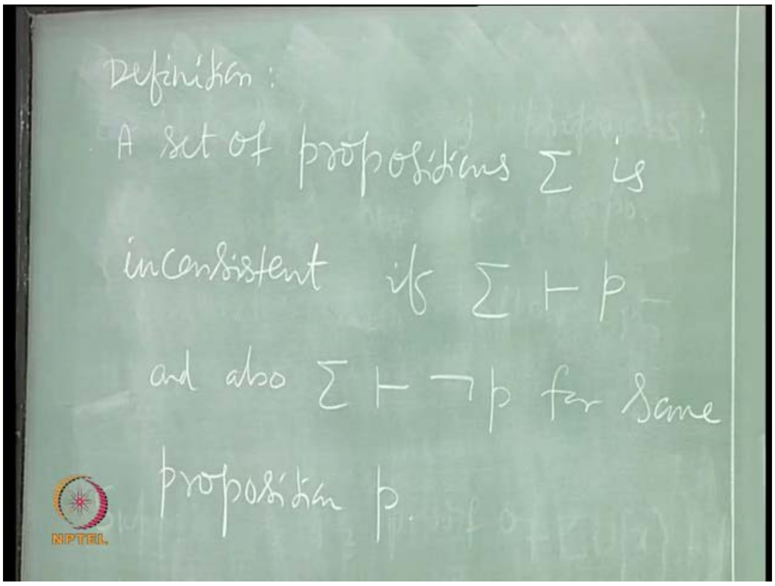
See, if at all we are going parallelly to semantics, then we should have other two theorems, monotonicity and reductio ad absurdum theorem. But monotonocity has two parts. If sigma is a sub set of gamma, sigma is satisfiable, then what can you conclude about gamma? Nothing, it may be satisfiable, it may be unsatisfiable, but the other direction, you can write. That is, if sigma is unsatisfiable, then gamma has to be unsatisfiable. The other form says if sigma entails w, then gamma also entails w. Gamma is a super set of sigma. Similarly, we have two options here, but then how to introduce unsatisfiability?

Student: Sir, sigma is a subset of gamma.

Yes. Well, if gamma is satisfiable, then sigma is satisfiable. Do you agree with this? When sigma is unsatisfiable, then gamma is unsatisfiable. So, what it says, directly? If sigma is unsatisfiable, then whatever interpretation you take, all of them cannot be simultaneously one. If you add another, still all of them cannot be satisfied because those things which could be satisfied still could not be satisfied. That is why. Well, now what to do here? There is no unsatisfiability. There is no satisfiability. We have to introduce something in parallel to that. We will call them inconsistent rather than unsatisfiable. We have to define some new terms.

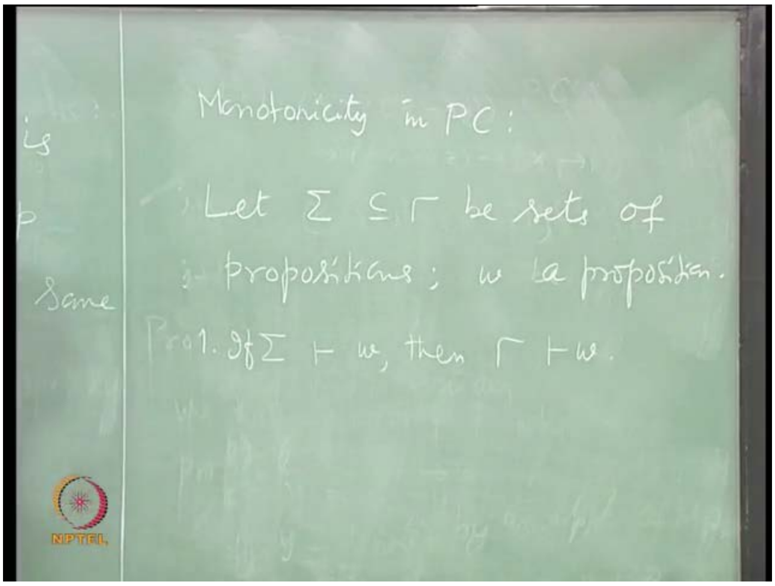
We say that a set of propositions sigma is inconsistent if, what happens, if sigma entails p and also sigma entails not p for some proposition p. This is what you mean by “contradictions are there”. There is a contradiction in the system means you can derive some proposition and also its negation.

(Refer Slide Time: 41:20)



That is what we are telling, that it is an inconsistent set. Everything does not fall into place. It entails p, it gives you p, it also gives you not p. Now, with this definition of inconsistency, how do we formulate monotonicity? Just in case of unsatisfiable, we have to write inconsistent. Let us formulate it first.

(Refer Slide Time: 42:38)



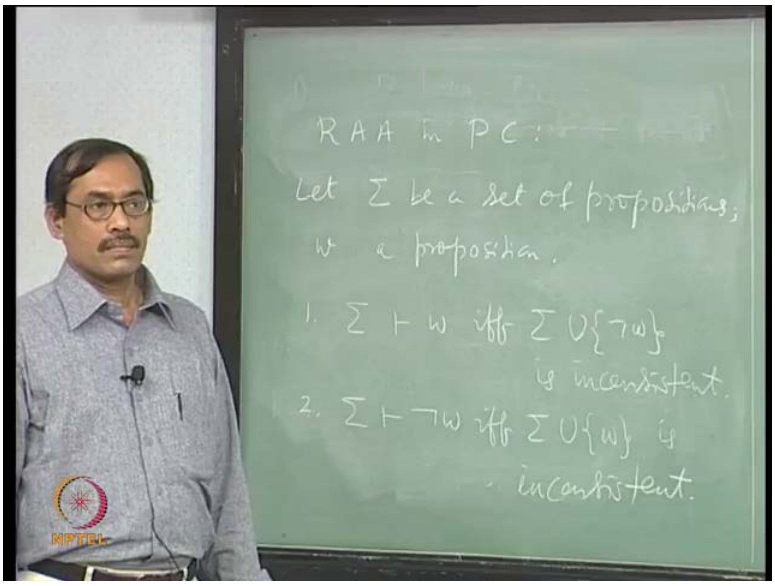
Then, what happens? First thing is if sigma entails w, then gamma entails w. Second thing is, if sigma is inconsistent, then gamma is inconsistent. Formulation is all right.

How do we prove this? Say, first one, how do we prove? No, first one, there is nothing to prove. If sigma entails w, you have the proof of sigma entails w. Last line is w where premises from sigma are possibly used, but that proof itself is a proof of gamma entails w; possibly premises from gamma are used. That is all.

What about second one? Same thing, sigma is inconsistent, so sigma entails p, sigma entails not p for some p. Now, sigma entails p gives you by first one, gamma entails p, that gives first one again, gamma entails not p. Therefore, gamma is inconsistent. You do not have to argue again. You have already argued. So, monotonicity is clear.

Then you can formulate reductio ad absurdum. Again we take sigma to be a set of propositions, w and so, a proposition. Now in PL, how did you formulate reductio ad absurdum? Sigma entails w if and only if, is inconsistent. Instead of unsatisfiable, we will say inconsistent. So, sigma entails w if and only if sigma union not w is inconsistent. Similarly, the other part, sigma entails not w if and only if sigma union w is inconsistent. How do you prove this sigma entails w?

(Refer Slide Time: 45:00)



Student: Sigma entails not w.

Sigma entails not w.

Student: Sigma entails not w.

Which entails not w?

Student: We already have the proof that not w is a…

By monotonicity, sigma union not w entails, and sigma union not w, is not w, one line proof not w. Is that okay? So, sigma union not w is inconsistent. See, sigma entails w. Suppose sigma entails w. Then by monotonicity, sigma union not w entails w. It is a super set of sigma.

Student: It is a super set of sigma.

Is that okay? So, sigma union not w entails w as well as not w, therefore it is inconsistent. So, one part here, you have proved. Let us see that one part here. What happens? Same thing, sigma entails not w, therefore sigma union w entails not w and sigma union w entails w. Therefore, sigma union w is inconsistent.

Student: Sir, how are you saying that sigma entails not w, therefore sigma union w entails not w.

One line proof in PC, in PC.

Student: Not not w is w.

No, I have told you that, that is in PC.

Student: Sir, but you are using that here.

Nowhere, that is why, I am formulating two ways. If I have not not w, same thing as w, I will not formulate another. Now, think about these converses. If you can prove one of the converses, the other one you can prove.