Start of Lecture 2

Last time: Propositions, Predicates, Quantifiers, Logical Operators

Today: Some definitions, Proofs

Recap

Propositions: Statements that are either true or false.

Predicates: Like propositions but with one or more variables.

Quantifiers:

- "for all" ($\forall$)
- "there exists" ($\exists$)

Logical Operators:

- and ($\wedge$)
- or ($\vee$)
- not ($\neg$)
- implies/if-then ($\implies$)
- if and only if ($\iff$)

Some Sets of Numbers:

- $\mathbb{N}$: Natural numbers
- $\mathbb{Z}$: Integers
- $\mathbb{Q}$: Rational numbers
- $\mathbb{R}$: Real numbers

Definitions: Even Numbers

Definition: An integer n is even if there exists an integer k such that $n = 2k$.

Definitions: Even Numbers

Definition: An integer n is even if there exists an integer k such that $n = 2k$.

n is even $\iff \exists k \in \mathbb{Z}$ such that $n = 2k$.

Definitions: Odd Numbers

Definition: An integer n is odd if there exists an integer k such that $n = 2k + 1$.

Definitions: Odd Numbers

Definition: An integer n is odd if there exists an integer k such that $n = 2k + 1$.

n is odd $\iff \exists k \in \mathbb{Z}$ such that $n = 2k + 1$.

Definitions: Odd Numbers

Definition: An integer n is odd if there exists an integer k such that $n = 2k + 1$.

n is odd $\iff \exists k \in \mathbb{Z}$ such that $n = 2k + 1$.

Note: Every integer is either even or odd, but not both.

Definitions: Divisibility

Quesion: What does it mean when we say "n is divisible by m"?

Definitions: Divisibility

Quesion: What does it mean when we say "n is divisible by m"?

Definition: An integer n is divisible by an integer m if there exists an integer k such that $n = mk$.

Definitions: Divisibility

Quesion: What does it mean when we say "n is divisible by m"?

Definition: An integer n is divisible by an integer m if there exists an integer k such that $n = mk$.

n is divisible by m $\iff$ $\exists k \in \mathbb{Z}$ such that $n = mk$.

Definitions: Divisibility

Quesion: What does it mean when we say "n is divisible by m"?

Definition: An integer n is divisible by an integer m if there exists an integer k such that $n = mk$.

n is divisible by m $\iff$ $\exists k \in \mathbb{Z}$ such that $n = mk$.

Sometimes denoted as $m \mid n$ (read as "m divides n").

Question: What does it mean when we say "p is prime"?

Definitions: Prime Numbers

Question: What does it mean when we say "p is prime"?

Definition: An integer p is prime if $p > 1$ and its only positive divisors are 1 and p.

Definitions: Prime Numbers

Question: What does it mean when we say "p is prime"?

Definition: An integer p is prime if $p > 1$ and its only positive divisors are 1 and p.

$$p \text{ is prime} \iff p > 1 \text{ and } \forall m \in \mathbb{N},\ m \mid p \implies (m = 1 \vee m = p).$$

Definitions: Rational Numbers

Question: What does it mean when we say "x is rational"?

Definitions: Rational Numbers

Question: What does it mean when we say "x is rational"?

Definition: A real number x is rational if there exist integers a and b, such that $x = \frac{a}{b}$.

Definitions: Rational Numbers

Question: What does it mean when we say "x is rational"?

Definition: A real number x is rational if there exist integers a and b, such that $x = \frac{a}{b}$.

$x \in \mathbb{Q} \iff \exists a, b \in \mathbb{Z}$ such that $x = \frac{a}{b}$.

Definitions: Rational Numbers

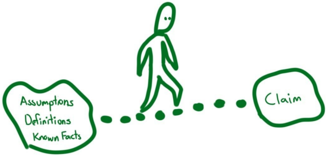
Question: What does it mean when we say "x is rational"?

Definition: A real number x is rational if there exist integers a and b, such that $x = \frac{a}{b}$.

$x \in \mathbb{Q} \iff \exists a, b \in \mathbb{Z}$ such that $x = \frac{a}{b}$.

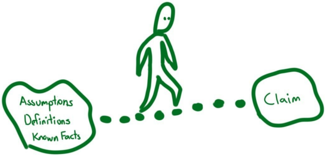
Note: We can always find a and b that share no common divisors greater than 1 (i.e. the fraction is in reduced form).

What is a proof?



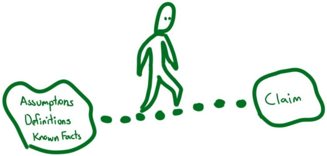
What is a proof?

- An explanation of why a statement is true.



What is a proof?

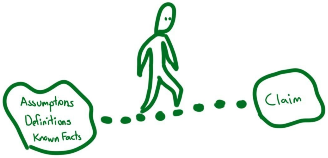
- An explanation of why a statement is true.
- Uses precise mathematical language.



Proofs

What is a proof?

- An explanation of why a statement is true.
- Uses precise mathematical language.
- Can be thought of as a sequence of logical steps that lead from assumptions, definitions, and known facts to the desired conclusion.

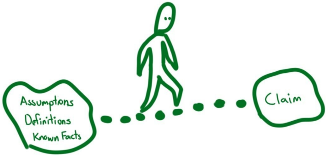


Proofs

What is a proof?

- An explanation of why a statement is true.
- Uses precise mathematical language.
- Can be thought of as a sequence of logical steps that lead from assumptions, definitions, and known facts to the desired conclusion.

What makes a proof good?



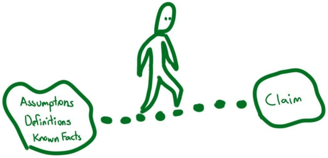
Proofs

What is a proof?

- An explanation of why a statement is true.
- Uses precise mathematical language.
- Can be thought of as a sequence of logical steps that lead from assumptions, definitions, and known facts to the desired conclusion.

What makes a proof good?

- Correct

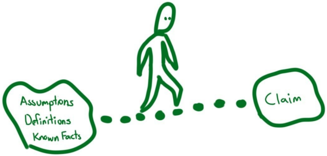


What is a proof?

- An explanation of why a statement is true.
- Uses precise mathematical language.
- Can be thought of as a sequence of logical steps that lead from assumptions, definitions, and known facts to the desired conclusion.

What makes a proof good?

- Correct
- Clear

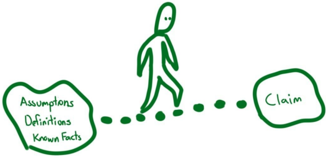


What is a proof?

- An explanation of why a statement is true.
- Uses precise mathematical language.
- Can be thought of as a sequence of logical steps that lead from assumptions, definitions, and known facts to the desired conclusion.

What makes a proof good?

- Correct
- Clear
- Concise



Proofs: Direct Proof Example

Claim: An integer x is odd $\implies$ x^2 is also odd.

Proofs: Direct Proof Example

Claim: An integer x is odd $\implies$ x^2 is also odd.

Proof: Suppose x is odd. Then there exists an integer k such that $x = 2k + 1$.

Proofs: Direct Proof Example

Claim: An integer x is odd $\implies$ x^2 is also odd.

Proof: Suppose x is odd. Then there exists an integer k such that $x = 2k + 1$.Then we have

$$\begin{aligned} x^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

Proofs: Direct Proof Example

Claim: An integer x is odd $\implies$ x^2 is also odd.

Proof: Suppose x is odd. Then there exists an integer k such that $x = 2k + 1$. Then we have

$$\begin{aligned} x^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

This implies that x^2 is odd, since $2k^2 + 2k$ is an integer. $\square$

Proof by Contradiction: To prove a statement, assume the opposite is true and show that this leads to a contradiction.

Proofs: Proof by Contradiction

Proof by Contradiction: To prove a statement, assume the opposite is true and show that this leads to a contradiction.

Structure:

Claim: p is true.

Proof: Assume p is false.

...

$\implies$ Something that is false.

Proofs: Proof by Contradiction Example

Claim: $\sqrt{2}$ is irrational.

Proofs: Proof by Contradiction Example

Claim: $\sqrt{2}$ is irrational.

Proof: Suppose, for the sake of contradiction, that $\sqrt{2}$ is rational.

Proofs: Proof by Contradiction Example

Claim: $\sqrt{2}$ is irrational.

Proof: Suppose, for the sake of contradiction, that $\sqrt{2}$ is rational.

Then we can write

$$\sqrt{2} = \frac{a}{b}.$$

Here a and b are integers with no common factors; the fraction is in reduced form.

Proofs: Proof by Contradiction Example

Claim: $\sqrt{2}$ is irrational.

Proof: Suppose, for the sake of contradiction, that $\sqrt{2}$ is rational.

Then we can write

$$\sqrt{2} = \frac{a}{b}.$$

Here a and b are integers with no common factors; the fraction is in reduced form.In particular, a and b are not both even.

Proofs: Proof by Contradiction Example

Claim: $\sqrt{2}$ is irrational.

Proof: Suppose, for the sake of contradiction, that $\sqrt{2}$ is rational.

Then we can write

$$\sqrt{2} = \frac{a}{b}.$$

Here a and b are integers with no common factors; the fraction is in reduced form.In particular, a and b are not both even.

Squaring both sides and rearranging gives

$$a^2 = 2b^2.$$

Thus a^2 is even, so a is even.

Proofs: Proof by Contradiction Example

Claim: $\sqrt{2}$ is irrational.

Proof: Suppose, for the sake of contradiction, that $\sqrt{2}$ is rational.

Then we can write

$$\sqrt{2} = \frac{a}{b}.$$

Here a and b are integers with no common factors; the fraction is in reduced form.In particular, a and b are not both even.

Squaring both sides and rearranging gives

$$a^2 = 2b^2.$$

Thus a^2 is even, so a is even.Hence $a = 2k$ for some integer k.

Proofs: Proof by Contradiction Example

Claim: $\sqrt{2}$ is irrational.

Proof: Suppose, for the sake of contradiction, that $\sqrt{2}$ is rational.

Then we can write

$$\sqrt{2} = \frac{a}{b}.$$

Here a and b are integers with no common factors; the fraction is in reduced form.In particular, a and b are not both even.

Squaring both sides and rearranging gives

$$a^2 = 2b^2.$$

Thus a^2 is even, so a is even.Hence $a = 2k$ for some integer k.

Substituting $a = 2k$ gives

$$(2k)^2 = 2b^2 \quad \Longrightarrow \quad b^2 = 2k^2.$$

Thus b^2 is even, so b is also even.

Proofs: Proof by Contradiction Example

Claim: $\sqrt{2}$ is irrational.

Proof: Suppose, for the sake of contradiction, that $\sqrt{2}$ is rational.

Then we can write

$$\sqrt{2} = \frac{a}{b}.$$

Here a and b are integers with no common factors; the fraction is in reduced form.In particular, a and b are not both even.

Squaring both sides and rearranging gives

$$a^2 = 2b^2.$$

Thus a^2 is even, so a is even.Hence $a = 2k$ for some integer k.

Substituting $a = 2k$ gives

$$(2k)^2 = 2b^2 \quad \Longrightarrow \quad b^2 = 2k^2.$$

Thus b^2 is even, so b is also even.

We have a contradiction, so $\sqrt{2}$ must be irrational. $\square$

Proofs: Proof by Contradiction Example

Claim: $\sqrt{2}$ is irrational.

Proof: Suppose, for the sake of contradiction, that $\sqrt{2}$ is rational.

Then we can write
$$\sqrt{2} = \frac{a}{b}.$$

Here a and b are integers with no common factors; the fraction is in reduced form.In particular, a and b are not both even.

Squaring both sides and rearranging gives
$$a^2 = 2b^2.$$

Thus a^2 is even, so a is even.Hence $a = 2k$ for some integer k.

Substituting $a = 2k$ gives
$$(2k)^2 = 2b^2 \quad \Longrightarrow \quad b^2 = 2k^2.$$

Thus b^2 is even, so b is also even.

We have a contradiction, so $\sqrt{2}$ must be irrational. □

De Morgan's Laws

"a and b are not both even"

De Morgan's Laws

"a and b are not both even" $\iff$ "a is odd or b is odd"

De Morgan's Laws

$$\text{“}a \text{ and } b \text{ are not both even”} \iff \text{“}a \text{ is odd or } b \text{ is odd”}$$

$$\neg(a \text{ is even} \land b \text{ is even})$$

De Morgan's Laws

"a and b are not both even" $\iff$ "a is odd or b is odd"

$$\begin{aligned} &\neg(a \text{ is even} \land b \text{ is even}) \\ \iff \quad &\neg(a \text{ is even}) \lor \neg(b \text{ is even}) \end{aligned}$$

De Morgan's Laws

"a and b are not both even" $\iff$ "a is odd or b is odd"

$$\begin{aligned} & \neg(a \text{ is even} \wedge b \text{ is even}) \\ \iff & \neg(a \text{ is even}) \vee \neg(b \text{ is even}) \\ \iff & a \text{ is odd} \vee b \text{ is odd} \end{aligned}$$

De Morgan's Laws

"a and b are not both even" $\iff$ "a is odd or b is odd"

$$\begin{aligned} & \neg(a \text{ is even} \wedge b \text{ is even}) \\ \iff & \neg(a \text{ is even}) \vee \neg(b \text{ is even}) \\ \iff & a \text{ is odd} \vee b \text{ is odd} \end{aligned}$$

For propositions p and q, we have $\neg(p \wedge q) \iff \neg p \vee \neg q$

De Morgan's Laws:

- $\neg(p \wedge q) \iff \neg p \vee \neg q$
- $\neg(p \vee q) \iff \neg p \wedge \neg q$

De Morgan's Laws

De Morgan's Laws:

- $\neg(p \wedge q) \iff \neg p \vee \neg q$
- $\neg(p \vee q) \iff \neg p \wedge \neg q$

Example: Suppose x is a real number and n is an integer. What is the opposite of "x is rational and n is odd"?

De Morgan's Laws:

- $\neg(p \wedge q) \iff \neg p \vee \neg q$
- $\neg(p \vee q) \iff \neg p \wedge \neg q$

Example: Suppose x is a real number and n is an integer. What is the opposite of "x is rational and n is odd"?

"x is irrational or n is even"

Proofs: Proof by Contradiction Example 2

Fact: Every integer $n > 1$ is divisible by some prime number.

Proofs: Proof by Contradiction Example 2

Fact: Every integer $n > 1$ is divisible by some prime number.

Claim: There are infinitely many prime numbers.

Proofs: Proof by Contradiction Example 2

Fact: Every integer $n > 1$ is divisible by some prime number.

Claim: There are infinitely many prime numbers.

Proof: Suppose, for the sake of contradiction, that there are finitely many prime numbers. Let $p_1, p_2, \ldots, p_k$ be all the prime numbers.

Proofs: Proof by Contradiction Example 2

Fact: Every integer $n > 1$ is divisible by some prime number.

Claim: There are infinitely many prime numbers.

Proof: Suppose, for the sake of contradiction, that there are finitely many prime numbers. Let $p_1, p_2, \ldots, p_k$ be all the prime numbers.

Consider the number $N = p_1 p_2 \cdots p_k + 1$.

Proofs: Proof by Contradiction Example 2

Fact: Every integer $n > 1$ is divisible by some prime number.

Claim: There are infinitely many prime numbers.

Proof: Suppose, for the sake of contradiction, that there are finitely many prime numbers. Let $p_1, p_2, \ldots, p_k$ be all the prime numbers.

Consider the number $N = p_1 p_2 \cdots p_k + 1$.

By the fact above, N is divisible by some prime number.

Proofs: Proof by Contradiction Example 2

Fact: Every integer $n > 1$ is divisible by some prime number.

Claim: There are infinitely many prime numbers.

Proof: Suppose, for the sake of contradiction, that there are finitely many prime numbers. Let $p_1, p_2, \ldots, p_k$ be all the prime numbers.

Consider the number $N = p_1 p_2 \cdots p_k + 1$.

By the fact above, N is divisible by some prime number.

However, N is not divisible by any of the primes $p_1, p_2, \ldots, p_k$, since it leaves a remainder of 1 when divided by any of them.

Proofs: Proof by Contradiction Example 2

Fact: Every integer $n > 1$ is divisible by some prime number.

Claim: There are infinitely many prime numbers.

Proof: Suppose, for the sake of contradiction, that there are finitely many prime numbers. Let $p_1, p_2, \ldots, p_k$ be all the prime numbers.

Consider the number $N = p_1 p_2 \cdots p_k + 1$.

By the fact above, N is divisible by some prime number.

However, N is not divisible by any of the primes $p_1, p_2, \ldots, p_k$, since it leaves a remainder of 1 when divided by any of them.

This is a contradiction, so there must be infinitely many prime numbers. $\square$