Discrete Mathematics

Lecture 10: Proof Technique (Contradiction)

Instructor: Sourav Chakraborty

Proof Techniques

To prove statement $A \implies B$.

There are different proof techniques:

- Constructive Proofs
- Proof by Contradiction
- Proof by Contrapositive
- Induction
- Counter example
- Existential Proof

Which approach to apply

Which approach to apply

- It depends on the problem.

Which approach to apply

- It depends on the problem.
- Sometimes the problem can be split into smaller problems that can be easier to tackle individually.

Which approach to apply

- It depends on the problem.
- Sometimes the problem can be split into smaller problems that can be easier to tackle individually.
- Sometimes viewing the problem is a different way can also help in tackling the problem easily.

Which approach to apply

- It depends on the problem.
- Sometimes the problem can be split into smaller problems that can be easier to tackle individually.
- Sometimes viewing the problem is a different way can also help in tackling the problem easily.
- Whether to split a problem or how to split a problem or how to look at a problem is an ART that has to be developed.

Which approach to apply

- It depends on the problem.
- Sometimes the problem can be split into smaller problems that can be easier to tackle individually.
- Sometimes viewing the problem is a different way can also help in tackling the problem easily.
- Whether to split a problem or how to split a problem or how to look at a problem is an ART that has to be developed.
- There are some thumb rules but at the end it is a skill you develop using a lot of practice.

Splitting into smaller problem

- If the problem is to prove $A \implies B$ and B can be written as $B = C \wedge D$ then note that

$$(A \implies B) \equiv (A \implies C \wedge D) \equiv (A \implies C) \wedge (A \implies D).$$

Redundant Assumptions

Redundant Assumptions

- There can be assumption that are not necessary.

Redundant Assumptions

- There can be assumption that are not necessary.
- We can throw them.

Redundant Assumptions

- There can be assumption that are not necessary.
- We can throw them.
- If $A \implies B$ then $A \wedge C$ also implies B.

Redundant Assumptions

- There can be assumption that are not necessary.
- We can throw them.
- If $A \implies B$ then $A \wedge C$ also implies B.

$$(A \implies B) \implies (A \wedge C \implies B) = True$$

Redundant Assumptions

- There can be assumption that are not necessary.
- We can throw them.
- If $A \implies B$ then $A \wedge C$ also implies B.

$$(A \implies B) \implies (A \wedge C \implies B) = True$$

- Which assumption are not needed is something to guess using your intelligence.

Sometimes proving something stronger is easier

If we have to prove $A \implies B$

Sometimes proving something stronger is easier

If we have to prove $A \implies B$

- If $C \implies B$ then

$$(A \implies C) \implies (A \implies B).$$

Sometimes proving something stronger is easier

If we have to prove $A \implies B$

- If $C \implies B$ then

$$(A \implies C) \implies (A \implies B).$$

Constructive Proof

To prove $A \implies B$.

There are two techniques:

Constructive Proof

To prove $A \implies B$.

There are two techniques:

- Direct Proof: You directly proof $A \implies B$.

Constructive Proof

To prove $A \implies B$.

There are two techniques:

- Direct Proof: You directly proof $A \implies B$.
- Case Studies: You split the problem into smaller problems.

Direct proof

- For proving $A \implies B$ we can start with the assumption A and step-by-step prove that B is true.

Direct proof

- For proving $A \implies B$ we can start with the assumption A and step-by-step prove that B is true.
- Sometimes a direct proof (as in the previous example) can be magical and hard to understand how to obtain.

Direct proof

- For proving $A \implies B$ we can start with the assumption A and step-by-step prove that B is true.
- Sometimes a direct proof (as in the previous example) can be magical and hard to understand how to obtain.
- A simpler technique is to have a backward proof.

Direct proof

- For proving $A \implies B$ we can start with the assumption A and step-by-step prove that B is true.
- Sometimes a direct proof (as in the previous example) can be magical and hard to understand how to obtain.
- A simpler technique is to have a backward proof.
- If we have to prove $(A \implies B)$ then the idea is to simplify B.

Direct proof

- For proving $A \implies B$ we can start with the assumption A and step-by-step prove that B is true.
- Sometimes a direct proof (as in the previous example) can be magical and hard to understand how to obtain.
- A simpler technique is to have a backward proof.
- If we have to prove $(A \implies B)$ then the idea is to simplify B.
- And if $C \iff B$ then $(A \implies B) \equiv (A \implies C)$.

Case Studies: Splitting the assumption into cases

Case Studies: Splitting the assumption into cases

- Sometimes the assumption or the premise can be split into different cases. In that case we can split the problem according to cases.

Case Studies: Splitting the assumption into cases

- Sometimes the assumption or the premise can be split into different cases. In that case we can split the problem according to cases.
- If $A = C \vee D$ then

$$(A \implies B) \equiv (C \implies B) \wedge (D \implies B).$$

Proof by Contradiction

- Note that

$$(A \implies B) \equiv (\neg B \wedge A = \text{False})$$

This is called "proof by contradiction"

- To proof $A \implies B$ sometimes its easier to prove that

$$\neg B \wedge A = \text{False}.$$

- A similar statement is

$$(A \implies B) \equiv (\neg B \implies \neg A)$$

This is called "proof by contra-positive"

Proof by Contradiction

Proof by Contradiction

Example: **Prove that earth is not flat.**

Proof by Contradiction

Example: **Prove that earth is not flat.**

Attempt 1:

Proof by Contradiction

Example: **Prove that earth is not flat.**

Attempt 1: If a ship is coming from the horizon we first see the mast (top) of the ship and slowly the complete ship. So the earth must be round hence not flat.

Proof by Contradiction

Example: **Prove that earth is not flat.**

Attempt 1: If a ship is coming from the horizon we first see the mast (top) of the ship and slowly the complete ship. So the earth must be round hence not flat.

Attempt 2:

Proof by Contradiction

Example: **Prove that earth is not flat.**

Attempt 1: If a ship is coming from the horizon we first see the mast (top) of the ship and slowly the complete ship. So the earth must be round hence not flat.

Attempt 2: Lets assume the earth is flat. Then when a ship came from the horizon the whole ship would appear at the same time.

Proof by Contradiction

Example: **Prove that earth is not flat.**

Attempt 1: If a ship is coming from the horizon we first see the mast (top) of the ship and slowly the complete ship. So the earth must be round hence not flat.

Attempt 2: Lets assume the earth is flat. Then when a ship came from the horizon the whole ship would appear at the same time.
But that does not happen - first the mast is seen then the whole ship. So a contradiction.

Proof by Contradiction

Example: **Prove that earth is not flat.**

Attempt 1: If a ship is coming from the horizon we first see the mast (top) of the ship and slowly the complete ship. So the earth must be round hence not flat.

Attempt 2: Lets assume the earth is flat. Then when a ship came from the horizon the whole ship would appear at the same time.
But that does not happen - first the mast is seen then the whole ship. So a contradiction.
Hence initial assumption that earth is flat does not hold.

Infiniteness of Primes

Prove that primes are infinite.

Infiniteness of Primes

Prove that primes are infinite.

That is, $\forall n \in \mathbb{Z}^+ \; \exists x > n \; x$ is a prime.

Proof of Infiniteness of Primes

Let there be finitely many primes : let them be

$$p_1, p_2, \ldots, p_t$$

With p_t being the largest prime

Proof of Infiniteness of Primes

Let there be finitely many primes : let them be

$$p_1, p_2, \ldots, p_t$$

With p_t being the largest prime

Consider the number $(p_1 \times p_2 \times \cdots \times p_t) + 1$

Infiniteness of Primes

Let there be finitely many primes : let them be

$$p_1, p_2, \ldots, p_t$$

With p_t being the largest prime
Consider the number $(p_1 \times p_2 \times \cdots \times p_t) + 1$
If $(p_1 \times p_2 \times \cdots \times p_t) + 1$ is a prime then we get a contradiction as

$$(p_1 \times p_2 \times \cdots \times p_t) + 1 > p_t$$

Infiniteness of Primes

If $(p_1 \times p_2 \times \cdots \times p_t) + 1$ is a prime then we get a contradiction as

$$(p_1 \times p_2 \times \cdots \times p_t) + 1 > p_t$$

Infiniteness of Primes

If $(p_1 \times p_2 \times \cdots \times p_t) + 1$ is a prime then we get a contradiction as

$$(p_1 \times p_2 \times \cdots \times p_t) + 1 > p_t$$

If $(p_1 \times p_2 \times \cdots \times p_t) + 1$ is not a prime then a prime must divide it.

Infiniteness of Primes

If $(p_1 \times p_2 \times \cdots \times p_t) + 1$ is a prime then we get a contradiction as

$$(p_1 \times p_2 \times \cdots \times p_t) + 1 > p_t$$

If $(p_1 \times p_2 \times \cdots \times p_t) + 1$ is not a prime then a prime must divide it.

But all the primes $p_1, p_2, \ldots, p_t$ divides $(p_1 \times p_2 \times \cdots \times p_t)$. So the remainder is 1 when any prime divides $(p_1 \times p_2 \times \cdots \times p_t) + 1$

Infiniteness of Primes

If $(p_1 \times p_2 \times \cdots \times p_t) + 1$ is a prime then we get a contradiction as

$$(p_1 \times p_2 \times \cdots \times p_t) + 1 > p_t$$

If $(p_1 \times p_2 \times \cdots \times p_t) + 1$ is not a prime then a prime must divide it.

But all the primes $p_1, p_2, \ldots, p_t$ divides $(p_1 \times p_2 \times \cdots \times p_t)$. So the remainder is 1 when any prime divides $(p_1 \times p_2 \times \cdots \times p_t) + 1$

So no prime can divide $(p_1 \times p_2 \times \cdots \times p_t) + 1$

Infiniteness of Primes

If $(p_1 \times p_2 \times \cdots \times p_t) + 1$ is a prime then we get a contradiction as

$$(p_1 \times p_2 \times \cdots \times p_t) + 1 > p_t$$

If $(p_1 \times p_2 \times \cdots \times p_t) + 1$ is not a prime then a prime must divide it.

But all the primes $p_1, p_2, \ldots, p_t$ divides $(p_1 \times p_2 \times \cdots \times p_t)$. So the remainder is 1 when any prime divides $(p_1 \times p_2 \times \cdots \times p_t) + 1$

So no prime can divide $(p_1 \times p_2 \times \cdots \times p_t) + 1$
Hence $(p_1 \times p_2 \times \cdots \times p_t) + 1$ is a prime.

Proof of Infiniteness of primes

Let there be finitely many primes : let them be

$$p_1, p_2, \ldots, p_t$$

With p_t being the largest prime

Then we prove that in that case: $(p_1 \times p_2 \times \cdots \times p_t) + 1$ is a prime.

Proof of Infiniteness of primes

Let there be finitely many primes : let them be

$$p_1, p_2, \ldots, p_t$$

With p_t being the largest prime

Then we prove that in that case: $(p_1 \times p_2 \times \cdots \times p_t) + 1$ is a prime.

Hence we have an even larger prime and hence that contradicts that p_t was the largest prime. And so by contradiction we are done.

Related Problems

- Prove that there are infinitely many primes of the form $1 \pmod 4$.

Related Problems

- Prove that there are infinitely many primes of the form $1 \pmod 4$.
- Prove that there are infinitely many primes of the form $3 \pmod 4$.

Related Problems

- Prove that there are infinitely many primes of the form $1 \pmod{4}$.
- Prove that there are infinitely many primes of the form $3 \pmod{4}$.
- Prove that there are infinitely many primes of the form $1 \pmod{6}$.

Related Problems

- Prove that there are infinitely many primes of the form $1 \pmod 4$.
- Prove that there are infinitely many primes of the form $3 \pmod 4$.
- Prove that there are infinitely many primes of the form $1 \pmod 6$.
- Prove that there are infinitely many primes of the form $5 \pmod 6$.

Problem for Next Video ...

- A real number is rational if it can be written as p/q where p and q are two integers.
- For example: $1, 2, 3, 2/3, 49/99$ are rational numbers.

Problem for Next Video ...

- A real number is rational if it can be written as p/q where p and q are two integers.
- For example: $1, 2, 3, 2/3, 49/99$ are rational numbers.

Problem

Prove that $\sqrt{2}$ is not a rational number.