Discrete Mathematics

Rules of Inference and Mathematical Proofs

(c) Marcin Sydow

Contents

- Proofs
- Rules of inference
- Proof types

Proof

A **mathematical proof** is a (logical) procedure to establish the truth of a mathematical statement.

Proof

A **mathematical proof** is a (logical) procedure to establish the truth of a mathematical statement.

Theorem - a true (proven) mathematical statement.

Proof

A **mathematical proof** is a (logical) procedure to establish the truth of a mathematical statement.

Theorem - a true (proven) mathematical statement.

Lemma - a small, helper (technical) theorem.

Proof

A **mathematical proof** is a (logical) procedure to establish the truth of a mathematical statement.

Theorem - a true (proven) mathematical statement.

Lemma - a small, helper (technical) theorem.

Conjecture - a statement that has not been proven (but is suspected to be true)

Formal proof

Let $P = \{P_1, P_2, ..., P_m\}$ be a set of **premises** or **axioms** and let C be a **conclusion** do be proven.

Formal proof

Let $P = \{P_1, P_2, ..., P_m\}$ be a set of **premises** or **axioms** and let C be a **conclusion** do be proven.

A **formal proof** of the conclusion C based on the set of premises and axioms P is a sequence $S = \{S_1, S_2, ..., S_n\}$ of logical statements so that each statement S_i is either:

Formal proof

Let $P = \{P_1, P_2, ..., P_m\}$ be a set of **premises** or **axioms** and let C be a **conclusion** do be proven.

A **formal proof** of the conclusion C based on the set of premises and axioms P is a sequence $S = \{S_1, S_2, ..., S_n\}$ of logical statements so that each statement S_i is either:

- a premise or axiom from the set P
- a tautology
- a subconclusion **derived from** (some of) the previous statements S_k, $k < i$ in the sequence using some of the allowed **inference rules** or **substitution rules**.

Substition rules

The following rules make it possible to build "new" tautologies out of the existing ones.

- If a compound proposition P is a tautology and all the occurrences of some specific variable of P are substituted with the same proposition E, then the resulting compound proposition is also a tautology.

Substition rules

The following rules make it possible to build “new” tautologies out of the existing ones.

- If a compound proposition P is a tautology and all the occurrences of some specific variable of P are substituted with the same proposition E, then the resulting compound proposition is also a tautology.
- If a compound proposition P is a tautology and contains another proposition Q and all the occurrences of Q are substituted with another proposition Q^* that is logically equivalent to Q, then the resulting compound proposition is also a tautology.

Inference rules 1

The following rules make it possible to derive next steps of a proof based on the previous steps or premises and axioms:

Rule of inference	Tautology	Name
$\frac{p \wedge q}{\therefore p}$	$(p \wedge q) \to p$	simplification

Inference rules 1

The following rules make it possible to derive next steps of a proof based on the previous steps or premises and axioms:

Rule of inference	Tautology	Name
$\dfrac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	simplification
$\dfrac{\begin{array}{c} p \\ q \end{array}}{\therefore p \wedge q}$	$[(p) \wedge (q)] \rightarrow (p \wedge q)$	conjunction

Inference rules 1

The following rules make it possible to derive next steps of a proof based on the previous steps or premises and axioms:

Rule of inference	Tautology	Name
$\frac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	simplification
$\frac{p \quad q}{\therefore p \wedge q}$	$[(p) \wedge (q)] \rightarrow (p \wedge q)$	conjunction
$\frac{p}{\therefore p \vee q}$	$p \rightarrow (p \vee q)$	addition

Inference rules 1

The following rules make it possible to derive next steps of a proof based on the previous steps or premises and axioms:

Rule of inference	Tautology	Name
$\dfrac{p \wedge q}{\therefore p}$	$(p \wedge q) \to p$	simplification
$\dfrac{p \quad q}{\therefore p \wedge q}$	$[(p) \wedge (q)] \to (p \wedge q)$	conjunction
$\dfrac{p}{\therefore p \vee q}$	$p \to (p \vee q)$	addition
$\dfrac{p \vee q \quad \neg p \vee r}{\therefore q \vee r}$	$[(p \vee q) \wedge (\neg p \vee r)] \to (q \vee r)$	resolution

(to be continued on the next slide)

Inference rules 2

Rule of inference	Tautology	Name
p $p \to q$ $\therefore q$	$[p \wedge (p \to q)] \to q$	Modus ponens

Inference rules 2

Rule of inference	Tautology	Name
p $\underline{p \rightarrow q}$ $\therefore q$	$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus ponens
$\neg q$ $\underline{p \rightarrow q}$ $\therefore \neg p$	$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	Modus tollens

Inference rules 2

Rule of inference	Tautology	Name
p $\underline{p \to q}$ $\therefore q$	$[p \land (p \to q)] \to q$	Modus ponens
$\neg q$ $\underline{p \to q}$ $\therefore \neg p$	$[\neg q \land (p \to q)] \to \neg p$	Modus tollens
$p \to q$ $\underline{q \to r}$ $\therefore p \to q$	$[(p \to q) \land (q \to r)] \to (p \to r)$	Hypothetical syllogism

Inference rules 2

Rule of inference	Tautology	Name
p $p \rightarrow q$ $\therefore q$	$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus ponens
$\neg q$ $p \rightarrow q$ $\therefore \neg p$	$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	Modus tollens
$p \rightarrow q$ $q \rightarrow r$ $\therefore p \rightarrow q$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore q$	$[(p \vee q) \wedge \neg p] \rightarrow q$	Disjunctive syllogism

Inference rules for quantified predicates

Rule of inference	Name
$$\frac{\forall_x P(x)}{\therefore P(c)}$$	Universal instantiation

Inference rules for quantified predicates

Rule of inference	Name
$\dfrac{\forall_x P(x)}{\therefore P(c)}$	Universal instantiation
$\dfrac{P(c) \text{ for an arbitrary c}}{\therefore \forall_x P(x)}$	Universal generalization

Inference rules for quantified predicates

Rule of inference	Name
$\dfrac{\forall_x P(x)}{\therefore P(c)}$	Universal instantiation
$\dfrac{P(c) \text{ for an arbitrary c}}{\therefore \forall_x P(x)}$	Universal generalization
$\dfrac{\exists_x P(x)}{\therefore P(c) \textit{ for some element } c}$	Existential instantiation

Inference rules for quantified predicates

Rule of inference	Name
$\dfrac{\forall_x P(x)}{\therefore P(c)}$	Universal instantiation
$\dfrac{P(c) \text{ for an arbitrary c}}{\therefore \forall_x P(x)}$	Universal generalization
$\dfrac{\exists_x P(x)}{\therefore P(c) \textit{ for some element } c}$	Existential instantiation
$\dfrac{P(c) \text{ for some element c}}{\therefore \exists_x P(x)}$	Existential generalization

Types of proof of implication

Assume that theorem is of the form:

$$P \Rightarrow C$$

(where $P = P_1 \wedge P_2 \wedge ...P_m$ is the conjunction of premises and axioms, and C is the conclusion to be proven)

Types of proof of implication

Assume that theorem is of the form:

$$P \Rightarrow C$$

(where $P = P_1 \wedge P_2 \wedge ...P_m$ is the conjunction of premises and axioms, and C is the conclusion to be proven)

The proof can have various forms, e.g.:

Types of proof of implication

Assume that theorem is of the form:

$$P \Rightarrow C$$

(where $P = P_1 \wedge P_2 \wedge ...P_m$ is the conjunction of premises and axioms, and C is the conclusion to be proven)

The proof can have various forms, e.g.:

- direct proof (using P to directly show C)

Types of proof of implication

Assume that theorem is of the form:

$$P \Rightarrow C$$

(where $P = P_1 \wedge P_2 \wedge ...P_m$ is the conjunction of premises and axioms, and C is the conclusion to be proven)

The proof can have various forms, e.g.:

- direct proof (using P to directly show C)
- indirect proof

Types of proof of implication

Assume that theorem is of the form:

$$P \Rightarrow C$$

(where $P = P_1 \wedge P_2 \wedge ... P_m$ is the conjunction of premises and axioms, and C is the conclusion to be proven)

The proof can have various forms, e.g.:

- direct proof (using P to directly show C)
- indirect proof
  - proof by contraposition (proving contrapostion $\neg C \Rightarrow \neg P$

Types of proof of implication

Assume that theorem is of the form:

$$P \Rightarrow C$$

(where $P = P_1 \wedge P_2 \wedge ...P_m$ is the conjunction of premises and axioms, and C is the conclusion to be proven)

The proof can have various forms, e.g.:

- direct proof (using P to directly show C)
- indirect proof
  - proof by contraposition (proving contrapostion $\neg C \Rightarrow \neg P$
  - proof by contradiction (reductio ad absurdum) (showing that $P \wedge \neg C$ leads to false (absurd))

Types of proof of implication

Assume that theorem is of the form:

$$P \Rightarrow C$$

(where $P = P_1 \wedge P_2 \wedge ...P_m$ is the conjunction of premises and axioms, and C is the conclusion to be proven)

The proof can have various forms, e.g.:

- direct proof (using P to directly show C)
- indirect proof
  - proof by contraposition (proving contrapostion $\neg C \Rightarrow \neg P$
  - proof by contradiction (reductio ad absurdum) (showing that $P \wedge \neg C$ leads to false (absurd))

Another proof scheme is “proof by cases” (when different cases are treated separately).

Example of a direct proof

Theorem: if n is odd integer then n^2 is odd.
(what is the mathematical form of the above statement?)

Example of a direct proof

Theorem: if n is odd integer then n^2 is odd.
(what is the mathematical form of the above statement?)
(actually more formally it is:
$\forall n \in Z(\exists k \in Z\ n = (2k+1)) \rightarrow (\exists m \in Z\ n^2 = (2m+1)))$

Example of a direct proof

Theorem: if n is odd integer then n^2 is odd.
(what is the mathematical form of the above statement?)
(actually more formally it is:
$\forall n \in Z (\exists k \in Z\ n = (2k+1)) \to (\exists m \in Z\ n^2 = (2m+1)))$
$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ (thus $m = (2k^2 + 2k)$)

Example of a direct proof

Theorem: if n is odd integer then n^2 is odd.
(what is the mathematical form of the above statement?)
(actually more formally it is:
$\forall n \in Z(\exists k \in Z\ n = (2k+1)) \rightarrow (\exists m \in Z\ n^2 = (2m+1)))$
$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ (thus $m = (2k^2 + 2k)$)

Another example: "if m and n are squares then mn is square"

Example of direct proof

"Sum of two rationals is rational"

Example of direct proof

"Sum of two rationals is rational"
x is rational if there exist two integers p,q so that $x = p/q$

Example of direct proof

"Sum of two rationals is rational"
x is rational if there exist two integers p,q so that $x = p/q$
(it is easy to use basic algebra to show that $x + y$ is also rational)

Logical identities useful in proving implications

Identity:	Name:
$(p \to q) \Leftrightarrow (\neg q \to \neg p)$	contraposition

Logical identities useful in proving implications

Identity:	Name:
$(p \rightarrow q) \Leftrightarrow (\neg q \rightarrow \neg p)$	contraposition
$(p \rightarrow q) \Leftrightarrow (\neg p \vee q)$	implication as alternative

Logical identities useful in proving implications

Identity:	Name:
$(p \to q) \Leftrightarrow (\neg q \to \neg p)$	contraposition
$(p \to q) \Leftrightarrow (\neg p \vee q)$	implication as alternative
$(p \to q) \Leftrightarrow \neg(p \wedge \neg q)$	implication as conjuction

Logical identities useful in proving implications

Identity:	Name:
$(p \to q) \Leftrightarrow (\neg q \to \neg p)$	contraposition
$(p \to q) \Leftrightarrow (\neg p \vee q)$	implication as alternative
$(p \to q) \Leftrightarrow \neg(p \wedge \neg q)$	implication as conjuction
$[p \to (q \wedge r)] \Leftrightarrow [(p \to q) \wedge (p \to r)]$	splitting a conjunction

Logical identities useful in proving implications

Identity:	Name:
$(p \to q) \Leftrightarrow (\neg q \to \neg p)$	contraposition
$(p \to q) \Leftrightarrow (\neg p \vee q)$	implication as alternative
$(p \to q) \Leftrightarrow \neg(p \wedge \neg q)$	implication as conjuction
$[p \to (q \wedge r)] \Leftrightarrow [(p \to q) \wedge (p \to r)]$	splitting a conjunction
$(p \to q) \Leftrightarrow [(p \wedge \neg q) \to F]$	reductio ad absurdum

Logical identities useful in proving implications

Identity:	Name:
$(p \rightarrow q) \Leftrightarrow (\neg q \rightarrow \neg p)$	contraposition
$(p \rightarrow q) \Leftrightarrow (\neg p \vee q)$	implication as alternative
$(p \rightarrow q) \Leftrightarrow \neg(p \wedge \neg q)$	implication as conjuction
$[p \rightarrow (q \wedge r)] \Leftrightarrow [(p \rightarrow q) \wedge (p \rightarrow r)]$	splitting a conjunction
$(p \rightarrow q) \Leftrightarrow [(p \wedge \neg q) \rightarrow F]$	reductio ad absurdum
$[(p \wedge q) \rightarrow r] \Leftrightarrow [p \rightarrow (q \rightarrow r)]$	exportation law

Logical identities useful in proving implications

Identity:	Name:
$(p \to q) \Leftrightarrow (\neg q \to \neg p)$	contraposition
$(p \to q) \Leftrightarrow (\neg p \vee q)$	implication as alternative
$(p \to q) \Leftrightarrow \neg(p \wedge \neg q)$	implication as conjuction
$[p \to (q \wedge r)] \Leftrightarrow [(p \to q) \wedge (p \to r)]$	splitting a conjunction
$(p \to q) \Leftrightarrow [(p \wedge \neg q) \to F]$	reductio ad absurdum
$[(p \wedge q) \to r] \Leftrightarrow [p \to (q \to r)]$	exportation law
$(p \leftrightarrow q) \Leftrightarrow [(p \to q) \wedge (q \to p)]$	bidirectional as implications

The last identity gives a schema for proving equivalences.

Logical identities useful in proving implications

Identity:	Name:
$(p \to q) \Leftrightarrow (\neg q \to \neg p)$	contraposition
$(p \to q) \Leftrightarrow (\neg p \vee q)$	implication as alternative
$(p \to q) \Leftrightarrow \neg(p \wedge \neg q)$	implication as conjuction
$[p \to (q \wedge r)] \Leftrightarrow [(p \to q) \wedge (p \to r)]$	splitting a conjunction
$(p \to q) \Leftrightarrow [(p \wedge \neg q) \to F]$	reductio ad absurdum
$[(p \wedge q) \to r] \Leftrightarrow [p \to (q \to r)]$	exportation law
$(p \leftrightarrow q) \Leftrightarrow [(p \to q) \wedge (q \to p)]$	bidirectional as implications

The last identity gives a schema for proving equivalences.

The above identities serve as a basis for various types of proofs, e.g.:

- indirect proof by contraposition (by proving the negation of the premise from the negation of the conclusion)

Logical identities useful in proving implications

Identity:	Name:
$(p \to q) \Leftrightarrow (\neg q \to \neg p)$	contraposition
$(p \to q) \Leftrightarrow (\neg p \lor q)$	implication as alternative
$(p \to q) \Leftrightarrow \neg(p \land \neg q)$	implication as conjuction
$[p \to (q \land r)] \Leftrightarrow [(p \to q) \land (p \to r)]$	splitting a conjunction
$(p \to q) \Leftrightarrow [(p \land \neg q) \to F]$	reductio ad absurdum
$[(p \land q) \to r] \Leftrightarrow [p \to (q \to r)]$	exportation law
$(p \leftrightarrow q) \Leftrightarrow [(p \to q) \land (q \to p)]$	bidirectional as implications

The last identity gives a schema for proving equivalences.
The above identities serve as a basis for various types of proofs, e.g.:

- indirect proof by contraposition (by proving the negation of the premise from the negation of the conclusion)
- indirect "vacuous proof" (by observing that the premise is false)

Logical identities useful in proving implications

Identity:	Name:
$(p \to q) \Leftrightarrow (\neg q \to \neg p)$	contraposition
$(p \to q) \Leftrightarrow (\neg p \vee q)$	implication as alternative
$(p \to q) \Leftrightarrow \neg(p \wedge \neg q)$	implication as conjuction
$[p \to (q \wedge r)] \Leftrightarrow [(p \to q) \wedge (p \to r)]$	splitting a conjunction
$(p \to q) \Leftrightarrow [(p \wedge \neg q) \to F]$	reductio ad absurdum
$[(p \wedge q) \to r] \Leftrightarrow [p \to (q \to r)]$	exportation law
$(p \leftrightarrow q) \Leftrightarrow [(p \to q) \wedge (q \to p)]$	bidirectional as implications

The last identity gives a schema for proving equivalences.
The above identities serve as a basis for various types of proofs, e.g.:

- indirect proof by contraposition (by proving the negation of the premise from the negation of the conclusion)
- indirect "vacuous proof" (by observing that the premise is false)
- indirect "trivial proof" (by ignoring the premise)

Logical identities useful in proving implications

Identity:	Name:
$(p \to q) \Leftrightarrow (\neg q \to \neg p)$	contraposition
$(p \to q) \Leftrightarrow (\neg p \vee q)$	implication as alternative
$(p \to q) \Leftrightarrow \neg(p \wedge \neg q)$	implication as conjuction
$[p \to (q \wedge r)] \Leftrightarrow [(p \to q) \wedge (p \to r)]$	splitting a conjunction
$(p \to q) \Leftrightarrow [(p \wedge \neg q) \to F]$	reductio ad absurdum
$[(p \wedge q) \to r] \Leftrightarrow [p \to (q \to r)]$	exportation law
$(p \leftrightarrow q) \Leftrightarrow [(p \to q) \wedge (q \to p)]$	bidirectional as implications

The last identity gives a schema for proving equivalences.
The above identities serve as a basis for various types of proofs, e.g.:

- indirect proof by contraposition (by proving the negation of the premise from the negation of the conclusion)
- indirect "vacuous proof" (by observing that the premise is false)
- indirect "trivial proof" (by ignoring the premise)
- indirect proof "by contradiction" (by showing that the negation of the conclusion leads to a contradiction)

Example of the need for indirect proofs

Prove: “for any integer n: if 3n+2 is odd then n is odd”

Example of the need for indirect proofs

Prove: "for any integer n: if 3n+2 is odd then n is odd"
(how to prove it with a direct proof?)

Example of the need for indirect proofs

Prove: “for any integer n: if 3n+2 is odd then n is odd”
(how to prove it with a direct proof?)
(it is not easy to construct a direct proof, but an indirect proof can be easily presented)

Example of a proof by contraposition

Prove: "for any integer n: if 3n+2 is odd then n is odd" (example of indirect proof):

Example of a proof by contraposition

Prove: "for any integer n: if 3n+2 is odd then n is odd"
(example of indirect proof):
(by contraposition):

Example of a proof by contraposition

Prove: "for any integer n: if 3n+2 is odd then n is odd" (example of indirect proof):
(by contraposition): Assume n is even: $\exists k \in Z\ n = 2k$, which implies: $3n + 2 = 3(2k) + 2 = 2(3k) + 2 = 2(3k + 1) = 2(l)$ (where $l = 3k + 1$) what would imply that the number $3n + 2$ is also an even number (contraposition)

Example of a *vacuous proof*

(when the hypothesis of the implication is false)

[1] a proof technique that will be presented later

Example of a *vacuous proof*

(when the hypothesis of the implication is false)
define a predicate P(n): if $n > 1$ then $n^2 > n$ $(n \in Z)$

[1] a proof technique that will be presented later

Example of a *vacuous proof*

(when the hypothesis of the implication is false)
define a predicate P(n): if $n > 1$ then $n^2 > n$ $(n \in Z)$
Prove P(0).

[1] a proof technique that will be presented later

Example of a *vacuous proof*

(when the hypothesis of the implication is false)
define a predicate P(n): if $n > 1$ then $n^2 > n$ $(n \in Z)$
Prove P(0).
The hypothesis $n > 1$ is false so the implication is automatically true.

[1] a proof technique that will be presented later

Example of a *vacuous proof*

(when the hypothesis of the implication is false)
define a predicate P(n): if $n > 1$ then $n^2 > n$ $(n \in Z)$
Prove P(0).
The hypothesis $n > 1$ is false so the implication is automatically true.
Vacuous proofs are useful for example for proving the base step in *mathematical induction*[1]

[1] a proof technique that will be presented later

An example of a *trivial proof*

(when the the hypothesis of the implication can be ignored)

An example of a *trivial proof*

(when the the hypothesis of the implication can be ignored) define the predicate: P(n): for all positive integers a,b and natural number n it holds that: $a \geq b \Rightarrow a^n \geq b^n$.

An example of a *trivial proof*

(when the the hypothesis of the implication can be ignored)
define the predicate: P(n): for all positive integers a,b and natural number n it holds that: $a \geq b \Rightarrow a^n \geq b^n$.
Prove P(0)

An example of a *trivial proof*

(when the the hypothesis of the implication can be ignored)
define the predicate: P(n): for all positive integers a,b and natural number n it holds that: $a \geq b \Rightarrow a^n \geq b^n$.
Prove P(0)
$a^0 = 1 = b^0$ so that the conclusion is true without the hypothesis assumption

Example of a proof by contradiction

"$\sqrt{2}$ is irrational"

Example of a proof by contradiction

"$\sqrt{2}$ is irrational"
(we use the fact that each natural n > 1 is a unique product of prime numbers)
Suppose that it is not true, i.e. $\sqrt{2} = a/b$ for some $a, b \in Z$ and a, b have no common factors (except 1).

Example of a proof by contradiction

"$\sqrt{2}$ is irrational"
(we use the fact that each natural n > 1 is a unique product of prime numbers)
Suppose that it is not true, i.e. $\sqrt{2} = a/b$ for some $a, b \in Z$ and a, b have no common factors (except 1).
$2 = a^2/b^2$ so $2b^2 = a^2$, so a^2 is even (divisible by 2). But this implies that b must also be divisible by 2, what contradicts the assumption.

Example of a proof by contradiction

"$\sqrt{2}$ is irrational"
(we use the fact that each natural n > 1 is a unique product of prime numbers)
Suppose that it is not true, i.e. $\sqrt{2} = a/b$ for some $a, b \in Z$ and a, b have no common factors (except 1).
$2 = a^2/b^2$ so $2b^2 = a^2$, so a^2 is even (divisible by 2). But this implies that b must also be divisible by 2, what contradicts the assumption.
Thus negating the thesis leads to a contradiction.

Proofs of existential statements

If the conclusion is of the form "there exists some object that has some properties" ($\exists$), the proof can be:

Proofs of existential statements

If the conclusion is of the form “there exists some object that has some properties” ($\exists$), the proof can be:

- **constructive** (by directly presenting an object having the properties or presenting a sure way in which such object can be constructed)

Proofs of existential statements

If the conclusion is of the form “there exists some object that has some properties” ($\exists$), the proof can be:

- **constructive** (by directly presenting an object having the properties or presenting a sure way in which such object can be constructed)
- **unconstructive** (without constructing or presenting the object)

Example of a constructive proof

"There exists pair of rational numbers x,y so that x^y is irrational"
Proof (constructive): x = 2, y = 1/2

Example of a non-constructive proof

“There exist irrational numbers x and y so that x^y is rational.

Example of a non-constructive proof

"There exist irrational numbers x and y so that x^y is rational. Proof: (use the premise that $\sqrt{2}$ is irrational that was proven before) Let's define $x = \sqrt{2}^{\sqrt{2}}$. If x is rational, this ends the proof. If x is irrational, then $x^{\sqrt{2}} = 2$ so that we found another pair.

Example of a non-constructive proof

"There exist irrational numbers x and y so that x^y is rational. Proof: (use the premise that $\sqrt{2}$ is irrational that was proven before) Let's define $x = \sqrt{2}^{\sqrt{2}}$. If x is rational, this ends the proof. If x is irrational, then $x^{\sqrt{2}} = 2$ so that we found another pair.
Notice: we do not know which case it true, but we've proven that at least one pair must exist!

Proofs of universal statements

If the conclusion to be proven starts with the universal quantifier $\forall$, we can **disprove** it (prove it is false) by finding a **counterexample** (it is an allowed value of the quantified variable that falsifies the statement).

Proofs of universal statements

If the conclusion to be proven starts with the universal quantifier $\forall$, we can **disprove** it (prove it is false) by finding a **counterexample** (it is an allowed value of the quantified variable that falsifies the statement).

To make a positive proof of a universal statement, if the domain is infinite, it is not possible to prove it for all cases. Instead, the negation of it can be falsified, for example.

Proving lists of equivalent statements

Some theorems have the form:

"*The following statements are equivalent:* $S_1, S_2, ..., S_n$."

Proving lists of equivalent statements

Some theorems have the form:

"*The following statements are equivalent:* $S_1, S_2, ..., S_n$."

A typical proof of such theorems is usually in the form of the following sequence:
$S_1 \Rightarrow S_2, ..., S_{n-1} \Rightarrow S_n, S_n \Rightarrow S_1$

Example of such theorem from graph theory:

The following conditions are equivalent:

Proving lists of equivalent statements

Some theorems have the form:

"*The following statements are equivalent:* $S_1, S_2, ..., S_n$."

A typical proof of such theorems is usually in the form of the following sequence:
$S_1 \Rightarrow S_2, ..., S_{n-1} \Rightarrow S_n, S_n \Rightarrow S_1$

Example of such theorem from graph theory:

The following conditions are equivalent:

- graph G is a tree

Proving lists of equivalent statements

Some theorems have the form:

"*The following statements are equivalent:* $S_1, S_2, ..., S_n$."

A typical proof of such theorems is usually in the form of the following sequence:
$S_1 \Rightarrow S_2, ..., S_{n-1} \Rightarrow S_n, S_n \Rightarrow S_1$

Example of such theorem from graph theory:

The following conditions are equivalent:

- graph G is a tree
- graph G is acyclic and connected

Proving lists of equivalent statements

Some theorems have the form:

"*The following statements are equivalent:* $S_1, S_2, ..., S_n$."

A typical proof of such theorems is usually in the form of the following sequence:
$S_1 \Rightarrow S_2, ..., S_{n-1} \Rightarrow S_n, S_n \Rightarrow S_1$

Example of such theorem from graph theory:

The following conditions are equivalent:

- graph G is a tree
- graph G is acyclic and connected
- graph G is connected and has exactly $|V| - 1$ edges

Proving lists of equivalent statements

Some theorems have the form:

"*The following statements are equivalent:* $S_1, S_2, ..., S_n$."

A typical proof of such theorems is usually in the form of the following sequence:

$S_1 \Rightarrow S_2, ..., S_{n-1} \Rightarrow S_n, S_n \Rightarrow S_1$

Example of such theorem from graph theory:

The following conditions are equivalent:

- graph G is a tree
- graph G is acyclic and connected
- graph G is connected and has exactly $|V| - 1$ edges
- each edge in G is a bridge

Proving lists of equivalent statements

Some theorems have the form:

"*The following statements are equivalent:* $S_1, S_2, ..., S_n$."

A typical proof of such theorems is usually in the form of the following sequence:
$S_1 \Rightarrow S_2, ..., S_{n-1} \Rightarrow S_n, S_n \Rightarrow S_1$

Example of such theorem from graph theory:

The following conditions are equivalent:

- graph G is a tree
- graph G is acyclic and connected
- graph G is connected and has exactly $|V| - 1$ edges
- each edge in G is a bridge
- each pair of 2 vertices in G is connected by exactly 1 simple path

Proving lists of equivalent statements

Some theorems have the form:

"*The following statements are equivalent:* $S_1, S_2, ..., S_n$."

A typical proof of such theorems is usually in the form of the following sequence:
$S_1 \Rightarrow S_2, ..., S_{n-1} \Rightarrow S_n, S_n \Rightarrow S_1$

Example of such theorem from graph theory:

The following conditions are equivalent:

- graph G is a tree
- graph G is acyclic and connected
- graph G is connected and has exactly $|V| - 1$ edges
- each edge in G is a bridge
- each pair of 2 vertices in G is connected by exactly 1 simple path
- adding any edge to G makes exactly 1 new cycle

Example: Proving set inclusion and set equality

To prove that some set is included in another set: $A \subseteq B$ it is enough to use the definition of inclusion. Thus, it is enough to prove the implication:
$\forall_x x \in A \Rightarrow x \in B$ (where x is any element of the universe)

Example: Proving set inclusion and set equality

To prove that some set is included in another set: $A \subseteq B$ it is enough to use the definition of inclusion. Thus, it is enough to prove the implication:
$\forall_x x \in A \Rightarrow x \in B$ (where x is any element of the universe)

To prove equality of two sets: $A = B$ it is enough to prove two set inclusions: $A \subseteq B$ and $B \subseteq A$, thus it is enough to prove the two implications of the above form.

Russels antinomy

There does not exist the set of all sets.[2]

[2] we call the family of all the sets *class*

Russels antinomy

There does not exist the set of all sets.[2]
Russel's antinomy:

$$Z = \{x : x \notin x\}$$

Does Z belong to itself?

[2] we call the family of all the sets *class*

Russels antinomy

There does not exist the set of all sets.[2]
Russel's antinomy:

$$Z = \{x : x \notin x\}$$

Does Z belong to itself?
$x \in Z \Leftrightarrow x \notin x$

[2] we call the family of all the sets *class*

Russels antinomy

There does not exist the set of all sets.[2]
Russel's antinomy:

$$Z = \{x : x \notin x\}$$

Does Z belong to itself?
$x \in Z \Leftrightarrow x \notin x$
$Z \in Z \Leftrightarrow Z \notin Z$
(a contradiction)

[2] we call the family of all the sets *class*

Russels antinomy

There does not exist the set of all sets.[2]
Russel's antinomy:

$$Z = \{x : x \notin x\}$$

Does Z belong to itself?
$x \in Z \Leftrightarrow x \notin x$
$Z \in Z \Leftrightarrow Z \notin Z$
(a contradiction)
Thus the existence of the set Z led to a contradiction.

[2] we call the family of all the sets *class*

Basic Axioms of Set Algebra

Primitive concepts:

- element of set
- the relation of "belonging to the set" ($x \in X$)

Basic Axioms of Set Algebra

Primitive concepts:

- element of set
- the relation of "belonging to the set" ($x \in X$)

1. Uniqueness Axiom (Axiom of extensionality): If the sets A and B have the same elements then A and B are identical.

Basic Axioms of Set Algebra

Primitive concepts:

- element of set
- the relation of "belonging to the set" ($x \in X$)

1. Uniqueness Axiom (Axiom of extensionality): If the sets A and B have the same elements then A and B are identical.
2. Union Axiom: for arbitrary sets A and B there exists the set whose elements are all the elements of the set A and all the elements of the set B (without repetitions) and no other elements

Basic Axioms of Set Algebra

Primitive concepts:

- element of set
- the relation of "belonging to the set" ($x \in X$)

1. Uniqueness Axiom (Axiom of extensionality): If the sets A and B have the same elements then A and B are identical.
2. Union Axiom: for arbitrary sets A and B there exists the set whose elements are all the elements of the set A and all the elements of the set B (without repetitions) and no other elements
3. Difference Axiom: For arbitrary sets A and B there exists the set whose elements are those and only those elements of the set A which are not the elements of the set B.

Basic Axioms of Set Algebra

Primitive concepts:

- element of set
- the relation of "belonging to the set" ($x \in X$)

1. Uniqueness Axiom (Axiom of extensionality): If the sets A and B have the same elements then A and B are identical.
2. Union Axiom: for arbitrary sets A and B there exists the set whose elements are all the elements of the set A and all the elements of the set B (without repetitions) and no other elements
3. Difference Axiom: For arbitrary sets A and B there exists the set whose elements are those and only those elements of the set A which are not the elements of the set B.
4. Existence Axiom: There exists at least one set.

(intersection, the existence of the empty set and all the basic set algebra theorems can be derived from the above axioms)

More Set Theory Axioms

More advanced set theory needs additional axioms:

[3] The axiom of choice is very strong and implies some non-intuitive theorems and is questioned by some mathematicians

More Set Theory Axioms

More advanced set theory needs additional axioms:

- 5: For every propositional function f(x) and for every set A there exists a set consisting of those and only those elements of the set A which satisfy f(x)

$$\{x : f(x) \wedge x \in A\}$$

[3] The axiom of choice is very strong and implies some non-intuitive theorems and is questioned by some mathematicians

More Set Theory Axioms

More advanced set theory needs additional axioms:

- 5: For every propositional function f(x) and for every set A there exists a set consisting of those and only those elements of the set A which satisfy f(x)

$$\{x : f(x) \wedge x \in A\}$$

- 6: for every set A there exists a set, denoted by 2^A, whose elements are all the subsets of A

[3] The axiom of choice is very strong and implies some non-intuitive theorems and is questioned by some mathematicians

More Set Theory Axioms

More advanced set theory needs additional axioms:

- 5: For every propositional function f(x) and for every set A there exists a set consisting of those and only those elements of the set A which satisfy f(x)

$$\{x : f(x) \land x \in A\}$$

- 6: for every set A there exists a set, denoted by 2^A, whose elements are all the subsets of A
- 7 (Axiom of Choice): For every family R of non-empty disjoint sets there exists a set which has one and only one element in common with each of the sets of the family R.[3]

[3] The axiom of choice is very strong and implies some non-intuitive theorems and is questioned by some mathematicians

More Set Theory Axioms

More advanced set theory needs additional axioms:

- 5: For every propositional function f(x) and for every set A there exists a set consisting of those and only those elements of the set A which satisfy f(x)

$$\{x : f(x) \land x \in A\}$$

- 6: for every set A there exists a set, denoted by 2^A, whose elements are all the subsets of A
- 7 (Axiom of Choice): For every family R of non-empty disjoint sets there exists a set which has one and only one element in common with each of the sets of the family R.[3]

(now axioms 2,3 are superfluous as they can be derived from the axioms 1 and 5-7)

[3] The axiom of choice is very strong and implies some non-intuitive theorems and is questioned by some mathematicians

The role of axioms

The introduction of the axioms of the set theory (at the beg. of the XX. century) eliminated the paradoxes and antinomies and cleaned the fundamentals of the theory.

The role of axioms

The introduction of the axioms of the set theory (at the beg. of the XX. century) eliminated the paradoxes and antinomies and cleaned the fundamentals of the theory.

Similar axiomatic approach is possible (and takes place) in other mathematical theories (e.g. theory of natural numbers, geometry, etc.)

Example tasks/questions/problems

- provide the definition of formal proof
- describe at least 6 different inference rules
- describe the following proof schemas: direct proof, proof by contraposition, reductio ad absurdum (proof by contradiction)
- prove the following small theorems:
  - "If an integer n is odd, then n^2 is also odd"
  - "If n is an integer and $3n + 2$ is odd, then n is odd"
  - "At least four of any 22 days must fall on the same day of the week"

  in each case, try the following schemas (in the given order): direct proof, proof by contraposition, reductio ad absurdum (proof by contradiction).

Thank you for your attention.