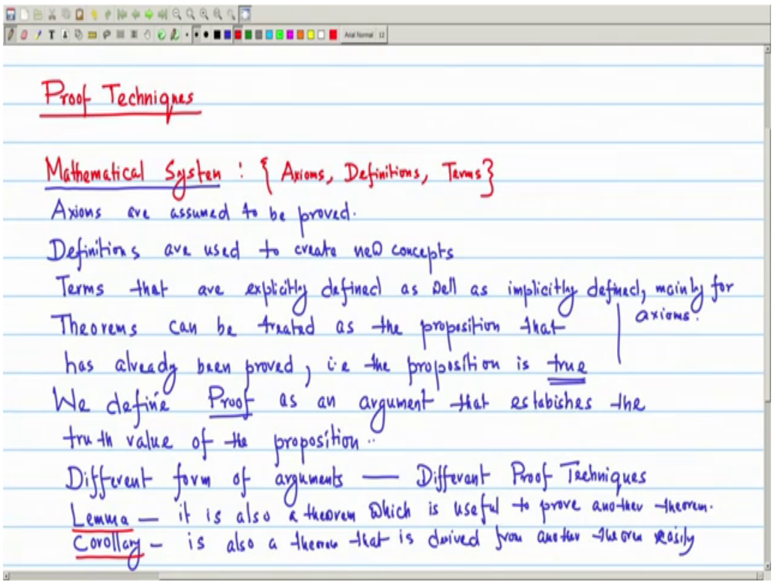
Discrete Structures
Prof. Dipanwita Roychoudhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 11
Proof Techniques

Today, we will read the different Proof Techniques. So, first we see that what do we mean by proofs and what to proof?

(Refer Slide Time: 00:41)



First we introduce a mathematical system. A mathematical system consists of axioms, then definitions some a number of terms that can be predefined or some terms are newly defined. Now, we know that axioms; so, first we write the mathematical systems you can write that it is a set of axioms then some definitions and a number of terms.

Now, these axioms we can think that that are it is assumed that they are already proved some statements or we can tell some theorems that are already proved. Axioms are assumed which is which are already alright or we can write directly or assume to be proved. And, definitions are used to create new concepts and terms that are explicitly defined as well as can be implicitly defined for mainly for axioms. So, we define a mathematical system mainly by these three parameters.

Now, we can think the theorems that can be treated as a proposition which has already been proved or some we have to prove that proposition. So, we define or that theorems can be treated as the propositions. Since, now we know the proposition we have read in logic. So, as if theorems we are thinking as a proposition which is that has already been proved or we have to prove or the; now proposition is to be proved means the truth value or we can tell that the proposition is true that is the proposition I have to show that proposition is true; that means, the truth value of the proposition is true.

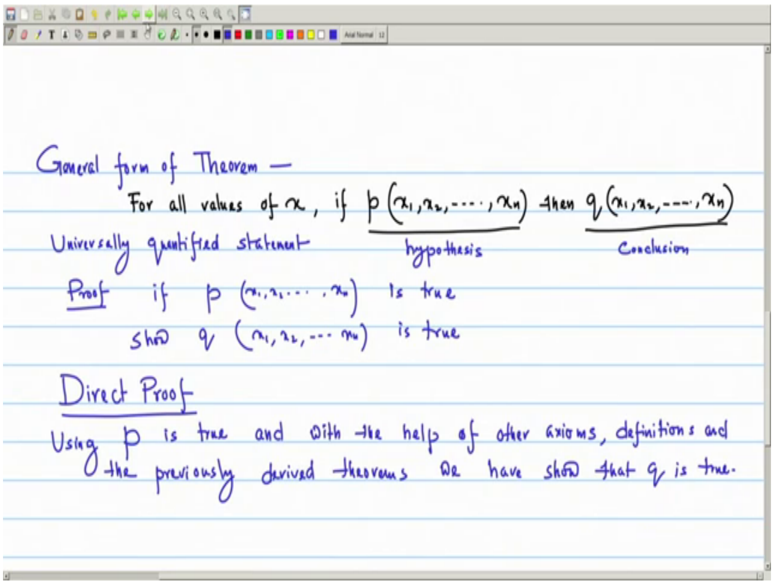
Now, an argument that establishes the fact that this proposition is true is a proof. So, we define the proof we define proof as an argument that establishes the truth value of the proposition. Now, this argument that can be defined or that can be presented in different way and that we call that there is this different way of establishing or the different way of arguments these are called the different proof techniques. So, different arguments or different form of arguments mainly at the different proof techniques.

Now, already from our previous knowledge we have we know the thumps, lemmas or corollary associated with theorem. So, lemma and corollaries these are again we can treat that as the different form of theorems. We know that lemma mainly this is also a theorem it is also a theorem which is not very important to prove, but is very useful to proof another theorem. It is also a theorem which is useful to prove another theorem.

And, we can tell corollary; corollary is another theorem. It is also is also a theorem that derives or it is derived from another theorem very easily which is derived from another theorem easily. So, in these basic definitions of a mathematical system that mainly in a mathematical system that we will define the different type different terms and then using those terms or definitions will state some theorems or some statements.

Since, now the theorem means it is nothing, but a propositions to be proved and then we will see how we can prove that statements or how we can show that the proposition the truth value of the proposition is true. So, before we give the different proof techniques first we see how the theorem can be treated as a proposition.

(Refer Slide Time: 11:58)

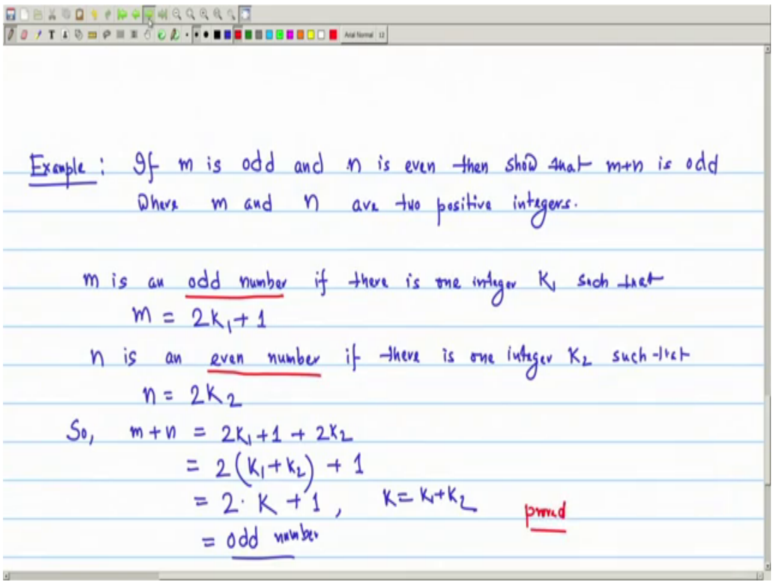


So, the general form of theorem; so, I can write that for all terms right so, for all values of x, if p x 1, x 2, x n then q x 1, x 2, x n so, this is some universally quantified statement. So, the general form of theorem is a nothing, but a universally quantified statement. Now, this is my hypothesis; this is my hypothesis and this is my conclusion.

So, given this proposition that if p is true what is the proof? What we have to prove? That if p is true; that means, all x 1, x 2, x n which are in the domain of discourse g if p is true we have to show that q is true. So, we represent the theorem like a proposition. Since now we know we have read the logic and we know that what is proposition and what are the true values of the proposition or what are the different logic rules or the laws of inference or different other rules we can apply to derive or to show that some conclusion to be true or false.

So, we have to we now we read that how we can do the proof? So, first we see that a direct proof is very simple always we use. So, the name is it is name is direct proof. So, director proof we as if p is true; that means, the hypothesis we assume p is true or better I write using is true since you are already it is given. So, using p is true and with the help of other axioms, definitions and the previously derived theorems; and the previously, we have to show that q is q is true, the conclusion is true. So, this is mainly the direct proof. So, we see one example of the direct proof.

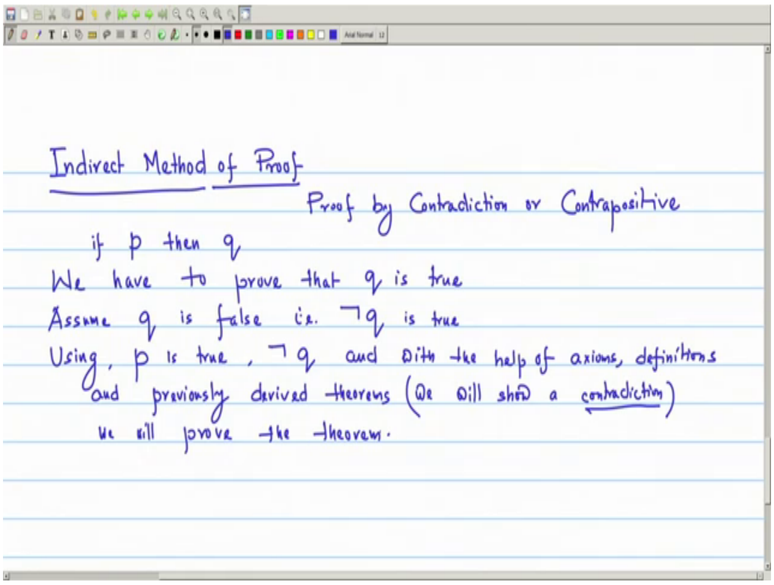
(Refer Slide Time: 17:22)



We give the statement that if m is odd and n is even, then show that m plus n is odd, where m and n are two positive integers. Now, what definition is required? All of you know the what is odd and what is even, but it has some proper definition. So, what is an odd number? We know that m is an odd number if there is one integer K 1 such that m equal to 2K 1 plus 1. Similarly, I can define an even number. So, n is an even number, if there is one integer say K 2 such that n equal to 2K 2. So, these are the two definitions prior definitions or these are our previous knowledge that we need to prove this statement of the prove this theorem.

So, what is then m and n? Since given m is odd and n is even; so, m plus n in terms of K 1 and K 2 we can write 2K 1 plus 1 plus 2K 2 is 2K 1 plus K 2 plus 1. So, K 1 plus K 2 that I can write a K and integer well K equal to K 1 plus K 2. So, this is of the form of odd because we have defined m equal to 2K 1 plus 1; that means, for integer m plus n there is one integer K equal to K 1 plus K 2 such that m plus n equal to 2K plus 1. So, this is some odd number. This is one odd number. So, it is proved. So, the theorem is proved. So, this is one direct method of profit proving the statements. Then, immediately we have to think that if there is a direct method then there must be one indirect method. So, what is that indirect method?

(Refer Slide Time: 22:00)



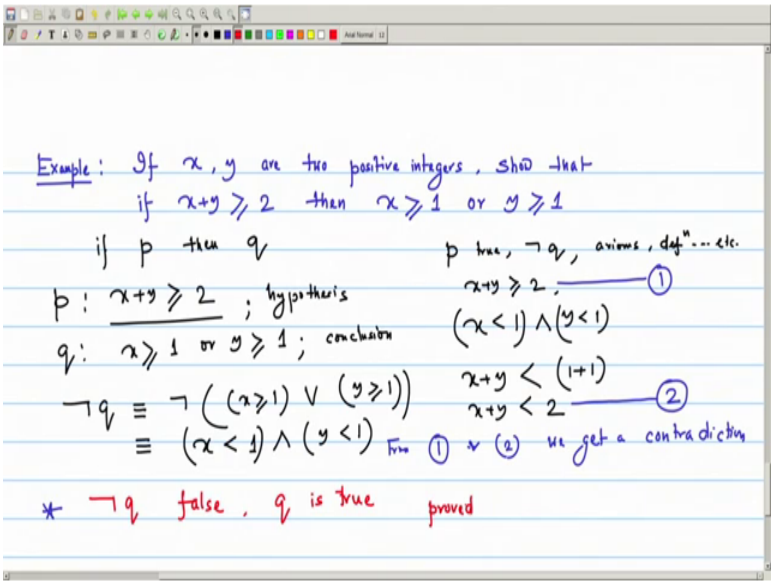
So, indirect method normally is some proof we do by the method of contradiction; that contradiction we have ready a study of logic. So, mainly the proof by; proof by contradiction or a special case of contradiction is called the contrapositive is the method of proof by indirect way; that means, indirect method of proof.

Now, we define this technique. So, our theorem now we know that if p, then q this is the proposition that we want to prove. Now here we assume that because we have to prove that q is true. I write we have to prove that q is true so, we assume q is false; that means, negation q is true.

So, using p; that means, p is true, negation q and with the help of axioms, definitions, and previously derived theorems we will show a contradiction. What is contradiction? We have to show q is true, but we assume negation q is true. So, we will show a contradiction and we will prove the theorem.

So, the difference from the direct method is that in the direct method greatly we have taken that the hypothesis is true and from there only under with the definitions or previously derived theorems, like the previous example we have taken the definition of odd numbers and even numbers. In addition here in proof of contradiction we assume that the our conclusion is false and from there we will derive that thing.

(Refer Slide Time: 26:21)



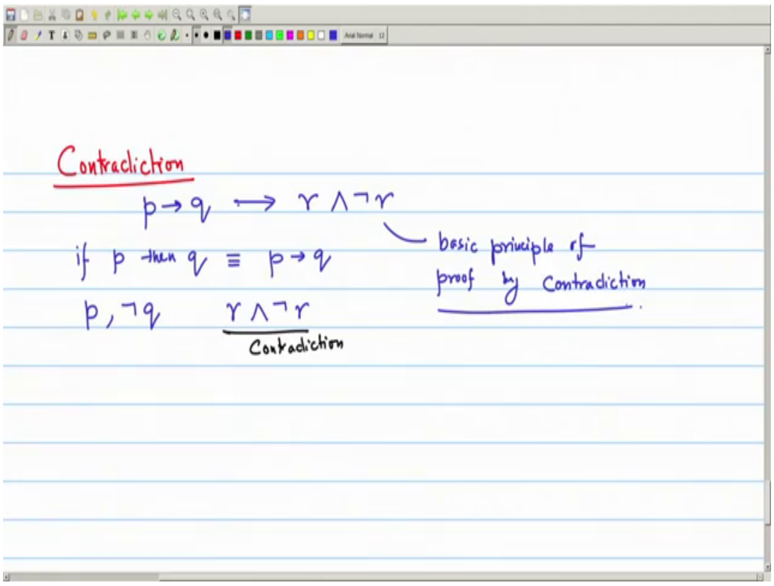
We take one example. See for if x, y or two positive integers, if x plus y greater than equal to 2 then x greater than equal to 1 or y greater than equal to 1. Now, here or if p then q, so, x plus y greater than equal to 2, this is my hypothesis p, this is my hypothesis q my conclusion is x greater than equal to 1 or y greater than equal to 1. So, this is my conclusion.

So, for contradiction or indirect proof we assume negation q. So, it is negation q; negation q is negation which is equivalent to negation, x greater than equal to 1 or y greater than equal to 1. So, with logical symbols you can write then we apply De Morgan's law. So, this becomes negation x greater than equal to 1 means x less than 1 or becomes and y less than 1.

Now, we know that we have p is true; that means, because we have to use p true, then negation q and the definitions or the previous knowledge and the previously derived theorems, axioms, definitions etcetera. P is true means that x plus y greater than equal to 2 and negation p negation q means just now, we got that x less than 1 and y less than; y less than 1. So, what is x plus y? X less than 1 and y 2 less than 1 so, x plus y less than 1 plus 1; that means, x plus y less than 2.

Now, see that p is true. So, my hypothesis was; hypothesis was that x plus y greater than 2, this was my hypothesis. Now, we got from negation q we got x plus y less than 2 so, this is the contradiction. So, we get or 1 and 2 from 1 and 2 we get a contradiction. So, that means, what we assumed that negation q true, we assume that negation q true the is false, that negation q actually this is false. So, q is true and it is the theorem is proved.

(Refer Slide Time: 32:00)



So, we can define the contradiction in this way that and if p implies q if p then q; that means, p implies q this is my proposition p p implies q that implies p implies q implies r and negation r. So, our theorem to be proved is if p then q which is if p then q which is p implies q.

Now, p implies q from there we take p true and negation q and if that implies one contradiction; that means, some proposition r and negation r, then this is; this is a contradiction, this is a contradiction. So, this is if we get p implies q implies r and negation r that mean contradiction then this is actually the basic principle of this is my basic principle of the proof by; proof by contradiction, this is proof by contradiction.

So, we see in this lecture we have read the very basic techniques of proof or very basic proof techniques is direct method and the indirect method. And, mainly how the theorems are represented as a proposition and then how they can be proved or the truth value of the conclusion can be made if the theorem is represented as a proposition.