INDIAN INSTITUTE OF TECHNOLOGY ROORKEE

NATIONAL PROGRAMME ON TECHNOLOGY ENHANCED LEARNING (NPTEL)

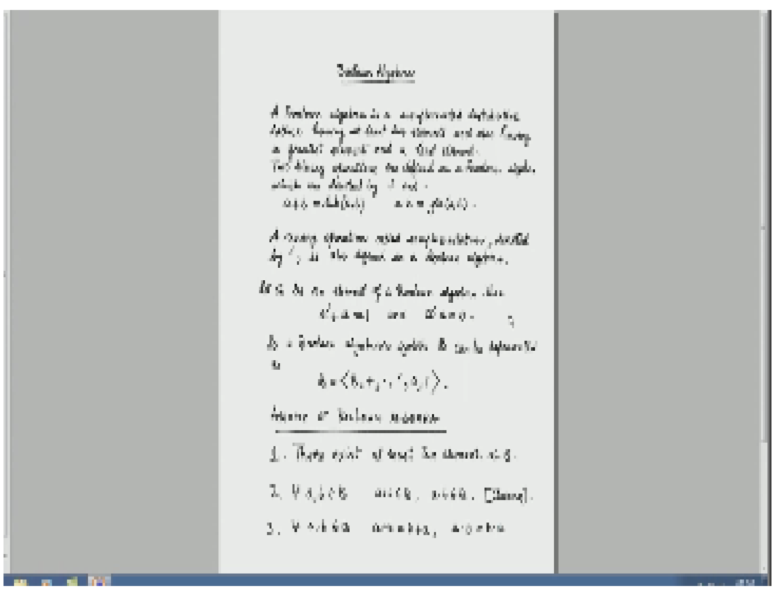
Discrete Mathematics

Module-08
Boolean algebra and Boolean function
Lecture-01
Boolean algebra

With
Dr. Sugata Gangopadhyay
Department of Mathematics
IIT Roorkee

Today's lecture we will continue our discussions on Boolean algebra and later move on to Boolean functions which are functions on Boolean algebras.

(Refer Slide Time: 00:51)



So let us recall the definition of a Boolean algebra a Boolean algebra is a complemented distributive lattice having at least two elements and also having a greatest element and a least element we will define operations on Boolean algebras which are induced from the idea of greatest lower bound and least upper bound of lattices so two of two of binary operations are denoted by plus and dot so we have two binary operations plus and dot where plus is the greatest sorry is the least upper bound of two elements.

So A + B is equal to the least upper bound of the two elements a b and a .b is equal to the greatest lower bound of the two elements a b these greatest lower bound and least upper bounds are defined as we define in lattices because after all will a Boolean algebra is a lattice next we have the complementation operation which gives us another operation on a Boolean algebra but in contrast with the previous two operations this operation needs only one element and

So it is called unary operation so we have a unary operation complementation a unary operation called complementation denoted by prime is also defined on a Boolean algebra now this complementation when it acts on an element a suppose a is an element of a Boolean algebra then an element of a Boolean algebra then the complement of a compliment plus a gives me one and a compliment dot a gives me zero.

Now the fact that compliments exist is due to the definition of Boolean algebra where we say that it is a complimented lattice a complemented lattice means that any element has a complement and complement means that when you take the conjunction or plus of that element with its complement you will get the greatest element and when you take the product sorry it is not conjunction when you take the disjunction or plus with the complement of an element then you get the greatest element.

And when you take the conjunction or what some sometimes people say and or the product of or dot with, with the complement you will get zero so thus these things are defined on a Boolean algebra thus an algebraic system Boolean algebra system is a is a system which consists of some elements so a Boolean algebraic system script B can be represented as Scribed be well which context consists of a set b which is a set of elements then the operation plus and dot which are two binary operations.

Then we have the unary operation complement and then we specify the least element and the greatest element so it is a six topples consisting of a set b then plus dot the complement which we denote by a prime 0& 1 now we have already seen in the length nature that in the previous lecture some examples of a Boolean of Boolean algebras like we have seen the simplest possible Boolean algebra consisting of 0 & 1and then we have taken some tupelos some three tupelos of elements and of 0 & 1and have seen the Boolean algebra that we can construct by, by using them.

So we have basically seen that by taking Cartesian product of the set 0 1 we can construct Boolean algebra with larger number of elements however we should also check the basic axioms underlying the Boolean algebra and we should also check some basic results which can be derived from the basics basic axioms of Boolean algebra so now we will be doing some kind of axiomatic axiomatization so we have the algebraic system which we call a Boolean algebra we have defined operations.

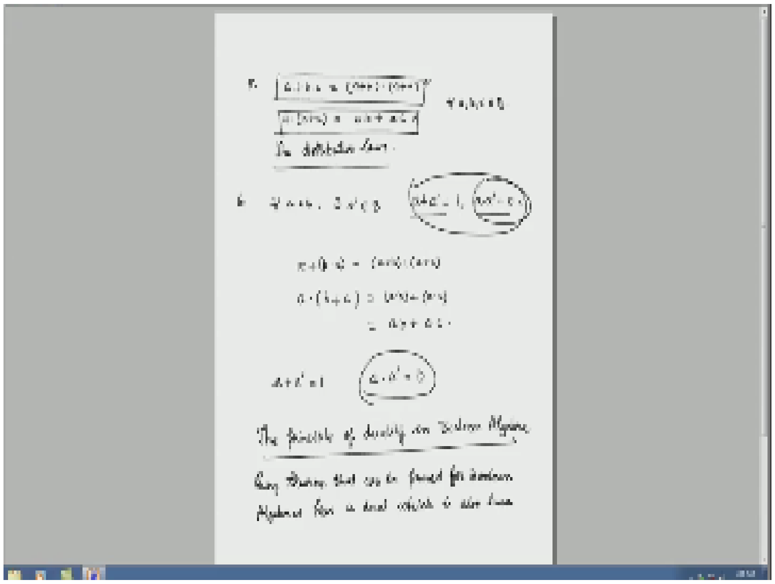
And we say that these nerd we explicitly write down a set of axioms that we say that this Boolean algebra must follow so the axioms of Boolean algebra the first one is that there exists at least two elements in b the second axiom is that for all a, b belonging to the bull belonging to the set b well here we will be often calling the script b as Boolean algebra but the other capital B also we will be calling Boolean algebra.

Now so for a b belonging to b a +b belongs to b and a .b belongs to b so this is a version of closure property so we can write it down as closure third property is that for all a b belonging to b a + b = b + a and a. b = b . a this is called the commutative law now at this point one may stop and say that wait a moment we proved all these four lattices yes indeed we proved all these four lattices but in this case we are trying to write down Boolean algebra with a explicitly defined axioms involving the set the operations.

And the greatest element list element so later on we will not be looking back to lattices but we will be looking at Boolean algebras and trying to derive more results by using these axioms although if we like we can of course see that all these things are satisfied in the, the environment of lattices now we have got the commutative law this is now an axiom here and then the fourth one is the existence of so-called additive identity.

So there exists an element 0 belonging to b such that a +0 = a for all a belonging to b and there exists one belonging to b such that a .1 = a for all a belonging to b so the first one is existence of zero and second one is existence of unity so we write existence of zero and existence of unit so we will call this element zero in a Boolean algebra and this has unit in a Boolean algebra now we have seen some axioms and we will see some more axioms the fifth axiom is the distributive law axiom number five so we have two kinds of distributive laws.

(Refer Slide Time: 16:59)



For example if you have a + b.c then we can write this as a + b. a+ c and if we have a . b +c we can write this as a .b + a dot C and this must hold for all a bc belonging to b this is called the distributive law now the last one is the compliment it relates to the compliment so for all a belonging to b there exists complement of a again belonging to b such that a plus a compliment equal to one and a . a compliment equal to zero.

Now if we look back to all these properties we will see that they appear in pairs for example if you look at this to these two laws you will see that they, they are in pairs in some way then these two are in pairs we see that we can in fact transfer from one, one expression within this pair to the another expression by interchanging + +. + 0 + 1 let me give an example suppose we start from the first equality in 5.

So we write it down again a + b . c=a +b . a + c now let us somewhat mechanically change the pluses two dots and dots two pluses so what will happen so I start from a, the instead of the plus I write a dot then of course here this means that I have a bracket over here so I will put a bracket and then c this is b instead of dot I will put a plus I put a plus here and then I write C this should equal now I have a bracket.

So I write a .b put a bracket around it and this dot here is replaced by a plus and then we write a .c and since V usually traditionally or take the precedence of dot over plus therefore we will write a . b+ a .c thus we see that we arrive at the second law now let us consider the laws or equality is that we have derived in the sixth axiom so we have got a +a complement equal to one what I said sometime back is that we have to change plus two dot and dot to +0 to 1 and 1 to 0 if I do that.

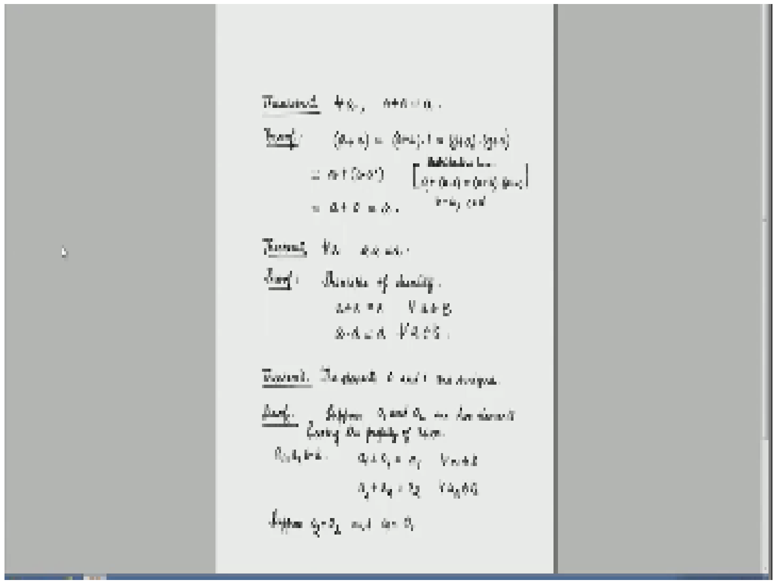
Then I have got a instead of plus I will put a dot and then I have got a complement and instead of 1 I will get 0and in fact this is this second one now this principle is called the principle of duality so the principle of duality in Boolean algebras which indeed makes our life easy in several locations now basically when we prove some equation or some relationship in tucked in, in a Boolean algebra like we have one expression.

And we say that okay this expression is equal to this expression then this will carry with itself a dual law or dual equality so what we can do is that we can change the dots to plus and plus two dots and exchange 0 & 1 and we will get another expression which is also valid so we will write that every theorem that can be proved for Boolean algebra every theorem so I made a mistake here every theorem that can be proved for Boolean algebras has a duel which is also true.

And is obtained by interchanging + and . as well as 0& 1 so very soon we will see the principle of duality in action now, now we move on to some results that we proved on Boolean algebras so I will start writing a sequence of theorems well it is somewhat, somewhat tedious to do that or to listen to that but we have to do that if we want to study Boolean algebras because these are the basic results that we need to work on Boolean algebras and work on Boolean functions which are defined on Boolean algebras.

So first theorem over here theorem one states that for all a, a + a gives me a all right now if you if you are looking at numbers if somebody gave you usual plus with numbers then suppose you take two and of course 2+2 gives you four but it does not happen like that in a Boolean algebra here we have a plus or something some binary operation which we are denoting by plus which, which is such that when I add that is a with a itself I do not get anywhere else.

(Refer Slide Time: 27:15)



But only a now the question is that how do we prove it now let us go to the proof now I start from the left hand side which is a + a and I recall one axiom which says that in a Boolean algebra anything dot one is that thing therefore I will write a + a .1 and I then recall what is one, one is nothing but a plus a complement that is also an axiom of Boolean algebra so I get a plus a dot a + a complement and now I will do something that is I will use the distributive law you will ask that how I am using the distributive law.

So please see here that a is repeating in these two terms I take a out and write plus over here and I will put a dot a compliment inside a bracket let us recall here distributive law distributive law recall that if you have a +b. c then you get a +b . a +c this is something that does not happen in numbers if you are considering plus as the usual plus in numbers and dot as usual product it does not happen.

But it happens in case of Boolean algebras so see a +b. c gives you a +b. a +c now in this case we are putting b=a and C equal to a compliment and that is why we are getting what we have we are getting so now we know that a . a complement gives me 0 therefore I have got a + 0 and this lets me prove that a +a = a so this is the end of theorem 1 we move on to theorem 2 here we stayed that for all a, a . a = a a question is how to prove that the answer is principle of duality.

So I write in the place of proof principle of duality we already know that a + a = a for all a belonging to b and the duality principle says that if I interchange plus and dot 0 and 1 then the relationship will hold so I write a . a = a for all a belonging to b and that is the proof so we will now go to theorem 3 okay now the theorem tree says that the elements 0 & 1 that we have defined in a Boolean algebra are unique that is there cannot be more than 1 0.

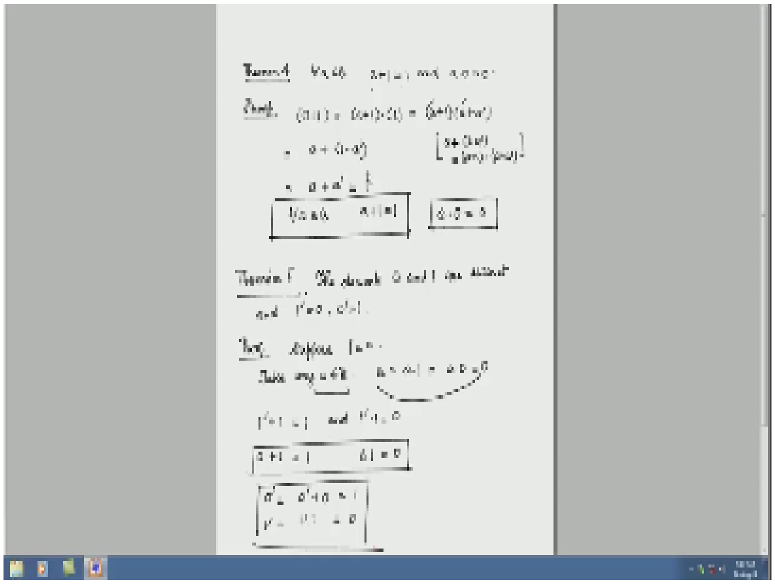
And there cannot be more than 1, 1 that means there cannot be more than 1 list element and there cannot be more than 1greatest element now let us see how to prove that proof now our way of proving is that we will start by the assumption that there are two elements which work as zero so suppose 0 1 and 0 2 are two elements having the property of well 0 now I know what is a zero because we have already seen in the axiom all right.

So suppose I take a 1 and a 2 in b then a 1 +0 1 is of course a 1 because of the property of 0 because we know that 01 is a 0 so it must follow the property of a 0 but this is for all a 1 belonging to b similarly I have 0 2 and a 2 which will give me a 2 now this should also work for all elements a 2 belonging to b now the question is that what happens if I take a 2 2 bz 2 0 2 so C suppose a 2=0 2 and a 1 = 0 1.

So C we will start from this one so it will come over here so I am putting let us let me change it a little so a -I will I will take zero one all right so let me let me correct it so instead of a- I will take zero one and instead of a one I will take zero - all right now we are starting here so we have got 0 2+a2 is 0 1 and this is equal to 0 1and if we consider this equation we have0 2 + 0 1 =a 1 but in this case a 1 is 0 2 but please note that this and this are one.

And same therefore 0 1 = 02 thus we have proved that we cannot have two zeros in a Boolean algebra and more or less in the same way or using the principle of duality one can prove that the unit element one in a Boolean algebra is also unique so I leave it as an exercise over here and move on to the next theorem which is theorem for in the order in which we are discussing.

(Refer Slide Time: 37:49)



And a .0 to 0 that is all now the question is that how do we prove it in order to prove it we have to start from a +1 and understand that a + 1 can be written as a +1.1 only one well because we know that one dot anything is that thing so that the that is a property of a unit now replace 1 / a + a compliment and then use the distributive law so take this a out so I have got a plus and then we have 1 + a compliment no I do not have that I have 1. a compliment.

So let me change it so here this is inside bracket 1.a compliment please see because if you have 1 + 1 .a compliment we can use distributive law this plus is distributing over these dots so I have got 1 a + 1 . a + a compliment right that is what we started with so we will have a plus a compliment because of course 1 dot anything is that thing and a +a complement by our axiom is 1.

So we see that ultimately for all a belonging to be a +1 = 1we have proved that and now to prove the other part as I said just some time back principle of duality makes our life easy so to the other part we have just use principle of duality so write a instead of dot plus like dot instead of 1 write 0 and instead of 1 write 0 so this is the other part of the theorem so we have done theorem for at this point well.

I know that this becomes tiring somewhere in the middle people start thinking that why we are doing these things but we have to remember that we are laying down the rules in algebra so after that we would have to think about lattices partial orders say gall b and all that so we will just think that we have a set of elements we have a set of binary operations one unary operation some special elements and we know what we can do with that so next one is the theorem five this is theorem 5 and this states that the element 0 and 1 are distinct and one compliment is zero.

And zero complement is 1 the elements 0 and 1 are distinct and one compliment is zero, zero complement is one we need a proof for that and the proof goes like this that suppose these elements are equal suppose 1=0 then what will happen take, take any a belonging to B all right and then we can start from a = a .1 and we know that by our assumption one is zero so it is a .0 therefore it is zero.

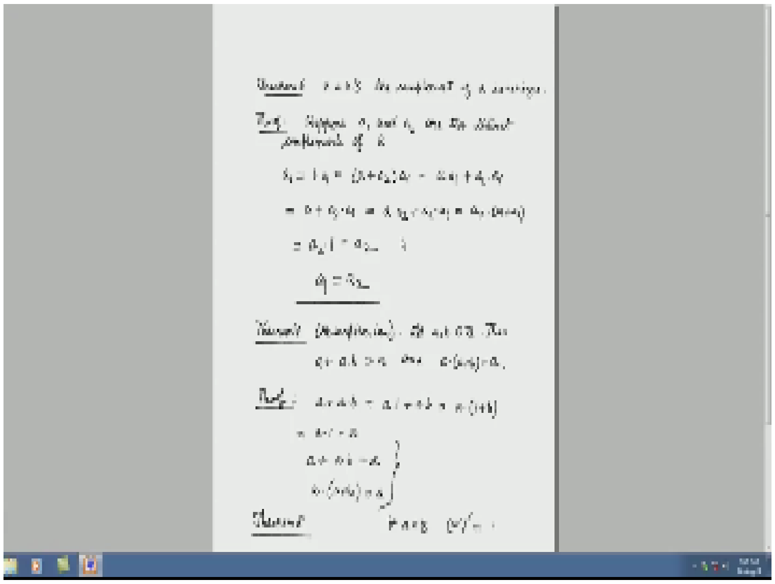
And that is the point if 1=0 then you cannot have any other element then any, any element other than zero in B so we start with an element a and Band we end up showing that that a is also equal to zero which is equal to 1so that means the whole Boolean algebra will collapse to a single element and by definition we say that a Boolean algebra must have two distinct elements so therefore 0 & 1 are distinct and now if we take one complement one compliment plus one should give me one.

And one compliment dot one should give me zero now 0+1 gives me one I know that because, because of the theorem for and 0.1 gives me zero as we see that zero works exactly as the compliment and we have seen in one of our previous theorems that compliments are unique now well we will prove it later but what we can prove here is that we will need something else over here.

So I can I can prove like this that zero compliment equal to zero compliment plus zero which is equal to one so that makes zero compliment equal to one and one compliment equal to one compliment into one which is equal to zero thus we see that zero complement is 1 and 1complement is zero.

Now I could have done something else that is here I could have shown that since this happens and if we can prove that compliments are unique then also this theorem holds but the problem is that we have not yet proved that the complements unique so we will now prove exactly that which is the sixth theorem which says that.

(Refer Slide Time: 48:23)



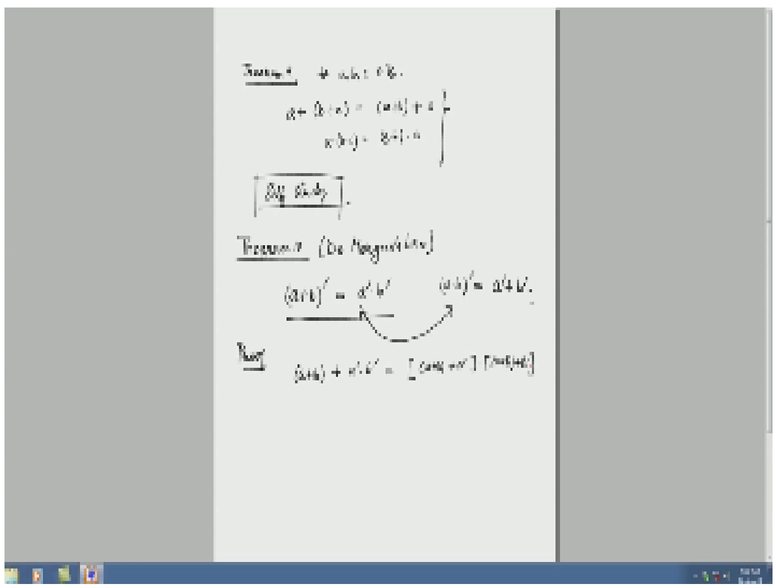
Theorem six for all a belonging to be the complement of a is unique proof now we will suppose that there are two distinct complements suppose, suppose a subscript one and a subscript two are two distinct complements of a therefore we have a 1 = 1. a 1 = a + a 2 a 1 which is equal to a. a 1+ a 2 . a 1which is equal to 0 + a 2 . a 1 and then I will replace 0 by I will replace 0 / a . a 2 and here a 2. a 1 and therefore I will have again by using distributive law a 2. a + a 1 and we know that a + a 1 is 1 so a 2.1.

And this is a 2 as we see that we get a 1 = a 2 thus complements are unique and therefore as I said we could have written a different roof for the previous theorem by showing that 1+ 0 is 1 and 1 into 0 is 0 so 0 works as a complement and therefore complement is unique therefore 1 complement is 0 and 0 complement is 1 so that is all so we will now come to another theorem which is called theorem 7 in the series in which we are discussing this is called absorption law.

This states that let a , b belonging to capital B then a + a . b= a and a + a +b is also equal to a we need a proof for that so if we start with a + a .b now we will replace a by a .1+ a .b which is equal to a .1+b now we know that 1+b is one this, this result we have already proved so a .1 so it is equal to a thus we say that a + a .b = a now we use the principle of duality to write a dot a +b is also equal to a that proves now the next theorem that is theorem eight states that for all a belonging to be a compliment of compliment is equal to a now this is called the involution law alright how to prove that.

Now we shall prove that in this way that suppose I take a compliment and then a compliment of compliment this should give me one and a complement dot complement of a compliment should give me zero but we already know that since a complement is the complement of a we have a complement + a =1 and a complement dot a =0 but we have already proved that complements are unique therefore I will have a = a complement of compliment theorem 9 now theorem 9 is the associative law says that for all abc belonging to b a +b+ c=a + b+c and a .b .c = a .b .c.

(Refer Slide Time: 55:59)



Now I will leave this proof for self-study this is a result that we all expect to happen but as a word of caution this does not happen in all the algebraic systems there are of course algebraic systems which are non associative but Boolean algebra is not an algebraic system like that it needs a proof though from the basic axioms.

But as I have said I leave it as self-study and move on to probably the most important result of today's lecture that is the last one that is the last theorem in this series of theorems and this is called de Morgan's law de Morgan's law states that a +b complement gives me a complement dot B complement and a dot B complement gives me a complement plus B complement now please see that again the principle of duality holds here I can arrive from this relation to this relation by interchanging plus and dot.

And well 1and 0 does not occur so we do not have to do anything now how to prove this one for this we will just prove that a +b is the complement of a complement dot B complement therefore we have this proof that we take a +b and consider a complement dot B complement and this is equal to by our distributive law a + b +a complement. a +b + b complement now I can use the -