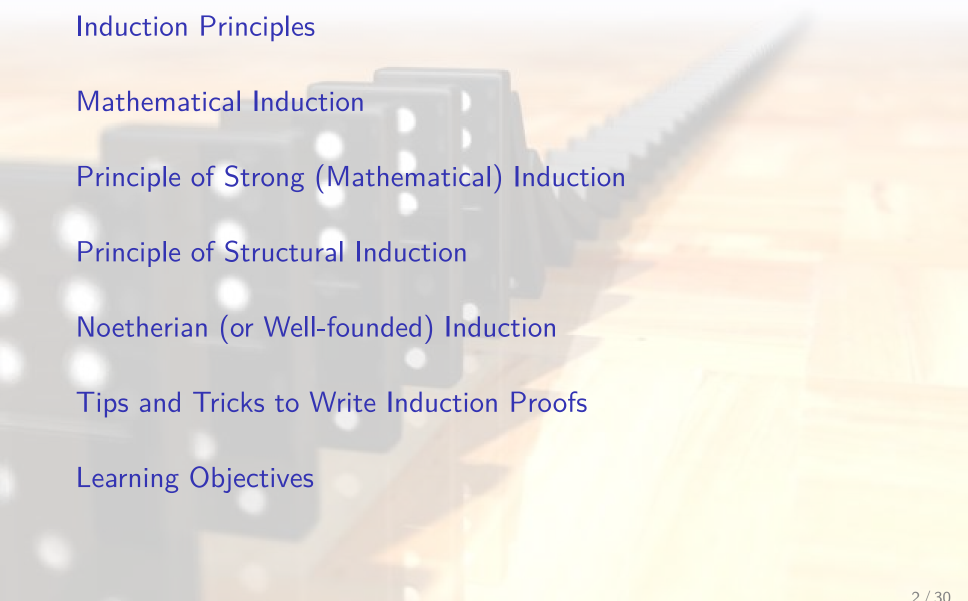
Formale Methoden der Informatik

Tutorial: Induction Proofs

Uwe Egly

Knowledge-Based Systems Group
Institute of Information Systems
Vienna University of Technology

Outline



Induction Principles

Mathematical Induction

Principle of Strong (Mathematical) Induction

Principle of Structural Induction

Noetherian (or Well-founded) Induction

Tips and Tricks to Write Induction Proofs

Learning Objectives

How can we prove the following statements?

- Summation formulas like $\sum_{i=0}^{n} 2^i = 2^{n+1}$ for all $n \in \mathbb{N}_0$
- Inequalities like $2^n < n!$ for each integer $n \geq 4$
- Divisibility results like $n^3 - n$ is divisible by 3 for each $n \in \mathbb{N}$
- Results about sets like any set of $n \in \mathbb{N}$ elements has 2^n subsets
- Correctness or termination results about algorithms like The function `fac(n) returns` $n!$ for all $n \in \mathbb{N}_0$

Induction Principles

- A central proof techniques in mathematics and computer science:

  Induction principles

- Formalized as an axiom schema like

$$[P(1) \land \forall k \in \mathbb{N}\, (P(k) \to P(k+1))] \to \forall n \in \mathbb{N}\, P(n)$$

- Different kinds of induction
  - Mathematical induction (and its variants)
  - Strong mathematical induction
  - Structural induction (e.g., for inductively defined data types)
  - Noetherian (or well-founded) induction
- Details and examples are presented later.

Principle of mathematical induction

Let $\mathcal{P}(n)$ be a statement involving a variable n. Suppose

1. $\mathcal{P}(1)$ is true;
2. if $\mathcal{P}(k)$ is true for some natural numbers $k \geq 1$, then $\mathcal{P}(k+1)$ is also true.

Then $\mathcal{P}(n)$ is true for all natural numbers $n = 1, 2, \ldots$

- In the base case, we prove that $\mathcal{P}(1)$ is true.
- We are allowed to assume that $\mathcal{P}(k)$ is true for some $k \geq 1$. This is the induction hypothesis.
- We prove $\mathcal{P}(k+1)$ true in the induction step. In the course of this proof, we (usually) apply the induction hypothesis.

Principle of mathematical induction

An example proof using mathematical induction

Theorem: The sum of the first n positive odd integers is n^2.

Proof. We want to prove that, for all natural numbers n, $\mathcal{P}(n)$ holds, where $\mathcal{P}(n)$ denotes $\sum_{i=0}^{n-1}(2i+1) = n^2$. The proof is by mathematical induction on n.

Base case. We show that $\mathcal{P}(1)$ is true. This is the case since

$$\sum_{i=0}^{n-1}(2i+1) = 1 = n^2 \,.$$

Induction hypothesis. Assume $\mathcal{P}(k)$ is true for some $k \geq 1$.

Induction step. We want to show that $\mathcal{P}(k+1)$ is true. Therefore, we need to show that $\sum_{i=0}^{k}(2i+1) = (k+1)^2$ holds.

Principle of mathematical induction

An example proof using mathematical induction (cont'd)

By the induction hypothesis, $\mathcal{P}(k)$ is true. Then we derive

$$
\begin{aligned}
&\mathcal{P}(k) \text{ is true iff} \\
\sum_{i=0}^{k-1} (2i+1) &= k^2 \quad \text{iff} \\
2k+1+\sum_{i=0}^{k-1} (2i+1) &= k^2 + 2k + 1 \quad \text{iff} \\
\sum_{i=0}^{k} (2i+1) &= (k+1)^2 \,.
\end{aligned}
$$

Hence, $\mathcal{P}(k+1)$ is true. □

Principle of mathematical induction

A correctness and termination proof by mathematical induction

```
Algorithm 1: The power function $pow(b, n) : \mathbb{N} \times \mathbb{N}_0 \mapsto \mathbb{N}$
Input: $b$, $n$: a positive and a non-negative integer
Output: The computed positive integer value for $b$, $n$
if $n == 0$ then return $1$ ;
else return $b \times pow(b, n-1)$ ;
```

We prove the correctness of $pow(\cdot, \cdot)$.

Proof. We want to prove that, for all natural numbers n (including 0), $\mathcal{P}(n)$ holds, where $\mathcal{P}(n)$ denotes the statement that for any positive integer b and the non-negative integer n, $pow(b, n)$ computes b^n. The proof is by mathematical induction on n.

Principle of mathematical induction

A correctness and termination proof by mathematical induction (cont'd)

Base case. We show that $\mathcal{P}(0)$ is true. This is the case since $pow(b, 0)$ terminates in line 1 and returns the correct value $b^0 = 1$ for any natural number b.

Induction hypothesis. Assume $\mathcal{P}(k)$ is true for some integer $k \geq 0$.

Induction step. We want to show that $\mathcal{P}(k + 1)$ is true. Consider $pow(b, k + 1)$ and observe that $k + 1 > 0$. Therefore, line 2 is reached and $b \times pow(b, k)$ is computed. From the induction hypothesis, we know that $pow(b, k)$ computes b^k for any positive integer b and therefore $pow(b, k + 1)$ computes the correct values $b \times b^k = b^{k+1}$. Hence, $\mathcal{P}(k + 1)$ is true. □

Remark: We started the induction from 0. What do we have to change in order to use exactly the mathematical induction schema from above?

Principle of mathematical induction: Variation 1

Let $\mathcal{P}(n)$ be a statement involving a variable n. Suppose

1. $\mathcal{P}(k_0)$ is true for some natural number k_0;
2. if $\mathcal{P}(k)$ is true for some natural numbers $k \geq k_0$, then $\mathcal{P}(k+1)$ is also true.

Then $\mathcal{P}(n)$ is true for all natural numbers $n = k_0, k_0 + 1, \ldots$

Useful, e.g., to prove that $2^n > n^2$ for all natural numbers $n \geq 5$.

Remark: Variation 1 can be translated to standard mathematical induction by $\mathcal{Q}(r - k_0 + 1) = \mathcal{P}(r)$, where $k_0 \leq r$.

Principle of mathematical induction: Variation 1

Prove: $2^n > n^2$ for all natural numbers $n \geq 5$.

Proof. Let $\mathcal{P}(n)$ denote the statement $2^n > n^2$. The proof is by mathematical induction on n starting with $n_0 = 5$.

Base case: $n_0 = 5$. $\mathcal{P}(n_0)$ is true because $2^5 = 32 > 25 = 5^2$.

Induction hypothesis. Assume $\mathcal{P}(n)$ is true for some $n \geq n_0$.

Induction step. We want to show that $\mathcal{P}(n+1)$ is true. By the induction hypothesis, $\mathcal{P}(n)$ is true. Then we derive

$$\begin{aligned} 2^n &> n^2 \quad \text{iff} \\ 2 \cdot 2^n &> 2 \cdot n^2 \quad \text{iff} \\ 2^{n+1} &> 2 \cdot n^2 \,. \end{aligned}$$

Since $n \geq 5$, $2 \cdot n^2 > (n+1)^2$ holds. Then $2^{n+1} > (n+1)^2$ follows by the transitivity of $>$. Hence, $\mathcal{P}(n+1)$ is true. □

Principle of mathematical induction: Variation 2

Its principle and a short example

Let $\mathcal{P}(n)$ be a statement involving a variable n. Suppose

1. $\mathcal{P}(1)$ and $\mathcal{P}(2)$ are true;
2. if $\mathcal{P}(k)$ and $\mathcal{P}(k+1)$ are true for some natural numbers k, then $\mathcal{P}(k+2)$ is also true.

Then $\mathcal{P}(n)$ is true for all natural numbers $n = 1, 2, \ldots$

Further generalizations are possible: Use more than two levels, start with some $n > 1$, etc.

Useful, e.g., to prove the following:
Let $\{a_n\}$ be a sequence of natural numbers such that $a_1 = 5$, $a_2 = 13$ and $a_{n+2} = 5a_{n+1} - 6a_n$ for all natural numbers n. Show that $a_n = 2^n + 3^n$ holds for all natural numbers n.

Principle of mathematical induction: Variation 2

A proof for the example

Proof. We want to prove that, for all natural numbers n, $\mathcal{P}(n)$ holds, where $\mathcal{P}(n)$ denotes $a_n = 2^n + 3^n$. The proof is by mathematical induction on n.

Base cases. $\mathcal{P}(1)$ is true, because $a_1 = 5 = 2^1 + 3^1$. Moreover, $\mathcal{P}(2)$ is true, because $a_2 = 13 = 2^2 + 3^2$.

Induction hypothesis. Assume $\mathcal{P}(k)$ and $\mathcal{P}(k+1)$ are true for some $k \geq 1$.

Induction step. We want to show that $\mathcal{P}(k+2)$ is true.

Principle of mathematical induction: Variation 2

A proof for the example (cont'd)

From the induction hypothesis, we have $a_k = 2^k + 3^k$ and $a_{k+1} = 2^{k+1} + 3^{k+1}$. We compute

$$\begin{aligned} a_{k+2} &= 5 \cdot a_{k+1} - 6 \cdot a_k \\ &= 5 \cdot 2^{k+1} + 5 \cdot 3^{k+1} - 6 \cdot 2^k - 6 \cdot 3^k \\ &= 5 \cdot 2^{k+1} + 5 \cdot 3^{k+1} - 3 \cdot 2^{k+1} - 2 \cdot 3^{k+1} \\ &= 2 \cdot 2^{k+1} + 3 \cdot 3^{k+1} \\ &= 2^{k+2} + 3^{k+2} \end{aligned}$$

Hence, $\mathcal{P}(k+2)$ is true. □

Principle of strong (mathematical) induction

Let $\mathcal{P}(n)$ be a statement involving a variable n. Suppose

1. $\mathcal{P}(1)$ is true;
2. if, for some natural numbers k, $\mathcal{P}(1), \mathcal{P}(2), \ldots, \mathcal{P}(k)$ are all true, then $\mathcal{P}(k+1)$ is also true.

Then $\mathcal{P}(n)$ is true for all natural numbers $n = 1, 2, \ldots$

The induction hypothesis is stronger (compared to above).
NB: Stronger means potentially less models

Find examples where strong induction can be beneficially applied!

Principle of structural induction

In order to show that a statement holds for all elements of a recursively defined set, use the following:

Base case(s). Prove that the statement holds for all elements specified in the base case(s) of the set definition.

Induction step. Prove that if the statement is true for each of the elements used to construct elements in the inductive step of the set definition, then the result holds for these new elements.

➥ The structure of a structural induction proof "follows" the structure of the underlying definition.

Principle of structural induction

The basic definitions for the list example

Consider the following definition of lists

$$lst ::= nil \mid (c : lst)$$

where : means LISP cons and *nil* denotes the empty list.

Example

A list with three elements $1, 2, 3$ looks as follows:

$$(1 : (2 : (3 : nil)))$$

Principle of structural induction

Appending two lists

We want to implement an append (*app*) function recursively:

$$
\begin{aligned}
app(nil, y) &= y && (1)\\
app((c : x), y) &= (c : app(x, y)) && (2)
\end{aligned}
$$

Example

We want to append $(a : (b : nil))$ and $(c : nil)$

$$
\begin{aligned}
app((a : (b : nil)), (c : nil)) &=_{(2)} (a : app((b : nil), (c : nil)))\\
&=_{(2)} (a : (b : app(nil, (c : nil))))\\
&=_{(1)} (a : (b : (c : nil)))
\end{aligned}
$$

Principle of structural induction

Proving properties about *app*

Let $\mathcal{P}(x)$ denote $app(x, nil) = x$.

Show that, for all lists ℓ, $\mathcal{P}(\ell)$ holds.

Proof: We proceed by structural induction on the definition of lists.

Basis case: $\ell = nil$. Then $\mathcal{P}(\ell)$ is $app(nil, nil) = nil$ which follows immediately from the first defining equality (1).

Induction hypothesis. Assume that $\mathcal{P}(\ell)$ holds for some list ℓ.

Principle of structural induction

Proving properties about *app* (cont'd)

Induction step. We have to establish $\mathcal{P}((c : \ell))$. The induction hypothesis gives us

$$app(\ell, nil) = \ell.$$

We concatenate c to the left on both sides resulting in

$$(c : app(\ell, nil)) = (c : \ell).$$

By the second defining equality (2), we get

$$app((c : \ell), nil) = (c : \ell).$$

Hence, $\mathcal{P}((c : \ell))$ holds.
Consequently, $\mathcal{P}(\ell)$ is true for all lists. □

How can we use mathematical induction to prove the above result?

Noetherian[1] (or well-founded) induction

Partially ordered sets

Definition (Partially ordered sets (posets))

A partial order is a binary relation $\leq$ over a set S which is

1. reflexive: $a \leq a$ holds $\forall a \in S$;
2. antisymmetric: $a \leq b \wedge b \leq a \rightarrow a = b$ holds $\forall a, b \in S$; and
3. transitive: $a \leq b \wedge b \leq c \rightarrow a \leq c$ holds $\forall a, b, c \in S$.

$(S, \leq)$ (or often simply S) is called a partially ordered set.

Examples: $(\mathbb{X}, \leq)$ for $\mathbb{X} \in \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$

Fact: If $(S, \leq_S)$ is a poset, $T \subseteq S$, and $\leq_T$ is the restriction of $\leq_S$ to $T \times T$, then $(T, \leq_T)$ is also a poset.

A poset is totally ordered if every pair of elements are comparable.

[1] Named after Emmy Noether (1882–1935), an influential female German mathematician.

Noetherian (or well-founded) induction

Lexicographic orders

Definition (Lexicographic order)

Let $(S, \leq)$ be a poset. The lexicographic order $\sqsubseteq$ on $S \times S$ is given by

$$(s, t) \sqsubseteq (s', t') \qquad \text{iff} \qquad \begin{cases} s < s', \\ s = s' \text{ and } t \leq t' \end{cases}$$

for all s, s', t, t' in S.

Fact: If $(S, \leq)$ is a poset, then $(S \times S, \sqsubseteq)$ is a poset.

Noetherian (or well-founded) induction

Well-founded sets

Definition (Well-founded sets)

$(S, \leq)$ is well-founded iff every non-empty subset of S contains at least one minimal element with respect to the order relation $\leq$. An element $x \in S$ is called minimal if there is no element $y \in S$ such that $y < x$.

Examples: $(\mathbb{N}, \leq)$ is well-founded, but $(\mathbb{Z}, \leq)$ is not

Fact: Let $(S, \leq)$ be a poset. If $(S, \leq)$ is well-founded, then the lexicographically ordered set $(S \times S, \sqsubseteq)$ is also well-founded.

Noetherian[1] (or well-founded) induction

The principle

Let $(S, \leq)$ be a well-founded set and let $\mathcal{P}(x)$ be a statement involving a variable x. Suppose

1. $\mathcal{P}(m)$ is true for all minimal elements of S;
2. for each non-minimal element x, if $\mathcal{P}(y)$ is true for all $y < x$, then $\mathcal{P}(x)$ is also true.

Then $\mathcal{P}(x)$ is true for all $x \in S$.

The schema is as follows:

$$\forall x \in S \left[\forall y \in S \left(y < x \to \mathcal{P}(y)\right) \to \mathcal{P}(x)\right] \to \forall z \in S \; \mathcal{P}(z)$$

The Ackermann function

Definition of the function

Algorithm 2: Ackermann function $A(x, y) \colon \mathbb{N}_0 \times \mathbb{N}_0 \mapsto \mathbb{N}_0$

```
Input: $x$, $y$, two non-negative integers
Output: The computed non-negative integer value for $x$, $y$
if $x == 0$ then
    return $y + 1$;
else if $y == 0$ then
    return $A(x - 1, 1)$;
else return $A(x - 1, A(x, y - 1))$;
```

- This function is well known for its extraordinary growth. [Link to Wikipedia article on Ackermann function]
- Try it out by hand or implement it.
- Does the function terminate for all admissible inputs x and y and does it return a non-negative integer?

The Ackermann function

The termination proof

We know: $(\mathbb{N}_0 \times \mathbb{N}_0, \sqsubseteq)$ is well-founded with least element $(0,0)$. Let $\mathcal{P}(x,y)$ denote the statement

"$A(x,y)$ terminates on inputs $(x,y) \in \mathbb{N}_0 \times \mathbb{N}_0$ and returns a non-negative integer value".

The proof is by Noetherian induction on $\sqsubseteq$.

Base case: The least element is $(0,0)$. Then $\mathcal{P}(0,0)$ is true because $A(0,0) = 1$ (line 2).

Induction hypothesis. Pick arbitrarily a non-minimal element (x,y) and assume that $\mathcal{P}(x',y')$ is true for all $(x',y') \sqsubset (x,y)$.

Induction step. We want to show that $\mathcal{P}(x,y)$ is true. Recall that $x \geq 0$ and $y \geq 0$. We distinguish the following three cases.

The Ackermann function

The termination proof (cont'd)

Case 1: $x = 0$. Then $A(0, y) = y + 1$ (line 2) and $\mathcal{P}(0, y)$ is true.

Case 2: $x \neq 0 \wedge y = 0$. Then $(x - 1, 1) \sqsubset (x, 0)$. By the induction hypothesis, $\mathcal{P}(x - 1, 1)$ is true and $A(x, 0) = A(x - 1, 1)$ (line 4). Therefore, $\mathcal{P}(x, 0)$ is true.

Case 3: $x \neq 0 \wedge y \neq 0$. Then $(x, y - 1) \sqsubset (x, y)$ and, for all $z \in \mathbb{N}_0$, $(x - 1, z) \sqsubset (x, y)$. Then, $\mathcal{P}(x, y - 1)$ is true by the induction hypothesis. Moreover, for all $z \in \mathbb{N}_0$, $\mathcal{P}(x - 1, z)$ is also true by the induction hypothesis. $A(x, y) = A(x - 1, A(x, y - 1))$ (line 5) therefore terminates and computes a non-negative integer value. Hence, $\mathcal{P}(x, y)$ is true.

We conclude that $\mathcal{P}(x, y)$ is true for all $(x, y) \in \mathbb{N}_0 \times \mathbb{N}_0$. □

Induction principles not covered in this tutorial

Reverse induction [link]

Backward induction [link]

Cauchy induction [link]

How to write down an induction proof?

- Identify the claim you are going to prove.
- Let the reader know which kind of induction you will use.
- For structural induction, a claim is about all elements of some inductively defined set. It is a good idea to indicate the inductive definition on which the proof is based.
- Make clear (e.g., by labels) what the basis, the induction hypothesis and the induction step are.
- State precisely the induction hypothesis you are going to use and indicate the claim you prove in the induction step.
- Make clear where you apply the induction hypothesis.
- Check whether I followed the advise! Report violations!

Learning objectives

- Ability to discuss different induction principles in detail and to distinguish between them.
- Ability to apply these principles and to construct proofs by induction.