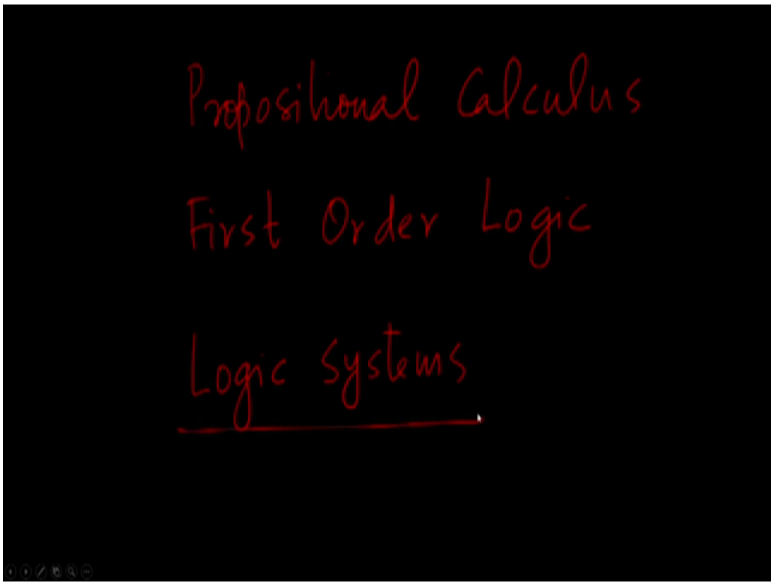
Discrete Mathematics
Professor Sajith Gopalan
Department of Computer Science & Engineering
Indian Institute of Technology, Guwahati
Lecture 5
Mathematical Logic

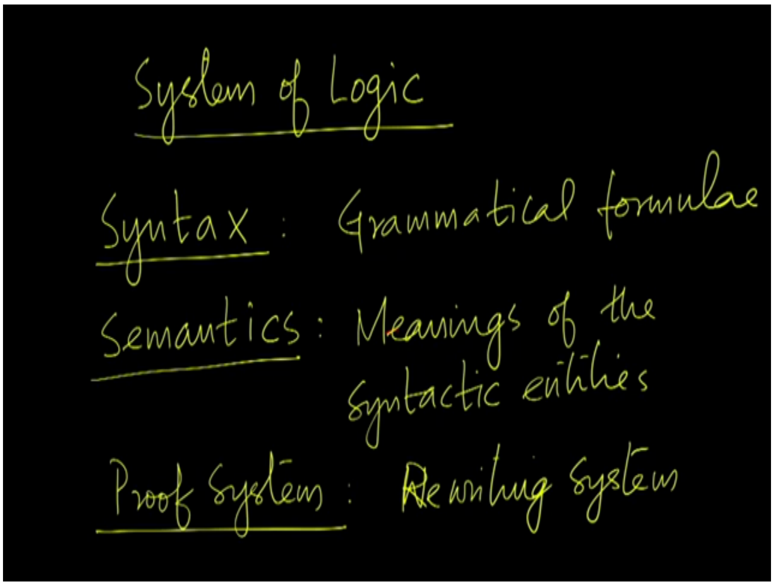
Welcome to the NPTEL MOOC on the Discrete Mathematics, this is the fifth lecture on mathematical logic.

(Refer Slide Time: 00:49)



In the previous four lectures, we had an informal discussion on propositional calculus and first order logic, these are examples of logic systems. Today let us have a formal discussion on these, these of systems of logic.

(Refer Slide Time: 01:18)

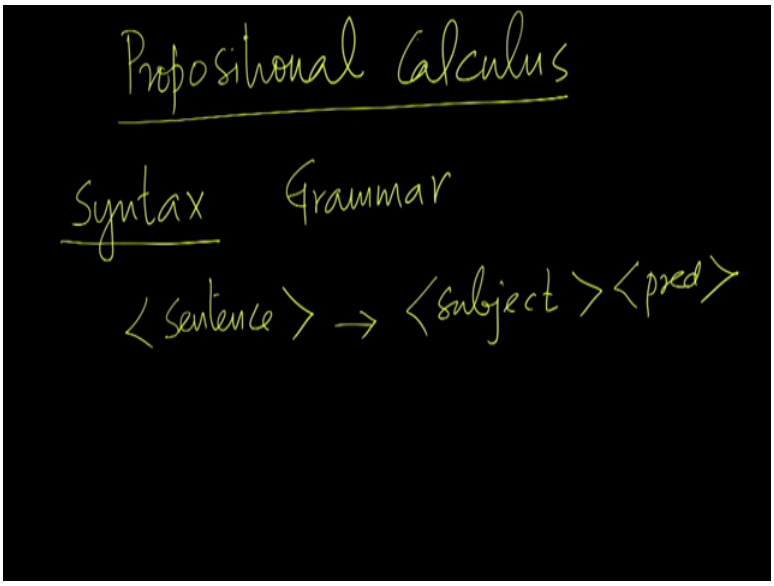


So, what is the system of logical? A system of logic essentially consists of these components the first one is, the syntax of the language this specifies what are the grammatical formulae or the grammatical sentences of the language. Then we have the semantic component of the system.

The semantics of the language specifies the meaning of the syntactic entities, it assigns meanings to the syntactic entities and finally we have a proof system which is a rewriting system which starts with a set of axioms has a rule of inference has many rules of inferences possibly and then using these rules of inference it writes new sentences and the process of writing these new sentences is called proving and what we get is a proof.

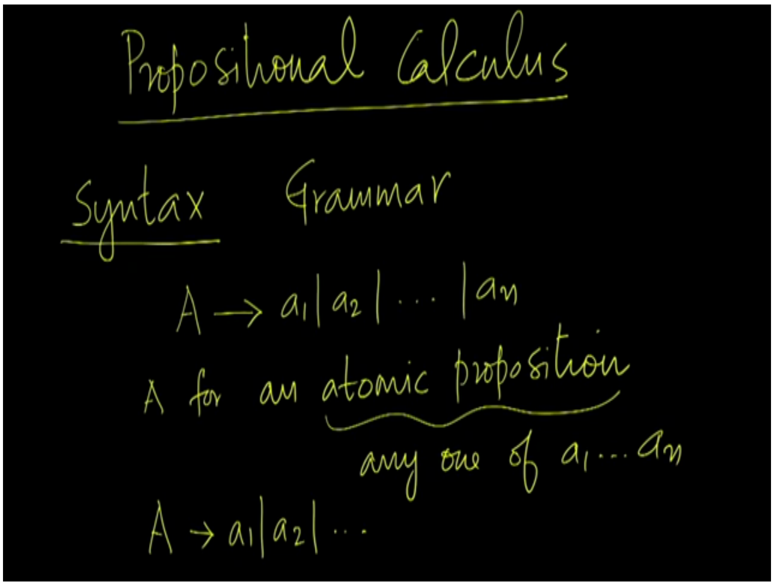
So, let us now see in detail what these components are for the two systems of logic that we have studied namely propositional calculus and first order logic.

(Refer Slide Time: 03:14)



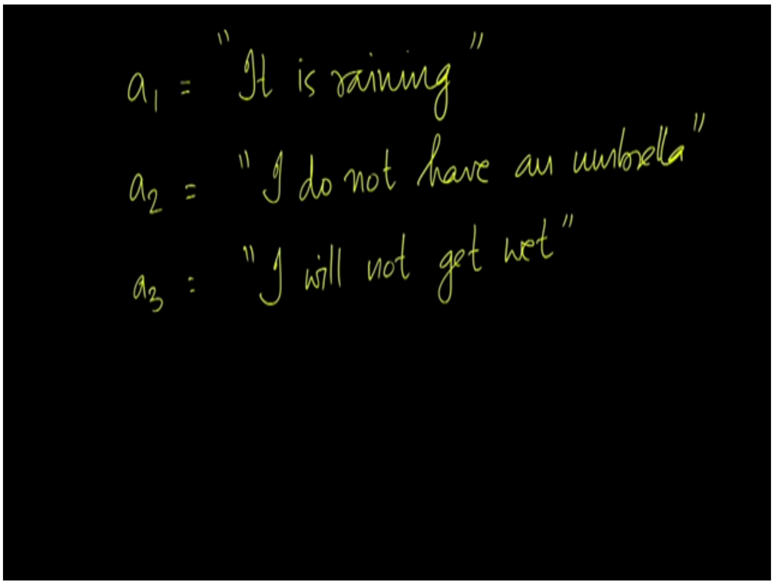
So, let us begin with propositional calculus, so let us begin with the syntax of propositional calculus. The syntax is specified using what is called a grammar, a grammar as in English for example we can say a sentence in English is made up of a subject and a predicate this is what is called the grammatical rule or a grammatical production.

(Refer Slide Time: 04:13)



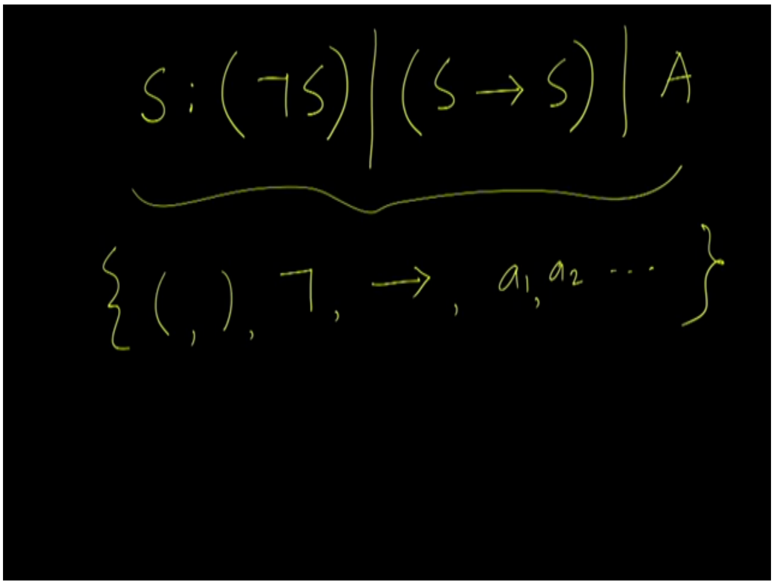
So, likewise we can write a set of productions for the sentences of propositional calculus. The first production is this here we say that the grammatical symbol A stands for an atomic proposition, so what this grammar rule says is that an atomic proposition could be any one a 1 through a n here of course this need not even be finite you might even have an infinite number of options. So, the rule could very well be this whereas our system might have an infinite number of atomic propositions which is also possible.

(Refer Slide Time: 05:22)



So, this specifies what the atomic propositions are for example, the atomic propositions could be that a 1 says it is raining a 1 stands for the atomic proposition it is raining, a 2 might stand for the atomic proposition I do not have an umbrella and a 3 might stand for I will not get wet and so on. So, your system might have several such atomic propositions, so this is the first grammar rule that we have.

(Refer Slide Time: 06:01)



Then, the second grammar rule says that the syntactic entity S which stands for of propositional formula could be made up in this fashion, what this says is that a formula could be the negation of another formula or it could be an implication one formula implying another could form a formula or it could be an iterate formula.

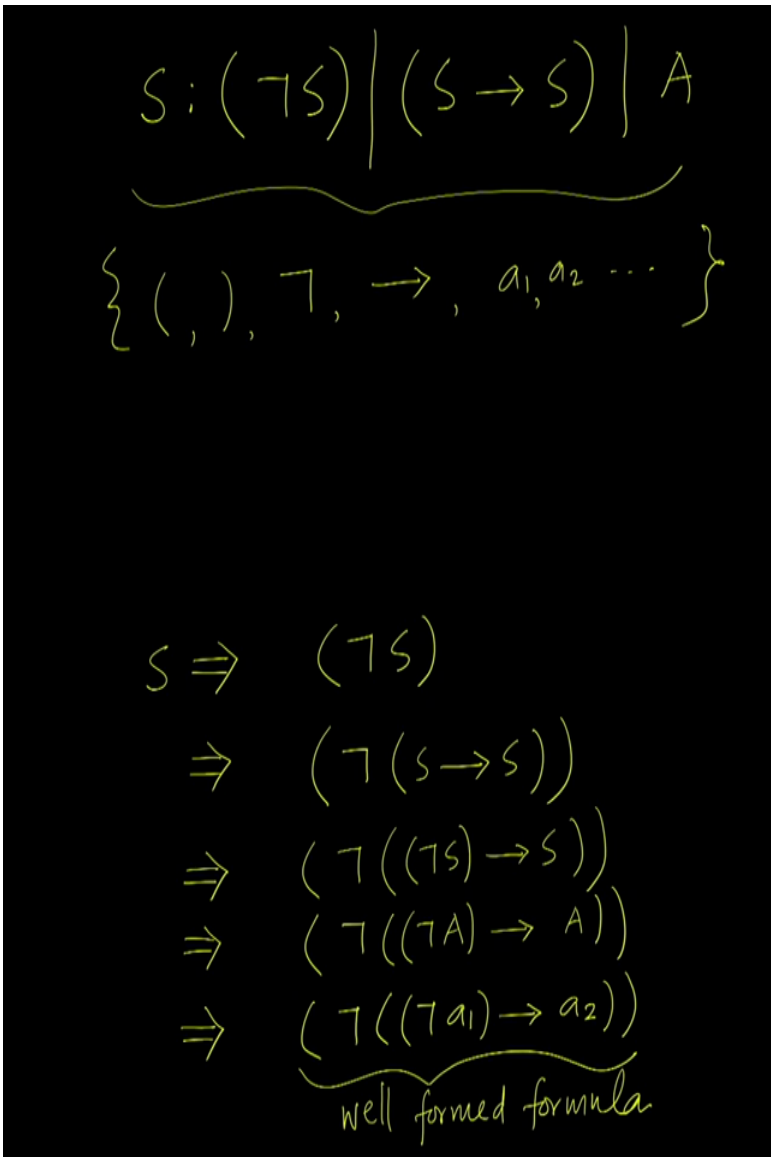
So, this is a recursive specification, what it says is that a formula could be a negation of another formula or it could be an implication made up of two formulae which two have to be synthesized afresh or the formula could be an iterate formula so that is where the recursion breaks off.

So, this is the other grammar rule that we have for forming propositional formulae. So, you can see that, in this we are using certain symbols the open and closed brackets, the negation symbol, the implication symbol in addition to the propositional symbols, a potentially infinite number of propositional symbols.

So, this we call our alphabet, so the language of propositional calculus is made up of this alphabet and from this alphabet using these two above grammar rules we synthesize formulae.

So, a formula could be a negation of another formula, it could be an implication of two formulae or it could be an atomic formula. An atom in formula could be any one of a 1, a 2, a 3 etcetera.

(Refer Slide Time: 07:49)



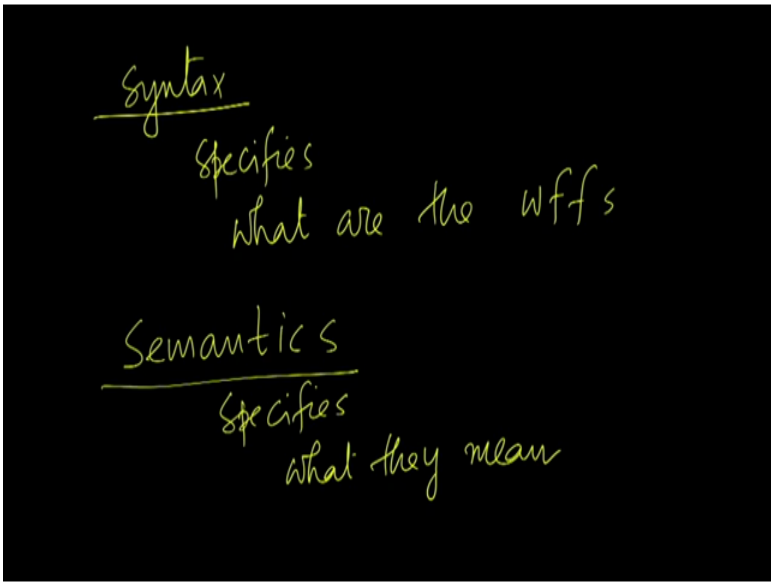
So, let us see an example of synthesizing a formulae, you could derive negation of S from S as the grammar rule shows here a formula could be a negation of a formula. So, a formula could be derived as a negation of another formula which could intern be derived as an implication.

Now, there are two formulae here, in the implication there is an antecedent as well as a consequent, we could decide that the antecedent is a negation of another formula. So, now the synthesized formula has two placeholders, two instances of S each will stand for a formula

. Now, we could decide that these two instances are in fact atomic formulae and then we could say that the first atomic formula stands for propositional symbol a 1 and the second atomic formula stands for the propositional symbol a 2. Now, this is a concrete propositional formula this is what we call a well-formed formula, this is a formula made up of the alphabet of our language, it has negation symbols, closing and opening brackets, two propositional symbols a 1 and a 2, negation symbol and then implication symbol.

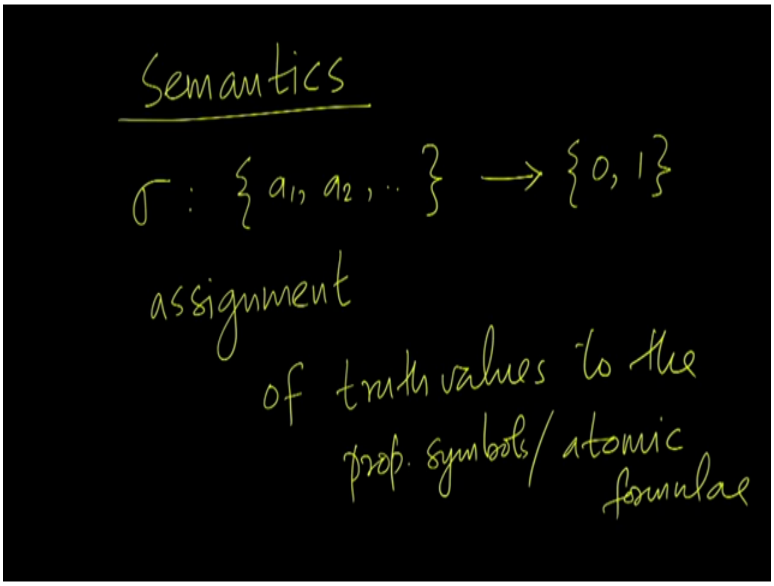
So, this is a well-formed formula of the alphabet of our language. So, this is how we derive the formulae of the language using these two grammar rules we can derive the formulae of our language.

(Refer Slide Time: 09:56)



So, this is the syntax, the syntax specifies, what are the well-formed formulae? The semantics of the proof system specifies what they mean, what the formula mean. So, now let us go on to the semantics of our proof system, how do we specify truth values for these formulae.

(Refer Slide Time: 10:47)

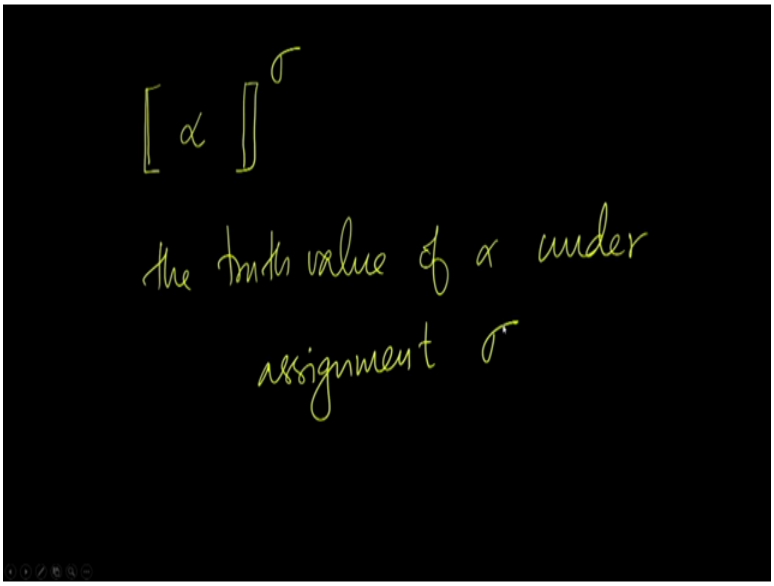


To specify the semantics, we consider functions of this form functions that map the propositional symbols or the atomic formula to the set 0 and 1 such a function is called an assignment.

So this is essentially an assignment of truth values to the propositional symbols. A propositional symbol is the same as an atomic formula, these two are synonyms. So, an assignment sigma at assigns truth values to the propositional symbols or the atomic formulae.

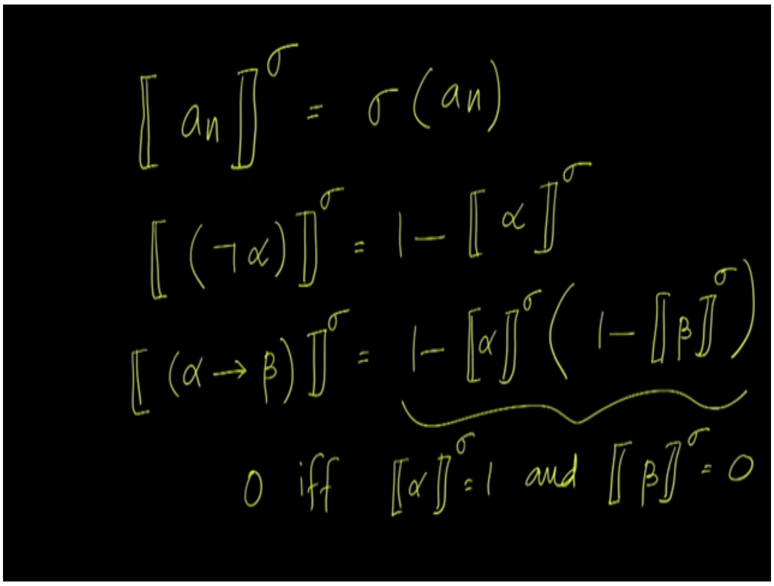
So, now once we have an assignment we can say which atomic formula are true and which are to make formulae are false but how do we know the truth values of a synthesized formula now, a well-formed formula.

(Refer Slide Time: 12:07)



So, the semantics of a well-formed formula is denoted like this, when I write like this, what I mean is the truth value of alpha under the assignment sigma, so this is a notation we shall use.

(Refer Slide Time: 12:37)



So, using this notation we say that for an atomic formula a n the truth value of the formula a n under the assignment sigma is nothing but the truth value explicitly assigned by sigma to it. So, sigma is a mapping from the propositional symbols to the truth values, so the truth value which is mapped to a n will be the meaning of a n, so that specifies the truth values for all atomic propositions.

Now, let us consider formulae of this form, formulae that our negations the truth value assigned to the negation of a formula will be defined in this manner you compute the truth value of the formula alpha under sigma and then subtract that from 1.

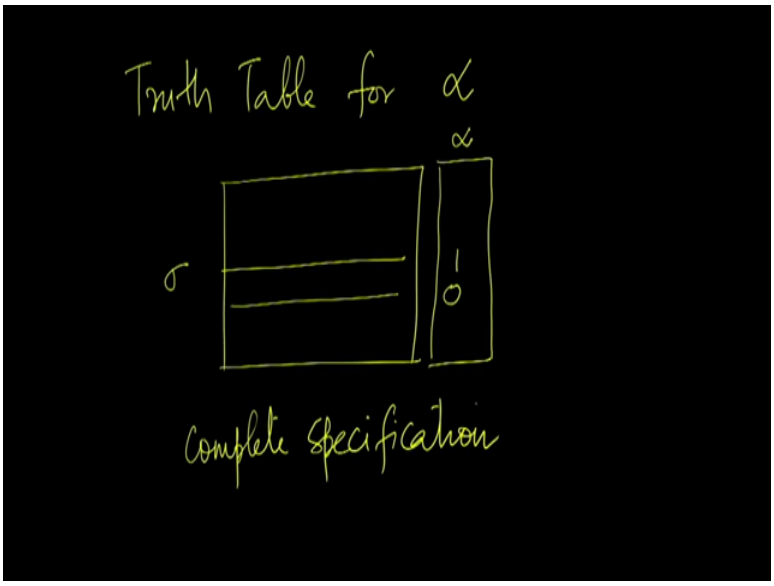
This is the truth value that is assigned to the negation of alpha. So, if alpha evaluates to 1 under sigma then not of alpha will be assigned 0, if alpha evaluates to 0 under sigma then not of alpha will be assigned a value of 0 under sigma, so this is how you assign a truth value to a negation.

For an implication, likewise we can say this is 1 minus the meaning of alpha under sigma multiplied by 1 minus the meaning of beta under sigma that is the truth value assigned to alpha implies beta under the assignment sigma would be this quantity. So, you can see that this assigns a truth value of 0 if and only if alpha evaluates to true and beta evaluates to false under sigma.

Or in other words, if alpha is 0 or beta is 1 then alpha implies beta will be assigned a truth value of 1. So, this is how we assign truth values to composite formulae, so this now specifies a truth value for every single well-formed formula.

So, given a well-formed formula we can parse the formula, see how the formula was derived using the grammar and then running along the derivation we can assign truth values to the constituents of the formula. So, it is possible to calculate the truth value of a formula given an assignment.

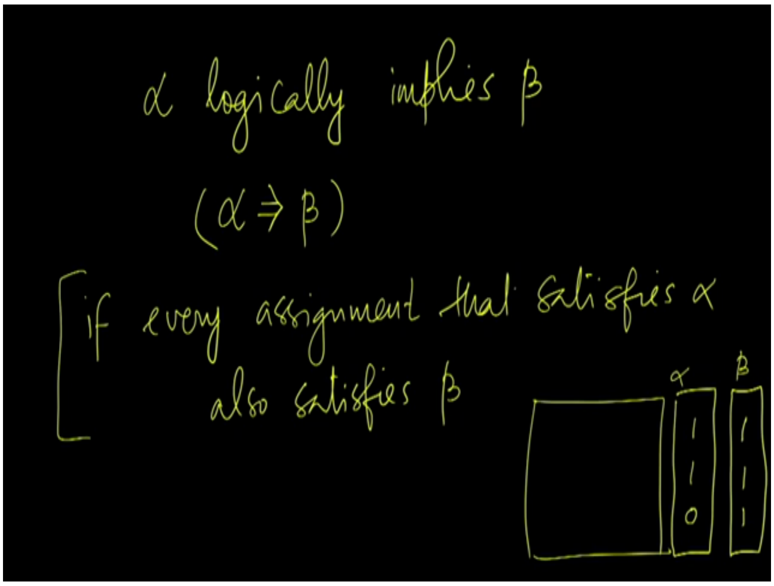
(Refer Slide Time: 15:39)



So, consider a truth table for a formula alpha. In the truth table, we find that we have one row corresponding to each assignment, so if the formula evaluates to 1 under this assignment then the corresponding entry in the truth table in the final column would be 1 instead if the formula evaluates to 0 then the corresponding entry will be 0. So, looking at the truth table we can understand what the meaning of the formula is under any assignment.

So, a truth table is a complete specification of the semantics of a formula. So, given a formula alpha, we can and as an assignment sigma we can refer to the truth table to see whether sigma satisfies it or not once the truth table is available.

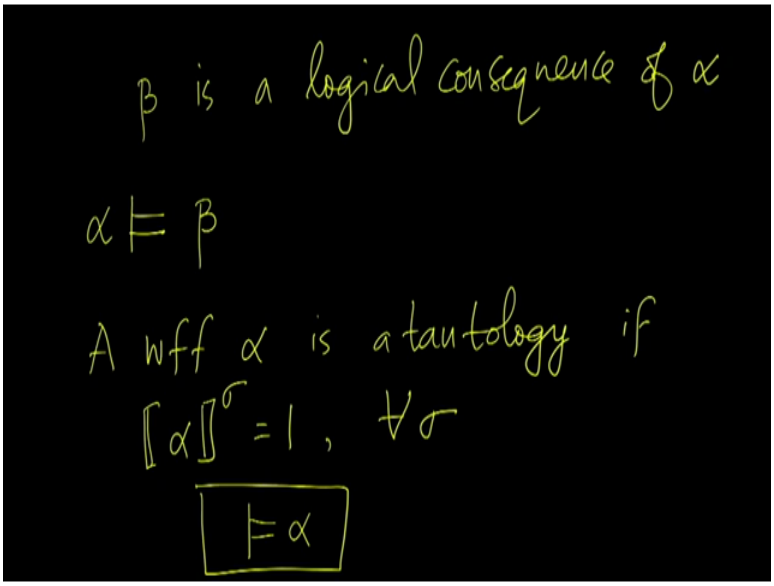
(Refer Slide Time: 16:43)



We say that alpha logically implies beta which we denote in this fashion the double implication is supposed to mean that alpha logically implies beta. If every assignment that satisfies alpha also satisfies beta that is when we say that alpha logically implies beta.

In other words, if you look at the truth table and the columns corresponding to alpha and beta we find that whenever alpha is true beta is also true but of course beta could be true even when alpha is false in some assignments where alpha is false beta could be true but what we know is that whenever alpha is true beta is true. Therefore, we say that beta is a logical consequence of alpha, if alpha holds then beta has to necessarily hold.

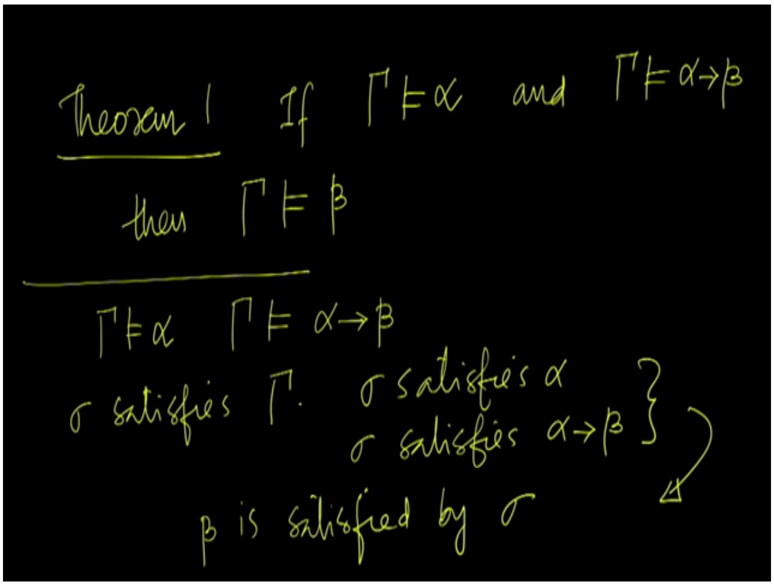
(Refer Slide Time: 18:02)



So, another way of saying is this, beta is a logical consequence of alpha we could write this way to, to say that beta is a logical consequence of alpha and we say that a formula well-formed formula alpha is a tautology if the truth value of alpha in sigma is 1 for all possible assignments sigma.

So, a tautology is a formula which is true always in every single assignment the formula happens to be true when we write like this what we mean is that alpha is a tautology, alpha is a logical consequence of nothing. In other words, alpha is true everywhere in which case we say that alpha is a tautology.

(Refer Slide Time: 19:20)



So, let us look at a theorem now which we call theorem 1. This says that, if alpha is a logical consequence of a set of formulae gamma, gamma is a set of formula remind you if alpha is a logical consequence of gamma.

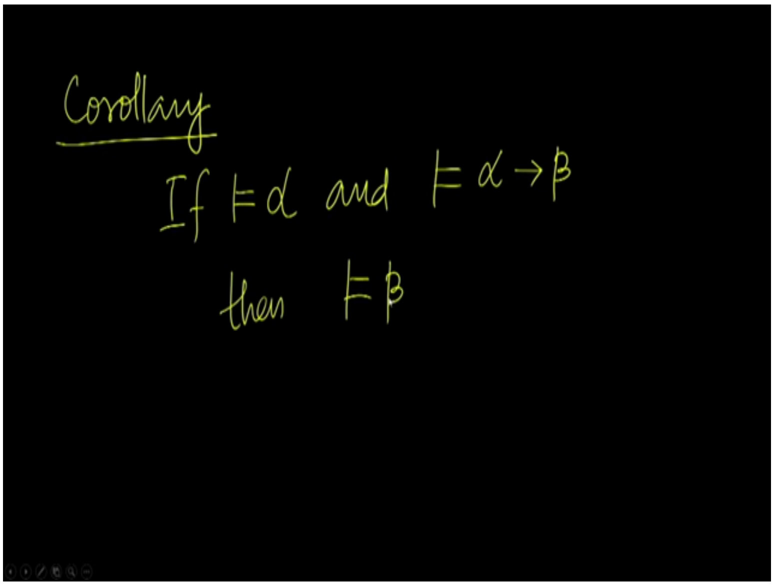
In other words, when the whole of gamma is true gamma conscious of several formulae when each of these formulae is correct then alpha is also true and alpha implies beta is a logical consequence of gamma then beta is a logical consequence of gamma, so this is what we want to show.

Let us assume that alpha is a logical consequence of gamma and alpha implies beta is a logical consequence of gamma, so what it means is that in an assignment which satisfies the whole of gamma alpha is true as well as alpha implies beta is true.

So, suppose sigma satisfies gamma then sigma satisfies alpha and sigma satisfies alpha implies beta. So, if under this assignment alpha is true and alpha implies beta is true then beta must also be true because if beta is not true then alpha is true and beta is false.

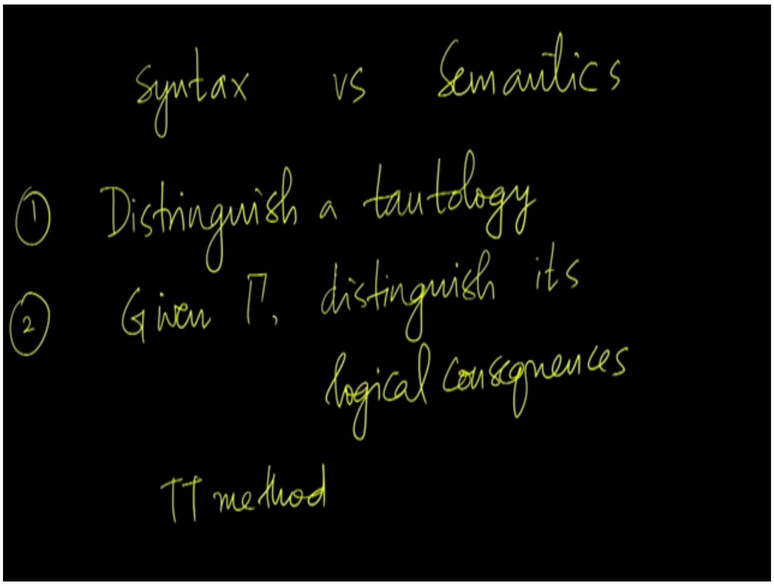
Therefore, alpha implies beta must be false which is a contradiction. Therefore, these two together ensures that beta is satisfied by gamma that proves the theorem.

(Refer Slide Time: 21:38)



So, as a corollary we see that if alpha is a tautology and alpha implies beta is also a tautology then beta is also a tautology.

(Refer Slide Time: 22:03)



Now, we have seen the syntax as well as the semantics of the system of logic, how do we correlate the two? How do you distinguish a tautology when you see one? That is one question, when you has given a formula you have to say whether it is a tautology or not.

The second question is this, given gamma distinguish it is logical consequences. So, we have these two questions, first we want to distinguish tautologies given a formula, we have to say whether it is a tautology or not.

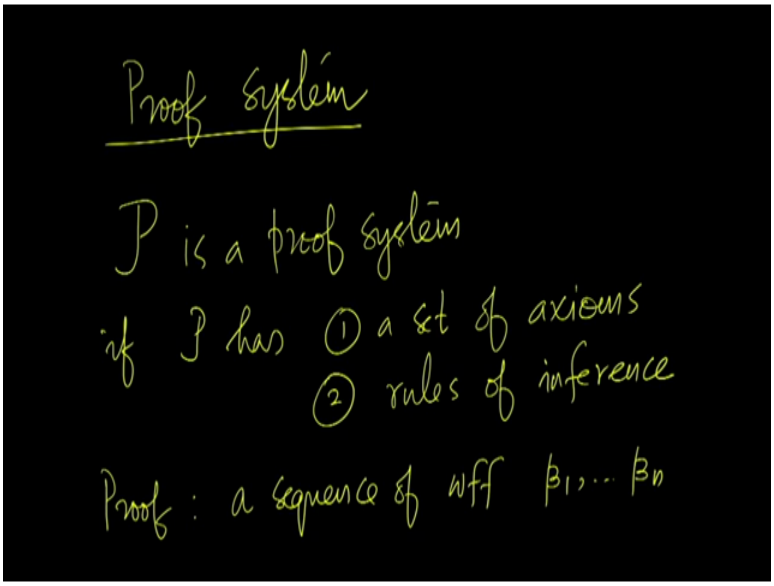
And secondly given gamma, gamma could be finite or infinite we have to distinguish it's logical consequences, that is given gamma in the context of gamma when we are given a formula alpha we have to say whether alpha is a logical consequence of gamma or not.

If gamma is finite then these two questions can be answered using the truth table method that is you drop the truth table you have a formula alpha, you drop the truth table if the truth table says that the formula is true in every single assignment then the formula is a tautology.

Similarly, you drop the truth table for every single formula in gamma, if gamma is finite and then you also drop the truth table of alpha and you find that in every assignment which satisfies the whole of gamma alpha is also true in which case alpha is a logical consequence of gamma. So, the truth table method will help us in answering these questions in situations where gamma is finite.

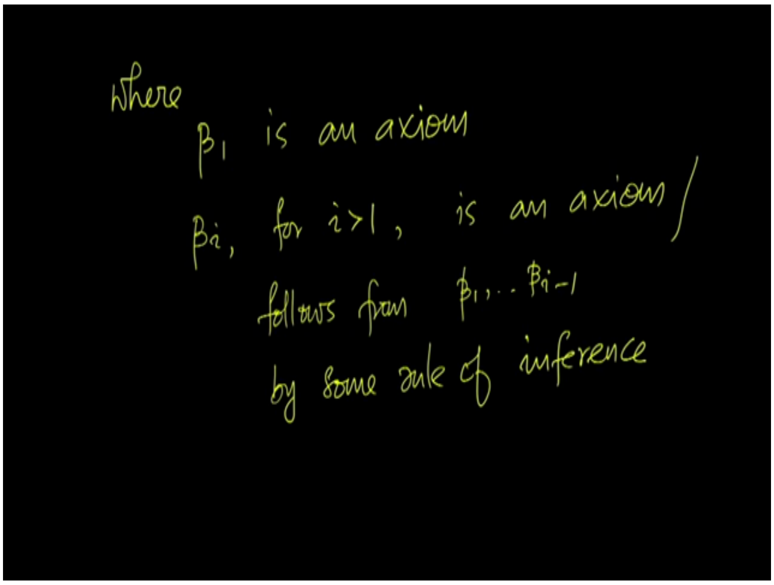
But the truth table method is a luxury that we have in the case of propositional calculus but when we come to first order logic as we shall soon we find that we do not have a method which is analogues to the truth table method because the semantic space there could be infinite. Therefore, we need a different way of saying is distinguishing logical consequences as well as tautologies.

(Refer Slide Time: 24:35)



For this we have what is called a proof system. In a proof system, we say that P is a proof system, if P has a set of axioms an axioms is nothing but a formula so a set of axioms is a set of formulae and a set of rules of inference, a rule of inference is a relation on formulae. So, a proof system consists of these two components, a set of axioms and a set of rules of inference and then a proof. In this proof system is a sequence of formulae, a sequence beta 1 through beta n is called a proof.

(Refer Slide Time: 25:56)

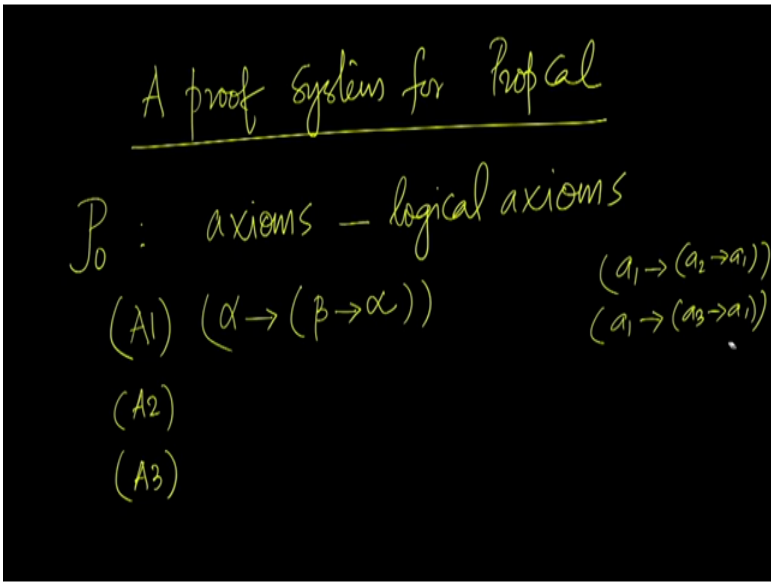


Where beta 1 is an axiom, so a proof always begins with an axiom and beta i for i greater than 1 is an axiom you could use an axiom anywhere in the proof. So, beta i is either an axiom or follows from beta 1 through beta i minus 1 the previous formula in the proof by some rule of inference.

So, this is our notion of a proof, we have a set of axioms and we have a set of rules of inference. A proof is a sequence of formulae beta 1 through beta n, so that the first formula in the sequence is necessarily an axiom and any subsequent formula in the proof is either an axiom or follows from the previous formulae in the proof by some rule of inference.

So, what it means is that within a proof you can use an axiom anywhere you want and at any point in time you can use some of the previous formulae combine them to using a rule of inference to create a new formula which could be the next formula within the proof. So, such a sequence of formula is called a proof.

(Refer Slide Time: 27:28)



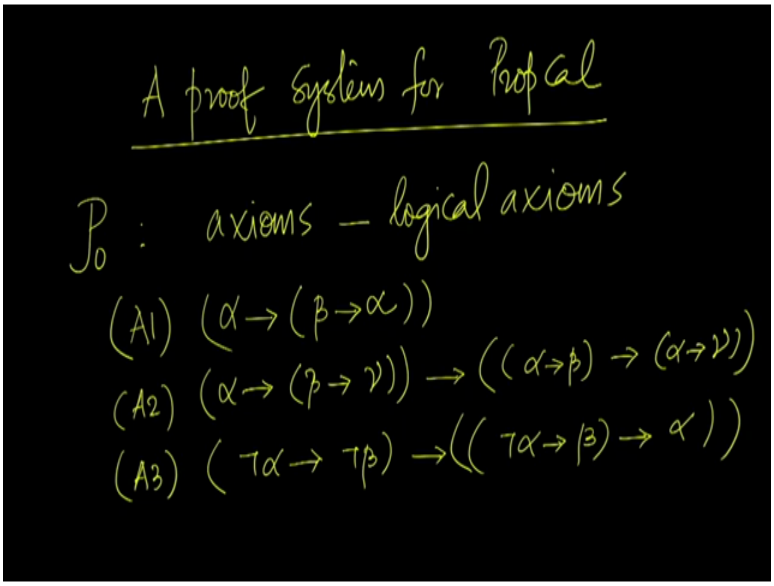
So, now let us see a proof system for propositional calculus. A proof system P 0 for propositional calculus consists of some axioms that are called logical axioms, so axioms could be classified into logical axioms and proper axioms.

So, the logical axioms would belong to these templates, so in this proof system that we are going to talk about there are three templates, these templates are these.

The first template is of the form alpha implies beta implies alpha this is the first template. So, from this template you can form concrete axioms by substituting formulae for alpha, beta and alpha and beta in this case.

So, you could write a 1 implies a 2 implies a 1; a 1 implies a 3 implies a 1 and so on. So, these are all concrete formulae that are derived using this template. Therefore, we will say that a 1 is an axiom schema.

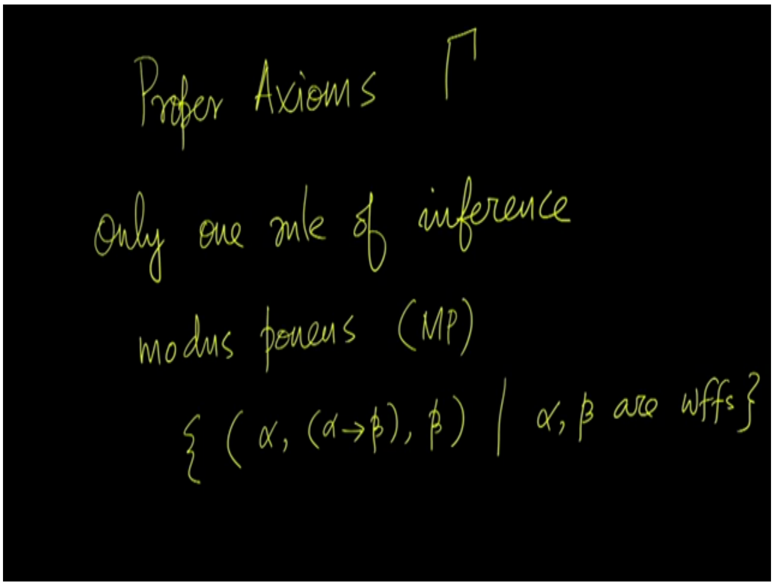
(Refer Slide Time: 29:14)



The second axiom or the second family of axioms of this form alpha implies beta implies gamma implies alpha implies beta implies alpha implies gamma. And the third family of axioms says that not alpha implies not beta implies not alpha implies beta implies alpha.

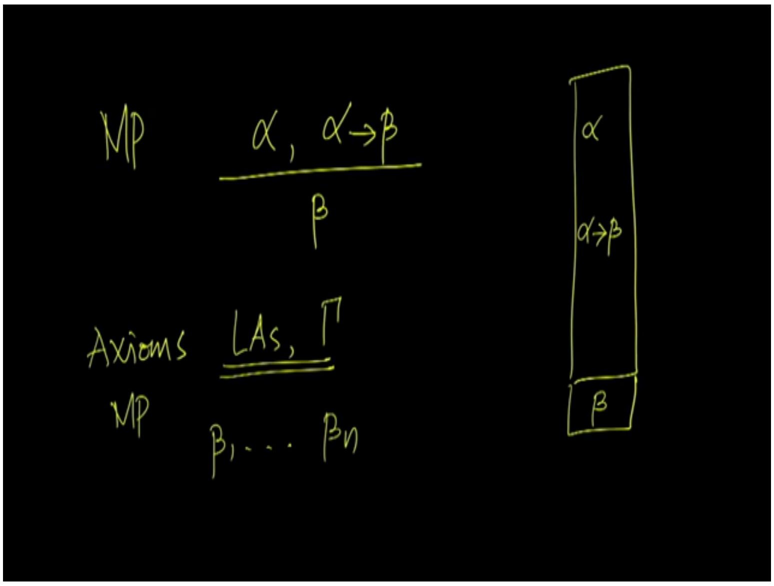
So, that these are the three families of axioms that we have, these are the families of logical axioms by substituting any formula in a well-formed formula for alpha, beta and gamma in these templates we can derive an infinite number of logical axioms. So, P 0 consists of an infinite number of logical axioms.

(Refer Slide Time: 30:06)



In addition to that, we could also have called proper axioms. Let us say, we have a set of proper axioms called gamma. So, this could be any set of arbitrary formulae that suits our convenience and we have only one rule of inference, this rule of inference is called modus ponens or MP for short it is triplets of this form alpha, alpha implies beta and beta where alpha and beta are well formed formulae.

(Refer Slide Time: 31:10)

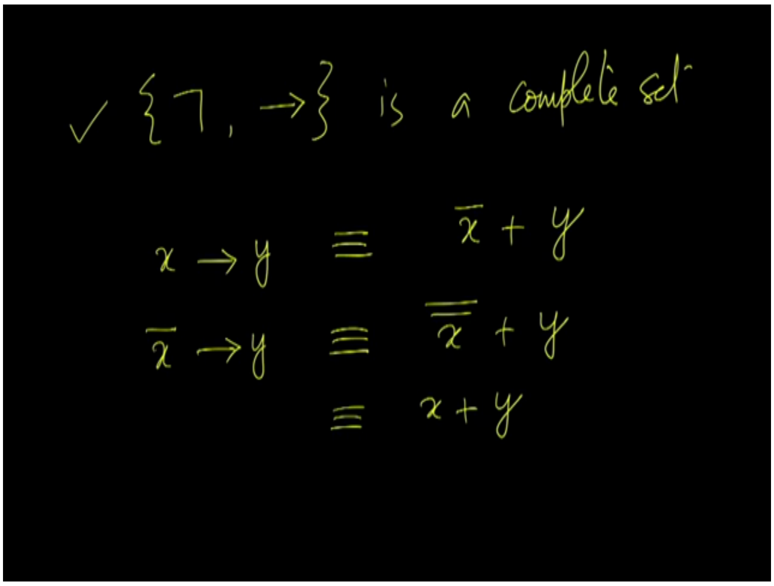


Or we could write like this, a rule of inference could be written like this when you have alpha and alpha implies beta then beta is derivable. So, what it means is that, within a proof if you have already proved alpha and you have proved alpha implies beta then as the next step in the proof you could write beta, that is if alpha and alpha implies beta are among the previous formulae within the proof then the next formula within the proof could be beta.

So, this is a rewriting rule called modus ponens, so this is the only role of inference that we have. So, in the sense our axioms are logical axioms or the formulae, the set of formulae in the set of formula gamma.

So, axioms are from these and MP is our only rule of inference therefore a proof will consist of a sequence beta 1 through beta n where beta 1 is necessarily an axiom it is either a logical axiom or is a formula from gamma and any subsequent formula is either a logical axiom or a formula from gamma or follows from two previous formulae by modus ponens. So, such a sequence of formulae is what we call a proof

(Refer Slide Time: 32:43)

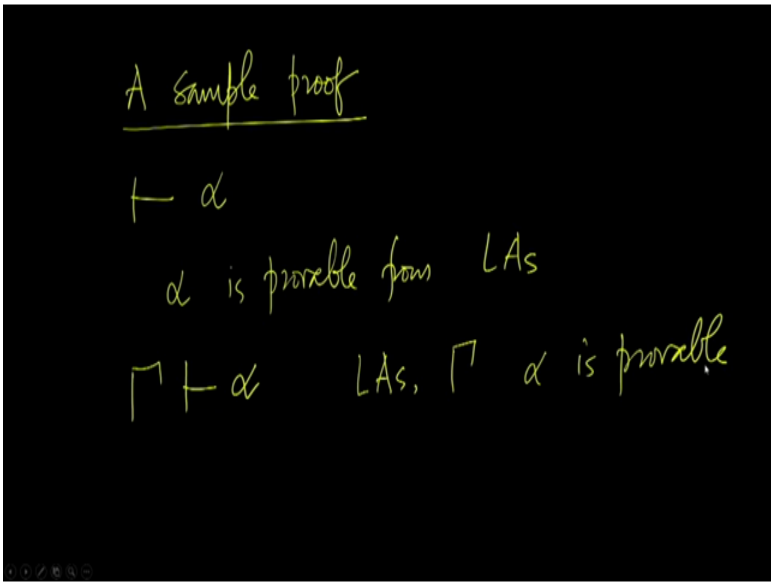


So, you may have noticed that here in our system we have only two logical connectives for example we have negation and implication but we have not used any other connective that is because this set is a complete set of connectives, why is that? That is because we know that x implies alpha x implies y is logically equivalent to x bar or y, negation of x or y. therefore, negation of x implies y will be logically equivalent negation of negation of x or y but negation of negation of x is the same as x.

Therefore, negation of x implies y is nothing but the OR of x and y that is OR can be synthesized using negation and implication. Now, we know that OR and NOT together form a complete set of connectives therefore negation and implication also form a complete set of connectors.

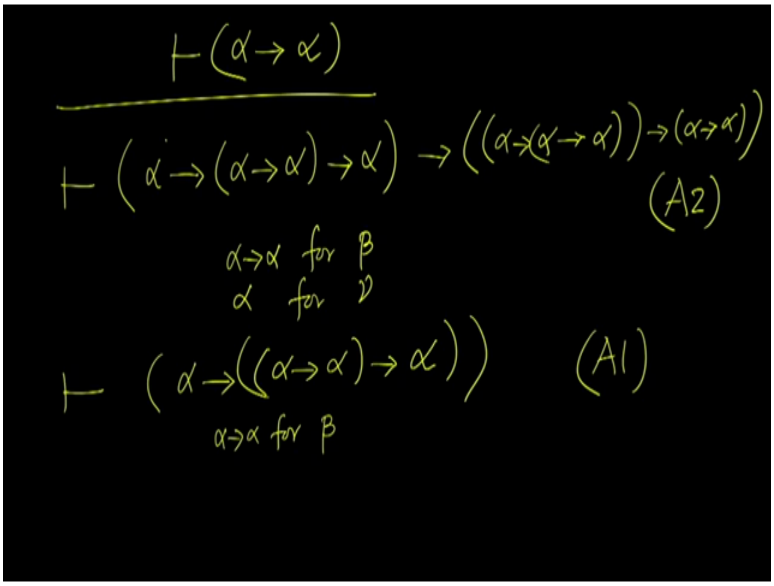
Therefore, in our system if we have only these two connectives still we can synthesize any Boolean function as we have seen before. So, that is why we have used only these two connectives in our system.

(Refer Slide Time: 34:15)



Now, let us see a sample proof, when we write like this what we mean is that alpha is provable from the logical axioms alone without any proper axioms, when we write like this what we say is that alpha is provable from gamma, so in this case what we mean is that from logical axioms and the set of proper axioms gamma alpha is provable.

(Refer Slide Time: 35:10)



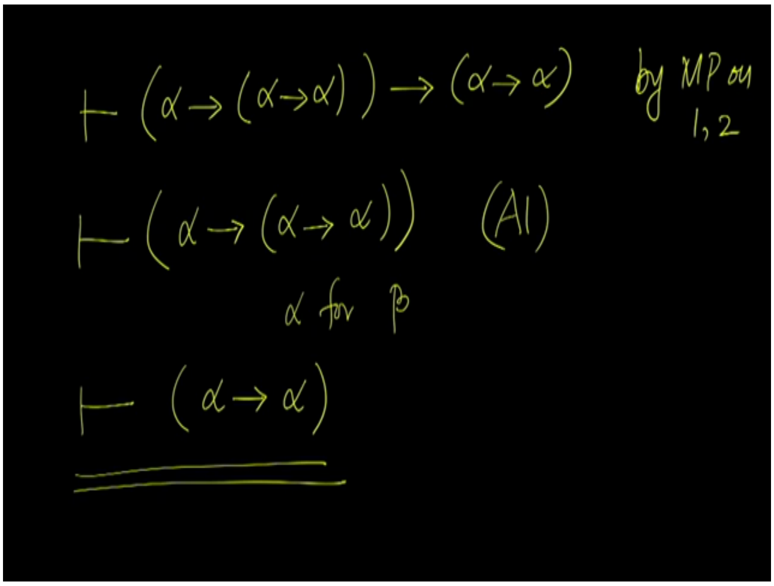
So, in the sense we will show that alpha implies alpha disprovable from gamma. So, this is what we want to establish alpha implies alpha is provable from let us say nothing that is from logical axioms alone we can prove alpha implies alpha.

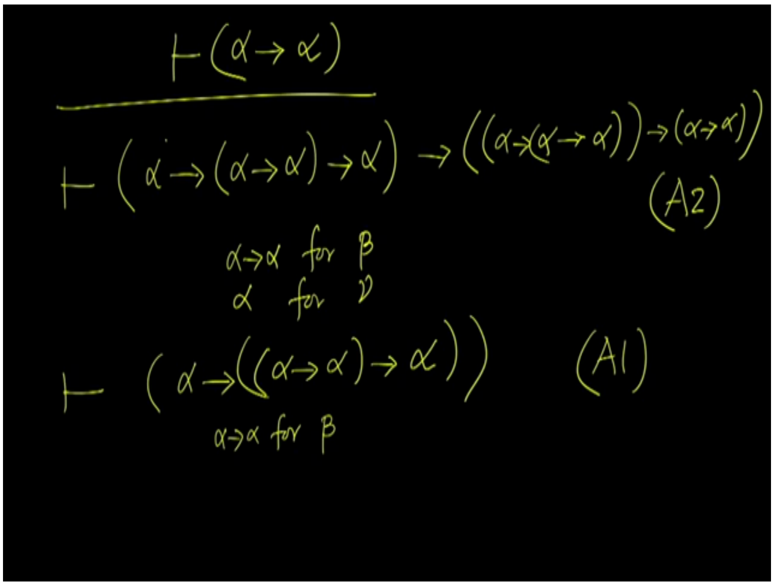
So, how we prove is this, the first statement has to be necessarily an axiom, so the axiom that we chooses this. So, this is the first statement in the proof, the first statement has to be necessarily an axiom, now is this an axiom we find that it is indeed an axiom because this is from the second template.

In the second template, we have alpha implies beta implies gamma implies alpha implies beta implies alpha implies gamma. So, if you substitute alpha implies alpha for beta and alpha for gamma what we get is exactly this, so this is an instance of axiom schema 2. By substituting alpha implies alpha for beta and alpha for gamma this is what we get. So, this is the first statement in our proof.

The second statement in our proof is, alpha implies alpha implies alpha implies alpha this you can see is an instance of axiom schema 1, if you substitute beta for or other alpha implies alpha for beta in axiom schema 1 this is precisely what we get, so this is the second statement in the proof.

(Refer Slide Time: 37:23)





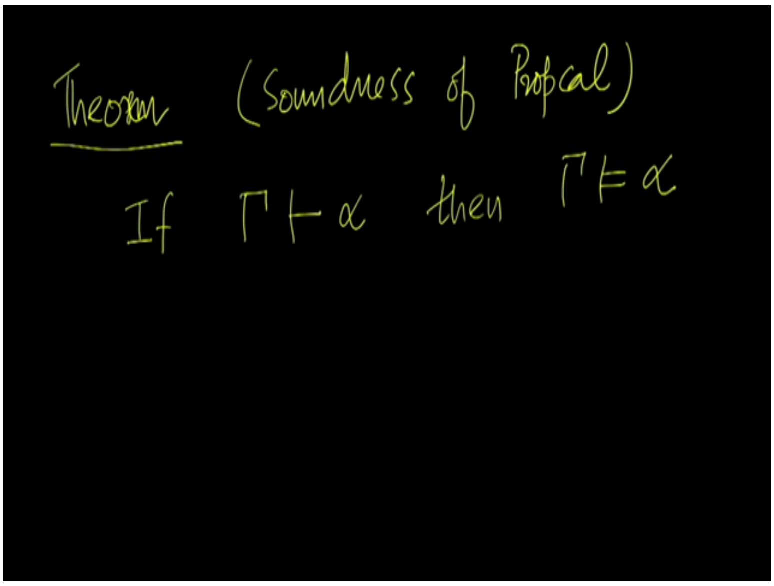
Then the third statement is an implication alpha implies alpha implies alpha implies alpha implies alpha, how do we get this? We get this from the first two statements. So, if you observe the first two statements we find that the second statement is in fact the antecedent of the implication which is the first statement, the second statement and the antecedent here are identical.

Therefore, once we have these two statements in our proof we can apply the rule of inference modus ponens on these and we can write the consequent as the next statement that is precisely what we have done, this happens to be the consequent of the first statement in the proof.

So, this is by modus ponens on statements 1 and 2 and then, we have alpha implies alpha implies alpha how? By A 1, if in axiom schema 1 you substitute alpha for beta this is precisely what you get alpha implies alpha implies alpha, so this is the fourth statement in the proof.

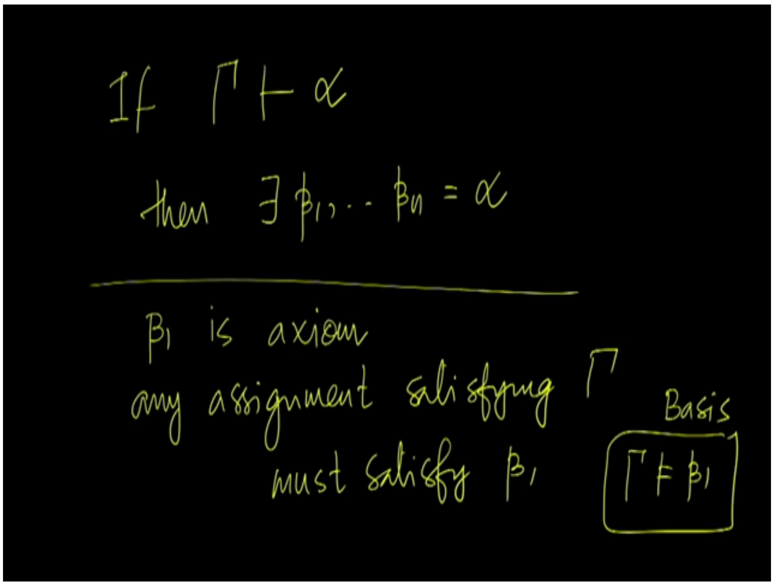
Now, you compare the third statement with the fourth statement we find that the fourth statement is the same as the antecedent of the third statement. Therefore, we can now derive the consequent of the third statement as the next statement in the proof and this is precisely what we wanted to prove. We wanted to show that alpha implies alpha is provable from logical axioms alone that is precisely what we have done, so this is an example of a proof in our system.

(Refer Slide Time: 39:25)



Now, we prove what is called the soundness of the system of logic, we say that a system of logic is sound if whatever you prove in that system happens to be the logical consequences. In other words, if you take gamma as the set of proper axioms and manage to prove alpha then alpha is indeed a logical consequence of gamma that is whatever you prove is a logical consequence therefore the system of proof that we have is sound. So, how do you prove this?

(Refer Slide Time: 40:23)



If alpha is provable from gamma that is what we have assumed alpha is provable from gamma and then we want to show that alpha is indeed a logical consequence of gamma. If this is provable from gamma then there exists a sequence beta 1 through beta and culminating in alpha, so that beta 1 is an axiom and any other formula in the sequence is derived from two previous formulae by modus ponens.

Or in other words, there exist a proof which is culminating in alpha that is when we say that alpha is provable from gamma. So, this we know if alpha is provable then there is a proof.

Now, let us look at beta 1, beta 1 is surely an axiom, so any assignment that satisfies the whole of gamma must satisfy beta 1 too, why is that? if beta 1 is an axiom either it is a logical axiom or it is a proper axiom, if it is a proper axiom it is a member of gamma.

Now, we are looking at an assignment which satisfies the whole of gamma therefore in particular beta 1 was also satisfied, if beta 1 happens to be a proper axiom. On the other hand, if beta 1 is a logical axiom then beta 1 must subscribe to one of the three templates a 1, a 2 and a 3.

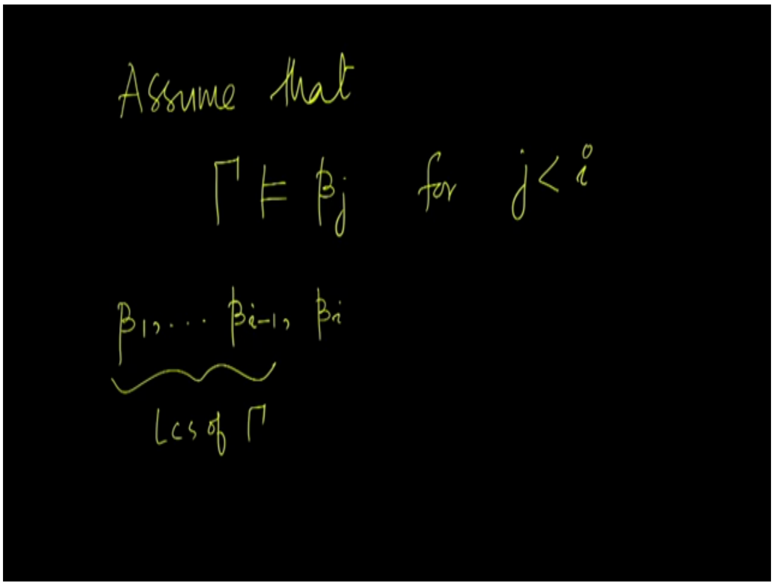
If you look at a 1, a 2 and a 3 you find that these three templates are essentially tautologies that is whatever you substitute for the variables here what you get is a tautology, you can drop the truth table and see that if whatever truth values you assigned to alpha, beta and gamma these formulae will always evaluate it true.

Therefore, our logical axioms are always tautologies therefore they are satisfied in every single assignment. So, if beta 1 is a logical axiom then it is true in every single assignment not just in the assignments that satisfy the whole of gamma.

So, in particular in any assignment which satisfies the whole of gamma beta 1 is true also. Therefore, if beta 1 is an axiom then any assignment that satisfies gamma must necessarily satisfy beta 1.

Or in other words, beta 1 is a logical consequence of gamma. So, we are now proving by induction this is the basis of the induction, the first statement in the proof is a logical consequence of gamma.

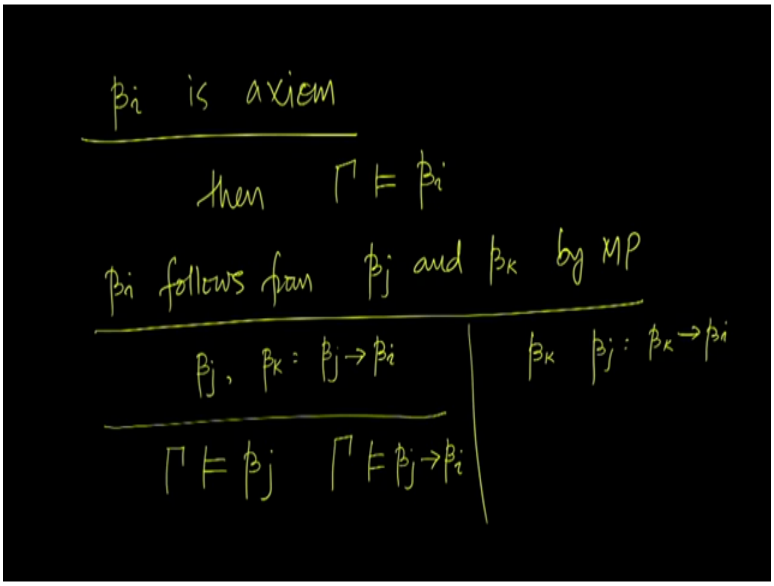
(Refer Slide Time: 43:18)



Now, assume that beta j is a logical consequence of gamma for every j less than i and we are going to look at beta i consider the sequence from beta 1 through beta i this is also a proof culminating in beta i every formula here is either an axiom or follows from two of the previous formulaes modus ponens.

Therefore, this is also a proof and here we know that beta 1 to beta i minus 1 are all logical consequences of gamma, what we want to show is that beta i is also a logical consequence of gamma.

(Refer Slide Time: 44:11)



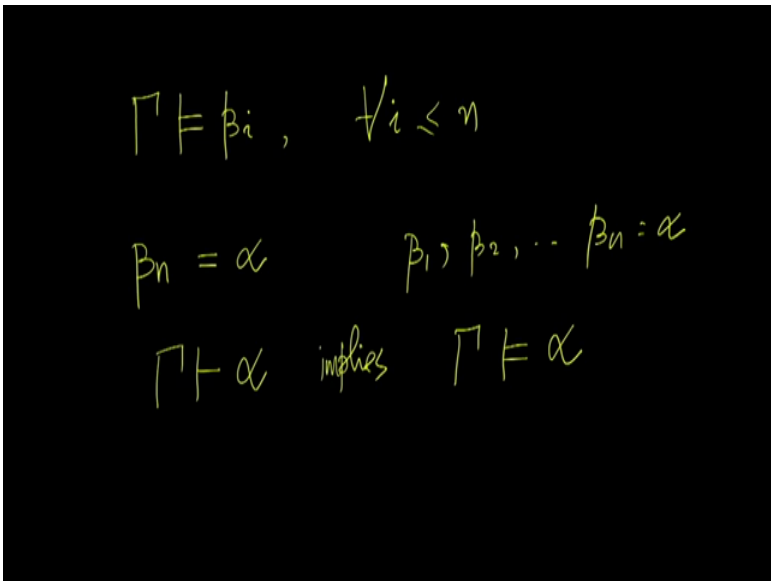
Now, beta i could be several, beta i could be an axiom if beta i is an axiom we have an argument that we made in the case of beta 1 that argument is valid here to if beta i is a logical axiom it is true everywhere, so it is true in particular in the assignment which makes gamma true, if beta i is a proper axiom then it is a member of gamma. So, in any assignment which makes the whole of gamma this is also true trivially.

So, if beta i is an axiom then we know that beta i is a logical consequence of gamma. Suppose beta i follows from some beta j and beta k by modus ponens, if this is the case then either it is the case that we have beta j and beta k which is the same as beta j implies beta i or it is the case that we have beta k and beta j which is the same as beta k implies beta I, the two are symmetric so we will discuss only one.

It is exactly in these two situations when we will be able to derive beta i from beta j and beta k using modus ponens. So, let us consider the first case, let us assume that beta k is beta j implies beta I.

Now, what we know is that all the previous j's are logical consequences of gamma therefore we know that beta j is a logical consequence of gamma and beta k which is beta j implies beta i is also a logical consequence of gamma.

(Refer Slide Time: 46:15)



By the theorem, we have just shown if beta j is a logical consequence and beta j implies beta i is a logical consequence then beta i is also a logical consequence. Therefore, what we have found is that for i beta i is a logical consequence of gamma.

Therefore, by induction we can say that this is the case for every i less than or equal to n. In the proof, that we are going to consider beta 1 to beta n but then what is beta n? Beta n happens to be alpha that is the culmination of the proof, the original proof that we started with.

We started with the proof of this form which ends in alpha that is why we claimed that alpha is provable from gamma. So, now what we have shown is that the culminating statement which is beta n is also a logical consequence of gamma by induction.

In other words, alpha is a logical consequence of gamma. In other words, if alpha is provable from gamma then alpha is a logical consequence of gamma. In other words, whatever we prove is sound in this system of proof, okay that is it from this lecture. In the next lecture, we will see a proof system for the first order logic, thank you.