Discrete Mathematics

Lecture 7: Proof Technique (Direct Proof)

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 $A \wedge C$ 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.

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: Example 1

Problem

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

Direct Proof: Example 1

Problem

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

Since n is odd. So $N = 2k + 1$ for some integer k.

Direct Proof: Example 1

Problem

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

Since n is odd. So $N = 2k + 1$ for some integer k.
So $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$.

Direct Proof: Example 1

Problem

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

Since n is odd. So $N = 2k + 1$ for some integer k.
So $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$.
So $(n^2 - 1) = 4(k^2 + k)$.

Direct Proof: Example 1

Problem

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

Since n is odd. So $N = 2k + 1$ for some integer k.
So $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$.
So $(n^2 - 1) = 4(k^2 + k)$.
Since k is an integer so $k^2 + k$ is also an integer and hence $4 \mid n^2 - 1$.

Direct Proof: Example 1

Problem

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

Since n is odd. So $N = 2k + 1$ for some integer k.
So $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$.
So $(n^2 - 1) = 4(k^2 + k)$.
Since k is an integer so $k^2 + k$ is also an integer and hence $4 \mid n^2 - 1$.
Hence $n^2 \equiv 1 (\mathrm{mod}\ 4)$.

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

First Proof:

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

First Proof:

Since $b \geq 3$ so $(b-1) \geq 2$ and hence $(b-1)^2 \geq 4$.

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

First Proof:

Since $b \geq 3$ so $(b-1) \geq 2$ and hence $(b-1)^2 \geq 4$.
Thus $(b-1)^2 > 2$.

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

First Proof:

Since $b \geq 3$ so $(b-1) \geq 2$ and hence $(b-1)^2 \geq 4$.
Thus $(b-1)^2 > 2$.
So $b^2 - 2b + 1 > 2$.

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

First Proof:

Since $b \geq 3$ so $(b-1) \geq 2$ and hence $(b-1)^2 \geq 4$.
Thus $(b-1)^2 > 2$.
So $b^2 - 2b + 1 > 2$.
Hence $b^2 > 2b + 1$.

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

First Proof:

Since $b \geq 3$ so $(b-1) \geq 2$ and hence $(b-1)^2 \geq 4$.
Thus $(b-1)^2 > 2$.
So $b^2 - 2b + 1 > 2$.
Hence $b^2 > 2b + 1$.
Adding b^2 to both sides we get $2b^2 > b^2 + 2b + 1 = (b+1)^2$.

A simple approach to obtain a proof

- Sometimes a direct proof (as in the previous example) can be magical and hard to understand how to obtain.

A simple approach to obtain a proof

- 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 back ward proof.

A simple approach to obtain a proof

- 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 back ward proof.
- If we have to prove $(A \implies B)$ then the idea is to simplify B.

A simple approach to obtain a proof

- 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 back ward proof.
- If we have to prove $(A \implies B)$ then the idea is to simplify B.
- And if $C \iff B$ then $(A \implies B) \equiv (A \implies C)$.

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

Second Proof (Backward Proof):

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

Second Proof (Backward Proof):

To prove: $2b^2 > (b+1)^2$ for $b \geq 3$

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

Second Proof (Backward Proof):

To prove: $2b^2 > (b+1)^2$ for $b \geq 3$

$\iff 2b^2 > b^2 + 2b + 1$ for $b \geq 3$

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

Second Proof (Backward Proof):

To prove: $2b^2 > (b+1)^2$ for $b \geq 3$

$\iff 2b^2 > b^2 + 2b + 1$ for $b \geq 3$

$\iff b^2 - 2b - 1 > 0$ for $b \geq 3$

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

Second Proof (Backward Proof):

To prove: $2b^2 > (b+1)^2$ for $b \geq 3$

$\iff 2b^2 > b^2 + 2b + 1$ for $b \geq 3$

$\iff b^2 - 2b - 1 > 0$ for $b \geq 3$

$\iff (b-1)^2 - 2 > 0$ for $b \geq 3$

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

Second Proof (Backward Proof):

To prove: $2b^2 > (b+1)^2$ for $b \geq 3$

$\iff 2b^2 > b^2 + 2b + 1$ for $b \geq 3$

$\iff b^2 - 2b - 1 > 0$ for $b \geq 3$

$\iff (b-1)^2 - 2 > 0$ for $b \geq 3$

$\iff (b-1)^2 > 2$ for $b \geq 3$

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

Second Proof (Backward Proof):

To prove: $2b^2 > (b+1)^2$ for $b \geq 3$

$\iff 2b^2 > b^2 + 2b + 1$ for $b \geq 3$

$\iff b^2 - 2b - 1 > 0$ for $b \geq 3$

$\iff (b-1)^2 - 2 > 0$ for $b \geq 3$

$\iff (b-1)^2 > 2$ for $b \geq 3$

And this is true because $b \geq 3 \implies (b-1) \geq 2$

$\implies (b-1)^2 \geq 4 > 2$.

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