Mathematical Logic

An overview of Proof methods

Chiara Ghidini

FBK-IRST, Trento, Italy

September 25, 2013

Goal

In these slides we present an overview of the basic proof techniques adopted in mathematics and computer science to prove theorems. We consider:

1. direct proof
2. proof by "reductio ad absurdum", or, indirect proof
3. proof under hypothesis
4. proof by cases
5. proof of a universal statement
6. proof of an existential statement
7. proof of a universal implication
8. proof by induction

Direct proof of a fact A

Theorem

the fact A is true

Schema of a direct proof (example).

- from axiom A_1 it follows that A_2,
- from axiom B_1 it follows B_2,
- form A_2 and B_2 it follows C
- from C we can conclude that either C_1 or C_2, then
- from C_1 it follows that A
- and also from C_2 it follows that A.

So we can conclude that A is true. □

Direct proof of a fact A

Remark

- Axioms (A_1 and B_1) are facts that are accepted to be true without a proof.
- from axioms we can infer other facts (e.g., A_2, B_2)
- form inferred facts we can infer other facts (e.g., C)
- from a fact we can infer some alternative facts (e.g., either C_1 or C_2),
- alternatives can be treated separately, to prove the theorem. In this case we have to show that it is true in all the possible alternatives (see proof by cases).

Example of direct proof

Theorem

The sum of two even integers is always even.

Proof.

- Let x and y two arbitrary even numbers.
  They can be written as
  $$x = 2a \text{ and } y = 2b$$
- Then the sum $x + y = 2a + 2b = 2(a + b)$
- From this it is clear that 2 is a factor of $x + y$.

So, the sum of two even integers is always an even number. □

Proof by "reductio ad absurdum"

Theorem

It is the case that A is true

By reductio ad absurdum.

Suppose that A is not the case, then by reasoning, you try to reach an impossible situation. □

Example of proof by "reductio ad absurdum"

Theorem

$\sqrt{2}$ is not a rational number

Proof.

1. Suppose that $\sqrt{2}$ is a rational number
2. then there are two coprime integers n and m such that $\sqrt{2} = n/m$ (n/m is an irreducible fraction)
3. which means that $2 = n^2/m^2$
4. which implies that $n^2 = 2 * m^2$.
5. This implies that n is an even number and there exists k such that $n = 2 * k$.
6. From $n^2 = 2m^2$ (step 4), we obtain that $(2 * k)^2 = 2 * m^2$
7. which can be rewritten in $m^2 = 2 * k^2$.
8. Similarly to above this means that m^2 is even, and that m is even.
9. but this contradicts the hypothesis that n and m are coprime, and is therefore impossible.
10. Therefore $\sqrt{2}$ is not a rational number

□

Proof under hypothesis

Theorem

if A then B

Schema 1: Direct proof.

If A is true, then A_1 is also true, then $\dots A_n$ is true, and therefore B is true. □

Schema 2: Proof by reductio ad absurdum.

Suppose that B is not the case, then B_1 is the case, then $\dots$, then B_n is the case, and therefore A is not the case □

Proof of an "if ... then..." theorem

Theorem

If $A \cup B = A$ *then* $B \subseteq A$

Direct Proof.

- Suppose that $A \cup B = A$, then
- $x \in B$ implies that $x \in A \cup B$.
- This implies that $x \in A$,
- and therefore $A \subseteq B$.

□

Proof of an "if . . . then. . ." theorem

Theorem

If $A \cup B = A$ *then* $B \subseteq A$

Proof by reductio ad absurdum.

- Suppose that $B \not\subseteq A$
- This implies that there exists $x \in B$ such that $x \notin A$.
- This implies that $x \in A \cup B$ such that $x \notin A$,
- and therefore $A \cup B \neq A$.

□

Proof by cases

Theorem

If A then B

Proof.

If A then either A_1 or A_2 or $\ldots$ or A_n. Then, let us consider all the cases one by one

- if A_1, then $\ldots$ then B
- if A_2, then $\ldots$ then B
- $\ldots$
- if A_n, then $\ldots$ then B

So in all the cases we managed to proof the same conclusion B. This implies that the theorem is correct. □

Example of proof by cases

Theorem

If n is an integer then $n^2 \geq n$.

Proof.

If n is an integer then we have three cases:

1. $n = 0$,
2. $n > 0$,
3. $n < 0$

1. $n = 0$, then $n^2 = 0$, and therefore $n^2 \geq n$.
2. $n \geq 1$, then by multiplying the inequality for a positive integer n, we have that $n^2 \geq n$.
3. if $n \leq -1$, then since n^2 is always positive we have that $n^2 \geq n$.

Since in all the cases we have conclude that $n^2 \geq n$ we can conclude that the theorem is correct. □

Proof of a universal statement

Theorem

The property A holds for all x.[a]

[a] In symbols, $\forall x A(x)$.

Proof Schema.

Consider a generic element x and try to show that it satisfies property A.
In doing that you are not allowed to make any additional assumptions on the nature of x. If you make some extra assumption on x, say for instance that x has the property B, then you have proved a different theorem which is "for every x, if x has the property B then it has the property A". □

Example of a universal statement

Theorem

For any integer a, if a is odd then a^2 is also odd.

Proof (direct proof in this case).

1. If a is odd, then $a = 2m + 1$ for some integer m (By definition)
2. Then $a^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$
3. Let $z = 2m^2 + 2m$. z is an integer (trivial proof because of the fact that m is an integer).
4. Then $a^2 = 2z + 1$ for an integer z, which means, by definition, that a^2 is an odd number.

□

Proof of an existential statement

Theorem

There is an x that has a property A.[a]

[a] In symbols, $\exists x.A(x)$

Schema 1: Constructive proof.

1. Construct a special element x (usually by means of a procedure (a set of steps))
2. Show that x has the property A

□

Schema 2: Non Constructive proof (reductio ad absurdum).

Assume that there is no such an x such that the property A holds for x and try to reach an inconsistent (absurd) situation. □

Example of an existential statement

Theorem

There is an integer $n > 5$ such that $2^n - 1$ is a prime number.

Proof (constructive).

1. Examine all integers $n > 5$.
2. $n = 6$. $2^6 - 1 = 64 - 1 = 63$. NO!
3. $n = 7$. $2^7 - 1 = 128 - 1 = 127$. YES!

□

Universal and existential statements

- Disproving universal statements reduces in proving an existential one.

  Dont try to construct a general argument when a single specific counterexample would be sufficient!

Example

For every rational number q, there is a rational number r such that $qr = 1$

This statement is false. In fact 0 has no inverse.

Universal and existential statements

- Disproving an existential statement needs proving a universal one.

Example

There is an integer k such that $k^2 + 2k + 1 < 0$

This statement is false. Indeed it can be proved that $k^2 + 2k + 1 \geq 0$

Proof of a universal implication

Theorem

For all x, if x has a property A, then x has the property B.[a]

[a] In symbols, $\forall x(A(x) \Rightarrow B(x))$.

Proof.

The proof is a combination of the proof method for universal statements, and the proof for implication statements.
Take an arbitrary x that satisfies the property A. then show, either with a direct proof or by reductio ad absurdum, that if x has property A, then x has property B as well. □

Remark

If there is no such an x that has a property A, the theorem $\forall x(A(x) \Rightarrow B(x))$ is true.
For instance the statement

> *"For every number x (if $x > y$ for all y, then $y = 23$)"*

is a theorem.
The proof consists in showing that there is no x which is greater than all the numbers.

Proof by induction

The simplest and most common form of mathematical induction infers that a statement involving a natural number n holds for all values of n.

The proof consists of two steps:

1. The basis (**base case**): prove that the statement holds for the first natural number n. Usually, $n = 0$ or $n = 1$.
2. The **inductive step**: prove that, if the statement holds for some natural number n, then the statement holds for $n + 1$.

The hypothesis in the inductive step that the statement holds for some n is called the **inductive hypothesis**.

Proof by induction: example

Theorem

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

proof

Base case Show that the statement holds for $n = 0$.

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

Inductive step Show that if the statement holds for n, then it holds for $n + 1$.

Assume that $0 + 1 + \ldots + n = \frac{n(n+1)}{2}$, we have to show that

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

Proof by induction: example - cont'd

1. $0 + 1 + \ldots + n + (n+1) = \frac{n(n+1)}{2} + (n+1)$ from the inductive hypothesis
2. Algebraically, $\frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2}$
3. $= \frac{n^2 + n + 2n + 2}{2}$
4. $= \frac{(n+1)(n+2)}{2}$
5. $= \frac{(n+1)(n+1+1)}{2}$
6. $= \frac{(n+1)((n+1)+1)}{2}$

Induction on inductively defined sets.

Main idea

Prove a statement of the form

forall x, x has the property A

when x is an element of a set which is inductively defined.

Definition (Inductive definition of A)

The set A is inductively defined as follows:

Base: $a_1 \in A$, $a_2 \in A$, ..., $a_n \in A$

Step 1: if $y_1 \dots y_{k_1} \in A$, then $S_1(y_1, \dots y_{k_1}) \in A$

Step 2: if $y_1 \dots y_{k_2} \in A$, then $S_2(y_1, \dots y_{k_2}) \in A$

⋮

Step m: if $y_1 \dots y_{k_m} \in A$, then $S_m(y_1, \dots y_{k_m}) \in A$

Closure: Nothing else is contained in A

Example of set defined by induction

Definition

We inductively define a set P of strings, built starting from the Latin alphabet, as follows:

Base $\langle \mathtt{a} \rangle, \langle \mathtt{b} \rangle, \dots, \langle \mathtt{z} \rangle \in P$

Step 1 if $x \in P$ then $concat(x, x) \in P$

Step 2 if $x, y \in P$, then $concat(x, y, x) \in P$

Closure nothing else is in P

where $concat(\langle x_1 \dots x_n \rangle, \langle y_1 \dots y_n \rangle) = \langle x_1 \dots x_n y_1 \dots y_n \rangle$.

Example of proof by induction on sets defined by induction.

Theorem

For any $x \in P$, x *is a palindrome, i.e.,* $x = \langle x_1 \dots x_n \rangle \in P$ *and for all* $1 \leq k \leq n$, $x_k = x_{n-k+1}$.

Proof.

Base case We have to prove that x is palindrome for all strings in the Base set.

If x belongs to P because of the base case definition, then it is either $\langle \mathtt{a} \rangle$ or $\dots \langle \mathtt{z} \rangle$, then it is of the form $x = \langle x_1 \rangle$, then $n = 1$ and for all $k \leq 1 \leq 1$, i.e., for $k = 1$ we have that $x_1 = x_{1-1+1}$.

Inductive step Show that if the statement holds for a certain P, then it holds also for P enriched by the strings at steps 1 and 2.

Step 1. If $x \in P$ because of step 1, then x is of the form $concat(y, y)$, for some $y \in P$. From the definition of "concat", x is of the form $\langle y_1 \dots y_{n/2} y_1 \dots y_{n/2} \rangle$, where $\langle y_1 \dots y_{n/2} \rangle \in P$ (i.e., is palindrome).
By induction for all $1 \leq k \leq n/2$, $y_k = y_{n/2-k+1}$.
This implies that, for all $1 \leq k \leq n$, if $k \leq n/2$, then
$x_k = y_k = y_{n/2-k+1} = x_{n/2+n/2-k+1} = x_{n-k+1}$.

□

Example of proof by induction on sets defined by induction.

Proof.

Inductive step Show that if the statement holds for a certain P, then it holds also for P enriched by the strings at steps 1 and 2.

Step 2. If $x \in P$ because of step 2, then x is of the form $concat(z, y, z)$, for some $z, y \in P$. From the definition of "concat", x is of the form $\langle z_1 \dots z_l y_1 \dots y_h z_1 \dots z_l \rangle$, where $\langle z_1 \dots z_l \rangle \in P$ and $\langle y_1 \dots y_h \rangle \in P$ (i.e., are palindrome).
By induction for all $1 \leq k \leq l$, $z_k = z_{l-k+1}$ and for all $1 \leq k \leq h$, $y_k = y_{h-k+1}$.
This implies that for all $1 \leq k \leq n$ we have that:
Case 1 if $k \leq l$, then $x_k = z_k = z_{l-k+1} = x_{l+h+l-k-k+1} = x_{n-k+1}$.
Case 2 if $l + 1 \leq k \leq l + 1 + h/2$, then
$x_k = y_{k-l} = y_{h-k+l+1} = x_{h-k+l+l+1} = x_{n-k+1}$.

□