Logical and Theoretical Foundations of Computer Science

LaTFoCS

Pamela Fleischmann

fpa@informatik.uni-kiel.de

Winter Semester 2019

Kiel University
Dependable Systems Group

Mathematical Induction

Mathematical Induction

- Proving technique that elements of a *somehow* structured set have a specific property.

Mathematical Induction

- Proving technique that elements of a *somehow* structured set have a specific property.
- What does *somehow structured* mean?

Mathematical Induction

- Proving technique that elements of a *somehow* structured set have a specific property.
- What does *somehow structured* mean?
  - The set has to have a basis - a set of building atoms which are not dividable.

Mathematical Induction

- Proving technique that elements of a *somehow* structured set have a specific property.
- What does *somehow structured* mean?
  - The set has to have a basis - a set of building atoms which are not dividable.
  - The set needs to have rules how to build the complete set just with the atoms and some operators.

Somehow Structured Sets

What do we get if we have

- 1 and the function $s : \mathbb{N} \to \mathbb{N};\ n \mapsto n + 1$?
- 0 and the function $s : \mathbb{N} \to \mathbb{N};\ n \mapsto n + 2$?
- $\Sigma = \{a, b, c, \ldots, z, \sqcup\}$ and $\cdot$ as concatenation?
- $\mathbb{N} \cup \{(,), +, \cdot\}$ and concatenation?
- S a set of variables $V = \{A, B\}$, an alphabet $\Sigma = \{a, b\}$ and $S \to AB|a$, $A \to B|b$, and $B \to BA|ab$?

Natural Induction

- Proving technique that each natural number has a specific property.
- Based on the Peano Axioms: Let $s : \mathbb{N} \longrightarrow \mathbb{N};\ n \mapsto n+1$ be the successor function.
  1. $1 \in \mathbb{N}$
  2. $\forall n :\ n \in \mathbb{N} \longrightarrow s(n) \in \mathbb{N}$
  3. $\forall n :\ n \in \mathbb{N} \longrightarrow s(n) \neq 1$
  4. $\forall m, n :\ s(m) = s(n) \longrightarrow m = n$ (injectivity)
  5. induction axiom
     $\forall X :\ (1 \in X \wedge \forall n\, (n \in \mathbb{N} \longrightarrow (n \in X \longrightarrow s(n) \in X)) \longrightarrow \mathbb{N} \subseteq X)$

Induction Axiom

$$\forall X :\ (1 \in X \land \forall n\, (n \in \mathbb{N} \to (n \in X \to s(n) \in X)) \to \mathbb{N} \subseteq X)$$

Induction Axiom

$$\forall X: \ (1 \in X \land \forall n \, (n \in \mathbb{N} \longrightarrow (n \in X \longrightarrow s(n) \in X)) \longrightarrow \mathbb{N} \subseteq X)$$

- X arbitrary set

Induction Axiom

$$\forall X : (1 \in X \land \forall n\,(n \in \mathbb{N} \to (n \in X \to s(n) \in X)) \to \mathbb{N} \subseteq X)$$

- X arbitrary set
- if we prove that

Induction Axiom

$$\forall X : (1 \in X \land \forall n \, (n \in \mathbb{N} \rightarrow (n \in X \rightarrow s(n) \in X)) \rightarrow \mathbb{N} \subseteq X)$$

- X arbitrary set
- if we prove that
  - $1 \in X$ and

Induction Axiom

$$\forall X : (1 \in X \land \forall n \, (n \in \mathbb{N} \rightarrow (n \in X \rightarrow s(n) \in X)) \rightarrow \mathbb{N} \subseteq X)$$

- X arbitrary set
- if we prove that
  - $1 \in X$ and
  - for all natural numbers being in X their successor is also in X

Induction Axiom

$$\forall X : (1 \in X \land \forall n\, (n \in \mathbb{N} \rightarrow (n \in X \rightarrow s(n) \in X)) \rightarrow \mathbb{N} \subseteq X)$$

- X arbitrary set
- if we prove that
  - $1 \in X$ and
  - for all natural numbers being in X their successor is also in X
- then X has to contain all natural numbers

How to use the Induction Axiom

If we want to prove that all natural numbers have a property P (being either 1 or strictly greater than 1)

How to use the Induction Axiom

If we want to prove that all natural numbers have a property P (being either 1 or strictly greater than 1)

1. we define the set X by containing all natural numbers fulfilling P (notice $X \subseteq \mathbb{N}$)

How to use the Induction Axiom

If we want to prove that all natural numbers have a property P (being either 1 or strictly greater than 1)

1. we define the set X by containing all natural numbers fulfilling P (notice $X \subseteq \mathbb{N}$)
2. if we are able to prove that the induction axiom holds for this X, we know $N \subseteq X$ and consequently $\mathbb{N} = X$

How to use the Induction Axiom

If we want to prove that all natural numbers have a property P (being either 1 or strictly greater than 1)

1. we define the set X by containing all natural numbers fulfilling P (notice $X \subseteq \mathbb{N}$)
2. if we are able to prove that the induction axiom holds for this X, we know $N \subseteq X$ and consequently $\mathbb{N} = X$
3. since X has only elements with property P, $\mathbb{N}$ has only elements with property P

Example

Claim: Each natural number is either 1 or strictly greater than 1.

Proof:

Example

Claim: Each natural number is either 1 or strictly greater than 1.
Proof:

- Set $X = \{n \in \mathbb{N} \mid n = 1 \dot{\vee} n > 1\}$.

Example

Claim: Each natural number is either 1 or strictly greater than 1.
Proof:

- Set $X = \{n \in \mathbb{N} \mid n = 1 \dot{\vee} n > 1\}$.
- By $1 = 1$ we have $1 \in X$.

Example

Claim: Each natural number is either 1 or strictly greater than 1.

Proof:

- Set $X = \{n \in \mathbb{N} | \, n = 1 \dot{\vee} n > 1\}$.
- By $1 = 1$ we have $1 \in X$.
- Let be $n \in X$ for an arbitrary but fixed $n \in \mathbb{N}$.

Example

Claim: Each natural number is either 1 or strictly greater than 1.

Proof:

- Set $X = \{n \in \mathbb{N} | \, n = 1 \dot{\vee} n > 1\}$.
- By $1 = 1$ we have $1 \in X$.
- Let be $n \in X$ for an arbitrary but fixed $n \in \mathbb{N}$.
- We have to show $n + 1 \in X$. Since $n \in X$ we have two cases.

Example

Claim: Each natural number is either 1 or strictly greater than 1.
Proof:

- Set $X = \{n \in \mathbb{N} | \, n = 1 \dot{\vee} n > 1\}$.
- By $1 = 1$ we have $1 \in X$.
- Let be $n \in X$ for an arbitrary but fixed $n \in \mathbb{N}$.
- We have to show $n + 1 \in X$. Since $n \in X$ we have two cases.
- If $n = 1$ then $n + 1 = 2 > 1$ and thus $n + 1 \in X$.

Example

Claim: Each natural number is either 1 or strictly greater than 1.
Proof:

- Set $X = \{n \in \mathbb{N} | n = 1 \dot{\vee} n > 1\}$.
- By $1 = 1$ we have $1 \in X$.
- Let be $n \in X$ for an arbitrary but fixed $n \in \mathbb{N}$.
- We have to show $n + 1 \in X$. Since $n \in X$ we have two cases.
- If $n = 1$ then $n + 1 = 2 > 1$ and thus $n + 1 \in X$.
- If $n > 1$ then $n + 1 > n > 1$ and thus $n + 1 \in X$.

Example

Claim: Each natural number is either 1 or strictly greater than 1.
Proof:

- Set $X = \{n \in \mathbb{N} | n = 1 \dot{\vee} n > 1\}$.
- By $1 = 1$ we have $1 \in X$.
- Let be $n \in X$ for an arbitrary but fixed $n \in \mathbb{N}$.
- We have to show $n + 1 \in X$. Since $n \in X$ we have two cases.
- If $n = 1$ then $n + 1 = 2 > 1$ and thus $n + 1 \in X$.
- If $n > 1$ then $n + 1 > n > 1$ and thus $n + 1 \in X$.
- By the induction axiom we have $\mathbb{N} \subseteq X$ and thus $X = \mathbb{N}$. $\square$

Pecularities of the natural number

- natural induction works on every well-ordered set

Pecularities of the natural number

- natural induction works on every well-ordered set
- some claims hold only for all $n \in \mathbb{N}_{\geq x}$ and not all $n \in \mathbb{N}$

$$1 + 5n < (1 + 5)^n$$

Pecularities of the natural number

- natural induction works on every well-ordered set
- some claims hold only for all $n \in \mathbb{N}_{\geq x}$ and not all $n \in \mathbb{N}$

$$1 + 5n < (1 + 5)^n$$

- each subset of $\mathbb{N}$ of the shape $\mathbb{N}_{\geq x}$ is isomorphic to $\mathbb{N}$

Pecularities of the natural number

- natural induction works on every well-ordered set
- some claims hold only for all $n \in \mathbb{N}_{\geq x}$ and not all $n \in \mathbb{N}$

$$1 + 5n < (1 + 5)^n$$

- each subset of $\mathbb{N}$ of the shape $\mathbb{N}_{\geq x}$ is isomorphic to $\mathbb{N}$
- natural deduction works on $\mathbb{N}_{\geq x}$

More Practical Perspective on Natural Induction

Definition (Induction Principle)

If a property P holds for 1 (base case) and if the fact that P holds for a fixed but arbitrary $n \in \mathbb{N}$ already implies that $n+1$ has this property as well (induction step) then P holds for all natural numbers.

More Practical Perspective on Natural Induction

Definition (Induction Principle)

If a property P holds for 1 (base case) and if the fact that P holds for a fixed but arbitrary $n \in \mathbb{N}$ already implies that $n+1$ has this property as well (induction step) then P holds for all natural numbers.

in detail:

- base case: prove that the property holds for 1

More Practical Perspective on Natural Induction

Definition (Induction Principle)

If a property P holds for 1 (base case) and if the fact that P holds for a fixed but arbitrary $n \in \mathbb{N}$ already implies that $n + 1$ has this property as well (induction step) then P holds for all natural numbers.

in detail:

- base case: prove that the property holds for 1
- induction step: we have to prove an implication

More Practical Perspective on Natural Induction

Definition (Induction Principle)

If a property P holds for 1 (base case) and if the fact that P holds for a fixed but arbitrary $n \in \mathbb{N}$ already implies that $n+1$ has this property as well (induction step) then P holds for all natural numbers.

in detail:

- base case: prove that the property holds for 1
- induction step: we have to prove an implication
- thus we can assume that the premise is true (induction hypothesis)

More Practical Perspective on Natural Induction

Definition (Induction Principle)

If a property P holds for 1 (base case) and if the fact that P holds for a fixed but arbitrary $n \in \mathbb{N}$ already implies that $n + 1$ has this property as well (induction step) then P holds for all natural numbers.

in detail:

- base case: prove that the property holds for 1
- induction step: we have to prove an implication
- thus we can assume that the premise is true (induction hypothesis)
- we have to prove the conclusion, namely $P(n + 1)$

Avoiding Popular Mistakes

- Prove the base case decently even if it seems to be easy. $(1 + 5n < (1 + 5)^n)$

Avoiding Popular Mistakes

- Prove the base case decently even if it seems to be easy. $(1 + 5n < (1 + 5)^n)$
- the induction hypothesis is assumed for **one arbitrary but fixed** $n \in \mathbb{N}$ (not for all!)

Avoiding Popular Mistakes

- Prove the base case decently even if it seems to be easy. ($1 + 5n < (1 + 5)^n$)
- the induction hypothesis is assumed for **one arbitrary but fixed** $n \in \mathbb{N}$ (not for all!)
- in the induction step you are allowed to use the base case and the hypothesis

Example

Claim: $\forall n \in \mathbb{N} : \ (n+1)(n-1) = n^2 - 1$

Proof:

Example

Claim: $\forall n \in \mathbb{N} : \ (n+1)(n-1) = n^2 - 1$

Proof:

BC For $n = 1$ we have
$$(1+1)(1-1) = 2 \cdot 0 = 0 = 1 - 1 = 1^2 - 1.$$

Example

Claim: $\forall n \in \mathbb{N}: \; (n+1)(n-1) = n^2 - 1$

Proof:

BC For $n = 1$ we have
$(1+1)(1-1) = 2 \cdot 0 = 0 = 1 - 1 = 1^2 - 1.$

IH Assume that the claim holds for one arbitrary but fixed $n \in \mathbb{N}$

Example

Claim: $\forall n \in \mathbb{N} : (n+1)(n-1) = n^2 - 1$

Proof:

BC For $n = 1$ we have
$(1+1)(1-1) = 2 \cdot 0 = 0 = 1 - 1 = 1^2 - 1.$

IH Assume that the claim holds for one arbitrary but fixed $n \in \mathbb{N}$

IS We have

Example

Claim: $\forall n \in \mathbb{N}: \ (n+1)(n-1) = n^2 - 1$

Proof:

BC For $n = 1$ we have
$(1+1)(1-1) = 2 \cdot 0 = 0 = 1 - 1 = 1^2 - 1.$

IH Assume that the claim holds for one arbitrary but fixed $n \in \mathbb{N}$

IS We have

$$
\begin{aligned}
((n+1)+1)((n+1)-1) &= ((n+1)+1)((n-1)+1) \\
&= (n+1)(n-1) + (n+1) + (n-1) + 1 \\
&\overset{IH}{=} n^2 - 1 + 2n + 1 = (n^2 + 2n + 1) - 1 \\
&= (n+1)^2 - 1
\end{aligned}
$$

Noether (Course-of-value) Induction

- in the induction hypothesis we assume $P(n)$ for an arbitrary but fixed $n \in \mathbb{N}$

Noether (Course-of-value) Induction

- in the induction hypothesis we assume $P(n)$ for an arbitrary but fixed $n \in \mathbb{N}$
- in the induction step we prove $P(n+1)$ based on $P(n)$ and $P(1)$

Noether (Course-of-value) Induction

- in the induction hypothesis we assume $P(n)$ for an arbitrary but fixed $n \in \mathbb{N}$
- in the induction step we prove $P(n+1)$ based on $P(n)$ and $P(1)$
- in finitely many steps we can also prove $P(2), \ldots, P(n-1)$ (each time with the implication)

Noether (Course-of-value) Induction

- in the induction hypothesis we assume $P(n)$ for an arbitrary but fixed $n \in \mathbb{N}$
- in the induction step we prove $P(n+1)$ based on $P(n)$ and $P(1)$
- in finitely many steps we can also prove $P(2), \ldots, P(n-1)$ (each time with the implication)
- thus we are also allowed to use $P(k)$ for all $k \leq n$

Noether (Course-of-value) Induction

- in the induction hypothesis we assume $P(n)$ for an arbitrary but fixed $n \in \mathbb{N}$
- in the induction step we prove $P(n+1)$ based on $P(n)$ and $P(1)$
- in finitely many steps we can also prove $P(2), \dots, P(n-1)$ (each time with the implication)
- thus we are also allowed to use $P(k)$ for all $k \leq n$
- be careful: the induction hypothesis needs to be adjusted!

Prime Number Factorisation with Peano

Claim: All natural number have a prime number factorisation.
Proof: Define the predicate $P(n)$ that is true if n has a prime number factorisation. Set $X = \{n \in \mathbb{N} | P(n)\}$. Since 1 is a prime number it has a prime number factorisation and we have $1 \in X$. Let be $k \in X$ for all $k \leq n$ for an arbitrary but fixed $n \in \mathbb{N}$. We have to prove $n+1 \in X$. If $n+1$ is a prime number, $n+1 \in X$. If $n+1$ is not a prime number, then there exists $u, v \in \mathbb{N}_{<n}$ with $n+1 = uv$. By induction hypothesis u and v each have a prime number factorisation. The multiplication of these prime number products is a product of prime numbers and thus a prime number factorisation of $n+1$, i.e. $n+1 \in X$.

Structural Induction - Motivation

- **structure** of $\mathbb{N}$: you can get all elements by adding successively 1 starting by 1

Structural Induction - Motivation

- **structure** of $\mathbb{N}$: you can get all elements by adding successively 1 starting by 1
- **structure** of all the even numbers: adding successively 2 starting by 2

Structural Induction - Motivation

- **structure** of $\mathbb{N}$: you can get all elements by adding successively 1 starting by 1
- **structure** of all the even numbers: adding successively 2 starting by 2
- **structure** of the formulae: adding successively $\neg, \wedge, \vee, \rightarrow$ starting with the atoms

Structural Induction - Motivation

- **structure** of $\mathbb{N}$: you can get all elements by adding successively 1 starting by 1
- **structure** of all the even numbers: adding successively 2 starting by 2
- **structure** of the formulae: adding successively $\neg, \wedge, \vee, \rightarrow$ starting with the atoms
- induction uses the structure for covering all cases

Structural Induction - Motivation

- **structure** of $\mathbb{N}$: you can get all elements by adding successively 1 starting by 1
- **structure** of all the even numbers: adding successively 2 starting by 2
- **structure** of the formulae: adding successively $\neg, \wedge, \vee, \rightarrow$ starting with the atoms
- induction uses the structure for covering all cases
- structural induction and natural induction equivalent: each formula has a length and a height which are natural numbers

Structural Induction

Let $(\mathcal{M}, \mathcal{A}, \mathcal{S})$ be a structure with a set of atoms $\mathcal{A} \subseteq \mathcal{M}$ and a set of operator $\mathcal{S}$ such that $s(m_1, \ldots, m_k) \in \mathcal{M}$ for all k-ary operator $s \in \mathcal{S}$, $k \in \mathbb{N}$, and $m_1, \ldots, m_k \in \mathcal{M}$. Let ℓ be the highest arity in S.

Definition (Structural Induction Principle)

If a property P holds for all $a \in \mathcal{A}$ (base case) and if the fact that P holds for fixed but arbitrary $m_1, \ldots, m_\ell \in \mathcal{M}$ already implies that P holds for $s(m_1, \ldots, m_k)$ for all $s \in \mathcal{S}$ (induction step) then P holds for all elements of $\mathcal{M}$.

Structural Induction

Let $(\mathcal{M}, \mathcal{A}, \mathcal{S})$ be a structure with a set of atoms $\mathcal{A} \subseteq \mathcal{M}$ and a set of operator $\mathcal{S}$ such that $s(m_1, \ldots, m_k) \in \mathcal{M}$ for all k-ary operator $s \in \mathcal{S}$, $k \in \mathbb{N}$, and $m_1, \ldots, m_k \in \mathcal{M}$. Let ℓ be the highest arity in S.

Definition (Structural Induction Principle)

If a property P holds for all $a \in \mathcal{A}$ (base case) and if the fact that P holds for fixed but arbitrary $m_1, \ldots, m_\ell \in \mathcal{M}$ already implies that P holds for $s(m_1, \ldots, m_k)$ for all $s \in \mathcal{S}$ (induction step) then P holds for all elements of $\mathcal{M}$.

Examples later.