

# Theory of Computer Science

## A3. Proof Techniques

Gabriele Röger

University of Basel

February 23, 2022

# Theory of Computer Science

February 23, 2022 — A3. Proof Techniques

A3.1 Introduction

A3.2 Direct Proof

A3.3 Indirect Proof

A3.4 Contrapositive

A3.5 Mathematical Induction

A3.6 Summary

## A3.1 Introduction

# What is a Proof?

A **mathematical proof** is

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

What is a **statement**?

# Mathematical Statements

## Mathematical Statement

A **mathematical statement** consists of a set of **preconditions** and a set of **conclusions**.

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

**German:** mathematische Aussage, Voraussetzung, Folgerung/Konklusion, wahr

## Notes:

- ▶ set of preconditions is sometimes empty
- ▶ often, “assumptions” is used instead of “preconditions”; slightly unfortunate because “assumption” is also used with another meaning ( $\rightsquigarrow$  cf. indirect proofs)

# Examples of Mathematical Statements

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.”
- ▶ “Let  $p \in \mathbb{N}_0$  with  $p \geq 3$  be a prime number. Then  $p$  is odd.”
- ▶ “All prime numbers  $p \geq 3$  are odd.”
- ▶ “For all sets  $A, B, C$ :  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ”
- ▶ “The equation  $a^k + b^k = c^k$  has infinitely many solutions with  $a, b, c, k \in \mathbb{N}_1$  and  $k \geq 2$ .”
- ▶ “The equation  $a^k + b^k = c^k$  has no solutions with  $a, b, c, k \in \mathbb{N}_1$  and  $k \geq 3$ .”

What are the preconditions, what are the conclusions?

# 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 conclusion  
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

# What is a Logical Step?

A mathematical proof is

- ▶ a sequence of logical steps
- ▶ starting with one set of statements
- ▶ that comes to the conclusion  
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 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.

# 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.

**German:** Widerlegung

- ▶ Formally, disproofs are proofs of modified (“negated”) statements.
- ▶ Be careful about how to negate a statement!

# 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  $P$ ”.

German: “iff” = gdw. (“genau dann, wenn” )

# 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

most common proof techniques:

- ▶ direct proof
- ▶ indirect proof (proof by contradiction)
- ▶ proof by contrapositive
- ▶ mathematical induction

German: direkter Beweis, indirekter Beweis  
(Beweis durch Widerspruch), Kontraposition,  
vollständige Induktion, strukturelle Induktion

# Exercise

Negate the following statement:

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



## A3.2 Direct Proof

# Direct Proof

## Direct Proof

Direct derivation of the statement by deducing or rewriting.

## 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. □

## 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:

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



## A3.3 Indirect Proof

# Indirect Proof

## Indirect Proof (Proof by Contradiction)

- ▶ Make an **assumption** that the statement is false.
- ▶ Derive a **contradiction** from the assumption together with the preconditions of the statement.
- ▶ This shows that the assumption must be false given the preconditions of the statement, and hence the original statement must be true.

German: Annahme, Widerspruch

# Indirect Proof: Example

## 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  $m = p_1 \cdot \dots \cdot p_n + 1$ .

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  $m$ .

~~> **Contradiction**



## A3.4 Contrapositive

# Proof by Contrapositive

## Proof by Contrapositive

Prove “If  $A$ , then  $B$ ” by proving “If not  $B$ , then not  $A$ .”

**German:** (Beweis durch) Kontraposition

Examples:

- ▶ Prove “For all  $n \in \mathbb{N}_0$ : if  $n^2$  is odd, then  $n$  is odd” by proving “For all  $n \in \mathbb{N}_0$ , if  $n$  is even, then  $n^2$  is even.”
- ▶ Prove “For all  $n \in \mathbb{N}_0$ : if  $n$  is not a square number, then  $\sqrt{n}$  is irrational” by proving “For all  $n \in \mathbb{N}_0$ : if  $\sqrt{n}$  is rational, then  $n$  is a square number.”

# Exercise

How would you prove the following statement by contrapositive:

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



## A3.5 Mathematical Induction

# Mathematical Induction

## Mathematical Induction

Proof of a statement for all natural numbers  $n$  with  $n \geq m$

- ▶ **basis**: proof of the statement for  $n = m$
- ▶ **induction hypothesis (IH)**:  
suppose that the statement is true for all  $k$  with  $m \leq k \leq n$
- ▶ **inductive step**: proof of the statement for  $n + 1$   
using the induction hypothesis

**German**: vollständige Induktion, Induktionsanfang,  
Induktionsvoraussetzung, Induktionsschritt

# Mathematical Induction: Example

## Theorem

For all  $n \in \mathbb{N}_0$  with  $n \geq 1$ :  $\sum_{k=1}^n (2k - 1) = n^2$

## Proof.

Mathematical induction over  $n$ :

basis  $n = 1$ :  $\sum_{k=1}^1 (2k - 1) = 2 - 1 = 1 = 1^2$

IH:  $\sum_{k=1}^m (2k - 1) = m^2$  for all  $1 \leq m \leq n$

inductive step  $n \rightarrow n + 1$ :

$$\begin{aligned}\sum_{k=1}^{n+1} (2k - 1) &= \left( \sum_{k=1}^n (2k - 1) \right) + 2(n + 1) - 1 \\ &\stackrel{\text{IH}}{=} n^2 + 2(n + 1) - 1 \\ &= n^2 + 2n + 1 = (n + 1)^2\end{aligned}$$



## A3.6 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 the negated statement
- ▶ **contrapositive**: prove " $A \Rightarrow B$ " as "not  $B \Rightarrow$  not  $A$ "
- ▶ **mathematical induction**: prove statement for a starting point and show that it always carries over to the next number