Mathematical Statements and Their Proofs

Alexander Meduna, Lukáš Vrábel, and Petr Zemek

Brno University of Technology, Faculty of Information Technology
Božetěchova 1/2, 612 00 Brno, CZ
http://www.fit.vutbr.cz/~{meduna,ivrabel,izemek}

BRNO UNIVERSITY OF TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

Supported by the FRVŠ MŠMT FR271/2012/G1 grant, 2012.

Contents

Why Is Proving Important?

1. Proofs assure us that what we do is right.
2. Proofs convince people.
3. Proofs save time and money.
4. Proving is learning.
5. Last, but certainly not least, proofs are fun :-).

General Layout of a Statement

Statement

Formal wording of the statement.

Proof

Argumentation that the statement is true. $\square$

Theorem

A *theorem* is the most basic type of a statement that is proved using rigorous mathematical reasoning. Usually, theorems are regarded as the most important results.

A *theorem* is the most basic type of a statement that is proved using rigorous mathematical reasoning. Usually, theorems are regarded as the most important results.

Theorem

For a right triangle with legs a and b and hypotenuse c,

$$a^2 + b^2 = c^2$$

Theorem

A *theorem* is the most basic type of a statement that is proved using rigorous mathematical reasoning. Usually, theorems are regarded as the most important results.

Theorem

For a right triangle with legs a and b and hypotenuse c,

$$a^2 + b^2 = c^2$$

Theorem

For every finite automaton, there is an equivalent regular expression and vice versa.

Lemma

A *lemma* is a minor result whose purpose is to help in proving a theorem.

A *lemma* is a minor result whose purpose is to help in proving a theorem.

Lemma

For every finite automaton, there is an equivalent regular expression.

Lemma

For every regular expression, there is an equivalent finite automaton.

Corollary

A *corollary* is a consequence of some other result.

A *corollary* is a consequence of some other result.

Corollary

Finite automata and regular expressions define the same family of languages.

Summary of Mathematical Statements

Statement	Usage
Theorem	You want to write a statement that you prove on the basis of previously established results. As a rule of thumb, if you do not know what type of a statement you should use, use a theorem.
Lemma	You want to divide a proof of a theorem into several parts, where each part is a lemma. It is usually used as a stepping stone to a theorem. There is no formal distinction between a lemma and a theorem.
Corollary	You want to write a statement that follows readily from a previous statement. There is no formal distinction between a theorem, lemma, and corollary. Use of a corollary is plainly subjective.

Direct Proof

In a *direct proof*, we show that a statement is true by combining known facts.

In a *direct proof*, we show that a statement is true by combining known facts.

Theorem

The sum of two even integers is itself an even integer.

Proof

Let a and b be two even integers. Since they are even, they can be written in the forms $a = 2x$ and $b = 2y$ for some integers x and y, respectively. Then, $a + b$ can be written in the form $2x + 2y$, giving the following equation:

$$a + b = 2x + 2y = 2(x + y)$$

From this, we see that $a + b$ is divisible by 2. Hence, $a + b$ is an even integer, and the theorem holds. $\square$

Proof By Contradiction

A *proof by contradiction* is based on these two basic rules of mathematical logic:

1. Any mathematical statement is either true or false.
2. If a statement is true, its negation is false.

Proof By Contradiction

A *proof by contradiction* is based on these two basic rules of mathematical logic:

1. Any mathematical statement is either true or false.
2. If a statement is true, its negation is false.

A proof by contradiction works as follows: To prove that a statement A holds, we start by assuming that A does not hold. Then, we obtain a contradiction, and so we know that A has to hold.

Proof By Contradiction (Example)

Theorem

There are infinitely many primes.

Proof

To obtain a contradiction, we will assume that there exist only finitely many prime numbers

$$p_1 < p_2 < \cdots < p_n$$

Let $q = p_1 p_2 \cdots p_n + 1$ be the product of $p_1, p_2, \ldots, p_n$ plus one. Like any other natural number, q is divisible by at least one prime number (it is possible that q itself is a prime). However, none of the primes $p_1, p_2, \ldots, p_n$ divides q without a remainder because dividing q by any of them leaves a remainder 1. Therefore, there has to exist a yet other prime number than p_1, $p_2, \ldots, p_n$, which is a contradiction with the initial assumption. Therefore, there are infinitely many primes. $\square$

Proof By Induction

A *proof by induction* is typically used to prove that a statement holds for all natural numbers.

A *proof by induction* is typically used to prove that a statement holds for all natural numbers.

Formally, we need to prove the following statements:

1. A holds for 0 (the starting point, called *basis*).
2. If A holds for n, then it also holds for $n + 1$ (the spreading nature, called *induction step*).

Proof By Induction (Example 1/3)

For every natural number n, let $S(n)$ denote the sum of all the numbers $0, 1, 2, \ldots, n$. In symbols,

$$S(n) = \sum_{0 \leq i \leq n} i$$

Theorem

$S(n) = \frac{n(n+1)}{2}$

Proof

We prove this theorem by induction.

Basis. We show that the statement holds for 0. This means we have to prove that

$$0 = \frac{0(0+1)}{2}$$

Since the right-hand side can be simplified to 0, we have that $0 = 0$, so the basis holds.

Proof

Induction Step. In the induction step, we have to show that if the statement holds for $S(n)$, then it holds for $S(n+1)$. To this end, assume that it holds for $S(n)$ (that is, we ask the question "what would happen, if it holds for n?" in a mathematical way). Then, to prove that it holds for $S(n+1)$, we have to prove that

$$(0+1+2+\cdots+n)+(n+1)=\frac{(n+1)((n+1)+1)}{2}$$

Using the assumption that $S(n)$ is true, the left-hand side of the equation can be rewritten to

$$\frac{n(n+1)}{2}+(n+1)$$

Proof

$$\frac{n(n+1)}{2} + (n+1)$$

can be rewritten in the following way:

$$\begin{aligned}\frac{n(n+1)}{2} + (n+1) &= \frac{n(n+1)+2(n+1)}{2} \\ &= \frac{n^2+n+2n+2}{2} \\ &= \frac{(n+1)(n+2)}{2} \\ &= \frac{(n+1)((n+1)+1)}{2}\end{aligned}$$

This implies that $S(n+1)$ holds. Since we have proved both the basis and the induction step, by the principle of induction, the theorem holds. $\square$

References

A. Meduna, L. Vrábel, and P. Zemek.
Mathematical foundations of formal language theory, 2012.
http://www.fit.vutbr.cz/~izemek/frvs2012.

Discussion