

# Discrete Mathematics in Computer Science

## A3. Proofs II

Malte Helmert, Gabriele Röger

University of Basel

September 23, 2020

# Discrete Mathematics in Computer Science

September 23, 2020 — A3. Proofs II

## A3.1 Mathematical Induction

## A3.2 Structural Induction

## A3.1 Mathematical Induction

## Proof Techniques

most common proof techniques:

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

## Mathematical Induction

Concrete Mathematics by Graham, Knuth and Patashnik (p. 3)

Mathematical induction proves that

we can climb as high as we like on a ladder,

by proving that we can climb onto the bottom rung (the basis)

and that

from each rung we can climb up to the next one (the step).

## Propositions

Consider a statement on all natural numbers  $n$  with  $n \geq m$ .

▶ E.g. “Every natural number  $n \geq 2$  can be written as a product of prime numbers.”

▶  $P(2)$ : “2 can be written as a product of prime numbers.”

▶  $P(3)$ : “3 can be written as a product of prime numbers.”

▶  $P(4)$ : “4 can be written as a product of prime numbers.”

▶ ...

▶  $P(n)$ : “ $n$  can be written as a product of prime numbers.”

▶ For every natural number  $n \geq 2$  proposition  $P(n)$  is true.

A **proposition**  $P(n)$  is a mathematical statement that is defined in terms of natural number  $n$ .

## Mathematical Induction

### Mathematical Induction

Proof (of the truth) of proposition  $P(n)$   
for all natural numbers  $n$  with  $n \geq m$ :

▶ **basis**: proof of  $P(m)$

▶ **induction hypothesis** (IH):

suppose that  $P(k)$  is true for all  $k$  with  $m \leq k \leq n$

▶ **inductive step**: proof of  $P(n+1)$

using the induction hypothesis

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

$$\sum_{k=1}^{n+1} (2k-1) = \left( \sum_{k=1}^n (2k-1) \right) + 2(n+1) - 1$$

$$\stackrel{\text{IH}}{=} n^2 + 2(n+1) - 1$$

$$= n^2 + 2n + 1 = (n+1)^2$$

□

## 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  $n + 1 = q_1 \cdot \dots \cdot q_s \cdot r_1 \cdot \dots \cdot r_t$ .

□

## Weak vs. Strong Induction

- ▶ **Weak induction:** Induction hypothesis only supposes that  $P(k)$  is true for  $k = n$
- ▶ **Strong induction:** Induction hypothesis supposes that  $P(k)$  is true for all  $k \in \mathbb{N}_0$  with  $m \leq k \leq n$ 
  - ▶ also: **complete induction**

Our previous definition corresponds to **strong induction**.

Which of the examples had also worked with weak induction?

## Is Strong Induction More Powerful than Weak Induction?

Are there statements that we can prove with strong induction but not with weak induction?

We can always use a stronger proposition:

- ▶ “Every  $n \in \mathbb{N}_0$  with  $n \geq 2$  can be written as a product of prime numbers.”
- ▶  $P(n)$ : “ $n$  can be written as a product of prime numbers.”
- ▶  $P'(n)$ : “all  $k \in \mathbb{N}_0$  with  $2 \leq k \leq n$  can be written as a product of prime numbers.”

## Reformulating Statements

It is sometimes convenient to rephrase a statement.

For example:

- ▶ “ $7^n + 3^n$  is divisible by 10 for all odd  $n \in \mathbb{N}_0$ .”
- ▶ “For all  $n \in \mathbb{N}_0$ : if  $n$  is odd then  $7^n + 3^n$  is divisible by 10.”
  - ▶  $P(n) =$  “if  $n$  is odd then  $7^n + 3^n$  is divisible by 10.”
  - ▶ Need two base cases.
  - ▶ Case distinction ( $n$  even or odd) in inductive step
- ▶ “For all  $n \in \mathbb{N}_0$ :  $7^{(2n+1)} + 3^{(2n+1)}$  is divisible by 10.”
  - ▶  $P'(n) =$  “ $7^{(2n+1)} + 3^{(2n+1)}$  is divisible by 10.”

Be careful about how to reformulate a statement!

## A3.2 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  $\langle L, \circlearrowright, R \rangle$  is a binary tree (with inner node  $\circlearrowright$ ).

**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.”

## 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)

## Structural Induction: Example (1)

### Definition (Leaves of a Binary Tree)

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

$$\begin{aligned} leaves(\square) &= 1 \\ leaves(\langle L, \circlearrowleft, R \rangle) &= leaves(L) + leaves(R) \end{aligned}$$

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

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

$$\begin{aligned} inner(\square) &= 0 \\ inner(\langle L, \circlearrowleft, R \rangle) &= inner(L) + inner(R) + 1 \end{aligned}$$

## Structural Induction: Example (2)

### Theorem

For all binary trees  $B$ :  $inner(B) = leaves(B) - 1$ .

### Proof.

#### induction basis:

$$inner(\square) = 0 = 1 - 1 = leaves(\square) - 1$$

$\rightsquigarrow$  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  $\langle L, \circlearrowleft, R \rangle$ , we may use that it is true for the subtrees  $L$  and  $R$ .

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

$$\begin{aligned} inner(B) &= inner(L) + inner(R) + 1 \\ &\stackrel{\text{IH}}{=} (leaves(L) - 1) + (leaves(R) - 1) + 1 \\ &= leaves(L) + leaves(R) - 1 = leaves(B) - 1 \end{aligned}$$

□

## Structural Induction: Exercise

### Definition (Height of a Binary Tree)

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

$$height(\square) = 0$$
$$height(\langle L, \circlearrowleft, R \rangle) = \max\{height(L), height(R)\} + 1$$

Prove by structural induction:

### Theorem

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