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

Lecture - 15 Propositional Calculus (PC)

So, now if you look back, you can see that there are three proof procedures we have developed, calculations, informal proofs, and the resolutions. But all of them are semantic in nature. They first assume that there is some truth defined in it; because in calculations, you need equivalent substitutions, so which is semantic in nature, which needs first truth or falsity. Then you can see what is an equivalence? Same way, resolution needs first cnf conversion, and then you can do whatever. Informal proofs, they will also need substitutions, equivalence substitutions, because the laws you are using in the informal proofs can be used only with the help of equivalence substitution and uniform substitution.

What do you want is a completely different procedure rather than the truth. You want to play a game with symbols without knowing what truth is all about. Then we want to develop a proof system from there. Of course, it should be going hand in hand with the semantics, with the proofs. Proof should be going parallel to the truth or falsity; that we have to see, how it can go parallel.

In usual mathematics proofs, both the things are mixed together. You know that certain things are true. You take that as a theorem. Then, while proving we use axioms, some axioms have been there. Use them and continue. Now you want to demarcate between these two, because you want to study each of them separately. Once you do not do it, it will be difficult to study. Then, that how much import we have from the truth, how much import we have from the rule playing activity. You want to define only certain rules and follow it now; truth we have seen, how it matters.

What is usually done is, you think of some axioms as in geometry, for example you have certain axioms of Euclid's geometry. Then certain inference rules are given. You apply the inference rules, go for deriving the next theorems without knowing what the line is, what the point is. Lines and points are defined intrinsically by the axioms or the postulates because the way you think of straight line may not be that straight. You can have another model where the lines are not straight. That may be possible. You do not know that while developing

axiom system. Of course, we have certain things that are lines are like this, they are straight, point is, one point there. These are only intuitive concepts we want to formalize here. Similarly, we have the concept of truth, but we want to capture it by a rule playing activity.

We will have certain axioms. We will have certain inference rules. Then, starting from the axioms, applying the inference rules, we will be deriving some other things. Those will be the theorems. Now, as we go along, we should see that the theorems should be our valid propositions. The axioms must start from the valid propositions. Inference rule must be one of the laws and so on, but then that is only to make it parallelly going with the semantics. If you do not want that, say assume something which is unsatisfiable, then axiom, then apply whatever inference rules you have from the laws. Then, you will get every proposition there. That may be useless. So, we want to start with something else and then you notice something, which will be important for us, that all the connectives are not required. We can minimize the number of axioms in certain sense. We do not want to over-burden our memory.

You know that there are many truth functionally complete sets like not, or. That is enough to express all the other connectives, not and that also expresses all the connectives. We have not discussed nand and nor. Why? Those two are only truth functions, which are by themselves, truth functionally complete. All the other connectives can be expressed by them. Here we want to take one such truth functionally complete set and if necessary include other connectives later. These two, we will be taking: not and implies. Not and implies should be adequate, because or can be expressed through not and implies. Therefore, not and or are there in our system and that is an adequate set. So, it will become adequate.

We will not using the bottom and top symbols. We have only the propositional variables, not symbol, implies symbol. With that, you apply your PL rules, the grammars and generate all the propositions. Till now, truth has not come. You have to be observant, very observant there, no where we will be concerned with truth at all. We will just play a game with the symbols. Once you take this that we the propositional variables, then we have the punctuation marks and then we have the connectives. This is our alphabet now. So, from these alphabets, we are going to generate all our propositions where following the same grammar or rather similar grammar because we do not have the other symbols. It is a fragment of PL we are concerned with it, with only those two connectives. Then, you have to give some certain axioms. We give our axioms. First axiom is A implies B implies A. If you use the semantics, you know that it is a valid proposition, invariance, hypothesis invariance. That is our law.



Next axiom we take as A implies B implies C implies A implies B implies A implies C. These we can notice, to be distribution of implication, but slowly, we are not going back to the semantics. We forget whether they are laws or not. It is only for our reference, that is, they were laws. Then, third axiom we take as not B implies not A implies not B implies A implies B. This is also law of contradiction that we know. These are the only three axioms we are concerned with. First two, there is no negation symbol, but here we have the negations symbol. We will again assume the third one. These are the three axioms. When you say it is an axiom, it does not say that always you have to use A symbol. A, B, C, these are all variables there. They can be replaced by any proposition.

In fact, they are axiom schemes. Once you replace these symbols by some propositions, you get an axiom. The same thing is also followed everywhere else. When you say x plus y equal to y plus x, this means x and y can be replaced by any real numbers there. Both for the real numbers, you are telling this axiom. The same way you are taking these as axiom schemes, and we have only one inference rule, which is, let us write axioms here. They are axiom schemes and we have the inference rule, which is MP. MP stands for modus penance, which says from A and A implies B, you can derive B. Now see, we are not using the entailment sign even, because we do not want to go back to the semantics here. All that we say, if you have A, if you have B, then also you have A, if you have A, you have A implies B, and then also you have B. So, in the sense that, suppose you are writing a proof, you will say A is

there, A implies B also has been obtained till now in the proof. Then, you can write B next. That is what it says. Is it clear? Let us see one example of a proof, how does it look like.

(Refer Slide Time: 09:30)

Now, this itself is a proof, yes, because that as I have, an axiom, so I stop there. I say I have already got something. Yes, it is an axiom. So, I have got something, but then I can have something else. This is also axiom one. Is it okay? I have these as A, this as B, this as A. So, A implies B implies A, this is also axiom one. Now, you apply modus ponens. So, I have obtained this r implies p implies q implies p, so brackets of this are given. Now, can you tell me, what is a proof in the axiomatic system?

We are not reducing anything. We are rather starting from the axioms. Well, this is an example of a proof. In fact, only the middle column is the proof. The other things are just for reading the proofs. We are documenting them so that we can read them. Can you see that these line numbers and this documentations only help us to read that. How? Why it is a proof? That is all it says. Not only in these axiomatic system; in any axiomatic system, this is the case that a proof is only a finite sequence of propositions where each of the propositions is either an axiom or is derived by using some rules of inference given there.

Here, we have only one rule of inference MP, which uses two propositions A, A implies B. Therefore, we have to spell it out exactly. So, a proof is a finite sequence of propositions where each proposition is either an axiom or is derived by an application of MP from earlier two propositions. Therefore, that is what the definition of proof will be.

In this axiomatic system, we always have to say, in this axiomatic system, we rather give it a name. We will call it propositional calculus. Let us call it propositional calculus. In PC, a proof is a finite sequence and so on. That will be all, the concept of a proof.

Let us write it. A proof in PC or sometimes you say PC hyphen proof, a proof in PC is a finite sequence of propositions, each of which is an axiom or is derived from earlier two propositions by an application of MP. Is it clear? What is your theorem in PC? What you obtain is a theorem. It is our last proposition in a proof. That will be our definition. Now, it looks funny, but that is what we are doing. A theorem in PC is the last proposition in a PC-proof.

(Refer Slide Time: 15:15)

Now, our basic concern is just to derive theorems. We go on deriving theorems by following this rule. That is all we will be doing. Now we can say that r implies p implies q implies p is a PC-theorem. If w is a PC theorem, we have to develop some symbol. If w is a PC theorem, a theorem in PC is also written as PC-theorem, we write it as, so we have to develop some symbolism. Earlier, using two parallel lines; here only one parallel line we will use. This is called the turnstyle. We will use it as w is a theorem. Sometimes, we write PC here. We say that it is a theorem in PC, but if there is no other axiomatic system, we just write this symbol. We just write w is a theorem. This proof, which you have done in example one says that r implies p implies q implies p is a PC theorem. Once we use this along with other symbols, this will have the least precedence, whatever is there to that it qualifies. You may not have

brackets here. It is easier to read them with brackets or without brackets also, we will read this thing that the whole thing that follows that, is the theorem. We will prove a very simple thing first, show that p implies p is a theorem.

(Refer Slide Time: 17:49)



Now, question is how do we proceed, which axiom we start with? We have to start with axioms any way. If only two propositions are there, then you can use MP, otherwise you cannot use it. It requires at least two propositions to be used, exactly two. If there are more, then you choose two and then apply, wherever it can be applicable. But in order that it is applicable, they should be in this form. There is one proposition, a proposition, this arrow sign, another proposition. Any way, you may not read that arrow has implied now. We do not, what is that?

It looks consistent with or implies of the semantics of PL or propositional logic because these are the laws. These were some valid propositions and this is also a valid consequence that we know, but its counterpart in semantics or in propositional logic, not anywhere. Now, how do we proceed for showing that p implies p is a theorem, which axiom we should use? Well, let us take axiom one. What does it say? Axiom one, see always we have the target p implies p. To say that p implies p would come in a derivation, I should take both of them as p. I cannot take the whole thing as p. There is one implies sign. In p, there is no sign.

Let me say p implies p. Then, this axiom would be looking like p implies p implies p. Let us start with p implies p implies p. It looks like this. This is axiom one. Now, I want, I can use only MP, nothing else is there; if I use MP, because I am interested in p implies p, I have to eliminate this p somehow. In MP, you have A implies B. Then, A is eliminated, you get only B, provided you have already A. So, you should have already p somewhere. It does not look like I can get p. From which axiom, I will get p? It can be any proposition also. Where from I will get p itself? I do not know where from I will get it. This attempt really fails.

Let us see, which are axioms can be helpful. Let us take axiom two, where can p implies p come? You know that A implies B. then, A somehow can be eliminated and B can be obtained. That is our only inference rule, but it is a constant, but that also helps in thinking. Here, what I want; p implies p. That means the last implication can be obtained if everything else can be eliminated. This A implies C should be thought of as p implies p. Now, whatever this B mean if I, at all use axiom two, in that case, how the axiom will look like? Both A and C are p now. So, it is p implies B implies p implies p implies B implies p. That is how it will look. Axiom two will look like this if I substitute both A and C as p. B, I am keeping at free. I will substitute later whatever is required. In order to get that, I should have got this, apply MP twice. This I can get, this is A1; p implies B implies p that is A1. So, I can eliminate this portion by introducing A1 before it. Now, scheme is I start with this as A1, this as A2. Well, then I get p implies B implies p implies p. By modus ponens, some improvement is there.

(Refer Slide Time: 23:43)

Now, the thing is, I want only p implies p. So, I have to eliminate this p implies B, p implies B, we have to eliminate. Well, B is free. You have not substituted anything. So, what I should substitute in place of B so that it will be an axiom? p implies B or q implies p, any other q also will do. It does not matter because that is also an axiom. What you have to do is, replace everywhere; here, in all the three lines, B as q implies p or as p implies p. Is that okay? So, that means this should be p implies p, this should be p implies p, this should be p implies p. Is that clear?

Then, I can introduce p implies p implies p as A1 and I get p implies p. It is already there, if you have. So, you do not have to introduce. This is how it will be proceeding now. Can you complete the whole proof?

Student: All the theorems, which you get, all others we...

What is it?

Student: Like all the axioms are valid if you apply semantics, so that also mean that all the theorems; if you apply semantics to them, it will be valid.

For `surely' we need a proof.

Student: I am asking is it a...

We need a proof for it.

Student: Yeah.

We will do that after you get some experience with the proofs and I would rather ask the other question. If I have something valid, can you show that it is a theorem in PC? Well, both the questions we will tackle later.

So, where we are now? You wanted to show p implies p. Our plan is to start with p implies p implies p implies p. This is axiom one. Well, this is what the first line reads there: p implies p instead of B. Then, we take from this A implies B implies C, we go for axiom two. That, it says p implies p implies p implies p, they have all things, implies A implies B implies A implies C. This is axiom two. Then, we use modus ponens to get these, which is p implies p implies p implies p, which is one, two, modus ponens. Next, we introduce the

axiom p implies p implies p, which is axiom one. Next, I get p implies p by using modus ponens on four and three. That is the end of the proof.



(Refer Slide Time: 24:57)

What it says is that constructing a proof is not that easy. It is not mechanical, but checking whether a proof, a suggested proof, is a proof or not is mechanical. Once you write some proofs like this, something and you claim that it is a proof, you can easily verify, so that this is really a proof or not. The concept of proof or the notion of proof is effective. There is an algorithm to check, so that something suggested as a proof is a proof or not, but to construct a proof is not mechanical, it is not effective. It looks like that. We do not know whether it will be or not. You have to develop some intuition to create some more proofs. Let us take one more proof.

Student: Why we have these axioms?

Again, wait for some time. You will see why we have chosen these theorems, why not others, that is a good question, but wait for some time to get the answer. First, have some experience.

Student: Can any thing imply p implies p?

How do we show that r implies p implies p is a theorem? That is the question. See, why he is asking that, he is thinking about our example one.

In example one, we had shown that this is a theorem. This we have proved as a theorem in example one. How did you prove? We started this as an axiom. Then, this implies r implies, this is also same, axiom A1. Then, we used MP. Now, instead of this axiom, suppose I will use p implies p. Then, how the proof will go? It will start from where? From where it will start? It will start from p implies p implies r implies p implies p or you may start from p implies directly. So, I start from there. That is what example one says. Instead of the axiom, I am taking p implies p now.

Next step, you would get r implies p implies p by modus ponens. Is that right? Now, how to make it a proof? It is not yet a proof. It is our rough work. How do we proceed? Well, we have already proved p implies p. Bring that proof and insert it here. I have now one, something is starting. That line number was how much, 5 in example two. So, 5, I get p implies p. Doing the proof from example one, example two, up to this, you take the proof of p implies p. Next, you add them. Here, it is axiom one, here it is 5, 6 MP. So, proofs of earlier theorems can be used, as proofs can be inserted anywhere.

So, p implies p, if you have proved, then p implies p can be used later, but this leads to another question. If I ask you to prove p implies q implies p implies q, what will you do? What will you do? Exactly that is what. Go back to example two. In the whole proof, wherever p is coming, you substitute p implies q there. So, you get another proof.

Student: First, get p implies p.

No, just look at this proof what we have done here, the rough work. The same we will be doing; the rough work for p implies q, in axiom one, instead of p. Look at the fair proof. Here, what you do? Instead of p, you take p implies q implies p implies q implies q implies p implies q that is axiom one.

Student: Propositions are divided already.

No, axiom one says A implies B implies A where A, B are...

Student: Proposition, any proposition.

Axiom scheme, any instance of that is an axiom. Substitute anything for A and B that is axiom one. I substitute p implies q for A. I substitute p implies q, for B also. Then also, I get one axiom. Instead of B, taking p implies q, I will take p implies q implies p implies q. That is still all right. That is also axiom one. What it says is that if you have already proved p implies p, then you can use that as a theorem scheme. Each theorem is a theorem scheme now. Just like your axioms, axioms schemes, theorem is a theorem scheme. We give a proof of this. What we should do? It says that you take the proof of p implies p. There you substitute anything. Every occurrence of p by p implies q. Instead of doing all those things, we will just mention this way. We will accept it as a proof, p implies p already a theorem.

Now, substituting you get this, but all these steps will be taken together. Instead of writing all these things, we will simply write p implies q implies p implies q is a theorem; already we have done it. We can refer back, for example, example two that is where you have proved it, since each theorem can be taken as a theorem scheme, but the only thing is always you are substituting uniformly. There is no equivalence substitution here, you do not want semantics.

Student: What if we substitute for A as p implies p and B...

Substitute.

Student: We directly prove this in...

Yes, yeah.

Student: Why do we have to go through getting p implies p?

You want to substitute, yes.

Student: A as p implies p.

A as p implies...

Student: p implies p.

p implies p, so after substituting, what do you get?

Student: I get p implies p implies r implies p.

(Refer Slide Time: 35:09)



That is what we had got here no? We have done with p. We can say p implies p. So, now it will tell us p implies p. It will be something like this. It does not matter.

Student: Take an axiom and directly, I do not need...

Then?

Student: I do not need to prove one to five.

Then, what? After this, after this, this is axiom one, but that is not your interest. Your interest is this one only. So, you have to eliminate the first one. There you use p implies as a theorem. Clear? Yes? Just to write it in shortened way.

Student: But, how do we know? I mean I can just come after even without the proof, I know this is two, p implies p is two, p with my knowledge.

There is no truth. Once you say p implies p is a theorem, you should have a proof for it.

Student: Unless we have written down the theorem, we cannot apply.

Yes, so it develops systematically because we have only three axioms. From three, we are going to thousands. That may be implies x. We will see slowly. In fact, it is infinite. Why? This is because you take any axiom A implies B implies A, you can substitute any proposition there. So, that itself gives you infinite number of axioms, which are theorems. Is this clear? The concept of the proofs and how to use them as theorem. So, only this much is enough. Now, we write it is as a theorem because already we have proved it as a theorem, which is p implies p, and each theorem is a theorem scheme. Let us take one more example.

(Refer Slide Time: 37:10)



Yes, now try this. See it looks that we will be using axiom three somewhere; but where exactly we do not know. Axiom three looks like not A or let us write, not p implies not q implies not p implies p. Now, look at the pattern. All that you can do is look at the pattern, nothing else. Same, we should take same, suppose I take same. It looks like this. Now, use this as a theorem. The job is done. Yes, that we have proved already. We will be starting with not p implies not p, theorem. Next, not p implies not p implies not p implies p implies p, axiom three. Next, not p implies p, one, two, modus ponens. That is the end of the proof; done.

(Refer Slide Time: 39:37)

We will go to the next. Now, there is something we do not know. What is the meaning of this? We have not defined it at all. What does it say? It needs some generalization of the concept of a theorem, of proof itself, because theorems are defined from the proofs. Here is a consequence. You have a set and then another proposition. You are using the same symbol as theorem, for entailment, like that sigma you have to read it somehow. We will say sigma syntactically entails w because there is no semantics now. The other one is semantic entailment.

(Refer Slide Time: 41:50)

A derivation for Z + w is a finite axion or is derived from two earlier propositions; and which the last proposition.

So, sigma syntactically entails w. What happens? If there is a derivation for it just like your proofs, so what is a derivation? It is a proof where you can use axioms or you may use this or that or the premises in sigma. What we do is, first we derive w from somewhere and those somewhere are the propositions, which are in sigma. We can also use the axioms that are bonus. So, how to give the definition of this derivation? It is again a finite, set of sequences or a finite sequence?

So, we say that a derivation for sigma entails w is a finite sequence of propositions, each of which is in sigma or an axiom or is derived or obtained from two earlier propositions; and w is the last proposition in this derivation. Such a derivation is also called a proof of sigma syntactically entails w. That is also called a proof of sigma entails w. The question is how to prove this? Ok.

(Refer Slide Time: 43:25)



As usual if sigma is a finite set, you can write as w1 to wn. Then, you omit the curly brackets. As we write here, instead it should have written with curly brackets. We just omit them as a convention. Now, how do we proceed? It says that in our derivation, the last line should have p implies q, p implies r. In between, we might use p implies q, q implies r. It does not say. We have to use. Is that okay? Just like in proofs, we have the axioms. You do not have to use all the axioms. Only A1 you can use and prove p implies p, that is fine. Similarly, here you do not have to use all the premises, but all that can be used are from sigma or axioms. That is what the derivation says. Now, how to proceed?

Student: The element of sigma that also scheme or are they fixed?

They are just giving propositions, actual propositions, just as in your theorem p implies p. Now, p implies p, only we know. Once we see that p implies p is a theorem, it can be thought of as a scheme also. We will come to that later. First, let us see whether this holds or how to make a derivation from this. Well, where from it can come, this p implies r? See here I see, there is a premise, which is q implies r. There is also p implies r. I have axiom two, which has such a pattern. The second part of the axiom two, just look at it. It says A implies C, A implies B, A implies C, but it is r; r is common with q implies r and p implies r, r is common. Axiom two says first part should be common. A implies B implies A implies C, first part should be common. Instead of these, I should concentrate on this. It may come to something like p implies q implies p implies r. Once this is given, I can apply this and get this by modus ponens. Modus ponens is there.

We have only one method. Look at the eliminating the left side of the implication that is modus ponens. If it is already there, I can get and come to p implies r, but this I have to prove from the first part of the axiom two. I should have before it, p implies q implies r, but I have q implies r. Can I prove p implies q implies r? Yes, you have seen already in example one. It is not axiom one. Using axiom one, you can prove this. So, you start from q implies r, use axiom one, come to p implies q implies r, use axiom two, come to this is p implies q come to q implies r. This will be our procedure.

(Refer Slide Time: 47:37)

So, let us start. Our rough work says I should start from q implies r. This is a given premise. We will write on the third column as p, it is a premise. Next, we want to use axiom one. I say, q implies r implies p implies q implies r. This is axiom one, A implies B implies A. Next, I use modus ponens to get p implies q implies r. Next, we use axiom two here. So, p implies q implies r implies r implies p implies q implies r, axiom two. Next, use three and four to obtain p implies q implies p implies r; three, four, and modus ponens. Next, use p implies q as a premise. Next, p implies r is obtained from these two by modus ponens. Is that okay?

Now, you identify this as your hypothetical syllogism. If you take, think syntactic entailment is like semantic entailment, then it is hypothetical syllogism.