

# Theory of Computer Science

## A3. Proof Techniques

Gabriele Röger

University of Basel

February 17/19, 2020

# Theory of Computer Science

## February 17/19, 2020 — A3. Proof Techniques

### A3.1 Introduction

### A3.2 Direct Proof

### A3.3 Indirect Proof

### A3.4 Contraposition

### A3.5 Mathematical Induction

### A3.6 Structural Induction

### A3.7 Summary

## A3.1 Introduction

## 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?

## Proofs

### Proof

A **proof** derives the correctness of a mathematical statement from a set of **axioms** and **previously proven statements**.

It consists of a sequence of **proof steps**, each of which **directly follows** from the axioms, previously proven statements and the preconditions of the statement, ending with the conclusions of the theorem.

German: Beweis, Axiom, Beweisschritt

## Disproofs

- ▶ A **disproof** (**refutation**) analogously 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)
- ▶ contraposition
- ▶ mathematical induction
- ▶ structural induction

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

## 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 Contraposition

## Contraposition

### (Proof by) Contraposition

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.”

## 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 I

### 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  $n \rightarrow n + 1$ :**

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

□

## Mathematical Induction: Example II

### Theorem

Every natural number  $n \geq 2$  can be written as a product of prime numbers, i. e.  $n = p_1 \cdot p_2 \cdot \dots \cdot p_m$  with prime numbers  $p_1, \dots, p_m$ .

### Proof.

Mathematical Induction over  $n$ :

**basis  $n = 2$ :** trivially satisfied, since 2 is prime

**IH:** Every natural number  $k$  with  $2 \leq k \leq n$   
can be written as a product of prime numbers.

...

## Mathematical Induction: Example II

### Theorem

Every natural number  $n \geq 2$  can be written as a product of prime numbers, i. e.  $n = p_1 \cdot p_2 \cdot \dots \cdot p_m$  with prime numbers  $p_1, \dots, p_m$ .

### Proof (continued).

**inductive step  $n \rightarrow n + 1$ :**

▶ **Case 1:**  $n + 1$  is a prime number  $\rightsquigarrow$  trivial

▶ **Case 2:**  $n + 1$  is not a prime number.

There are natural numbers  $2 \leq q, r \leq n$  with  $n + 1 = q \cdot r$ .

Using IH shows that there are prime numbers

$q_1, \dots, q_s$  with  $q = q_1 \cdot \dots \cdot q_s$  and

$r_1, \dots, r_t$  with  $r = r_1 \cdot \dots \cdot r_t$ .

Together this means  $n + 1 = q_1 \cdot \dots \cdot q_s \cdot r_1 \cdot \dots \cdot r_t$ .

□

## A3.6 Structural Induction

### Inductively Defined Sets: Examples

#### Example (Natural Numbers)

The set  $\mathbb{N}_0$  of natural numbers is inductively defined as follows:

- ▶ 0 is a natural number.
- ▶ If  $n$  is a natural number, then  $n + 1$  is a natural number.

#### Example (Binary Tree)

The set  $\mathcal{B}$  of binary trees is inductively defined as follows:

- ▶  $\square$  is a binary tree (a **leaf**)
- ▶ If  $L$  and  $R$  are binary trees, then  $\langle L, \bigcirc, R \rangle$  is a binary tree (with **inner node**  $\bigcirc$ ).

**German:** Binärbaum, Blatt, innerer Knoten

**Implicit statement:** all elements of the set can be constructed by finite application of these rules

## Inductive Definition of a Set

#### Inductive Definition

A set  $M$  can be defined **inductively** by specifying

- ▶ **basic elements** that are contained in  $M$
- ▶ **construction rules** of the form  
“Given some elements of  $M$ , another element of  $M$  can be constructed like this.”

**German:** induktive Definition, Basiselemente, Konstruktionsregeln

## Structural Induction

#### Structural Induction

Proof of statement for all elements of an inductively defined set

- ▶ **basis:** proof of the statement for the basic elements
- ▶ **induction hypothesis (IH):**  
suppose that the statement is true for some elements  $M$
- ▶ **inductive step:** proof of the statement for elements constructed by applying a construction rule to  $M$   
(one inductive step for each construction rule)

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

## Structural Induction: Example (1)

### Definition (Leaves of a Binary Tree)

The number of **leaves** of a binary tree  $B$ , written  $\text{leaves}(B)$ , is defined as follows:

$$\text{leaves}(\square) = 1$$

$$\text{leaves}(\langle L, \bigcirc, R \rangle) = \text{leaves}(L) + \text{leaves}(R)$$

### Definition (Inner Nodes of a Binary Tree)

The number of **inner nodes** of a binary tree  $B$ , written  $\text{inner}(B)$ , is defined as follows:

$$\text{inner}(\square) = 0$$

$$\text{inner}(\langle L, \bigcirc, R \rangle) = \text{inner}(L) + \text{inner}(R) + 1$$

## Structural Induction: Example (2)

### Theorem

For all binary trees  $B$ :  $\text{inner}(B) = \text{leaves}(B) - 1$ .

### Proof.

induction basis:

$$\text{inner}(\square) = 0 = 1 - 1 = \text{leaves}(\square) - 1$$

↪ statement is true for base case

...

## Structural Induction: Example (3)

### Proof (continued).

#### induction hypothesis:

to prove that the statement is true for a composite tree  $\langle L, \bigcirc, R \rangle$ , we may use that it is true for the subtrees  $L$  and  $R$ .

#### inductive step for $B = \langle L, \bigcirc, R \rangle$ :

$$\text{inner}(B) = \text{inner}(L) + \text{inner}(R) + 1$$

$$\stackrel{\text{IH}}{=} (\text{leaves}(L) - 1) + (\text{leaves}(R) - 1) + 1$$

$$= \text{leaves}(L) + \text{leaves}(R) - 1 = \text{leaves}(B) - 1$$



## Structural Induction: Exercise

### Definition (Height of a Binary Tree)

The **height** of a binary tree  $B$ , written  $\text{height}(B)$ , is defined as follows:

$$\text{height}(\square) = 0$$

$$\text{height}(\langle L, \bigcirc, R \rangle) = \max\{\text{height}(L), \text{height}(R)\} + 1$$

Prove by structural induction:

### Theorem

For all binary trees  $B$ :  $\text{leaves}(B) \leq 2^{\text{height}(B)}$ .

## A3.7 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
- ▶ **contraposition**: 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
- ▶ **structural induction**: generalization of mathematical induction to arbitrary recursive structures