Proofs by Induction

Stefan Kurtz

October 15, 2022

Induction on natural numbers

- one of the most important foundations of discrete mathematics are the Peano Axioms, which define the set $\mathbb{N}$ of natural numbers
- here is a slightly simplified version of the original set of axioms:

Peano Axioms

1. $0 \in \mathbb{N}$, i.e. 0 is a natural number
2. $i \in \mathbb{N} \Rightarrow (i+1) \in \mathbb{N}$, i.e. if i is a natural number, then so is $i+1$
3. $\mathbb{N}$ is the smallest set satisfying 1 and 2

Induction on natural numbers (cont.)

Induction principle

- goal: prove that statement $P(i)$ holds for all $i \in \mathbb{N}$.
- steps:
  - prove that $P(0)$ and/or $P(1)$[1] holds (base case)
  - assume that $P(i)$ holds for arbitrary $i \in \mathbb{N}$ (ind. assumption)
  - prove that $P(i+1)$ holds (induction step)

[1] Sometimes a statement does not makes sense for $i = 0$, so that one starts with $i = 1$. Sometimes $P(1)$ is defined independently of $P(0)$ so that one additionally has to prove $P(1)$.

Example 1: Induction proof for sum of integers

We show by induction on n that

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2} \tag{1}$$

holds for all $n \in \mathbb{N}$.

base case:

for $n = 0$ we have $\sum_{j=1}^{n} j = \sum_{j=1}^{0} j = 0 = 0 \cdot 1 = \frac{0 \cdot 1}{2} = \frac{n(n+1)}{2}$. So statement (1) holds for $n = 0$

induction assumption

Assume that statement (1) holds for any $n \in \mathbb{N}$.

induction step

Example 1: Induction proof for sum of integers (cont.)

$$
\begin{aligned}
\sum_{j=1}^{n+1} j &= \left(\sum_{j=1}^{n} j\right) + (n+1) && \text{(split sum)} \\
&= \frac{n(n+1)}{2} + (n+1) && \text{(apply assumption)} \\
&= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} && \text{(unify denominator} \\
&= \frac{n(n+1) + 2(n+1)}{2} && \text{(add fractions)} \\
&= \frac{(n+1)(n+2)}{2} \\
&= \frac{(n+1)((n+1)+1)}{2}
\end{aligned}
$$

Example 2: Induction proof for fibonacci series bound

The sequence of fibonacci numbers $f_0, f_1, f_2, \ldots$ is defined by $f_0 = 0,\ f_1 = 1$ and $f_n = f_{n-2} + f_{n-1}$ for $n \geq 2$:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, \ldots$$

We prove by induction on n that $f_n \leq 2^n$.

base case

- for $n = 0$: $f_n = f_0 = 0 \leq 1 = 2^0 = 2^n$
- for $n = 1$: $f_n = f_1 = 1 \leq 2 = 2^1 = 2^n$.

induction assumpt.

assume that $f_n \leq 2^n$ holds for all $n \geq 1$

induction step

$$\begin{aligned} f_{n+1} &= f_{n-1} + f_n \\ &\leq 2^{n-1} + 2^n \\ &= 2^{n-1} + 2 \cdot 2^{n-1} = (1+2) \cdot 2^{n-1} \leq 4 \cdot 2^{n-1} = 2^2 \cdot 2^{n-1} = 2^{n+1} \end{aligned}$$

Example 3: Induction proof for sum of squares

We prove by induction that

$$\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6} \tag{2}$$

base case

For $n = 0$ we have $\sum_{j=1}^{n} j^2 = \sum_{j=1}^{0} j^2 = 0 = \frac{0 \cdot 1 \cdot 1}{6} = \frac{n(n+1)(2n+1)}{6}$

induction assumption

Assume that (2) holds for arbitrary n.

induction step

Example 3: Induction proof for sum of squares (cont.)

$$
\begin{aligned}
\sum_{j=1}^{n+1} j^2 &= \left(\sum_{j=1}^{n} j^2\right) + (n+1)^2 \\
&= \frac{n(n+1)(2n+1)}{6} + \frac{6(n+1)^2}{6} \\
&= \frac{(n^2+n)(2n+1) + 6(n^2+2n+1)}{6} \\
&= \frac{2n \cdot (n^2+n) + n^2 + n + 6n^2 + 12n + 6}{6} \\
&= \frac{2n^3 + 2n^2 + n^2 + n + 6n^2 + 12n + 6}{6} \qquad (3)
\end{aligned}
$$

Example 3: Induction proof for sum of squares (cont.)

- continuing with (3) leads to the simplified term (2) for $n + 1$

$$\begin{aligned}
\frac{2n^3 + 9n^2 + 13n + 6}{6} &= \frac{2n^3 + 6n^2 + 4n + 3n^2 + 9n + 6}{6} \\
&= \frac{2n(n^2 + 3n + 2) + 3(n^2 + 3n + 2)}{6} \\
&= \frac{2n(n^2 + n + 2n + 2) + 3(n^2 + n + 2n + 2)}{6} \\
&= \frac{(n^2 + n + 2n + 2)(2n + 3)}{6} \\
&= \frac{(n(n + 1) + 2(n + 1))(2n + 3)}{6} \\
&= \frac{(n + 1)(n + 2)(2n + 3)}{6} \\
&= \frac{(n + 1)(n + 1 + 1)(2(n + 1) + 1)}{6}
\end{aligned}$$

Induction for multi parameter statements

- sometimes one has to prove statements involving more than one parameter, say $n \in \mathbb{N}$ and $m \in \mathbb{N}$
- here one applies the induction principle by ordering pairs using an order $\preceq$ on pairs (i, j)
- as a simple example consider the proof that the following function *gcd* to compute the greatest common divisor of two natural numbers terminates.

$$gcd(i,j) = \begin{cases} i + j & \text{if } i = 0 \text{ or } j = 0 \\ gcd(i-j, j) & \text{if } j < i \\ gcd(i, j-i) & \text{otherwise} \end{cases}$$

We use the order $\preceq$ defined by $(i', j') \preceq (i, j) \iff i' + j' \leq i + j$ for all $i', j', i, j \in \mathbb{N}$.

Induction for multi parameter statements (cont.)

base case

let $i + j = 0$. Then $i = 0$ and $j = 0$ and (i, j) is the smallest element with respect to order $\preceq$. By definition we have $gcd(i, j) = i + j$. So $gcd(i, j)$ terminates.

induction assumption

- assume that $gcd(i', j')$ terminates for all (i', j'), $i, j \in \mathbb{N}$.

induction step

Induction for multi parameter statements (cont.)

- we have to show that $gcd(i,j)$ terminates for (i,j) such that $(i',j') \prec (i,j)$ which is equivalent to $i'+j' < i+j$

  case 1: let $i = 0$ or $j = 0$. Then $gcd(i,j) = i+j$ and so gcd terminates

  case 2: let $i > 0$ and $j > 0$.

  case 2a: if $j < i$, then $gcd(i,j) = gcd(i-j,j)$ and $i-j+j = i < i+j$. So we can apply the induction assumption according to which $gcd(i-j,j)$ terminates. So $gcd(i,j)$ also terminates

  case 2b: if $i < j$, then $gcd(i,j) = gcd(i,j-i)$ and $i+j-i = j < i+j$. So we can apply the induction assumption according to which $gcd(i,j-i)$ terminates. So $gcd(i,j)$ terminates.

Generalizing integer induction

Inductive definition of M[1]

- let A be a a set of objects, called atoms.
- let C be a set of constructors which allow to combine smaller objects to larger objects.
- the set M inductively defined by A and C is the minimum set satisfying
  - $A \subseteq M$
  - if $c \in C$ has $k \geq 1$ arguments and m_1, m_2, ..., $m_k \in M$, then $c(m_1, m_2, \ldots, m_k) \in M$

The Peano Axioms are based on this general induction principle:

Peano Axioms	induction principle
$0 \in \mathbb{N}$	$A = \{0\}$
$i \in \mathbb{N} \Rightarrow (i+1) \in \mathbb{N}$	$c(i) = i + 1$

- the induction on natural numbers can be generalized to inductively defined sets $\Rightarrow$ *structural induction*

1: Bernhard Steffen, Vorlesungsfolien, Mathematik für Informatiker, TU Dortmund, 2013

Structural Induction[1]

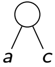
- let M be a set inductively defined via atom set set A and constructor set C
- let P be a statement on all elements of M
- to prove by structural induction that $P(m)$ holds for all $m \in M$ one follows these steps:
  - prove that $P(a)$ holds for all $a \in A$ (base cases)
  - assume for all m_1, m_2, ..., $m_k \in M$, that $P(m_1)$, $P(m_2)$, ..., $P(m_k)$ holds (ind. assumpt.)
  - prove that $P(c(m_1, m_2, \ldots, m_k))$ holds for all constructors $c \in C$

1: Bernhard Steffen, Vorlesungsfolien, Mathematik für Informatiker, TU Dortmund, 2013

Proving an important property about binary trees

binary trees

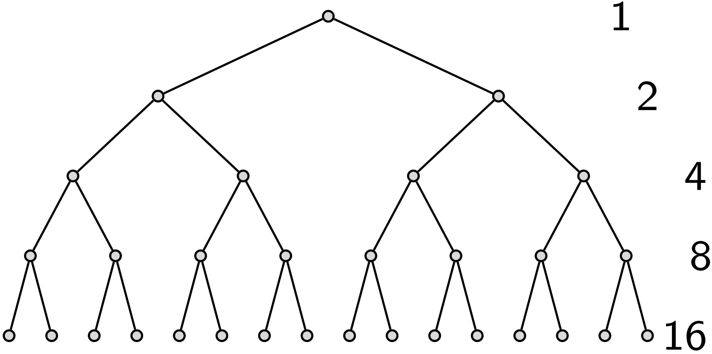
- hierarchical data structure with a root and parent/children relationship
- used to represent e.g. taxonomic relationship (like genus/species)
- or structure of data in file system
- inductive definition of binary tree:
  - a leaf $\bigcirc$ is a binary tree of height 0.
  - if a is binary trees of height h, then 

is a binary tree of height $1 + h$ with a root $\bigcirc$
  - if a and c are binary trees of height h_a and h_c, then 

is a binary tree of height $1 + \max\{h_a, h_c\}$ with a root $\bigcirc$

Proving an important property about binary trees (cont.)

- Example: a perfect binary tree of height 4 with $1 + 2 + 4 + 8 + 16 = 31 = 2^5 - 1 = 2^{4+1} - 1$ nodes (which are either leaves or branching)



Proving an important property about binary trees (cont.)

- prove by structural induction that a binary tree of height h contains at most $2^{h+1} - 1$ nodes (the circles)

base case: show property for all atoms

- consider a binary tree consisting of a leaf only
- by definition it has height 0
- number of nodes in the binary tree is $1 = 2 - 1 = 2^1 - 1 = 2^{0+1} = 2^{h+1} - 1$

induction assumption

- assume that any binary tree of height h contains at most $2^{h+1} - 1$ nodes

Proving an important property about binary trees (cont.)

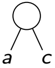
induction step for first constructor

- let a be a binary tree of height h
- by the induction assumption, tree a contains at most $2^{h+1} - 1$ nodes
- so the tree 

is of height $1 + h$ and it contains at most $1+2^{h+1}-1 = 2^{h+1} = 2\cdot 2^{h+1}-2^{h+1} = 2^{h+2}-\underbrace{2^{h+1}}_{\geq 1} \leq 2^{h+2}-1$ nodes

Proving an important property about binary trees (cont.)

induction step for second constructor

- let a and c be binary trees of height h_a and h_c, respectively
- by the induction assumption, tree a contains at most $2^{h_a+1} - 1$ and tree b contains at most $2^{h_c+1} - 1$ nodes
- so the tree 

is of height $h = 1 + \max\{h_a, h_c\}$ and the number of its nodes is at most

$$\begin{aligned}
1 + 2^{h_a+1} - 1 + 2^{h_c+1} - 1 &= 2^{h_a+1} + 2^{h_c+1} - 1 \\
&\leq 2^{\max\{h_a,h_c\}+1} + 2^{\max\{h_a,h_c\}+1} - 1 \\
&= 2 \cdot 2^{\max\{h_a,h_c\}+1} - 1 \\
&= 2^{1+\max\{h_a,h_c\}+1} - 1 \\
&= 2^{h+1} - 1
\end{aligned}$$