Definitions, Theorems, and Proofs

Note

These three entities are central to every mathematical subject, including the theory of computation

Note

These three entities are central to every mathematical subject, including the theory of computation

- Theorems are the heart of mathematics

Note

These three entities are central to every mathematical subject, including the theory of computation

- Theorems are the heart of mathematics
- Proofs are the soul of mathematics

Note

These three entities are central to every mathematical subject, including the theory of computation

- Theorems are the heart of mathematics
- Proofs are the soul of mathematics
- Definitions are the spirit of mathematics

Definitions

- A definition describes the objects and the notions used by the mathematical subject

Definitions

- A definition describes the objects and the notions used by the mathematical subject
- A definition may be simple, as in the definition of a set, or it can be complex as in the definition of the security in cryptography

Definitions

- A definition describes the objects and the notions used by the mathematical subject
- A definition may be simple, as in the definition of a set, or it can be complex as in the definition of the security in cryptography
- Precision is essential to any mathematical definition

Definitions

- A definition describes the objects and the notions used by the mathematical subject
- A definition may be simple, as in the definition of a set, or it can be complex as in the definition of the security in cryptography
- Precision is essential to any mathematical definition

Note: a definition must make clear what constitutes the defined object and what does not

Formally

A definition has two parts:

Formally

A definition has two parts:

- A class of objects to which the defined object belongs.

Formally

A definition has two parts:

- A class of objects to which the defined object belongs.

  Example: when defining prime numbers this class is

Formally

A definition has two parts:

- A class of objects to which the defined object belongs.

  Example: when defining prime numbers this class is the set on natural numbers

Formally

A definition has two parts:

- A class of objects to which the defined object belongs.

  Example: when defining prime numbers this class is the set on natural numbers

- A property that distinguishes the defined object within the class.

Formally

A definition has two parts:

- A class of objects to which the defined object belongs.

  Example: when defining prime numbers this class is the set on natural numbers

- A property that distinguishes the defined object within the class.

  Example: $p \in \mathcal{N}$ is prime iff

Formally

A definition has two parts:

- A class of objects to which the defined object belongs.

  Example: when defining prime numbers this class is the set on natural numbers

- A property that distinguishes the defined object within the class.

  Example: $p \in \mathcal{N}$ is prime iff $\nexists k, q \in \mathcal{N} : k, q \neq p, 1 \wedge p = kq$

Formally

A definition has two parts:

- A class of objects to which the defined object belongs.

  Example: when defining prime numbers this class is the set on natural numbers

- A property that distinguishes the defined object within the class.

  Example: $p \in \mathcal{N}$ is prime iff $\nexists k, q \in \mathcal{N} : k, q \neq p, 1 \wedge p = kq$

Note: a formal definition implies that both components are formal

Mathematical statements

- Typically a mathematical statement expresses that some object has certain property

Mathematical statements

- Typically a mathematical statement expresses that some object has certain property
- A mathematical statement may or may not be true. However, like a definition it must be precise

Mathematical statements

- Typically a mathematical statement expresses that some object has certain property
- A mathematical statement may or may not be true. However, like a definition it must be precise
- There must not be any ambiguity about the meaning of mathematical statement

Mathematical statements

- Typically a mathematical statement expresses that some object has certain property
- A mathematical statement may or may not be true. However, like a definition it must be precise
- There must not be any ambiguity about the meaning of mathematical statement

Note: to make a mathematical statement precise one needs to formalize both the object and the property stated.

Proofs

- A proof is a convincing logical argument that a statement is true

Proofs

- A proof is a convincing logical argument that a statement is true
- A mathematical proof must be convincing in an absolute sense; this is rather different from the notion of proof in everyday life or in law

Proofs

- A proof is a convincing logical argument that a statement is true
- A mathematical proof must be convincing in an absolute sense; this is rather different from the notion of proof in everyday life or in law
- In everyday life or in law a proof is convincing “beyond any reasonable doubt" and is based on compelling evidence

Proofs

- A proof is a convincing logical argument that a statement is true
- A mathematical proof must be convincing in an absolute sense; this is rather different from the notion of proof in everyday life or in law
- In everyday life or in law a proof is convincing “beyond any reasonable doubt" and is based on compelling evidence
- However, evidence plays no role in a mathematical proof. A mathematician demands “proof beyond any doubt"

Theorems

- Theorems: mathematical statements proved true

Theorems

- Theorems: mathematical statements proved true
- **Note:** mathematicians reserve the word theorem for statements of special interest

Theorems

- Theorems: mathematical statements proved true
- **Note:** mathematicians reserve the word theorem for statements of special interest
- Lemmas: mathematical statements proved true, that are interesting only because they assist in the proofs of another, more significant statement

Theorems

- Theorems: mathematical statements proved true
- **Note:** mathematicians reserve the word theorem for statements of special interest
- Lemmas: mathematical statements proved true, that are interesting only because they assist in the proofs of another, more significant statement
- Corollaries: true statements that are consequences of theorems or their proofs

Finding proofs

Note: the only way to determine the truth or falsity of a mathematical statement is with a mathematical proof!

Finding proofs

Note: the only way to determine the truth or falsity of a mathematical statement is with a mathematical proof!

- Finding proofs is not always simple!

Finding proofs

Note: the only way to determine the truth or falsity of a mathematical statement is with a mathematical proof!

- Finding proofs is not always simple!
- Sometimes a proof is a simple set of rules or processes

Finding proofs

Note: the only way to determine the truth or falsity of a mathematical statement is with a mathematical proof!

- Finding proofs is not always simple!
- Sometimes a proof is a simple set of rules or processes
- Other times, it requires inspiration and transpiration

Finding proofs

Note: the only way to determine the truth or falsity of a mathematical statement is with a mathematical proof!

- Finding proofs is not always simple!
- Sometimes a proof is a simple set of rules or processes
- Other times, it requires inspiration and transpiration
- This course requires you to produce proofs!

Note

- The author of the textbook advise us: “do not despair at the prospect of finding a proof"

Note

- The author of the textbook advise us: “do not despair at the prospect of finding a proof"
- Even though no one has a recipe for producing proofs, some helpful general strategies are available

Strategies for finding proofs

- Read carefully the statement you want to prove

Strategies for finding proofs

- Read carefully the statement you want to prove
- Be sure that you understand all the notation

Strategies for finding proofs

- Read carefully the statement you want to prove
- Be sure that you understand all the notation
- Rewrite the statement in your own words

Strategies for finding proofs

- Read carefully the statement you want to prove
- Be sure that you understand all the notation
- Rewrite the statement in your own words
- Break the statement down and consider each part separately; sometimes the parts of a multipart statement are not immediately evident

Example multipart statement

P if and only if Q, often written P iff Q, where both P and Q are mathematical statements

Example multipart statement

P if and only if Q, often written P iff Q, where both P and Q are mathematical statements

- The first part is "P only if Q", which means: *if P is true then Q is true, written* $P \Rightarrow Q$

Example multipart statement

P if and only if Q, often written P iff Q, where both P and Q are mathematical statements

- The first part is "P only if Q", which means: *if P is true then Q is true, written* $P \Rightarrow Q$
- The second part is "P if Q", which means: *if Q is true then P is true, written* $P \Leftarrow Q$

Terms used by “iff" proofs

- $P \Rightarrow Q$ is called forward direction of the original statement

Terms used by “iff" proofs

- $P \Rightarrow Q$ is called forward direction of the original statement
- $P \Leftarrow Q$ is called reverse direction of the original statement

Terms used by “iff" proofs

- $P \Rightarrow Q$ is called forward direction of the original statement
- $P \Leftarrow Q$ is called reverse direction of the original statement
- The original statement can be written $P \Leftrightarrow Q$

Note

- To prove an iff statement one must prove each of the two implications constituting “iff"

Note

- To prove an iff statement one must prove each of the two implications constituting “iff"
- Often one of these implications is easier to prove than the other. Always start with the easy one.

Other multipart statements

Statements stating that two sets A and B are equal

Other multipart statements

Statements stating that two sets A and B are equal

- The first part states that “A is a subset of B"

Other multipart statements

Statements stating that two sets A and B are equal

- The first part states that “A is a subset of B"
- The second part states that “B is a subset of A"

Other multipart statements

Statements stating that two sets A and B are equal

- The first part states that “A is a subset of B"
- The second part states that “B is a subset of A"

Proof:

Other multipart statements

Statements stating that two sets A and B are equal

- The first part states that “A is a subset of B"
- The second part states that “B is a subset of A"

Proof:

1. $\forall a \in A$ show that $a \in B$ and

Other multipart statements

Statements stating that two sets A and B are equal

- The first part states that “A is a subset of B"
- The second part states that “B is a subset of A"

Proof:

1. $\forall a \in A$ show that $a \in B$ and
2. $\forall b \in B$ show that $b \in A$

Advise

Try to get an intuitive “gut" feeling of why the statement should be true

Advise

Try to get an intuitive “gut" feeling of why the statement should be true

- Experimenting with examples is helpful

Advise

Try to get an intuitive “gut" feeling of why the statement should be true

- Experimenting with examples is helpful
- **Example:** If a statement says that all objects of certain type have a particular property

Advise

Try to get an intuitive “gut" feeling of why the statement should be true

- Experimenting with examples is helpful
- **Example:** If a statement says that all objects of certain type have a particular property
  - First, pick a few objects of that type and observe that they actually do have that property

Advise

Try to get an intuitive “gut" feeling of why the statement should be true

- Experimenting with examples is helpful
- **Example:** If a statement says that all objects of certain type have a particular property
  - First, pick a few objects of that type and observe that they actually do have that property
  - Then, try find an object that fails to have the property, called a counterexample

Note

- If the statement to prove is true one cannot find counterexamples

Note

- If the statement to prove is true one cannot find counterexamples
- Seeing where one runs into difficulty when attempting to find counterexamples can help understand why the statement is true

Example statement and proof

Statement: for every graph G, the sum of the degrees of all the nodes in G is an even number

The “gut" feeling

Pick up a few graphs and observe:

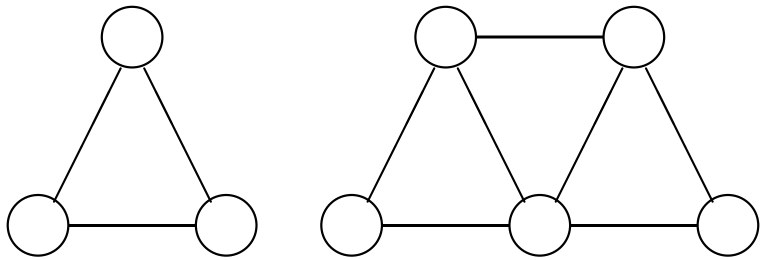

Figure 1: Example graphs and degrees

Find a counter example

That is, try to find a graph in which the sum of node degrees is an odd number, Figure 2

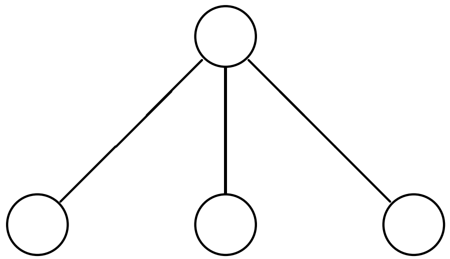

Figure 2: Try a counterexample

Why statement is true?

- Every time an edge is added sum increases by 2

Why statement is true?

- Every time an edge is added sum increases by 2
- The sum of degrees is

Why statement is true?

- Every time an edge is added sum increases by 2
- The sum of degrees is the sum of edges multiplied by 2

Another suggestion

If you are stuck trying to prove a statement, try something easier!

Another suggestion

If you are stuck trying to prove a statement, try something easier!

- Attempt to prove a special case of the statement.

Another suggestion

If you are stuck trying to prove a statement, try something easier!

- Attempt to prove a special case of the statement.

  Example: if you try to prove that some property is true $\forall k > 0$,

Another suggestion

If you are stuck trying to prove a statement, try something easier!

- Attempt to prove a special case of the statement.

  Example: if you try to prove that some property is true $\forall k > 0$, first try to prove it for $k = 1$

Another suggestion

If you are stuck trying to prove a statement, try something easier!

- Attempt to prove a special case of the statement.

  Example: if you try to prove that some property is true $\forall k > 0$, first try to prove it for $k = 1$
- If you succeed with a special case, try one a little more complicated.

Another suggestion

If you are stuck trying to prove a statement, try something easier!

- Attempt to prove a special case of the statement.

  Example: if you try to prove that some property is true $\forall k > 0$, first try to prove it for $k = 1$

- If you succeed with a special case, try one a little more complicated.

  Example: if you succeeded with $k = 1$

Another suggestion

If you are stuck trying to prove a statement, try something easier!

- Attempt to prove a special case of the statement.

  Example: if you try to prove that some property is true $\forall k > 0$, first try to prove it for $k = 1$

- If you succeed with a special case, try one a little more complicated.

  Example: if you succeeded with $k = 1$ try $k = 2$

Another suggestion

If you are stuck trying to prove a statement, try something easier!

- Attempt to prove a special case of the statement.

  Example: if you try to prove that some property is true $\forall k > 0$, first try to prove it for $k = 1$

- If you succeed with a special case, try one a little more complicated.

  Example: if you succeeded with $k = 1$ try $k = 2$

- Repeat this procedure until you can get the general proof

Note

When you have found a proof, write it up properly!

Note

When you have found a proof, write it up properly!

- A well-written proof is a sequence of statements, wherein each one follows by simple reasoning from previous statements in the sequence

Note

When you have found a proof, write it up properly!

- A well-written proof is a sequence of statements, wherein each one follows by simple reasoning from previous statements in the sequence
- Carefully writing a proof is important, both to enable a reader to understand it and for the prover to be sure that it is free from errors

Tips for producing proofs

- Be patient. Finding proofs takes time. If you don't see how to do it right away, don't worry. One can work for weeks, or even years!

Tips for producing proofs

- Be patient. Finding proofs takes time. If you don't see how to do it right away, don't worry. One can work for weeks, or even years!
- Come back to it. Look over the statement you want to prove, think about it a bit, leave it, and return a few minutes or hours later. Let the unconscious, intuitive part of your mind have a chance to work.

More tips

- Be neat. When you are building your intuition for the statement you want to prove, use simple, clear pictures and text. Furthermore, when you are writing a solution for another person to read, neatness will help that person understand it.

More tips

- Be neat. When you are building your intuition for the statement you want to prove, use simple, clear pictures and text. Furthermore, when you are writing a solution for another person to read, neatness will help that person understand it.
- Be concise. Brevity helps you express high-level ideas without getting lost in details. Good mathematical notation is useful for expressing ideas concisely. However, do not forget Einstein's suggestion: simple, as simple as possible, but not simpler

Example: DeMorgan's Laws

Theorem: for any two sets A and B,

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

Example: DeMorgan's Laws

Theorem: for any two sets A and B,

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

Understanding the statement

Example: DeMorgan's Laws

Theorem: for any two sets A and B,

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

Understanding the statement

- Is the meaning of this theorem clear?

Example: DeMorgan's Laws

Theorem: for any two sets A and B,

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

Understanding the statement

- Is the meaning of this theorem clear? Do you understand the meaning of $\cup$, $\cap$, $\overline{A}$?

Example: DeMorgan's Laws

Theorem: for any two sets A and B,

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

Understanding the statement

- Is the meaning of this theorem clear? Do you understand the meaning of $\cup$, $\cap$, $\overline{A}$?
- We must show that two sets are equal.

Example: DeMorgan's Laws

Theorem: for any two sets A and B,

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

Understanding the statement

- Is the meaning of this theorem clear? Do you understand the meaning of $\cup$, $\cap$, $\overline{A}$?
- We must show that two sets are equal. Do you remember how this can be done?

Example: DeMorgan's Laws

Theorem: for any two sets A and B,

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

Understanding the statement

- Is the meaning of this theorem clear? Do you understand the meaning of $\cup$, $\cap$, $\overline{A}$?
- We must show that two sets are equal. Do you remember how this can be done?
- Can you consider a few examples before trying the proof?

The proof

Prove the assertion $\overline{A \cup B} = \overline{A} \cap \overline{B}$ by showing

The proof

Prove the assertion $\overline{A \cup B} = \overline{A} \cap \overline{B}$ by showing

1. $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$:

The proof

Prove the assertion $\overline{A \cup B} = \overline{A} \cap \overline{B}$ by showing

1. $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$: Suppose $x \in \overline{A \cup B}$.

The proof

Prove the assertion $\overline{A \cup B} = \overline{A} \cap \overline{B}$ by showing

1. $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$: Suppose $x \in \overline{A \cup B}$. Then, from the definition of the complement of a set it follows that $x \notin A \cup B$.

The proof

Prove the assertion $\overline{A \cup B} = \overline{A} \cap \overline{B}$ by showing

1. $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$: Suppose $x \in \overline{A \cup B}$. Then, from the definition of the complement of a set it follows that $x \notin A \cup B$. Hence, $x \notin A$ and $x \notin B$.

The proof

Prove the assertion $\overline{A \cup B} = \overline{A} \cap \overline{B}$ by showing

1. $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$: Suppose $x \in \overline{A \cup B}$. Then, from the definition of the complement of a set it follows that $x \notin A \cup B$. Hence, $x \notin A$ and $x \notin B$. Then $x \in \overline{A}$ and $x \in \overline{B}$.

The proof

Prove the assertion $\overline{A \cup B} = \overline{A} \cap \overline{B}$ by showing

1. $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$: Suppose $x \in \overline{A \cup B}$. Then, from the definition of the complement of a set it follows that $x \notin A \cup B$. Hence, $x \notin A$ and $x \notin B$. Then $x \in \overline{A}$ and $x \in \overline{B}$. That is, $x \in \overline{A} \cap \overline{B}$

The proof

Prove the assertion $\overline{A \cup B} = \overline{A} \cap \overline{B}$ by showing

1. $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$: Suppose $x \in \overline{A \cup B}$. Then, from the definition of the complement of a set it follows that $x \notin A \cup B$. Hence, $x \notin A$ and $x \notin B$. Then $x \in \overline{A}$ and $x \in \overline{B}$. That is, $x \in \overline{A} \cap \overline{B}$

2. $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$:

The proof

Prove the assertion $\overline{A \cup B} = \overline{A} \cap \overline{B}$ by showing

1. $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$: Suppose $x \in \overline{A \cup B}$. Then, from the definition of the complement of a set it follows that $x \notin A \cup B$. Hence, $x \notin A$ and $x \notin B$. Then $x \in \overline{A}$ and $x \in \overline{B}$. That is, $x \in \overline{A} \cap \overline{B}$

2. $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$: Suppose $x \in \overline{A} \cap \overline{B}$.

The proof

Prove the assertion $\overline{A \cup B} = \overline{A} \cap \overline{B}$ by showing

1. $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$: Suppose $x \in \overline{A \cup B}$. Then, from the definition of the complement of a set it follows that $x \notin A \cup B$. Hence, $x \notin A$ and $x \notin B$. Then $x \in \overline{A}$ and $x \in \overline{B}$. That is, $x \in \overline{A} \cap \overline{B}$

2. $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$: Suppose $x \in \overline{A} \cap \overline{B}$. By the definition of intersection, $x \in \overline{A}$ and $x \in \overline{B}$.

The proof

Prove the assertion $\overline{A \cup B} = \overline{A} \cap \overline{B}$ by showing

1. $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$: Suppose $x \in \overline{A \cup B}$. Then, from the definition of the complement of a set it follows that $x \notin A \cup B$. Hence, $x \notin A$ and $x \notin B$. Then $x \in \overline{A}$ and $x \in \overline{B}$. That is, $x \in \overline{A} \cap \overline{B}$

2. $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$: Suppose $x \in \overline{A} \cap \overline{B}$. By the definition of intersection, $x \in \overline{A}$ and $x \in \overline{B}$. Hence, by definition of complement, $x \notin A$ and $x \notin B$.

The proof

Prove the assertion $\overline{A \cup B} = \overline{A} \cap \overline{B}$ by showing

1. $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$: Suppose $x \in \overline{A \cup B}$. Then, from the definition of the complement of a set it follows that $x \notin A \cup B$. Hence, $x \notin A$ and $x \notin B$. Then $x \in \overline{A}$ and $x \in \overline{B}$. That is, $x \in \overline{A} \cap \overline{B}$

2. $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$: Suppose $x \in \overline{A} \cap \overline{B}$. By the definition of intersection, $x \in \overline{A}$ and $x \in \overline{B}$. Hence, by definition of complement, $x \notin A$ and $x \notin B$. That is, $x \notin A \cup B$.

The proof

Prove the assertion $\overline{A \cup B} = \overline{A} \cap \overline{B}$ by showing

1. $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$: Suppose $x \in \overline{A \cup B}$. Then, from the definition of the complement of a set it follows that $x \notin A \cup B$. Hence, $x \notin A$ and $x \notin B$. Then $x \in \overline{A}$ and $x \in \overline{B}$. That is, $x \in \overline{A} \cap \overline{B}$

2. $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$: Suppose $x \in \overline{A} \cap \overline{B}$. By the definition of intersection, $x \in \overline{A}$ and $x \in \overline{B}$. Hence, by definition of complement, $x \notin A$ and $x \notin B$. That is, $x \notin A \cup B$. Hence, $x \in \overline{A \cup B}$

Another Example

Theorem: In a graph G the sum of the degrees of the nodes of G is an even number.

Another Example

Theorem: In a graph G the sum of the degrees of the nodes of G is an even number.

Proof:

Another Example

Theorem: In a graph G the sum of the degrees of the nodes of G is an even number.

Proof:

1. Every edge in G is connected to two nodes.

Another Example

Theorem: In a graph G the sum of the degrees of the nodes of G is an even number.

Proof:

1. Every edge in G is connected to two nodes.
2. Each edge contributes 1 to each node to which it is connected

Another Example

Theorem: In a graph G the sum of the degrees of the nodes of G is an even number.

Proof:

1. Every edge in G is connected to two nodes.
2. Each edge contributes 1 to each node to which it is connected
3. Therefore, each edge contributes 2 to the sum of the degrees of all nodes

Another Example

Theorem: In a graph G the sum of the degrees of the nodes of G is an even number.

Proof:

1. Every edge in G is connected to two nodes.
2. Each edge contributes 1 to each node to which it is connected
3. Therefore, each edge contributes 2 to the sum of the degrees of all nodes
4. Hence, if G contains e edges, the sum of the degrees of all nodes of G is $2e$, which is an even number

Types of proofs

Several types of arguments arise frequently in mathematical proofs. The few that often occur in the theory of computation are:

Types of proofs

Several types of arguments arise frequently in mathematical proofs. The few that often occur in the theory of computation are:

- Proof by construction

Types of proofs

Several types of arguments arise frequently in mathematical proofs. The few that often occur in the theory of computation are:

- Proof by construction
- Proof by contradiction

Types of proofs

Several types of arguments arise frequently in mathematical proofs. The few that often occur in the theory of computation are:

- Proof by construction
- Proof by contradiction
- Proof by induction

Note

A proof may contain more than one type of argument because the proof may contain several different subproofs of several components of the main statement

Proof by construction

- Many theorems state that a particular type of object exists.

Proof by construction

- Many theorems state that a particular type of object exists.
- One way to prove such a theorem is by demonstrating how to construct that object.

Proof by construction

- Many theorems state that a particular type of object exists.
- One way to prove such a theorem is by demonstrating how to construct that object.

Note: this technique is called a proof by construction

Example proof by construction

Theorem: For each even number $n > 2$ there exists a 3-regular graph with n nodes.

Example proof by construction

Theorem: For each even number $n > 2$ there exists a 3-regular graph with n nodes.

Note: a 3-regular graph is a graph where every node has the degree 3

Proof

Method: by construction

Proof

Method: by construction

Proof: Construct $G = (V, E)$, $V = \{0, 1, 2, \ldots, n-1\}$, and

Proof

Method: by construction

Proof: Construct $G = (V, E)$, $V = \{0, 1, 2, \ldots, n-1\}$, and

$E = \{\{i, i+1\} \mid 0 \leq i \leq n-2\} \cup \{\{n-1, 0\}\} \cup \{\{i, i+n/2\} \mid 0 \leq i \leq n/2-1\}$

Proof

Method: by construction

Proof: Construct $G = (V, E)$, $V = \{0, 1, 2, \ldots, n-1\}$, and

$E = \{\{i, i+1\} \mid 0 \leq i \leq n-2\} \cup \{\{n-1, 0\}\} \cup \{\{i, i+n/2\} \mid 0 \leq i \leq n/2 - 1\}$

1. Take a particular value of n and picture the nodes of this graph written consecutively around the circumference of a circle

Proof

Method: by construction

Proof: Construct $G = (V, E)$, $V = \{0, 1, 2, \ldots, n-1\}$, and

$$E = \{\{i, i+1\} \mid 0 \le i \le n-2\} \cup \{\{n-1, 0\}\} \cup \{\{i, i+n/2\} \mid 0 \le i \le n/2 - 1\}$$

1. Take a particular value of n and picture the nodes of this graph written consecutively around the circumference of a circle
2. The edges described by $0 \le i \le n-2$ and $\{n-1, 0\}$ go between adjacent pairs around the circle

Proof

Method: by construction

Proof: Construct $G = (V, E)$, $V = \{0, 1, 2, \ldots, n-1\}$, and

$$E = \{\{i, i+1\} \mid 0 \le i \le n-2\} \cup \{\{n-1, 0\}\} \cup \{\{i, i+n/2\} \mid 0 \le i \le n/2-1\}$$

1. Take a particular value of n and picture the nodes of this graph written consecutively around the circumference of a circle
2. The edges described by $0 \le i \le n-2$ and $\{n-1, 0\}$ go between adjacent pairs around the circle
3. The edges described by $0 \le i \le n/2-1$ go between nodes of opposite sides of the circle

Proof

Method: by construction

Proof: Construct $G = (V, E)$, $V = \{0, 1, 2, \ldots, n-1\}$, and

$E = \{\{i, i+1\} \mid 0 \leq i \leq n-2\} \cup \{\{n-1, 0\}\} \cup \{\{i, i+n/2\} \mid 0 \leq i \leq n/2 - 1\}$

1. Take a particular value of n and picture the nodes of this graph written consecutively around the circumference of a circle
2. The edges described by $0 \leq i \leq n-2$ and $\{n-1, 0\}$ go between adjacent pairs around the circle
3. The edges described by $0 \leq i \leq n/2 - 1$ go between nodes of opposite sides of the circle

Note: use a circle to picture this figure and thus increase intuition

Proof by contradiction

- Assume that the theorem is false

Proof by contradiction

- Assume that the theorem is false
- Show that this assumption leads to an obviously false consequence called a contradiction

Proof by contradiction

- Assume that the theorem is false
- Show that this assumption leads to an obviously false consequence called a contradiction

Note: this kind of reasoning is often used in everyday life

Examples from everyday life

- Jacks sees Jill, who just come from outdoors

Examples from everyday life

- Jacks sees Jill, who just come from outdoors
- On observing that she is completely dry, he knows that it is not raining

Examples from everyday life

- Jacks sees Jill, who just come from outdoors
- On observing that she is completely dry, he knows that it is not raining
- His “proof" that it is not raining: if it were raining (the assumption) Jill would be wet (obvious false conclusion). Therefore it must not be raining

A mathematical proof

Theorem: $\sqrt{2}$ is irrational

A mathematical proof

Theorem: $\sqrt{2}$ is irrational

Proof: by contradiction

A mathematical proof

Theorem: $\sqrt{2}$ is irrational

Proof: by contradiction

Assume that $\sqrt{2} = m/n$, where m, n are integers, and have no common divisors (if they have we may simplify the fraction m/n by their common divisors)

Proof, continuation

1. Multiply both sides of the equality $\sqrt{2} = m/n$ by n, obtaining $n\sqrt{2} = m$

Proof, continuation

1. Multiply both sides of the equality $\sqrt{2} = m/n$ by n, obtaining $n\sqrt{2} = m$
2. Square both sides of the equality, obtaining $2n^2 = m^2$

Proof, continuation

1. Multiply both sides of the equality $\sqrt{2} = m/n$ by n, obtaining $n\sqrt{2} = m$
2. Square both sides of the equality, obtaining $2n^2 = m^2$
3. Because m^2 is $2n^2$ it result that m^2 is even, hence m is also even, i.e., $m = 2k$, (square of an odd number is always odd).

Proof, continuation

1. Multiply both sides of the equality $\sqrt{2} = m/n$ by n, obtaining $n\sqrt{2} = m$
2. Square both sides of the equality, obtaining $2n^2 = m^2$
3. Because m^2 is $2n^2$ it result that m^2 is even, hence m is also even, i.e., $m = 2k$, (square of an odd number is always odd).
4. Replacing m with $2k$ in the above equality we get: $2n^2 = (2k)^2 = 4k^2$

Proof, continuation

1. Multiply both sides of the equality $\sqrt{2} = m/n$ by n, obtaining $n\sqrt{2} = m$
2. Square both sides of the equality, obtaining $2n^2 = m^2$
3. Because m^2 is $2n^2$ it result that m^2 is even, hence m is also even, i.e., $m = 2k$, (square of an odd number is always odd).
4. Replacing m with $2k$ in the above equality we get: $2n^2 = (2k)^2 = 4k^2$
5. Dividing both sides by 2 we obtain $n^2 = 2k^2$, i.e. n is even.

Proof, continuation

1. Multiply both sides of the equality $\sqrt{2} = m/n$ by n, obtaining $n\sqrt{2} = m$
2. Square both sides of the equality, obtaining $2n^2 = m^2$
3. Because m^2 is $2n^2$ it result that m^2 is even, hence m is also even, i.e., $m = 2k$, (square of an odd number is always odd).
4. Replacing m with $2k$ in the above equality we get: $2n^2 = (2k)^2 = 4k^2$
5. Dividing both sides by 2 we obtain $n^2 = 2k^2$, i.e. n is even.
6. We have thus established that both m and n are even, i.e., they have a common divisor, what is a contradiction

Proof by induction

- This is an advanced proof-method used to show that all elements of a set have a specified property
- Examples:
  1. we may use the proof by induction to show that an arithmetic expression computes a desired quantity for every assignment to its variables, such as $\sum_{i=1}^{i=n} i = n(n+1)/2$
  2. we may proof by induction that a program works correctly at all steps for all inputs!

Proof by induction

- This is an advanced proof-method used to show that all elements of a set have a specified property
- Examples:
  1. we may use the proof by induction to show that an arithmetic expression computes a desired quantity for every assignment to its variables, such as $\sum_{i=1}^{i=n} i = n(n+1)/2$
  2. we may proof by induction that a program works correctly at all steps for all inputs!

Proof by induction

- This is an advanced proof-method used to show that all elements of a set have a specified property
- Examples:
  1. we may use the proof by induction to show that an arithmetic expression computes a desired quantity for every assignment to its variables, such as $\sum_{i=1}^{i=n} i = n(n+1)/2$
  2. we may proof by induction that a program works correctly at all steps for all inputs!

Illustration

Let us take the infinite set to be $\mathcal{N} = \{1, 2, \ldots\}$ and say that we want to show that a property P is true for all natural numbers, i.e., $P(k)$ is true for all $k \in \mathcal{N}$

Illustration

Let us take the infinite set to be $\mathcal{N} = \{1, 2, \ldots\}$ and say that we want to show that a property P is true for all natural numbers, i.e., $P(k)$ is true for all $k \in \mathcal{N}$

- Induction basis: show that $P(1)$ is true

Illustration

Let us take the infinite set to be $\mathcal{N} = \{1, 2, \ldots\}$ and say that we want to show that a property P is true for all natural numbers, i.e., $P(k)$ is true for all $k \in \mathcal{N}$

- Induction basis: show that $P(1)$ is true
- Induction step: show that for each $i \geq 1$, if $P(i)$ (called induction hypothesis) is true then so is $P(i + 1)$

Illustration

Let us take the infinite set to be $\mathcal{N} = \{1, 2, \ldots\}$ and say that we want to show that a property P is true for all natural numbers, i.e., $P(k)$ is true for all $k \in \mathcal{N}$

- Induction basis: show that $P(1)$ is true
- Induction step: show that for each $i \geq 1$, if $P(i)$ (called induction hypothesis) is true then so is $P(i + 1)$

When both of these parts are proved, it result that $P(i)$ is true for every $i \in \mathcal{N}$.

Question

Why can we conclude that $P(i)$ is true for all $i \in \mathcal{N}$?

Formal rationale

The mathematical foundation resides in the structure of $\mathcal{N}$, which is an inductive set:

...

Formal rationale

The mathematical foundation resides in the structure of $\mathcal{N}$, which is an inductive set:

Definition: A is inductive if:

$\ldots$

Formal rationale

The mathematical foundation resides in the structure of $\mathcal{N}$, which is an inductive set:

Definition: A is inductive if:

(1) $\emptyset \in A$ and

$\ldots$

Formal rationale

The mathematical foundation resides in the structure of $\mathcal{N}$, which is an inductive set:

Definition: A is inductive if:

(1) $\emptyset \in A$ and
(2) $\forall a \in A \Rightarrow succ(a) = \{a \cup \{a\}\} \in A$

$\ldots$

Formal rationale

The mathematical foundation resides in the structure of $\mathcal{N}$, which is an inductive set:

Definition: A is inductive if:

(1) $\emptyset \in A$ and
(2) $\forall a \in A \Rightarrow succ(a) = \{a \cup \{a\}\} \in A$

Construction: $\mathcal{N}$ was constructed by the rules:

...

Formal rationale

The mathematical foundation resides in the structure of $\mathcal{N}$, which is an inductive set:

Definition: A is inductive if:

(1) $\emptyset \in A$ and
(2) $\forall a \in A \Rightarrow succ(a) = \{a \cup \{a\}\} \in A$

Construction: $\mathcal{N}$ was constructed by the rules:

$0 = \emptyset$

$\ldots$

Formal rationale

The mathematical foundation resides in the structure of $\mathcal{N}$, which is an inductive set:

Definition: A is inductive if:

(1) $\emptyset \in A$ and
(2) $\forall a \in A \Rightarrow succ(a) = \{a \cup \{a\}\} \in A$

Construction: $\mathcal{N}$ was constructed by the rules:

$0 = \emptyset$

$1 = \{\emptyset\} = \{0\}$

$\ldots$

Formal rationale

The mathematical foundation resides in the structure of $\mathcal{N}$, which is an inductive set:

Definition: A is inductive if:

(1) $\emptyset \in A$ and
(2) $\forall a \in A \Rightarrow succ(a) = \{a \cup \{a\}\} \in A$

Construction: $\mathcal{N}$ was constructed by the rules:

$0 = \emptyset$

$1 = \{\emptyset\} = \{0\}$

$2 = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$

$\ldots$

Formal rationale

The mathematical foundation resides in the structure of $\mathcal{N}$, which is an inductive set:

Definition: A is inductive if:

(1) $\emptyset \in A$ and
(2) $\forall a \in A \Rightarrow succ(a) = \{a \cup \{a\}\} \in A$

Construction: $\mathcal{N}$ was constructed by the rules:

$0 = \emptyset$

$1 = \{\emptyset\} = \{0\}$

$2 = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$

$3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\}$

$\ldots$

Intuitive rationale

1. $P(1)$ is true in virtue of Induction basis
2. If $P(1)$ is true then $P(2)$ is true in virtue of Induction step
3. If $P(2)$ is true then $P(3)$ is true in virtue of Induction step
4. The process can continue for all natural numbers

Intuitive rationale

1. $P(1)$ is true in virtue of Induction basis
2. If $P(1)$ is true then $P(2)$ is true in virtue of Induction step
3. If $P(2)$ is true then $P(3)$ is true in virtue of Induction step
4. The process can continue for all natural numbers

Intuitive rationale

1. $P(1)$ is true in virtue of Induction basis
2. If $P(1)$ is true then $P(2)$ is true in virtue of Induction step
3. If $P(2)$ is true then $P(3)$ is true in virtue of Induction step
4. The process can continue for all natural numbers

Variations and generalizations

- The Induction basis doesn't necessarily need to start with 1; it may start with any value b. In this case Induction step must show that $P(k)$ implies $P(k+1)$ for $k \geq b$

Variations and generalizations

- The Induction basis doesn't necessarily need to start with 1; it may start with any value b. In this case Induction step must show that $P(k)$ implies $P(k+1)$ for $k \geq b$
- Sometimes a stronger induction hypothesis is useful, such as $P(j)$ for all $j \leq i$

Variations and generalizations

- The Induction basis doesn't necessarily need to start with 1; it may start with any value b. In this case Induction step must show that $P(k)$ implies $P(k+1)$ for $k \geq b$
- Sometimes a stronger induction hypothesis is useful, such as $P(j)$ for all $j \leq i$
- One can use instead of $\mathcal{N}$ a set isomorphic with $\mathcal{N}$; one can also generalize $\mathcal{N}$ to a transitive set A.

  Transitive set: A is transitive if $\forall a \in A \wedge \forall x \in a \Rightarrow x \in A$

Application

We will prove by induction the correctness of the formula used to calculate the size of the monthly payments of mortgages

Application

We will prove by induction the correctness of the formula used to calculate the size of the monthly payments of mortgages

Application

We will prove by induction the correctness of the formula used to calculate the size of the monthly payments of mortgages

Observations

- For investment reasons people borrow money (called loan) and repay the loan over a certain number of years

Observations

- For investment reasons people borrow money (called loan) and repay the loan over a certain number of years
- The terms of such repayments stipulate that a fixed amount of money is payed each month to cover the interest as well as the part of the original sum so that total is repayed in say 30 years

Observations

- For investment reasons people borrow money (called loan) and repay the loan over a certain number of years
- The terms of such repayments stipulate that a fixed amount of money is payed each month to cover the interest as well as the part of the original sum so that total is repayed in say 30 years
- Formula for calculating monthly payments is shrouded in mystery. But it is actually quite simple. We will show by induction that it is correct

Notations

- Let P be the principal,i.e., the amount of the original loan

Notations

- Let P be the principal,i.e., the amount of the original loan
- Let I be the yearly interest rate of the loan. The value $I = 0.06$ indicates a 6% interest rate

Notations

- Let P be the principal,i.e., the amount of the original loan
- Let I be the yearly interest rate of the loan. The value $I = 0.06$ indicates a 6% interest rate
- Let Y be the monthly payment

Things happening each month

- The amount of loan tends to increase because of the monthly multiplier

Things happening each month

- The amount of loan tends to increase because of the monthly multiplier
- The amount of loan tends to decrease because of the monthly payment

Things happening each month

- The amount of loan tends to increase because of the monthly multiplier
- The amount of loan tends to decrease because of the monthly payment
- Let P_t be the amount of the loan outstanding after the t-th month

Relationships

- $P_0 = P$, i.e., no loan has been payed

Relationships

- $P_0 = P$, i.e., no loan has been payed
- $P_1 = MP_0 - Y$, is the amount of loan after one month

Relationships

- $P_0 = P$, i.e., no loan has been payed
- $P_1 = MP_0 - Y$, is the amount of loan after one month
- $P_2 = MP_1 - Y$ is the amount of loan after 2 months

Putting all together

Theorem 0.5 For each $t \geq 0$,

$$P_t = PM^t - Y(\frac{M^t - 1}{M - 1})$$

Proof: By induction

- Induction basis: Prove that formula is true for $t = 0$.
  Proof: replacing $t = 0$ in the formula and observing that $M^0 = 1$ we obtain $P_0 = P$

Putting all together

Theorem 0.5 For each $t \geq 0$,

$$P_t = PM^t - Y(\frac{M^t - 1}{M - 1})$$

Proof: By induction

- Induction basis: Prove that formula is true for $t = 0$.
  Proof: replacing $t = 0$ in the formula and observing that $M^0 = 1$ we obtain $P_0 = P$

Putting all together

Theorem 0.5 For each $t \geq 0$,

$$P_t = PM^t - Y(\frac{M^t - 1}{M - 1})$$

Proof: By induction

- Induction basis: Prove that formula is true for $t = 0$.
  Proof: replacing $t = 0$ in the formula and observing that $M^0 = 1$ we obtain $P_0 = P$

Proof, continuation

- Induction step: For each $k \geq 0$ assume that the formula is true for $t = k$ and show that then it is true for $t = k + 1$; the induction hypothesis states that:
  $P_k = PM^k - Y(\frac{M^k-1}{M-1})$ implies $P_{k+1} = PM^{k+1} - Y(\frac{M^{k+1}-1}{M-1})$

Proof, continuation

- Induction step: For each $k \geq 0$ assume that the formula is true for $t = k$ and show that then it is true for $t = k + 1$; the induction hypothesis states that:
  $P_k = PM^k - Y(\frac{M^k - 1}{M - 1})$ implies $P_{k+1} = PM^{k+1} - Y(\frac{M^{k+1} - 1}{M - 1})$
  1. From the definition we have: $P_{k+1} = P_k M - Y$

Proof, continuation

- Induction step: For each $k \geq 0$ assume that the formula is true for $t = k$ and show that then it is true for $t = k + 1$; the induction hypothesis states that:
  $P_k = PM^k - Y(\frac{M^k - 1}{M-1})$ implies $P_{k+1} = PM^{k+1} - Y(\frac{M^{k+1} - 1}{M-1})$
  1. From the definition we have: $P_{k+1} = P_k M - Y$
  2. Using the induction hypothesis to calculate P_k we get $P_{k+1} = [PM^k - Y(\frac{M^k - 1}{M-1})]M - Y$