Discrete Mathematics

Lecture 8: Proof Technique (Case Study)

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

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

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

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

- For example:

Problem

If b is an odd prime then $2b^2 \geq (b+1)^2$ and $b^2 \equiv 1 (mod\ 4)$.

Splitting of Problems in Smaller Problems

Problem

If b is an odd prime then $2b^2 \geq (b+1)^2$ and $b^2 \equiv 1(mod\ 4)$.

Splitting of Problems in Smaller Problems

Problem

If b is an odd prime then $2b^2 \geq (b+1)^2$ *and* $b^2 \equiv 1 (mod\ 4)$.

The above problem is same as proving the following two problems:

Problem (First Part)

If b is an odd prime then $b^2 \equiv 1 (mod\ 4)$.

Problem (Second Part)

If b is an odd prime then $2b^2 \geq (b+1)^2$.

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 $A \land C$ also implies B.

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

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

Splitting of Problems in Smaller Problems

Problem

If b is an odd prime then $2b^2 \geq (b+1)^2$ and $b^2 \equiv 1 (mod\ 4)$.

The above problem is same as proving the following two problems:

Problem (First Part)

If b is an odd prime then $b^2 \equiv 1 (mod\ 4)$.

Problem (Second Part)

If b is an odd prime then $2b^2 \geq (b+1)^2$.

Splitting of Problems in Smaller Problems

Problem

If b is an odd prime then $2b^2 \geq (b+1)^2$ and $b^2 \equiv 1(mod\ 4)$.

The above problem is same as proving the following two problems:

Problem (First Part)

If b is an odd integer then $b^2 \equiv 1(mod\ 4)$.

Problem (Second Part)

If b is a real number ≥ 3 then $2b^2 \geq (b+1)^2$.

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

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

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

- For example:

Problem

If b is a real number and $b \geq 2$ then $2b^3 > 3b + 2$

Sometimes proving something stronger is easier

Problem

If b *is a real number and* $b \geq 2$ *then* $2b^3 \geq 3b + 2$

Sometimes proving something stronger is easier

Problem

If b is a real number and $b \geq 2$ then $2b^3 \geq 3b + 2$

Proof:

Sometimes proving something stronger is easier

Problem

If b is a real number and $b \geq 2$ then $2b^3 \geq 3b + 2$

Proof:

Since $b \geq 2$ so $b^3 \geq b^2$.

Sometimes proving something stronger is easier

Problem

If b is a real number and $b \geq 2$ then $2b^3 \geq 3b + 2$

Proof:

Since $b \geq 2$ so $b^3 \geq b^2$.So,

$2b^3 \geq 3b + 2$ (for $b \geq 2$)

Sometimes proving something stronger is easier

Problem

If b is a real number and $b \geq 2$ then $2b^3 \geq 3b+2$

Proof:
Since $b \geq 2$ so $b^3 \geq b^2$.So,
$2b^3 \geq 3b+2$ (for $b \geq 2$)
$\Leftarrow 2b^2 \geq 3b+2$ (for $b \geq 2$)

Sometimes proving something stronger is easier

Problem

If b is a real number and $b \geq 2$ then $2b^3 \geq 3b + 2$

Proof:

Since $b \geq 2$ so $b^3 \geq b^2$.So,

$2b^3 \geq 3b + 2$ (for $b \geq 2$)

$\Leftarrow 2b^2 \geq 3b + 2$ (for $b \geq 2$)

$\Leftrightarrow b^2 + (b^2 - b) \geq 2b + 2$ (for $b \geq 2$)

Sometimes proving something stronger is easier

Problem

If b is a real number and $b \geq 2$ then $2b^3 \geq 3b + 2$

Proof:

Since $b \geq 2$ so $b^3 \geq b^2$.So,

$2b^3 \geq 3b + 2$ (for $b \geq 2$)

$\Leftarrow 2b^2 \geq 3b + 2$ (for $b \geq 2$)

$\Leftrightarrow b^2 + (b^2 - b) \geq 2b + 2$ (for $b \geq 2$)

$\Leftarrow b^2 + 2 \geq 2b + 2$ (for $b \geq 2$) [Since $(b^2 - b) \geq 2$ for $b \geq 2$]

Sometimes proving something stronger is easier

Problem

If b is a real number and $b \geq 2$ then $2b^3 \geq 3b + 2$

Proof:

Since $b \geq 2$ so $b^3 \geq b^2$.So,

$2b^3 \geq 3b + 2$ (for $b \geq 2$)

$\Leftarrow 2b^2 \geq 3b + 2$ (for $b \geq 2$)

$\Leftrightarrow b^2 + (b^2 - b) \geq 2b + 2$ (for $b \geq 2$)

$\Leftarrow b^2 + 2 \geq 2b + 2$ (for $b \geq 2$) [Since $(b^2 - b) \geq 2$ for $b \geq 2$]

$\Leftrightarrow (b - 1)^2 \geq 1$ (for $b \geq 2$)

Sometimes proving something stronger is easier

Problem

If b is a real number and $b \geq 2$ then $2b^3 \geq 3b + 2$

Proof:

Since $b \geq 2$ so $b^3 \geq b^2$.So,

$2b^3 \geq 3b + 2$ (for $b \geq 2$)

$\Leftarrow 2b^2 \geq 3b + 2$ (for $b \geq 2$)

$\Leftrightarrow b^2 + (b^2 - b) \geq 2b + 2$ (for $b \geq 2$)

$\Leftarrow b^2 + 2 \geq 2b + 2$ (for $b \geq 2$) [Since $(b^2 - b) \geq 2$ for $b \geq 2$]

$\Leftrightarrow (b-1)^2 \geq 1$ (for $b \geq 2$)

And this is true as $(b \geq 2) \implies (b-1) \geq 1$ and hence $(b-1)^2 > 1$.

Techniques so far

To prove $A \implies B$

Techniques so far

To prove $A \implies B$

- If $B = C \wedge D$ then $A \implies B$ is same as $(A \implies C) \wedge (A \implies D)$.

Techniques so far

To prove $A \implies B$

- If $B = C \wedge D$ then $A \implies B$ is same as $(A \implies C) \wedge (A \implies D)$.
- If $B \equiv C$ then $A \implies B$ is same as $A \implies C$

Techniques so far

To prove $A \implies B$

- If $B = C \wedge D$ then $A \implies B$ is same as $(A \implies C) \wedge (A \implies D)$.
- If $B \equiv C$ then $A \implies B$ is same as $A \implies C$
- If $C \implies B$ then to show $A \implies B$ it is enough to show $A \implies C$.

Splitting the assumption into cases

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.

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

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

Example of Splitting the Premise into Cases

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Example of Splitting the Premise into Cases

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Thus we have to prove that for any positive integer a

$$a^2 \not\equiv 2(\text{mod } 4)$$

Proof

If a positive integer a is divided by 4 then the possible remainders are $0, 1, 2$ and 3.

Proof

If a positive integer a is divided by 4 then the possible remainders are $0, 1, 2$ and 3.

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Proof

If a positive integer a is divided by 4 then the possible remainders are $0, 1, 2$ and 3.

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

We will solve in in case by case basis.

Proof

If a positive integer a is divided by 4 then the possible remainders are $0, 1, 2$ and 3.

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

We will solve in in case by case basis.
We split the problem into 4 case depending on the remainder when a is divided by 4.

Proof

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Case 1 The remainder when a is divided by 4 is 0

Case 2 The remainder when a is divided by 4 is 1

Case 3 The remainder when a is divided by 4 is 2

Case 4 The remainder when a is divided by 4 is 3

Proof: Case 1

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Case 1 The remainder when a is divided by 4 is 0

Proof: Case 1

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Case 1 The remainder when a is divided by 4 is 0

- $a = 4r$ for some positive integer r.

Proof: Case 1

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Case 1 The remainder when a is divided by 4 is 0

- $a = 4r$ for some positive integer r.
- So $a^2 = 16r^2$.

Proof: Case 1

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Case 1 The remainder when a is divided by 4 is 0

- $a = 4r$ for some positive integer r.
- So $a^2 = 16r^2$.
- Thus $a^2 - 4b = 16r^2 - 4b = 4(4r^2 - b)$

Proof: Case 1

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Case 1 The remainder when a is divided by 4 is 0

- $a = 4r$ for some positive integer r.
- So $a^2 = 16r^2$.
- Thus $a^2 - 4b = 16r^2 - 4b = 4(4r^2 - b)$
- Since $4r^2 - b$ is an integer and 4 time an integer can never be 2 so $a^2 - 4b$ cannot be equal to 2.

Proof: Case 2

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Case 2 The remainder when a is divided by 4 is 1

Proof: Case 2

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Case 2 The remainder when a is divided by 4 is 1

- $a = 4r + 1$ for some positive integer r.

Proof: Case 2

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Case 2 The remainder when a is divided by 4 is 1

- $a = 4r + 1$ for some positive integer r.
- So $a^2 = 16r^2 + 8r + 1$.

Proof: Case 2

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Case 2 The remainder when a is divided by 4 is 1

- $a = 4r + 1$ for some positive integer r.
- So $a^2 = 16r^2 + 8r + 1$.
- Thus $a^2 - 4b = 16r^2 + 8r + 1 - 4b = 4(4r^2 + 2r - b) + 1$

Proof: Case 2

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Case 2 The remainder when a is divided by 4 is 1

- $a = 4r + 1$ for some positive integer r.
- So $a^2 = 16r^2 + 8r + 1$.
- Thus $a^2 - 4b = 16r^2 + 8r + 1 - 4b = 4(4r^2 + 2r - b) + 1$
- Since $4r^2 + 2r - b$ is an integer and 4 time an integer can never be 1

Proof: Case 2

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Case 2 The remainder when a is divided by 4 is 1

- $a = 4r + 1$ for some positive integer r.
- So $a^2 = 16r^2 + 8r + 1$.
- Thus $a^2 - 4b = 16r^2 + 8r + 1 - 4b = 4(4r^2 + 2r - b) + 1$
- Since $4r^2 + 2r - b$ is an integer and 4 time an integer can never be 1
- so $4(4r^2 + 2r - b) + 1$ cannot be equal to 2

Proof: Case 2

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Case 2 The remainder when a is divided by 4 is 1

- $a = 4r + 1$ for some positive integer r.
- So $a^2 = 16r^2 + 8r + 1$.
- Thus $a^2 - 4b = 16r^2 + 8r + 1 - 4b = 4(4r^2 + 2r - b) + 1$
- Since $4r^2 + 2r - b$ is an integer and 4 time an integer can never be 1
- so $4(4r^2 + 2r - b) + 1$ cannot be equal to 2
- and so $a^2 - 4b$ cannot be equal to 2.

Proof: Case 3

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Case 3 The remainder when a is divided by 4 is 2

Proof: Case 3

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Case 3 The remainder when a is divided by 4 is 2

- $a = 4r + 2$ for some positive integer r.

Proof: Case 3

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Case 3 The remainder when a is divided by 4 is 2

- $a = 4r + 2$ for some positive integer r.
- So $a^2 = 16r^2 + 16r + 4$.

Proof: Case 3

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Case 3 The remainder when a is divided by 4 is 2

- $a = 4r + 2$ for some positive integer r.
- So $a^2 = 16r^2 + 16r + 4$.
- Thus $a^2 - 4b = 16r^2 + 16r + 4 - 4b = 4(4r^2 + 4r + 1 - b)$

Proof: Case 3

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Case 3 The remainder when a is divided by 4 is 2

- $a = 4r + 2$ for some positive integer r.
- So $a^2 = 16r^2 + 16r + 4$.
- Thus $a^2 - 4b = 16r^2 + 16r + 4 - 4b = 4(4r^2 + 4r + 1 - b)$
- Since $4r^2 + 4r + 1 - b$ is an integer and 4 time an integer can never be 2 so $a^2 - 4b$ cannot be equal to 2.

Proof: Case 4

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 3.

Case 4 The remainder when a is divided by 4 is 3

Proof: Case 4

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 3.

Case 4 The remainder when a is divided by 4 is 3

- $a = 4r + 3$ for some positive integer r.

Proof: Case 4

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 3.

Case 4 The remainder when a is divided by 4 is 3

- $a = 4r + 3$ for some positive integer r.
- So $a^2 = 16r^2 + 24r + 9$.

Proof: Case 4

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 3.

Case 4 The remainder when a is divided by 4 is 3

- $a = 4r + 3$ for some positive integer r.
- So $a^2 = 16r^2 + 24r + 9$.
- Thus $a^2 - 4b = 16r^2 + 24r + 9 - 4b = 4(4r^2 + 6r + 2 - b) + 1$

Proof: Case 4

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 3.

Case 4 The remainder when a is divided by 4 is 3

- $a = 4r + 3$ for some positive integer r.
- So $a^2 = 16r^2 + 24r + 9$.
- Thus $a^2 - 4b = 16r^2 + 24r + 9 - 4b = 4(4r^2 + 6r + 2 - b) + 1$
- Since $4r^2 + 6r + 2 - b$ is an integer and 4 time an integer can never be 2 so $a^2 - 4b$ cannot be equal to 1.
- so $4(4r^2 + 6r + 2 - b) + 1$ cannot be equal to 2

Proof: Case 4

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 3.

Case 4 The remainder when a is divided by 4 is 3

- $a = 4r + 3$ for some positive integer r.
- So $a^2 = 16r^2 + 24r + 9$.
- Thus $a^2 - 4b = 16r^2 + 24r + 9 - 4b = 4(4r^2 + 6r + 2 - b) + 1$
- Since $4r^2 + 6r + 2 - b$ is an integer and 4 time an integer can never be 2 so $a^2 - 4b$ cannot be equal to 1.
- so $4(4r^2 + 6r + 2 - b) + 1$ cannot be equal to 2
- and so $a^2 - 4b$ cannot be equal to 2.

Complete Proof

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Complete Proof

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

If a positive integer a is divided by 4 then the possible remainders are $0, 1, 2$ and 3.

Complete Proof

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

If a positive integer a is divided by 4 then the possible remainders are $0, 1, 2$ and 3.

We will solve in a case by case basis.

Complete Proof

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

If a positive integer a is divided by 4 then the possible remainders are $0, 1, 2$ and 3.

We will solve in a case by case basis.

We split the problem into 4 case depending on the remainder when a is divided by 4 and show that for every case $a^2 - 4b$ cannot be equal to 2.