Discrete Mathematics

Lecture 6: Mathematical Proofs

Instructor: Sourav Chakraborty

Mathematical Proofs

How to check if a statement is correct?

Mathematical Proofs

How to check if a statement is correct?

For example:
For all n the integer $n^2 - n + 41$ is a prime.

Proof

Proof

One can prove the statement either

Proof

One can prove the statement either

- Empirically or experimentally: Try the statement for a number of cases and if the statement holds we would say the statement is correct.

Proof

One can prove the statement either

- Empirically or experimentally: Try the statement for a number of cases and if the statement holds we would say the statement is correct.
- Mathematically: Use mathematical reasoning to prove the statement.

Empirical Proof

For all n the integer $n^2 - n + 41$ is a prime.

Empirical Proof

For all n the integer $n^2 - n + 41$ is a prime.

Empirical Proof:

Empirical Proof

For all n the integer $n^2 - n + 41$ is a prime.

Empirical Proof:
For $n = 1$, we have $n^2 - n + 41 = 41$, which is a prime.

Empirical Proof

For all n the integer $n^2 - n + 41$ is a prime.

Empirical Proof:
For $n = 1$, we have $n^2 - n + 41 = 41$, which is a prime.
For $n = 2$, we have $n^2 - n + 41 = 43$, which is a prime.

Empirical Proof

For all n the integer $n^2 - n + 41$ is a prime.

Empirical Proof:
For $n = 1$, we have $n^2 - n + 41 = 41$, which is a prime.
For $n = 2$, we have $n^2 - n + 41 = 43$, which is a prime.
For $n = 3$, we have $n^2 - n + 41 = 47$, which is a prime.

Empirical Proof

For all n the integer $n^2 - n + 41$ is a prime.

Empirical Proof:
For $n = 1$, we have $n^2 - n + 41 = 41$, which is a prime.
For $n = 2$, we have $n^2 - n + 41 = 43$, which is a prime.
For $n = 3$, we have $n^2 - n + 41 = 47$, which is a prime.
For $n = 4$, we have $n^2 - n + 41 = 53$, which is a prime.

Empirical Proof

For all n the integer $n^2 - n + 41$ is a prime.

Empirical Proof:
For $n = 1$, we have $n^2 - n + 41 = 41$, which is a prime.
For $n = 2$, we have $n^2 - n + 41 = 43$, which is a prime.
For $n = 3$, we have $n^2 - n + 41 = 47$, which is a prime.
For $n = 4$, we have $n^2 - n + 41 = 53$, which is a prime.
....

Empirical Proof

For all n the integer $n^2 - n + 41$ is a prime.

Empirical Proof:
For $n = 1$, we have $n^2 - n + 41 = 41$, which is a prime.
For $n = 2$, we have $n^2 - n + 41 = 43$, which is a prime.
For $n = 3$, we have $n^2 - n + 41 = 47$, which is a prime.
For $n = 4$, we have $n^2 - n + 41 = 53$, which is a prime.
....

So we conclude that $n^2 - n + 41$ is always a prime.

Pros and Cons of Empirical and Mathematical Proofs

Pros and Cons of Empirical and Mathematical Proofs

Pros and cons of Empirical Proofs:

Pros and Cons of Empirical and Mathematical Proofs

Pros and cons of Empirical Proofs:

- (Pros): Easy to give a proof.

Pros and Cons of Empirical and Mathematical Proofs

Pros and cons of Empirical Proofs:

- (Pros): Easy to give a proof.
- (Cons): They are not 100% accurate.

Pros and Cons of Empirical and Mathematical Proofs

Pros and cons of Empirical Proofs:

- (Pros): Easy to give a proof.
- (Cons): They are not 100% accurate.

  For example in the previous statement: For $n = 41$ we have $n^2 - n + 41 = 1681 = 41^2$ which is not a prime.

Pros and Cons of Empirical and Mathematical Proofs

Pros and cons of Empirical Proofs:

- (Pros): Easy to give a proof.
- (Cons): They are not 100% accurate.

  For example in the previous statement: For $n = 41$ we have $n^2 - n + 41 = 1681 = 41^2$ which is not a prime.

  So the statement $n^2 - n + 41$ is always a prime is false.

Pros and Cons of Empirical and Mathematical Proofs

Pros and Cons of Empirical and Mathematical Proofs

Pros and cons of Mathematical Proofs:

Pros and Cons of Empirical and Mathematical Proofs

Pros and cons of Mathematical Proofs:

- (Pros): It is 100% accurate. No chance of any error in the deduction.

Pros and Cons of Empirical and Mathematical Proofs

Pros and cons of Mathematical Proofs:

- (Pros): It is 100% accurate. No chance of any error in the deduction.
- (Cons): It is hard to prove.

Thus ...

- Mathematical Proof are always better than the Empirical Proofs.

Thus ...

- Mathematical Proof are always better than the Empirical Proofs.
- We will always like to have a mathematical proof.

Thus ...

- Mathematical Proof are always better than the Empirical Proofs.
- We will always like to have a mathematical proof.
- To come up with different techniques of mathematical proof we will take the use of Propositional and Predicate Logic.

Propositional Logic and Predicate Logic

- Every statement is either TRUE or FALSE
- There are logical connectives $\vee$, $\wedge$, $\neg$, $\implies$ and $\iff$.
- A statement can have a undefined term, called a variable.
- But every variable has to be quantified using either of the quantifiers $\forall$ and $\exists$.
- Two logical statements can be equivalent if the two statements answer exactly in the same way on every input.
- To check whether two logical statements are equivalent one can do one of the following:
  - Checking the Truthtable of each statement
  - Reducing one to the other using reductions using rules.

Using Propositional Logic for designing proofs

- A mathematical statement comprises of a premise (or assumptions). And when the assumptions are satisfied the statement deduces something.

Using Propositional Logic for designing proofs

- A mathematical statement comprises of a premise (or assumptions). And when the assumptions are satisfied the statement deduces something.
- If A is the set of assumptions and B is the deduction then a mathematical statement is of the form

$$A \implies B$$

Using Propositional Logic for designing proofs

- A mathematical statement comprises of a premise (or assumptions). And when the assumptions are satisfied the statement deduces something.
- If A is the set of assumptions and B is the deduction then a mathematical statement is of the form

$$A \implies B$$

- Now how to check if the statement if correct? And if it is indeed correct how to prove the statement?

Using Propositional Logic for designing proofs

- A mathematical statement comprises of a premise (or assumptions). And when the assumptions are satisfied the statement deduces something.
- If A is the set of assumptions and B is the deduction then a mathematical statement is of the form

$$A \implies B$$

- Now how to check if the statement if correct? And if it is indeed correct how to prove the statement?
- Depending on whether A or B (or both) can be split into smaller statements and how the smaller statements are connected we can design different techniques for proving the overall statement of $A \implies B$.

Using Propositional Logic for designing proofs

- A mathematical statement comprises of a premise (or assumptions). And when the assumptions are satisfied the statement deduces something.
- If A is the set of assumptions and B is the deduction then a mathematical statement is of the form

$$A \implies B$$

- Now how to check if the statement if correct? And if it is indeed correct how to prove the statement?
- Depending on whether A or B (or both) can be split into smaller statements and how the smaller statements are connected we can design different techniques for proving the overall statement of $A \implies B$.
- If indeed we can proof that the statement is correct then we can call it a Theorem.

Proof Techniques

To prove statement B from A.

- 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.

Simplest Splitting

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

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

Simplest Splitting

- 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* $b^2 \equiv 1 (mod\ 4)$.

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 $2b^2 \geq (b+1)^2$.

Removing Assumptions

Removing Assumptions

Problem (First Part)

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

Removing Assumptions

Problem (First Part)

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

- An odd prime has many properties.

Removing Assumptions

Problem (First Part)

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

- An odd prime has many properties.
- Which property do we need to use for our proof.

Removing Assumptions

Problem (First Part)

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

- An odd prime has many properties.
- Which property do we need to use for our proof.
- In this problem we will only need the property that an odd prime is ≥ 3.

Removing Assumptions

Problem (First Part)

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

- An odd prime has many properties.
- Which property do we need to use for our proof.
- In this problem we will only need the property that an odd prime is ≥ 3.

So sufficient to prove :

Removing Assumptions

Problem (First Part)

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

- An odd prime has many properties.
- Which property do we need to use for our proof.
- In this problem we will only need the property that an odd prime is ≥ 3.

So sufficient to prove :

Problem

If b is a real number ≥ 3 then $b^2 \equiv 1 (mod\ 4)$.

Removing Assumptions

Problem (Second Part)

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

Removing Assumptions

Problem (Second Part)

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

- An odd prime has many properties.
- Which property do we need to use for our proof.

Removing Assumptions

Problem (Second Part)

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

- An odd prime has many properties.
- Which property do we need to use for our proof.
- In this problem we will only need the property that an odd prime is an odd integer.

Removing Assumptions

Problem (Second Part)

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

- An odd prime has many properties.
- Which property do we need to use for our proof.
- In this problem we will only need the property that an odd prime is an odd integer.

So sufficient to prove:

Problem (Second Part)

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

Now let us try to prove these problems...

Problem

If b is a real number ≥ 3 then $b^2 \equiv 1 (mod\ 4)$.

Problem (Second Part)

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

Now let us try to prove these problems...

Problem

If b is a real number ≥ 3 then $b^2 \equiv 1(mod\ 4)$.

Problem (Second Part)

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

We will give constructive proofs for these problems.

Constructive Proof

To prove B from A.
There are two techniques:

Constructive Proof

To prove B from A.
There are two techniques:

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

Constructive Proof

To prove B from A.
There are two techniques:

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

Next Video Lecture

We will use direct proof technique to prove the two problems:

Problem

If b *is a real number* ≥ 3 *then* $b^2 \equiv 1(mod\ 4)$.

Problem

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

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 $b \geq 3 \implies (b-1) \geq 2$

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

Next video lecture...

- In the next video lecture we will study other proof techniques.

Next video lecture...

- In the next video lecture we will study other proof techniques.
- Revise you propositional logic and prove that the followings
  1. If $C \implies B$ then
  $$(A \implies C) \implies (A \implies B).$$
  2. If $A = C \vee D$ then
  $$(A \implies B) \equiv (C \implies B) \wedge (D \implies B).$$