Discrete Mathematics in Computer Science

A3. Proofs: Introduction

Malte Helmert, Gabriele Röger

University of Basel

September 22, 2025

A3.1 What is a Proof?

A3.1 What is a Proof?

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 ⟨preconditions⟩ then ⟨conclusions⟩."

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 prime if p is odd.
- 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. □

German: Widerlegung

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.

Recommended reading (ADAM additional ressources):

- "Some Remarks on Writing Mathematical Proofs" (John M. Lee)
- "§1. Minicourse on technical writing" of "Mathematical Writing" (Donald E. Knuth, Tracy Larrabee, and Paul M. Roberts)

Summary

A proof should convince the reader by logical steps of the truth of some mathematical statement.