Methods of proof

Irina Prosvirnina

- Some terminology
- Direct argument
- Contrapositive argument
- Proof by contradiction
- Mathematical induction

Some terminology

A **theorem** is a statement that can be shown to be true.

In mathematical writing, the term theorem is usually reserved for a statement that is considered at least somewhat important.

Less important theorems sometimes are called **propositions**.

A theorem may be the universal quantification of a conditional statement with one or more premises and a conclusion.

Some terminology

We demonstrate that a theorem is true with a proof.
A **proof** is a valid argument that establishes the truth of a theorem.

Some terminology

The statements used in a proof can include

- axioms (or postulates), which are statements we assume to be true,
- the premises, if any, of the theorem,
- and previously proven theorems.

Some terminology

Axioms may be stated using **primitive** terms that do not require definition, but all other terms used in theorems and their proofs must be defined.

Some terminology

Rules of inference, together with definitions of terms, are used to draw conclusions from other assertions, tying together the steps of a proof. In practice, the final step of a proof is usually just the conclusion of the theorem.

Some terminology

A less important theorem that is helpful in the proof of other results is called a **lemma** (plural: lemmas or lemmata).

Complicated proofs are usually easier to understand when they are proved using a series of lemmas, where each lemma is proved individually.

Some terminology

A **corollary** is a theorem that can be established directly from a theorem that has been proved.

Some terminology

A **conjecture** is a statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert.

When a proof of a conjecture is found, the conjecture becomes a theorem. Many times conjectures are shown to be false, so they are not theorems.

Methods of proof

In practice, the proofs of theorems designed for human consumption are almost always informal proofs,

- where more than one rule of inference may be used in each step, where steps may be skipped,
- where the axioms being assumed and the rules of inference used are not explicitly stated.

Methods of proof

Informal proofs can often explain to humans why theorems are true, while computers are perfectly happy producing formal proofs using automated reasoning systems.

Methods of proof

The methods of proof discussed here are important not only because they are used to prove mathematical theorems, but also for their many applications to computer science.

These applications include

- verifying that computer programs are correct, establishing that operating systems are secure,
- making inferences in artificial intelligence,
- showing that system specifications are consistent, and so on.

Methods of proof

Consequently, understanding the techniques used in proofs is essential both in mathematics and in computer science.

Methods of proof

- Logical arguments are used to give us proofs of the theorems.

In computing such proofs are essential in the design and verification of algorithms.

The commonest types of proof are ones where we wish to establish the truth of a proposition of the form

$$P \rightarrow Q.$$

Methods of proof

There are several standard methods of proof, including the following:

- direct argument,
- contrapositive argument,
- proof by contradiction.

Direct argument

1. Direct argument

Assume P is true and show that Q is true. This rules out the situation where P is true and Q is false which is the only case where $P \rightarrow Q$ is false.

Contrapositive argument

2. Contrapositive argument

Assume Q is false and show that P is false. This demonstrates that

$$\neg Q \rightarrow \neg P$$

is true which is the same as showing that

$$P \rightarrow Q$$

is true.

Proof by contradiction

3. Proof by contradiction

Assume P is true and Q is false and derive a contradiction. This again rules out the situation where P is true and Q is false which is the only case where

$$P \to Q$$

is false.

Example 1 **Use a direct method of proof to show that if x and y are odd integers, then xy is also odd.**

Solution

First, notice that if x is an odd integer then $x = 2m + 1$, where m is an integer.Similarly, $y = 2n + 1$ for some integer n.

Then,

$$xy = (2m + 1)(2n + 1) =$$

$$= 4mn + 2m + 2 + 1 =$$

$$= 2(2mn + m + n) + 1$$

Is an odd integer. ■

Example 2 **Let *n* be a positive integer. Prove, using the contrapositive, that if n^2 is odd, then *n* is odd.**

Solution

The negation of ***n^2 is odd*** is ***n^2 is even***, and the negation of ***n is odd*** is ***n is even***. Therefore, we proof directly that

if n is even then n^2 is even

Since ***n is even,*** we can write $n = 2m$ for some integer m. Then, $n^2 = 4m^2 = 2(2m^2)$ is also even. ■

Example 3 Use a proof by contradiction to show that if $x^2 = 2$ then x is not a fraction.

Solution

By way of contradiction, assume that x is a fraction and write $x = m/n$ where n and m are integers, n is not equal to 0 and n and m have no common factors. Since $x^2 = 2$, we have that $(m/n)^2 = 2$. Therefore, $m^2 = 2n^2$. But this implies that m^2 is an even integer. Therefore, m is an even integer. Hence, $m = 2p$ for some other integer p.

Example 3 Use a proof by contradiction to show that if $x^2 = 2$ then x is not a fraction.

Solution

Substituting this information into the equation

$m^2 = 2n^2$ leads to $4p^2 = 2n^2$, $n^2 = 2p^2$. But then, n is also an even integer. We have shown that m and n have a common factor (of 2) which contradicts our original assertion that m and n have no common factors.

This contradiction can only be resolved by concluding that if $x^2 = 2$ then x is not a fraction. ■

Mathematical induction

In computing a program is said to be **correct** if it behaves in accordance with its specification. Whereas **program testing** shows that selected input values give acceptable output values, **proof of correctness** uses formal logic to prove that for any input values, the output values are correct.

Proving the correctness of algorithms containing loops requires a powerful method of proof called **mathematical induction.**

Mathematical induction

Consider the following recursive algorithm, intended to calculate the maximum element in a list $a_1, a_2, \ldots, a_n$ of positive integers.

```
begin
    r:=0;
    M:=0;
        while r < n do
            begin
                r :=r+1;
                M:=max(M, a_r);
            end
end
```

Mathematical induction

To see how the algorithm works consider the input list $a_1 = 4$, $a_2 = 7$, $a_3 = 3$ and $a_4 = 8$. The trace table is given in the next table.

r	M	r < 4 ?
0	0	Yes
1	4	Yes
2	7	Yes
3	7	Yes
4	8	No

Mathematical induction

r	M	r < 4 ?
0	0	Yes
1	4	Yes
2	7	Yes
3	7	Yes
4	8	No

The output is M = 8, which is correct. Notice that after each execution of the loop, M is the maximum of the elements of the list so far considered.

Mathematical induction

So does the algorithm for all lists of any length n?

Consider an input $a_1, a_2, \ldots, a_n$ of length n and let M_k be the value of M after k executions of the loop.

1) For an input list a_1 of length 1, the loop is executed once and M is assigned to be the maximum of 0 and a_1,which is just a_1. It is the correct input.
2) If after k executions of the loop, M_k is the maximum element of the list $a_1, a_2, \ldots, a_k$ then after one more loop M_{k+1} is assigned the value $\max(M_k, a_{k+1})$ which will then be the maximum element of the list $a_1, a_2, \ldots, a_{k+1}$.

Mathematical induction

By condition 1) the algorithm works for any list of length 1, and so by condition 2) it works for any list of length 2. By condition 2) again it works for any list of length 3, and so on. Hence, the algorithm works for any list of length *n* and so the algorithm is correct.

This process can be formalised as follows.

Mathematical induction

- **The principle of mathematical induction**

Let *P(n)* be a predicate that is defined for all natural *n.*

Suppose that

1) *P(1)* is true and

2) For all $k \geq 1$

(P(κ) → *P(k+1))* is true.

Then *P(n)* is true for all $n \geq 1$.

Mathematical induction

Example 1 Prove, by induction, that for all $n \geq 1$

$1+ 2 + \ldots + n = n(n+1)/2.$

Solution

Let $P(n)$ be the predicate $1+ 2 + \ldots + n = n(n+1)/2$.

In the case $n = 1$, the left-hand side is simply 1, and the right-hand side is $1(1+1)/2 = 1$.

Therefore, $P(1)$ is true.

Mathematical induction

Assume now that

$1+ 2 + \ldots + k = k(k+1)/2$ for some $k \geq 1$. Then

$$1+ 2 + \ldots + (k+1) = (1+ 2 + \ldots +k) + (k+1)$$
$$= k(k+1)/2 + (k+1)$$
$$= (k(k+1) + 2(k+1))/2$$
$$= ((k+2)(k+1))/2$$
$$= (k+1)(k+2)/2 .$$

Hence, for all $k \geq 1 (P(k) \rightarrow P(k+1))$ is true. Therefore, by induction $P(n)$ is true for all $n \geq 1$. ■

Mathematical induction

Example 2 Prove, by induction, that $7^n - 1$ is divisible by 6 for all $n \geq 1$.

Solution

First, note that an integer a is divisible by an integer b if there is some other integer m with

$a = mb$.

For example, 51 is divisible by 17 since $51 = 3 \bullet 17$.

Let *P(n)* be the predicate «$7^n - 1$ is divisible by 6».

In the case *n = 1,*

$$7^n - 1 = 7^1 - 1 = 7 - 1 = 6,$$

which is clearly divisible by 6. Therefore, *P(1)* is true.

Mathematical induction

Assume now that $7^k - 1$ is divisible by 6 for some $k \geq 1$. Then,

$$7^{k+1} - 1 = 7(7^k) - 1$$
$$= 7(7^k - 1) + 7 - 1$$
$$= 7(7^k - 1) + 6 .$$

Since $7^k - 1$ is divisible by 6 it follows that $7(7^k - 1) + 6$ is also is divisible by 6.

Hence, $7^{k+1} - 1$ is divisible by 6 and so $(P(k) \rightarrow P(k+1))$ for all $k \geq 1$ is true.

Therefore, by induction $P(n)$ is true for all $n \geq 1$. ■

Mathematical induction

Example 3

A sequence of integers $x_1, x_2, \ldots, x_n$ is defined recursively as follows:

$$x_1 = 1 \text{ and } x_{k+1} = x_k + 8k \text{ for } k >= 1.$$

Prove that

$$x_n = (2n - 1)^2 \text{ for all } n >= 1.$$

Solution

Let $P(n)$ be the predicate $x_n = (2n - 1)^2$. In the case $n = 1$, $(2n - 1)^2 = (2 \bullet 1 - 1)^2 = 1$. Therefore, $P(1)$ is true.

Mathematical induction

Assume now that $x_k = (2k - 1)^2$ for some $k \geq 1$.

Then

$$\begin{aligned} x_{k+1} &= x_k + 8k \\ &= (2k - 1)^2 + 8k \\ &= 4k^2 + 4k + 1 \\ &= (2k + 1)^2 . \end{aligned}$$

Hence,

$$x_{k+1} = (2(k + 1) - 1)^2 .$$

And so $(P(k) \rightarrow P(k+1))$ is true for all $k \geq 1$. Therefore, by induction $P(n)$ is true for all $n \geq 1$. ■