Theory of Computer Science

A3. Proof Techniques

Gabriele Röger

University of Basel

February 18, 2026

A3.1 Proofs

What is a Proof?

A mathematical proof is

- a sequence of logical steps
- starting with one set of statements
- that comes to the conlusion
  that some statement must be true.

What is a statement?

Mathematical Statements

Mathematical Statement

A mathematical statement is a declarative sentence that is either true or false (but not both).

Examples (some true, some false):

- Let $p \in \mathbb{N}_0$ be a prime number. Then p is odd.
- There exists an even prime number.
- The equation $a^k + b^k = c^k$ has infinitely many solutions with $a, b, c, k \in \mathbb{N}_1$ and $k \geq 2$.

German: Mathematische Aussage

Mathematical Statements: Quantification

Statements often use quantification.

- Universal quantification:
  "For all x in set S it holds that $\langle$sub-statement on $x\rangle$."
  This is true if the sub-statement is true for every x in S.

- Existential quantification:
  "There is an x in set S such that $\langle$sub-statement on $x\rangle$."
  This is true if there exists at least one x in S for which the sub-statement is true.

Examples (some true, some false):

- For all $x \in \mathbb{N}_1$ it holds that $x + 1$ is in $\mathbb{N}_1$.
- For all $x \in \mathbb{N}_1$ it holds that $x - 1$ is in $\mathbb{N}_1$.
- There is an $x \in \mathbb{N}_1$ such that $x = \sqrt{x}$.

Mathematical Statements: Preconditions and Conclusions

We can identify preconditions and conclusions.

"If $\langle$preconditions$\rangle$ then $\langle$conclusions$\rangle$."

The statement is true if the conclusions are true whenever the preconditions are true.

Not every statement has preconditions. Preconditions are often used in universally quantified sub-statements.

Examples (some true, some false):

- If 4 is a prime number then $2 \cdot 3 = 4$.
- If n is a prime number with $n > 2$ then n is odd.
- For all $p \in \mathbb{N}_1$ it holds that if p is a prime number then p is odd.

Different Statements with the same Meaning

The following statements have the same meaning, we just move preconditions into the quantification, make some aspects implicit, and change the structure.

- For all $p \in \mathbb{N}_1$ it holds that if p is a prime number with $p > 2$ then p is odd.
- For all prime numbers p it holds that if $p > 2$ then p is odd.
- Let p be a natural number with $p > 2$.
  Then p is odd if p is prime.
- If p is a prime number with $p > 2$ then p is odd.
- All prime numbers $p > 2$ are odd.

A single mathematical statement can be expressed in different ways, as long as the meaning stays the same.

Like paraphrasing a sentence in everyday language.

On what Statements can we Build the Proof?

A mathematical proof is

- a sequence of logical steps
- starting with one set of statements
- that comes to the conlusion
  that some statement must be true.

We can use:

- axioms: statements that are assumed to always be true
  in the current context
- theorems and lemmas: statements that were already proven
  - lemma: an intermediate tool
  - theorem: itself a relevant result
- premises: assumptions we make
  to see what consequences they have

German: Axiom, Theorem/Satz, Lemma, Prämisse/Annahme

What is a Logical Step?

A mathematical proof is

- a sequence of logical steps
- starting with one set of statements
- that comes to the conlusion
  that some statement must be true.

Each step directly follows

- from the axioms,
- premises,
- previously proven statements and
- the preconditions of the statement we want to prove.

For a formal definition, we would need formal logics.

The Role of Definitions

Definition

A set is an unordered collection of distinct objects.

The objects in a set are called the elements of the set. A set is said to contain its elements.

We write $x \in S$ to indicate that x is an element of set S, and $x \notin S$ to indicate that S does not contain x.

The set that does not contain any objects is the *empty set* $\emptyset$.

- A definition introduces an abbreviation.
- Whenever we say "set", we could instead say "an unordered collection of distinct objects" and vice versa.
- Definitions can also introduce notation.

German: Definition

Disproofs

- A disproof (refutation) shows that a given mathematical statement is false by giving an example where the preconditions are true, but the conclusion is false.
- This requires deriving, in a sequence of proof steps, the opposite (negation) of the conclusion.

Example (False statement)

"If $p \in \mathbb{N}_0$ is a prime number then p is odd."

Refutation.

Consider natural number 2 as a counter example. It is prime because it has exactly 2 divisors, 1 and itself. It is not odd, because it is divisible by 2. $\square$

German: Widerlegung

Exercise

You want to disprove the following statement with a counterexample:

If the sun is shining then all kids eat ice cream.

What properties must your counterexample have?

[Discuss with your neighbour; 2 minutes]

A Word on Style

A proof should help the reader to see why the result must be true.

- A proof should be easy to follow.
- Omit unnecessary information.
- Move self-contained parts into separate lemmas.
- In complicated proofs, reveal the overall structure in advance.
- Have a clear line of argument.

$\rightarrow$ Writing a proof is like writing an essay.

A3.2 Proof Strategies

Proof Strategies

typical proof/disproof strategies:

1. "All $x \in S$ with the property P also have the property Q."
   "For all $x \in S$: if x has property P, then x has property Q."
   - To prove, assume you are given an arbitrary $x \in S$ that has the property P.
     Give a sequence of proof steps showing that x must have the property Q.
   - To disprove, find a counterexample, i. e., find an $x \in S$ that has property P but not Q and prove this.

Proof Strategies

typical proof/disproof strategies:

2. "A is a subset of B."
   - To prove, assume you have an arbitrary element $x \in A$ and prove that $x \in B$.
   - To disprove, find an element in $x \in A \setminus B$ and prove that $x \in A \setminus B$.

Proof Strategies

typical proof/disproof strategies:

3. "For all $x \in S$: x has property P iff x has property Q."
   ("iff": "if and only if")
   - To prove, separately prove "if P then Q" and "if Q then P".
   - To disprove, disprove "if P then Q" or disprove "if Q then P".

Proof Strategies

typical proof/disproof strategies:

4. "$A = B$", where A and B are sets.
    - To prove, separately prove "$A \subseteq B$" and "$B \subseteq A$".
    - To disprove, disprove "$A \subseteq B$" or disprove "$B \subseteq A$".

Proof Techniques

proof techniques we use in this course:

- direct proof
- indirect proof (proof by contradiction)

A3.3 Direct Proof

Direct Proof

Direct Proof

Direct derivation of the statement by deducing or rewriting.

German: Direkter Beweis

Direct Proof: Example

Theorem (distributivity)

For all sets A, B, C: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof.

We first show that $x \in A \cap (B \cup C)$ implies $x \in (A \cap B) \cup (A \cap C)$ ($\subseteq$ part):

Let $x \in A \cap (B \cup C)$. Then by the definition of $\cap$ it holds that $x \in A$ and $x \in B \cup C$.

We make a case distinction between $x \in B$ and $x \notin B$:

If $x \in B$ then, because $x \in A$ is true, $x \in A \cap B$ must be true.

Otherwise, because $x \in B \cup C$ we know that $x \in C$ and thus with $x \in A$, that $x \in A \cap C$.

In both cases $x \in A \cap B$ or $x \in A \cap C$,
and we conclude $x \in (A \cap B) \cup (A \cap C)$. ...

Direct Proof: Example

Theorem (distributivity)

For all sets A, B, C: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof (continued).

$\supseteq$ part: we must show that $x \in (A \cap B) \cup (A \cap C)$ implies $x \in A \cap (B \cup C)$.

Let $x \in (A \cap B) \cup (A \cap C)$.

We make a case distinction between $x \in A \cap B$ and $x \notin A \cap B$:

If $x \in A \cap B$ then $x \in A$ and $x \in B$.
The latter implies $x \in B \cup C$ and hence $x \in A \cap (B \cup C)$.

If $x \notin A \cap B$ we know $x \in A \cap C$ due to $x \in (A \cap B) \cup (A \cap C)$.
This (analogously) implies $x \in A$ and $x \in C$, and hence $x \in B \cup C$ and thus $x \in A \cap (B \cup C)$.

In both cases we conclude $x \in A \cap (B \cup C)$. ...

Direct Proof: Example

Theorem (distributivity)

For all sets A, B, C: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof (continued).

We have shown that every element of $A \cap (B \cup C)$
is an element of $(A \cap B) \cup (A \cap C)$ and vice versa.
Thus, both sets are equal. $\square$

Direct Proof: Example

Theorem (distributivity)

For all sets A, B, C: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof.

Alternative:

$$\begin{aligned} A \cap (B \cup C) &= \{x \mid x \in A \text{ and } x \in B \cup C\} \\ &= \{x \mid x \in A \text{ and } (x \in B \text{ or } x \in C)\} \\ &= \{x \mid (x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C)\} \\ &= \{x \mid x \in A \cap B \text{ or } x \in A \cap C\} \\ &= (A \cap B) \cup (A \cap C) \end{aligned}$$

$\square$

A3.4 Indirect Proof

Indirect Proof

Indirect Proof (Proof by Contradiction)

- Make an assumption that the statement is false.
- Use the assumption to derive a contradiction.
- This shows that the assumption must be false and hence the original statement must be true.

German: Indirekter Beweis, Beweis durch Widerspruch

Indirect Proof: Example 1

Theorem

Let A and B be sets. If $A \setminus B = \emptyset$ then $A \subseteq B$.

Proof.

We prove the theorem by contradiction.

Assume that there are sets A and B with $A \setminus B = \emptyset$ and $A \not\subseteq B$.

Let A and B be such sets.

Since $A \not\subseteq B$ there is some $x \in A$ such that $x \notin B$.

For this x it holds that $x \in A \setminus B$.

This is a contradiction to $A \setminus B = \emptyset$.

We conclude that the assumption was false and thus the theorem is true. $\square$

Indirect Proof: Example 2

Theorem

There are infinitely many prime numbers.

Proof.

Assumption: There are only finitely many prime numbers.

Let $P = \{p_1, \dots, p_n\}$ be the set of all prime numbers.

Define $m = p_1 \cdot \ldots \cdot p_n + 1$.

Since $m \geq 2$, it must have a prime factor.
Let p be such a prime factor.

Since p is a prime number, p has to be in P.

The number m is not divisible without remainder
by any of the numbers in P. Hence p is no factor of m.

$\rightsquigarrow$ Contradiction $\square$

A3.5 Summary

Summary

- A proof is based on axioms and previously proven statements.
- Individual proof steps must be obvious derivations.
- direct proof: sequence of derivations or rewriting
- indirect proof: refute that the statement is false.