# Discrete Mathematics

## Lecture 13: Proof Technique (Counter Examples)

**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.

# Tricks for solving problems

- (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

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

- (Remove Redundant Assumptions) If $A \implies B$ then $A \wedge C$ also implies $B$.

# Tricks for solving problems

- (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

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

- (Remove Redundant Assumptions) If $A \implies B$ then $A \wedge C$ also implies $B$.

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

# Tricks for solving problems

- (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

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

- (Remove Redundant Assumptions) If $A \implies B$ then $A \wedge C$ also implies $B$.

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

- (Sometimes proving something stronger is easier) If $C \implies B$ then

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

# Constructive Proof: Direct Proof

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

# Constructive 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.

# Constructive 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.

# Constructive 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 $B$.

# Constructive 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 $B$.
- And if $C \iff B$ then $(A \implies B) \equiv (A \implies C)$.

# Constructive Proof: Case Studies

# Constructive Proof: Case Studies

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

# Constructive Proof: Case Studies

- 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

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

  This is called "proof by contradiction"

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

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

- A similar statement is

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

  This is called "proof by contra-positive"

# Contra-positive Proof

- A similar statement is

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

This is called "proof by contra-positive"

## Contra-positive Proof

- A similar statement is

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

  This is called "proof by contra-positive"
- This is particularly useful when $B$ (the deduction) is of the form $C \vee D$

# Contra-positive Proof

- A similar statement is

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

  This is called "proof by contra-positive"
- This is particularly useful when $B$ (the deduction) is of the form $C \vee D$
- In that case

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

## But what if the statement is false

- Let the problem state

**Problem**

*Prove or disprove* $A \implies B$.

# But what if the statement is false

- Let the problem state

**Problem**

*Prove or disprove* $A \implies B$.

- If the statement $A \implies B$ is not true then what to do.

# But what if the statement is false

- Let the problem state

**Problem**

*Prove or disprove* $A \implies B$.

- If the statement $A \implies B$ is not true then what to do.
- A statement is not true is for some setting of the variables (or sub-statements) to true and false the statement is False.

## But what if the statement is false

- Let the problem state

**Problem**

*Prove or disprove* $A \implies B$.

- If the statement $A \implies B$ is not true then what to do.
- A statement is not true is for some setting of the variables (or sub-statements) to true and false the statement is False.
- Prove that $\neg(A \implies B)$ is True for some instance.

# Proof by Counter Example

- To prove that $\neg(A \implies B)$ is True for some instance.

# Proof by Counter Example

- To prove that $\neg(A \implies B)$ is True for some instance.

# Proof by Counter Example

- To prove that $\neg(A \implies B)$ is True for some instance.
- If the problem is actually of the form $\forall x,\ A(x) \implies B(x)$ then the negation of this statement is

$$\exists x,\ A(x) \not\Rightarrow B(x)$$

# Proof by Counter Example

- To prove that $\neg(A \implies B)$ is True for some instance.
- If the problem is actually of the form $\forall x,\ A(x) \implies B(x)$ then the negation of this statement is

$$\exists x,\ A(x) \nRightarrow B(x)$$

- Recall $A \implies B$ is same as $(B \vee \neg A)$. So,

$$\exists x\ A(x) \nRightarrow B(x)\ \equiv \exists x\ \neg(B(x) \vee \neg A(x))\ \equiv\ \exists x(\neg B(x) \wedge A(x))$$

# Proof by Counter Example

- To prove that $\neg(A \implies B)$ is True for some instance.
- If the problem is actually of the form $\forall x,\ A(x) \implies B(x)$ then the negation of this statement is

$$\exists x,\ A(x) \not\Rightarrow B(x)$$

- Recall $A \implies B$ is same as $(B \vee \neg A)$. So,

$$\exists x\ A(x) \not\Rightarrow B(x)\ \equiv \exists x\ \neg(B(x) \vee \neg A(x))\ \equiv\ \exists x(\neg B(x) \wedge A(x))$$

- So to prove that the original statement is not true we have to find an $x$ such that $(\neg B(x) \wedge A(x))$ is true.

# Example 1

**Problem**

*Prove or disprove: for all positive integer $n$, $n^2 - n + 41$ is prime.*

# Example 1

**Problem**

*Prove or disprove: for all positive integer $n$, $n^2 - n + 41$ is prime.*

Let us disprove by counter example:

If this statement is not true and we have to find a positive integer $n$ such that $n^2 - n + 41$ is a not a prime.

# Example 1

**Problem**

*Prove or disprove: for all positive integer $n$, $n^2 - n + 41$ is prime.*

Let us disprove by counter example:

If this statement is not true and we have to find a positive integer $n$ such that $n^2 - n + 41$ is a not a prime.

Let $n = 41$. Then $n^2 - n + 41$ is $41^2$ which is not a prime.

# Example 1

**Problem**

*Prove or disprove: for all positive integer $n$, $n^2 - n + 41$ is prime.*

Let us disprove by counter example:

If this statement is not true and we have to find a positive integer $n$ such that $n^2 - n + 41$ is a not a prime.

Let $n = 41$. Then $n^2 - n + 41$ is $41^2$ which is not a prime.

Thus we disprove the statement by demonstrating a counter example.

# Finding Counter Examples can be hard

**Problem**

*Prove or disprove: for all positive integers* $n$*,* $2^{2^n} + 1$ *is a prime.*

# Finding Counter Examples can be hard

**Problem**

*Prove or disprove: for all positive integers $n$, $2^{2^n}+1$ is a prime.*

- For $n = 0$, $2^{2^n} + 1 = 3$ which is a prime.

# Finding Counter Examples can be hard

**Problem**

*Prove or disprove: for all positive integers $n$, $2^{2^n} + 1$ is a prime.*

- For $n = 0$, $2^{2^n} + 1 = 3$ which is a prime.
- For $n = 1$, $2^{2^n} + 1 = 5$ which is a prime.

# Finding Counter Examples can be hard

**Problem**

*Prove or disprove: for all positive integers $n$, $2^{2^n} + 1$ is a prime.*

- For $n = 0$, $2^{2^n} + 1 = 3$ which is a prime.
- For $n = 1$, $2^{2^n} + 1 = 5$ which is a prime.
- For $n = 2$, $2^{2^n} + 1 = 17$ which is a prime.

# Finding Counter Examples can be hard

**Problem**

*Prove or disprove: for all positive integers $n$, $2^{2^n}+1$ is a prime.*

- For $n = 0$, $2^{2^n} + 1 = 3$ which is a prime.
- For $n = 1$, $2^{2^n} + 1 = 5$ which is a prime.
- For $n = 2$, $2^{2^n} + 1 = 17$ which is a prime.
- For $n = 3$, $2^{2^n} + 1 = 257$ which is a prime.

# Finding Counter Examples can be hard

**Problem**

*Prove or disprove: for all positive integers $n$, $2^{2^n} + 1$ is a prime.*

- For $n = 0$, $2^{2^n} + 1 = 3$ which is a prime.
- For $n = 1$, $2^{2^n} + 1 = 5$ which is a prime.
- For $n = 2$, $2^{2^n} + 1 = 17$ which is a prime.
- For $n = 3$, $2^{2^n} + 1 = 257$ which is a prime.
- For $n = 4$, $2^{2^n} + 1 = 65537$ which is a prime.

# Finding Counter Examples can be hard

**Problem**

*Prove or disprove: for all positive integers $n$, $2^{2^n}+1$ is a prime.*

- For $n = 0$, $2^{2^n} + 1 = 3$ which is a prime.
- For $n = 1$, $2^{2^n} + 1 = 5$ which is a prime.
- For $n = 2$, $2^{2^n} + 1 = 17$ which is a prime.
- For $n = 3$, $2^{2^n} + 1 = 257$ which is a prime.
- For $n = 4$, $2^{2^n} + 1 = 65537$ which is a prime.
- For $n = 5$, $2^{2^n} + 1 = 4294967297$ which is a $641 \times 67700417$.

# Finding Counter Examples can be hard

**Problem**

*Prove or disprove: for all positive integers $n$, $2^{2^n}+1$ is a prime.*

- For $n = 0$, $2^{2^n} + 1 = 3$ which is a prime.
- For $n = 1$, $2^{2^n} + 1 = 5$ which is a prime.
- For $n = 2$, $2^{2^n} + 1 = 17$ which is a prime.
- For $n = 3$, $2^{2^n} + 1 = 257$ which is a prime.
- For $n = 4$, $2^{2^n} + 1 = 65537$ which is a prime.
- For $n = 5$, $2^{2^n} + 1 = 4294967297$ which is a $641 \times 67700417$.

# Thus ....

- Thus to disprove a statement one can do so by giving an instance where the statements fails.

# Thus ....

- Thus to disprove a statement one can do so by giving an instance where the statements fails.

- We call them proof by counter example

# Thus ....

- Thus to disprove a statement one can do so by giving an instance where the statements fails.
- We call them proof by counter example
- Finding a counter example can be very hard and require both ingenuity and sometimes high computational powers.