Discrete Mathematics in Computer Science

A5. Proof Techniques II

Malte Helmert, Gabriele Röger

University of Basel

September 30, 2024

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.

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

German: Vollständige Induktion, Induktionsanfang,
Induktionsannahme oder Induktionsvoraussetzung,
Induktionsschritt

Mathematical Induction: Example I

Theorem

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

Mathematical Induction: Example I

Theorem

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

Proof.

Mathematical Induction over n:

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

...

Mathematical Induction: Example I

Theorem

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

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 I

Theorem

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

Proof (continued).

inductive step $n \to n+1$:

- Case 1: $n+1$ is a prime number $\leadsto$ trivial

□

Mathematical Induction: Example I

Theorem

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

Proof (continued).

inductive step $n \to n+1$:

- 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 the IH shows that there are prime numbers
  $q_1, \ldots, q_s$ with $q = q_1 \cdot \ldots \cdot q_s$ and
  $r_1, \ldots, r_t$ with $r = r_1 \cdot \ldots \cdot r_t$.
  Together this means $n+1 = q_1 \cdot \ldots \cdot q_s \cdot r_1 \cdot \ldots \cdot r_t$.

□

Mathematical Induction: Example II

Theorem

Let S be a finite set. Then $|\mathcal{P}(S)| = 2^{|S|}$.

What proposition can we use to prove this with mathematical induction?

Proof by Induction

Proof.

By induction over $|S|$.

Basis ($|S| = 0$): Then $S = \emptyset$ and $|\mathcal{P}(S)| = |\{\emptyset\}| = 1 = 2^0$.

Proof by Induction

Proof.

By induction over $|S|$.

Basis ($|S| = 0$): Then $S = \emptyset$ and $|\mathcal{P}(S)| = |\{\emptyset\}| = 1 = 2^0$.

IH: For all sets S with $|S| \leq n$, it holds that $|\mathcal{P}(S)| = 2^{|S|}$.

Proof by Induction

Proof.

By induction over $|S|$.

Basis ($|S| = 0$): Then $S = \emptyset$ and $|\mathcal{P}(S)| = |\{\emptyset\}| = 1 = 2^0$.

IH: For all sets S with $|S| \leq n$, it holds that $|\mathcal{P}(S)| = 2^{|S|}$.

Inductive Step ($n \rightarrow n + 1$):

Let S' be an arbitrary set with $|S'| = n + 1$ and
let e be an arbitrary member of S'.

Proof by Induction

Proof.

By induction over $|S|$.

Basis ($|S| = 0$): Then $S = \emptyset$ and $|\mathcal{P}(S)| = |\{\emptyset\}| = 1 = 2^0$.

IH: For all sets S with $|S| \leq n$, it holds that $|\mathcal{P}(S)| = 2^{|S|}$.

Inductive Step ($n \rightarrow n + 1$):

Let S' be an arbitrary set with $|S'| = n + 1$ and
let e be an arbitrary member of S'.

Let further $S = S' \setminus \{e\}$ and $X = \{S'' \cup \{e\} \mid S'' \in \mathcal{P}(S)\}$.

Proof by Induction

Proof.

By induction over $|S|$.

Basis ($|S| = 0$): Then $S = \emptyset$ and $|\mathcal{P}(S)| = |\{\emptyset\}| = 1 = 2^0$.

IH: For all sets S with $|S| \leq n$, it holds that $|\mathcal{P}(S)| = 2^{|S|}$.

Inductive Step ($n \rightarrow n + 1$):

Let S' be an arbitrary set with $|S'| = n + 1$ and let e be an arbitrary member of S'.

Let further $S = S' \setminus \{e\}$ and $X = \{S'' \cup \{e\} \mid S'' \in \mathcal{P}(S)\}$.

Then $\mathcal{P}(S') = \mathcal{P}(S) \cup X$. As $\mathcal{P}(S)$ and X are disjoint and $|X| = |\mathcal{P}(S)|$, it holds that $|\mathcal{P}(S')| = 2|\mathcal{P}(S)|$.

Proof by Induction

Proof.

By induction over $|S|$.

Basis ($|S| = 0$): Then $S = \emptyset$ and $|\mathcal{P}(S)| = |\{\emptyset\}| = 1 = 2^0$.

IH: For all sets S with $|S| \leq n$, it holds that $|\mathcal{P}(S)| = 2^{|S|}$.

Inductive Step ($n \to n + 1$):

Let S' be an arbitrary set with $|S'| = n + 1$ and
let e be an arbitrary member of S'.

Let further $S = S' \setminus \{e\}$ and $X = \{S'' \cup \{e\} \mid S'' \in \mathcal{P}(S)\}$.

Then $\mathcal{P}(S') = \mathcal{P}(S) \cup X$. As $\mathcal{P}(S)$ and X are disjoint and $|X| = |\mathcal{P}(S)|$, it holds that $|\mathcal{P}(S')| = 2|\mathcal{P}(S)|$.

Since $|S| = n$, we can use the IH and get

$$|\mathcal{P}(S')| = 2 \cdot 2^{|S|} = 2 \cdot 2^n = 2^{n+1} = 2^{|S'|}.$$

□

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

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.

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?

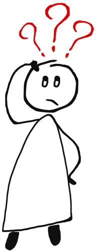
Is Strong Induction More Powerful than Weak Induction?

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."

Questions



Questions?

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.

German: Binärbaum, Blatt, innerer Knoten

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

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:

- $\Box$ 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 $\bigcirc$).

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

German: Binärbaum, Blatt, innerer Knoten

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

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:

$$leaves(\square) = 1$$
$$leaves(\langle L, \bigcirc, R\rangle) = leaves(L) + leaves(R)$$

Definition (Inner Nodes of a Binary Tree)

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

$$inner(\square) = 0$$
$$inner(\langle L, \bigcirc, R\rangle) = inner(L) + inner(R) + 1$$

Structural Induction: Example (2)

Theorem

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

Structural Induction: Example (2)

Theorem

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

Proof.

induction basis:

$\mathit{inner}(\Box) = 0 = 1 - 1 = \mathit{leaves}(\Box) - 1$

$\leadsto$ 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.

□

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 $B = \langle L, \bigcirc, R \rangle$:

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

□

Structural Induction: Exercise

Definition (Height of a Binary Tree)

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

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

Prove by structural induction:

Theorem

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

Example: Tarradiddles

Example (Tarradiddles)

The set of tarradiddles is inductively defined as follows:

- ✈ is a tarradiddle.
- ♥ is a tarradiddle.
- If x and y are tarradiddles, then x✿✿y is a tarradiddle.
- If x and y are tarradiddles, then ✿x✈y✿ is a tarradiddle.

Example: Tarradiddles

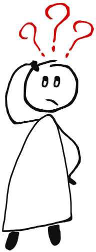
Example (Tarradiddles)

The set of tarradiddles is inductively defined as follows:

- ✈ is a tarradiddle.
- ♥ is a tarradiddle.
- If x and y are tarradiddles, then x✿✿y is a tarradiddle.
- If x and y are tarradiddles, then ✿x✈y✿ is a tarradiddle.

How do you prove with structural induction that every tarradiddle contains an even number of flowers?

Questions



Questions?

Excursus: Computer-assisted Theorem Proving

Computer-assisted Proofs

- Computers can help proving theorems.
- Computer-aided proofs have for example been used for proving theorems by exhaustion.
- Example: Four color theorem

Interactive Theorem Proving

- On the lowest abstraction level, rigorous mathematical proofs rely on formal logic.

Interactive Theorem Proving

- On the lowest abstraction level, rigorous mathematical proofs rely on formal logic.
- On this level, proofs can be automatically verified by computers.

Interactive Theorem Proving

- On the lowest abstraction level, rigorous mathematical proofs rely on formal logic.
- On this level, proofs can be automatically verified by computers.
- Nobody wants to write or read proofs on this level of detail.

Interactive Theorem Proving

- On the lowest abstraction level, rigorous mathematical proofs rely on formal logic.
- On this level, proofs can be automatically verified by computers.
- Nobody wants to write or read proofs on this level of detail.
- In Interactive Theorem Proving a human guides the proof and the computer tries to fill in the details.

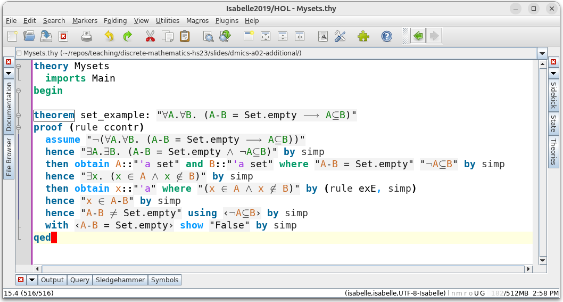
Interactive Theorem Proving

- On the lowest abstraction level, rigorous mathematical proofs rely on formal logic.
- On this level, proofs can be automatically verified by computers.
- Nobody wants to write or read proofs on this level of detail.
- In Interactive Theorem Proving a human guides the proof and the computer tries to fill in the details.
- If it succeeds, we can be very confident that the proof is valid.

Interactive Theorem Proving

- On the lowest abstraction level, rigorous mathematical proofs rely on formal logic.
- On this level, proofs can be automatically verified by computers.
- Nobody wants to write or read proofs on this level of detail.
- In Interactive Theorem Proving a human guides the proof and the computer tries to fill in the details.
- If it succeeds, we can be very confident that the proof is valid.
- Example theorem provers: Isabelle/HOL, Lean

Example



⇝ Demo

Summary

Summary

- Mathematical induction is used to prove a proposition P for all natural numbers $\geq m$.
  - Prove $P(m)$.
  - Make hypothesis that $P(k)$ is true for $m \leq k \leq n$.
  - Establish $P(n+1)$ using the hypothesis.
- Structural induction applies the same general concept to prove a proposition P for all elements of an inductively defined set.