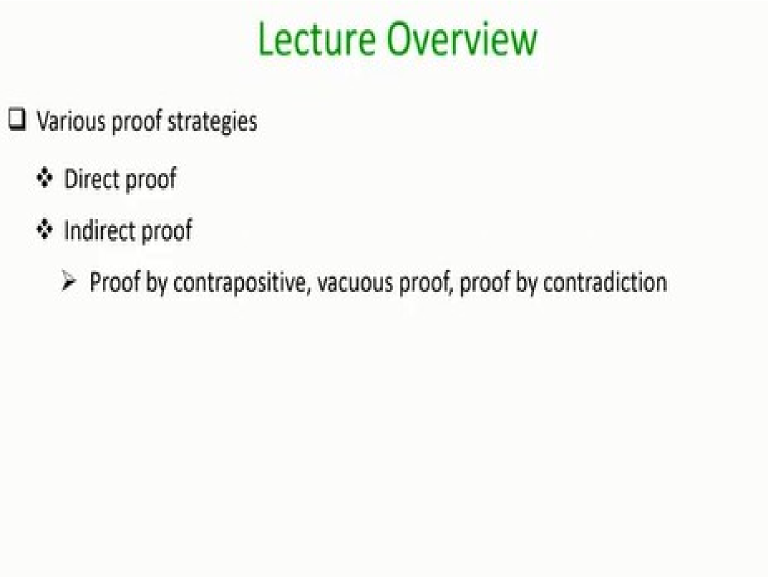
Discrete Mathematics

Prof. Ashish Choudhury
Department of Mathematics and Statistics
International Institute of Information Technology, Bangalore

Lecture -10
Proof Strategies-I

Hello everyone, welcome to the first part of proof strategies.

(Refer Slide Time: 00:24)

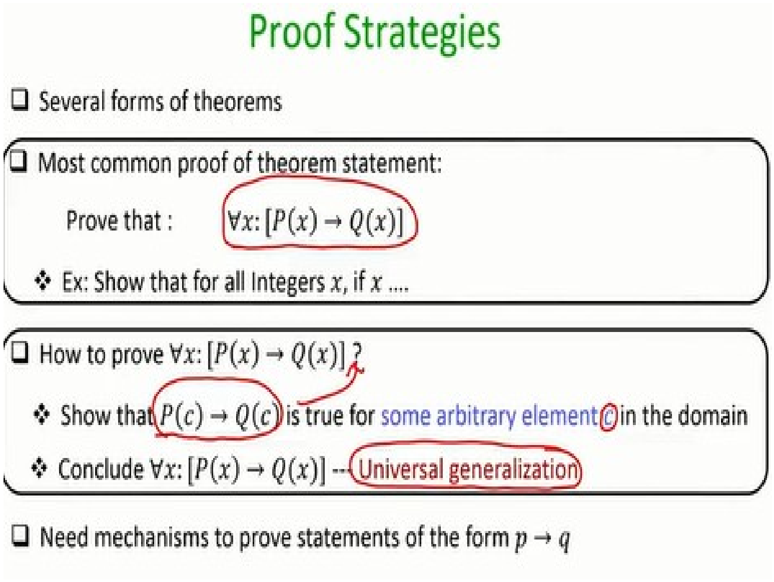


Lecture Overview

- ❑ Various proof strategies
  - ❖ Direct proof
  - ❖ Indirect proof
    - ➢ Proof by contrapositive, vacuous proof, proof by contradiction

The plan for this lecture is as follows we will introduce various proof strategies that we will be encountering in this course namely direct proofs and we will see some forms of indirect proof namely the proof by contrapositive, vacuous proof and proof by contradiction.

(Refer Slide Time: 00:41)



Proof Strategies

❑ Several forms of theorems

❑ Most common proof of theorem statement:

Prove that : $\forall x: [P(x) \rightarrow Q(x)]$

❖ Ex: Show that for all Integers x, if x ....

❑ How to prove $\forall x: [P(x) \rightarrow Q(x)]$?

❖ Show that $P(c) \rightarrow Q(c)$ is true for some arbitrary element c in the domain

❖ Conclude $\forall x: [P(x) \rightarrow Q(x)]$ -- Universal generalization

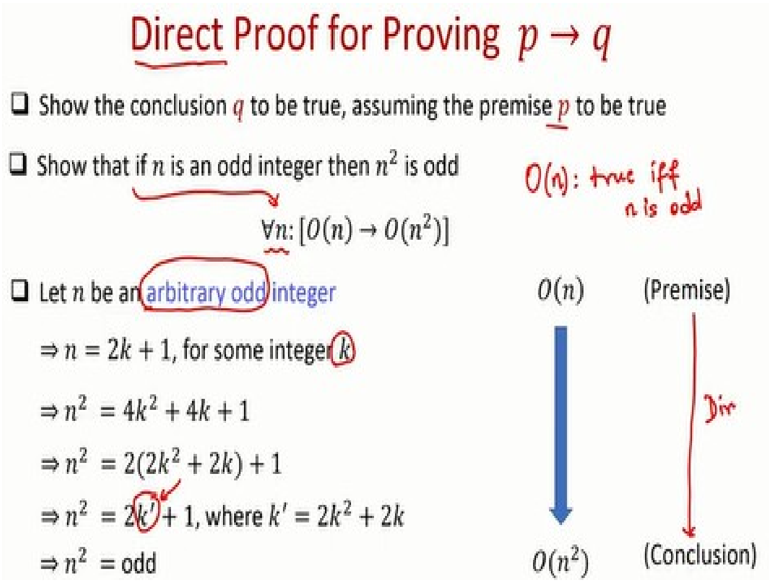
❑ Need mechanisms to prove statements of the form $p \rightarrow q$

So several form of theorems often involved a statement of the form, you have to prove an implication, which is universally quantified, say you have to prove statement of the form that for all integers x, if x satisfies some property then it has this condition or this extra property and so on. So those statements will be represented by this universally quantified implication and unique proof mechanisms to prove universal quantifications of this form.

So, how do we prove a universally quantified implication, we cannot take each and every x value in the domain and check whether P(x) → Q(x) is true or not, if my domain is infinitely large and that is why in the last lecture we saw that you can apply universal generalization to prove universally quantified statement, namely you can pick some arbitrary element c from the domain, where c has no extra property you do not know anything about c it just some arbitrary element and you show that the implication P(c) → Q(c) is true.

If you show that this implication P(c) → Q(c) is true then based on universal generalization, you can conclude that this universally quantified implication is also true. That means now our problem boils down to proving statements of the form a proposition implies another proposition, because P(c) is a proposition Q(c) is also a proposition because we have substituted x with c and we want to prove whether this implication is true or not.

(Refer Slide Time: 02:33)



Direct Proof for Proving $p \to q$

❑ Show the conclusion q to be true, assuming the premise p to be true

❑ Show that if n is an odd integer then n^2 is odd

$\forall n: [O(n) \to O(n^2)]$

❑ Let n be an arbitrary odd integer

$\Rightarrow n = 2k + 1$, for some integer k

$\Rightarrow n^2 = 4k^2 + 4k + 1$

$\Rightarrow n^2 = 2(2k^2 + 2k) + 1$

$\Rightarrow n^2 = 2k' + 1$, where $k' = 2k^2 + 2k$

$\Rightarrow n^2 = \text{odd}$

O(n): true iff
n is odd
O(n)
(Premise)
Dir
O(n²)
(Conclusion)

So now our goal will be to see various proof mechanisms for proving statements of the form p → q where both p and q are propositions. So we will start with the direct proof method as the name suggests it is direct because in this proof method we start assuming that my premise p is true and logically I show that my conclusion also will be true that is why this method is called a direct proof method.

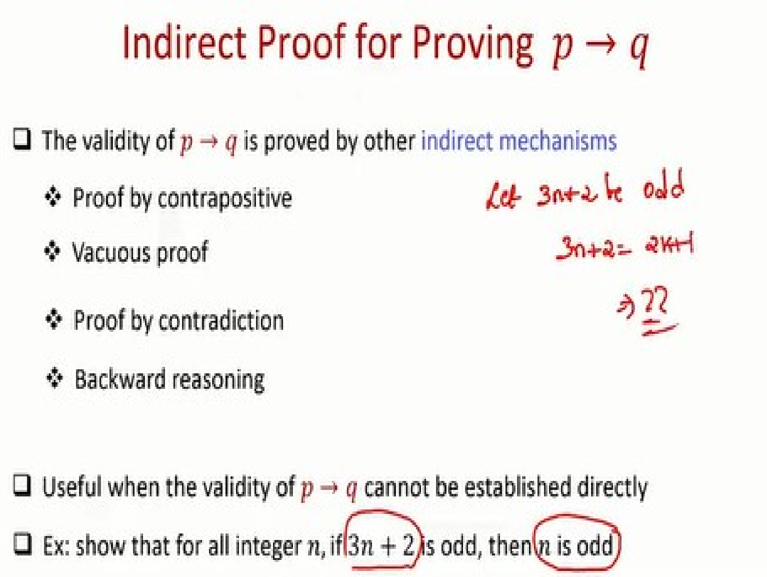
A very simple illustration of this proof method is the following, say I want to prove the statement that if n is an odd integer then n^2 is odd. First thing that you have to understand here is that this statement is about all integers n and even though the word all is not explicitly given here this is a universally quantified statement and say, O(n) is a predicate which is true if and only if n is odd.

So the statement that I want to prove here is the following, $O(n) \to O(n^2)$ is true for every integer n in the domain and I want to use a direct proof method. So, what I do in the direct proof method I assume my premise to be true, so I pick some arbitrary integer n here and assume it is an odd integer. Under that assumption I have to show that the square of the same odd integer is also odd.

So since n is an odd integer. I do not know the exact value of n that is important right because it is an arbitrarily chosen element from my domain but since it is odd, I know that I can write it in the form 2k + 1, where k is also some integer it could be positive it could be negative depending upon what is my n. Now if I take the square of the same n, by rearranging the term, I get n^2 is of this form.

And, now if I substitute ($2k^2 + 2k$) by another integer k’, then I come to the conclusion that n^2 is 2 times some integer plus 1 meaning n square is also odd that means starting with the premise I can directly come to the conclusion that is why this is a direct proof method.

(Refer Slide Time: 04:57)



Indirect Proof for Proving $p \rightarrow q$

❑ The validity of $p \rightarrow q$ is proved by other indirect mechanisms

- ❖ Proof by contrapositive
- ❖ Vacuous proof
- ❖ Proof by contradiction
- ❖ Backward reasoning

Let 3n+2 be odd

$3n+2 = 2k+1$

$\Rightarrow$??

❑ Useful when the validity of $p \rightarrow q$ cannot be established directly

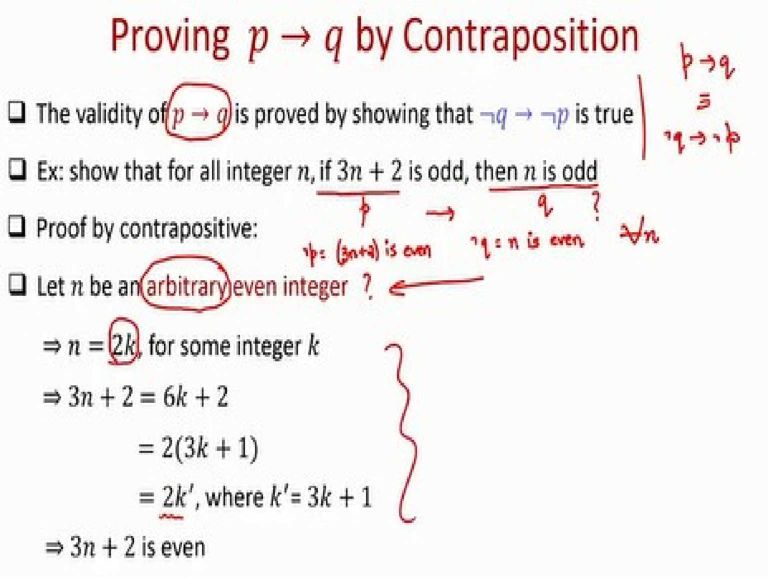
❑ Ex: show that for all integer n, if $3n + 2$ is odd, then n is odd

However, it turns out that it is not always possible to directly prove that p → q is true and for situations like that, we need to have mechanisms which are indirect, we still want to prove p → q but not based on the direct proof method and there are various proof mechanisms under this category of indirect proof. So, we will see each of them and as I said, indirect methods are used where we cannot apply the direct method.

So for instance if I want to prove the statement that for all integers n, if 3n+2 is odd then n is odd then I cannot prove this statement using the direct proof method even though this statement is true, because if I start with the direct proof method I will say let 3n + 2 be odd, where n is arbitrarily chosen then you can say that 3n + 2 since it is odd it is some two times k plus one.

And after that I do not know how to proceed and come to the conclusion that n is also odd my proof might become very complicated.

(Refer Slide Time: 06:11)



Proving $p \to q$ by Contraposition

- □ The validity of $p \to q$ is proved by showing that $\neg q \to \neg p$ is true
- □ Ex: show that for all integer n, if $3n + 2$ is odd, then n is odd
- □ Proof by contrapositive:
- □ Let n be an arbitrary even integer

$\Rightarrow n = 2k$, for some integer k

$\Rightarrow 3n + 2 = 6k + 2$

$= 2(3k + 1)$

$= 2k'$, where $k' = 3k + 1$

$\Rightarrow 3n + 2$ is even

So that is why I need additional methods here which are indirect methods. So let us see the first indirect method which is called proof by contraposition and idea behind proof by contraposition is the following: your goal is to prove the validity or the fact that p → q is true we do that by instead showing that negation of q → negation of p is true and why this is a valid proof method because we know that p → q is logically equivalent to ¬ q → ¬ p that means both p → q as well as ¬ q → ¬ p takes the same truth value.

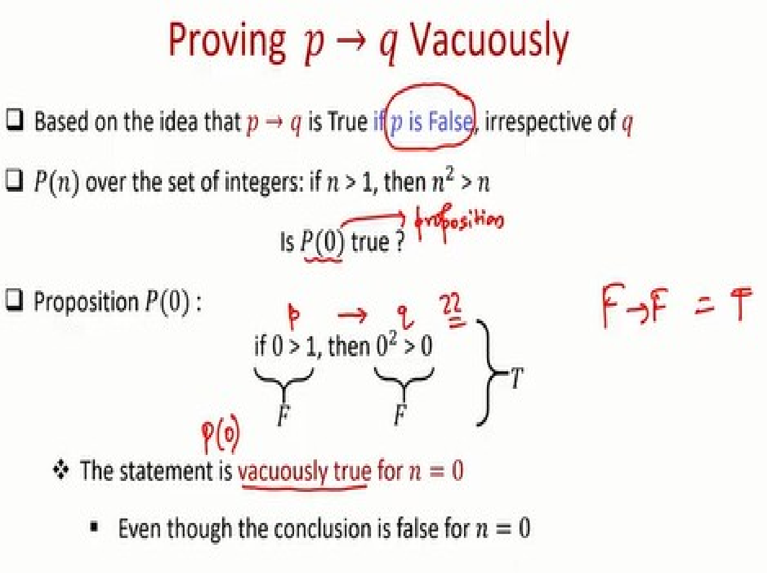
If p → q is F then so is ¬ q → ¬ p, if p → q is true then so is ¬ q → ¬ p. So now let us take the same example which we discuss in the last slide we want to prove that if 3n + 2 is odd then n is odd for every integer n and we want to prove it by contrapositive so what is the p part here the p part here is if 3n + 2 is odd the q part here is n is odd.

That is what you want to prove what will be negation of q, the negation of q will be n is even and what will be negation of p? Negation of p will be 3n + 2 is even. So now our goal will be to verify the implication in the reverse direction. We want to verify that if n is even then can we come to the conclusion that 3n + 2 is also even. If we can prove that then that is equivalent to proving our initial original implication.

So now I assume n is an even integer and it is arbitrary, why arbitrary? Because, we are still applying universal generalization because we are now trying to prove an implication which is universally quantified. So, I cannot take each and every n in the domain and prove this implication that is why I am taking an arbitrary n which is an even number. Since n is arbitrary, but I know it is even I can write it in the form 2k; where k is some integer which could be either positive or negative.

And then it is easy to see that 3n + 2 can also be represented as an integer of the form 2k'; where k' is some integer and hence my implication in the contrapositive direction is correct true and that is why my original implication is also true so now you can see the proof is so convenient.

(Refer Slide Time: 08:54)



Proving $p \rightarrow q$ Vacuously

❑ Based on the idea that $p \rightarrow q$ is True if p is False, irrespective of q

❑ $P(n)$ over the set of integers: if $n > 1$, then $n^2 > n$

Is $P(0)$ true ?

❑ Proposition $P(0)$:

$$\left.\underbrace{\text{if } 0 > 1}_{F}, \text{ then } \underbrace{0^2 > 0}_{F}\right\} T$$

❖ The statement is vacuously true for $n = 0$

- Even though the conclusion is false for $n = 0$

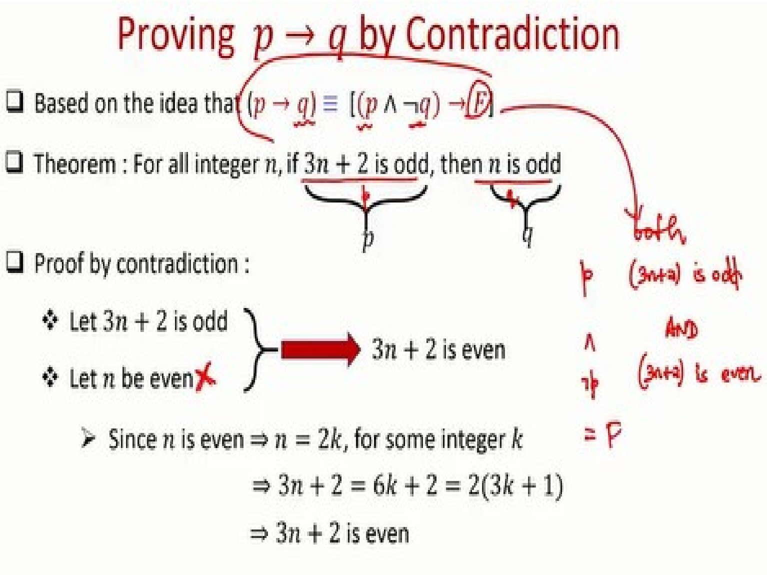
There is another indirect proof method for proving p → q, which is called vacuous proof and this is based on the idea that your implication p → q is always true if p is false irrespective of what is q, q could be true q could be a false it does not matter if your premise p is false then definitely p → q will be true. So for instance imagine P(n) is a predicate which is defined over the set of integers and P(n) represents the statement that if n is greater than 1 then n^2 is greater than n that is the definition of P(n).

Now, we want to check whether P(0) is true or not. So remember P(0) is now a proposition, which is obtained by substituting n equal to 0 in your predicate P(n). What is the proposition

P(0)? The proposition P(0) is, if 0 is greater than 1 then 0 square is greater than 0. So, this is your p part, this is your q part you want to prove p → q is true or not. So, now if you check the p part it is a false proposition because 0 is not greater than 1 then it does not matter what is q whether it is true or false.

In fact in this case q is false, the overall implication is true because F → F is defined to be true that is the truth value of implication that means I can say that the statement P(0) is vacuously true because the premise is false and it does not matter what is the conclusion, even though the conclusion is false, the overall implication is a true statement here. So here I am using a vacuous proof method.

(Refer Slide Time: 10:56)



Proving $p \to q$ by Contradiction

❑ Based on the idea that $(p \to q) \equiv [(p \wedge \neg q) \to \boxed{F}]$

❑ Theorem : For all integer n, if $\underbrace{3n + 2 \text{ is odd}}_{p}$, then $\underbrace{n \text{ is odd}}_{q}$

❑ Proof by contradiction :

- Let $3n + 2$ is odd
- Let n be even

⟹ $3n + 2$ is even

➢ Since n is even $\Rightarrow n = 2k$, for some integer k

$\Rightarrow 3n + 2 = 6k + 2 = 2(3k + 1)$

$\Rightarrow 3n + 2$ is even

We can prove p → q even by contradiction method, which is an indirect proof method for proving p → q and this is based on the idea that p → q is logically equivalent to p conjunction ¬ q → F, you can easily verify that you can draw the truth table of p → q and you can draw the truth table of this RHS expression and both the truth tables are same.

So, the idea here will be that if our goal is to prove that p → q is true then instead of assuming q to be true you assume that negation of q to be true and add it to the premise p and come to the false conclusion. If that is the case, then that is equivalent to showing that indeed q follows from p that is what is the basic essence of this proof method. So for instance if I want to prove this statement that if 3n + 2 is odd then n is odd we had already proved it by proof by contrapositive but let us see a proof by contradiction method.

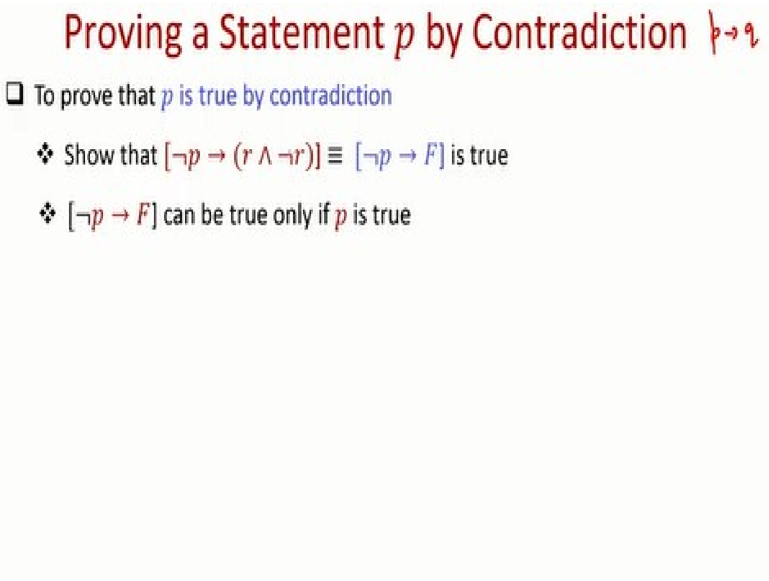
So this part is your p part this part is your q part and the proof by contradiction will proceed as follows. So you are assuming p to be true but you are assuming q to be false and then based on these two statements, you have to come to a false conclusion. If you do that, that means whatever you assumed about q is not correct that is what is the essense of this proof by contradiction method.

So since you are now assuming n to be even that means n is some 2k and since n is arbitrarily chosen because we are proving a universally quantified statement and we have chosen n to be arbitrary because we are applying the universal generalization here. So we do not know the exact value of n except that it is an arbitrarily chosen even integer that is why n will be some 2k and that gives us the conclusion that 3n + 2 is even.

So, now you can see that how do we get a contradiction here? So we started with the premise 3n + 2 to be odd and we assumed n to be even based on these two premises or these two statements, I come to the conclusion that 3n + 2 is even, how can that be possible simultaneously that 3n + 2 is odd as well as 3n + 2 is even that is not possible simultaneously these two things cannot exist simultaneously.

That means the problem due to which this situation has occurred is because you made this incorrect assumption that n is even, that means n has to be odd and that shows that $p \rightarrow q$ is true and this follows this structure. So p was the statement that 3n + 2 is odd to that you added the negation of the conclusion namely n is not even and based on these two things you come to a false statement a false situation that both 3n + 2 is odd and 3n + 2 is even that means both p and $\neg$ p, which is not simultaneously possible that means this is p and this is $\neg$ p which is equal to false, so you come to the false conclusion.

(Refer Slide Time: 14:50)



Proving a Statement p by Contradiction $p \to q$

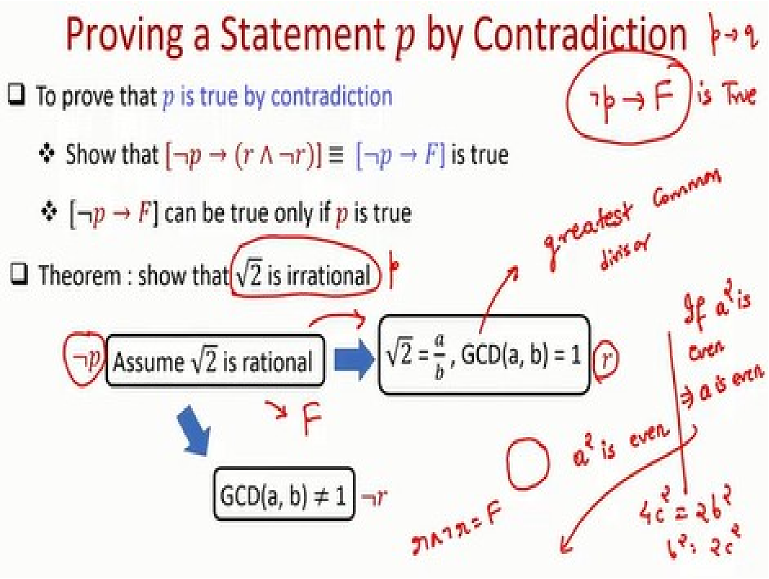
- ❑ To prove that p is true by contradiction
  - ❖ Show that $[\neg p \to (r \wedge \neg r)] \equiv [\neg p \to F]$ is true
  - ❖ $[\neg p \to F]$ can be true only if p is true

It turns out that we can use the proof by contradiction method even to prove that a single proposition p is true, we use proof by contradiction in the previous slide to prove the truth of an implication namely p → q, but you can use the proof by contradiction method even to prove that a statement a single statement p is true, and this is based on the following idea : this is based on the idea that negation of p implies conjunction of r and negation of r is logically equivalent to ¬ p → F that means your goal is to show p is true.

But in this proof method what we do is we instead assume that p is false and if we assume p is false then we have to show that based on that we come to a false conclusion that means we come to a scenario where both r as well as a statement negation of r is true and if that is the case that means if negation of p → F is true, then that can be possible only if p is true, because if negation of p turns out to be true then true → false can never be true.

So the only way negation of p → F can be true is if negation of p is also false and if negation of p is false that means my statement p is true so that is the proof mechanism here. So you start with the negation of whatever you are supposed to prove and from that you should be able to logically show that both a positive statement and the negative statement simultaneously can be derived.

(Refer Slide Time: 16:43)



Proving a Statement p by Contradiction

- To prove that p is true by contradiction
  - Show that $[\neg p \rightarrow (r \wedge \neg r)] \equiv [\neg p \rightarrow F]$ is true
  - $[\neg p \rightarrow F]$ can be true only if p is true
- Theorem : show that $\sqrt{2}$ is irrational

Assume $\sqrt{2}$ is rational

$\sqrt{2} = \frac{a}{b}$, GCD(a, b) = 1

GCD(a, b) ≠ 1

So let us see how this proof method is applicable to prove that √2 is irrational, so what I do here: is this is the statement p that I want to prove, my proposition p which I want to prove here is that √2 is irrational, I assume a negation of that, that means on contrary I assume that the √2 is rational that means I am now assuming negation p is true and based on that I have to come to a false conclusion; that means from negation p I have to come to a false statement, which will show that p is actually true.

Now since I am assuming √2 to be rational that means I can express it in the form a/b some integer a over some integer b where the greatest common divisor of (a,b) = 1 that is a definition of a rational number and say this statement is r that means from negation of p I have derived the statement r, I will show that from the same statement negation p I will derive the conclusion negation of r which will establish that negation p is not possible.

So let us see how we can derive negation of r as well from negation of p. So, since √2 is of the form a over b by taking square on both sides I get a square equal to $2b^2$ and now if a^2 is equal to $2b^2$, so a^2 is equal to $2b^2$ means a^2 is even, because it is two times some integer b^2 then if a^2 is even I can prove that a is also even. So I am not separately proving it you can easily verify this that if a^2 is even, it implies a is even.

You can easily verify that you can prove it by contrapositive you can show that if a is odd then a^2 is also odd. So, I am not separately proving that. So I come to the conclusion that a is even and if a is even then I can write it in the form 2 times some integer c. Now, if a is some 2c then I get that b^2 is also some $2c^2$ because if a is 2c, then a^2 will be $4c^2$.

So $4c^2$ is equal to $2b^2$ that means b^2 is equal to $2c^2$ and now b^2 is $2c^2$ then by applying the same property here that if b^2 is even I can prove that b is also even by applying the same rule here. So say b is even and b is even; that means b is some 2 times an integer d but if a is some 2c and b is some 2d that means what can you say about the G C D of a and b.

The G C D of a and b will be definitely more than 1, in fact 2 divides both a as well as b because both a and b are even that means I can say I can come to the conclusion that G C D of a and b is not 1 and that is the negation of r because r represented the statement that GCD of a and b is 1. Whereas negation of r represents, G C D of a and b is not 1. So you can see that now assuming negation of p namely the statement which I wanted to prove I can logically conclude that √2 is some a over b where GCD of a and b is 1.

And simultaneously, I can conclude that √2 is some a over b where GCD of (a, b) is not 1, which is not going to happen; how can it be possible that both r as well as negation of r holds and r and negation of r means false that means from p you can come to the false conclusion, that means we have shown here that $\neg p \rightarrow F$ is true, if this is true this is possible only if p is true.

So that brings me to the first end of this lecture. In this lecture, we introduced various proof methods, our main motivation is to prove implications because we often encountered universally quantified implications and to prove that, by applying universal generalization we have to prove implications involving propositions. So we have introduced a direct proof method for proving implications.

And, we have seen some indirect proof methods like proof by contrapositive or proof by contradiction and vacuous proof method to indirectly prove whether $p \rightarrow q$ is true or not. Thank you.