BIE-DML - Discrete Mathematics and Logic

Tutorial 4

Mathematical Induction

Francesco Dolce, Eva Pernecká, Jitka Rybníčková and Jiřina Scholtzová

Faculty of Information Technology
Czech Technical University in Prague

Winter semester 2023/2024

updated: 31/10/2023, 10:30

4.1 Introduction

In this chapter (and later on) we will use the following notation:

$$\mathbb{N} = \{1, 2, 3, \dots\}, \quad \mathbb{N}_0 = \{0, 1, 2, 3, \dots\}.$$

The sum and the product of a number of arguments $a(k)$ depending on $k \in \mathbb{Z}$, where k goes from a lower bound $d \in \mathbb{Z}$ to an upper bound $h \in \mathbb{Z}$ are defined as:

$$\sum_{k=d}^{h} a(k) = a(d) + a(d+1) + a(d+2) + \cdots + a(h),$$
$$\prod_{k=d}^{h} a(k) = a(d) \cdot a(d+1) \cdot a(d+2) \cdot \cdots \cdot a(h).$$

If the notation $\sum_{k=d}^{h} a(k)$ and $\prod_{k=d}^{h} a(k)$ is new for you, imagine a `for` cycle which performs the sum – respectlively, the product – of numbers $a(d)$, $a(d+1)$, …, $a(h)$.

4.1.1 Mathematical Induction

During the lectures, three principles of mathematical induction (MI) were presented: weak principle, strong principle (i.e., complete induction) and structural induction. Weak and strong principles are equivalent which means that every statement proved by one principle can be also proven by the second one. Both principles are then only a special case of structural induction. Thus it depends only on our choice how the statements will be proven. The base of both principles are natural numbers $\mathbb{N}$ (or $\mathbb{N}_0$) and their natural well order.

Definition 4.1. A set X is a well-ordered set if each of its nonempty subsets has a smallest element.

Obviously, this statement is true for positive integers, but e.g., for integers, rationals or reals we can find examples of subsets which do not have a lower bound (find some!).

Principles of Mathematical Induction

Assume that we want to prove a certain property $V(n)$ for every number $n \geq n_0$ (for some given fixed n_0) Then we use the following scheme:

Weak Principle:

1. **Base case:** $V(n_0)$ is true for $n_0 \in \mathbb{N}$.
2. **Inductive step:** For any $n \geq n_0$, if $V(n)$ is true, then $V(n+1)$ is also true.
3. **Conclusion:** $V(n)$ is true for every natural number $n \geq n_0$.

Strong Principle:

1. **Base case:** $V(n_0), V(n_0+1), \dots V(n_0+m)$ are true for some $n_0, m \in \mathbb{N}$ (i.e., $V(k)$ holds for every k in the range $n_0 \leq k \leq n_0 + m$).
2. **Inductive step:** If, for any $n \geq n_0$, $V(k)$ holds for every k in the range $n_0 \leq k \leq n$, then $V(n+1)$ is also true.
3. **Conclusion:** $V(n)$ is true for every natural number $n \geq n_0$.

Before we present structural induction, we will define a new type of set – an **inductively defined set**. A set S is inductively defined if it is defined by a set of rules which can be split into two groups: base rules (R0) and inductive rules (R1). Base rules directly list all elements which belong to the set; inductive rules generate elements from already existing elements of S (only finite usage of the rules is allowed). As an example of such a set we present the set S of all binary strings which start with 1. The set S can be defined by three rules:

(R0) $1 \in S$,

(R1) $w \in S \Rightarrow w0 \in S$,

(R1) $w \in S \Rightarrow w1 \in S$.

Structural Induction Let S be an inductively defined set given by rules (R0) a (R1). We want to prove that every element s from S satisfies a property $V(s)$. The usage of structural principle is very natural although it seams to be difficult if you see it for the first time. In short, we have to prove that a certain property is satisfied (and invariant) for all the rules which define the set. First we prove it for basic rules from (R0) and then in the inductive case for elements generated by rules in (R1). More precisely,

1. **Base case:** $V(s)$ holds for every $s \in S$, which is generated by somey rule in (R0).
2. **Inductive step:** For every rule in (R1) prove: if all elements $s \in S$ satisfy the property $V(s)$ before application of the rule from (R1) then this property is true also after the application of a rule from (R1).
3. **Conclusion:** $V(s)$ is true for every $s \in S$.

Unfortunately there is no universal principle which could be used to prove the implication in the inductive step. We often use some trick or a specific technique. Therefore it is useful to practice on as many exercises as possible. In the following exercises we will to introduce some basic tricks.

This notation will be used further: MI – mathematical induction, BC – base case, IS – inductive step, and IA – inductive assumption. Inductive assumption is the statement which serves as an assumption (antecedent/premise) in the implication of the inductive step (mostly introduced by word ”if”).

References:

1. BIE-ZDM at FIT:
   https://courses.fit.cvut.cz/BIE-ZDM/
2. Selftests and Exercises in Marast at FIT:
   https://marast.fit.cvut.cz/

4.2 Exercises

Exercise 4.1. Use mathematical induction to prove the following divisibility relations for every $n \in \mathbb{N}_0$:

a) $2|(n^2 - n)$,

b) $3|(n^3 + 2n)$,

c) $6|(n^3 - n)$,

d) $2|(n^2 + n)$,

e) $5|(n^5 - n)$,

f) $21|(4^{n+1} + 5^{2n-1})$ (for all $n \geq 1$).

Exercise 4.2. Use mathematical induction to prove the following properties:

a) $7^n - 1$ is divisible by 6 for $n = 1, 2, \ldots$.

b) $11^n - 6$ is divisible by 5 for $n = 1, 2, \ldots$.

c) $6 \cdot 7^n - 2 \cdot 3^n$ is divisible by 4 for $n = 1, 2, \ldots$.

d) $3^n + 7^n - 2$ is divisible by 8 for $n = 1, 2, \ldots$.

Exercise 4.3. Use mathematical induction to prove the following equalities:

a) $\sum_{k=1}^{n} k = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$.

b) $\sum_{k=1}^{n} k^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

c) $\sum_{k=1}^{n} k^3 = 1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$.

d) $\sum_{k=1}^{n} (-1)^k k = -1 + 2 - 3 + \cdots + (-1)^n n = -\frac{1}{4} + (-1)^n \cdot \frac{(2n+1)}{4}$.

Exercise 4.4. Prove the following statements for every $n \in \mathbb{N}$ using the weak principles of mathematical induction.

a) $\sum_{k=1}^{n} (2k - 1) = 1 + 3 + 5 + \cdots + (2n - 1) = n^2$,

b) $n < 2^n$,

c) $2^{n-1} \leq n!$,

d) $\Pi_{k=1}^{n} k = 1 \cdot 2 \cdot 3 \cdots n \leq n^n$,

e) $\Pi_{k=1}^{n} (2k)! = 2! \cdot 4! \cdot 6! \cdot \cdots \cdot (2n)! \geq ((n+1)!)^n$,

f) $\sum_{k=1}^{n} \frac{1}{k!} = \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!} \leq 2 - \frac{1}{n!}$,

g) $\sum_{k=1}^{n} \frac{1}{k^2} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$,

h) $n^2 \leq 2^n$, for $n \geq 4$

i) $\sum_{k=1}^{n} \frac{1}{(2k-1)(2k+1)} = \frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \frac{1}{5 \cdot 7} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$,

j) $\sum_{k=1}^{n} k \cdot k! = 1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n! = (n+1)! - 1$.

Exercise 4.5. Fibonacci numbers are defined as follows:

(R0) $f(0) = 0,\ f(1) = 1,$

(R1) $f(n) = f(n-1) + f(n-2)$ for $n \geq 2$.

Prove the following properties:

a) $f(n) > \alpha^{n-2}$ for every $n \geq 3$, where $\alpha = \frac{1+\sqrt{5}}{2}$ (it is called the *golden ratio*);

b) $f(n-1) \cdot f(n+1) = f^2(n) + (-1)^n$ for every $n \geq 1$;

c) $\sum_{i=0}^{n} f^2(i) = f(n) \cdot f(n+1)$.

Exercise 4.6 (*). An harmonic sequence is a sequence of elements $H(n) = 1 + 1/2 + 1/3 + \cdots + 1/n$. Prove the following properties for every $n \in \mathbb{N}$:

a) $H(1) + H(2) + \cdots + H(n) = (n+1) \cdot H(n) - n$;

b) $H(2^n) \leq 1 + n$;

c) $H(2^n) \geq 1 + \frac{n}{2}$.

Hint : $$\frac{1}{2^n+1} \geq \frac{1}{2^{n+1}}, \qquad \frac{1}{2^n+2} \geq \frac{1}{2^{n+1}}, \qquad \ldots, \qquad \frac{1}{2^n+2^n} \geq \frac{1}{2^{n+1}}.$$

Exercise 4.7. Let $\mathbb{R}^2$ be a vector space and let M be a set of vectors defined inductively:

(R0) $(1,0) \in M, \quad (0,-1) \in M, \quad (1,1) \in M$

(R1) $\forall\, \mathbf{a}, \mathbf{b} \in M:\ \mathbf{a} + \mathbf{b} \in M$ and $\forall\, \alpha \in \mathbb{R},\ \forall\, \mathbf{a} \in M:\ \alpha \cdot \mathbf{a} \in M$.

Prove that M is a subset of the linear span of vectors $(1,0), (0,-1)$, i.e., $M \subseteq \langle (1,0), (0,-1) \rangle$.

Exercise 4.8. Consider the inductively defined set S of integers:

(R0) $6, 8 \in S$,

(R1) if $m, n \in S$, then $m + n \in S,\ m - n \in S$,

and all numbers in S are obtained by a finite application of these rules.
Find a property V which describes the elements of S and prove your guess by structural induction.

Exercise 4.9. Consider all formulas of propositional logic:

(R0) Elementary formulas are formulas of propositional logic.

(R1) If A, B are formulas then also $\neg(A), (A \wedge B), (A \vee B), (A \Rightarrow B), (A \Leftrightarrow B)$ are formulas.

Every formula can be obtained by a finite number of applications of rules (R0) and (R1).

Use **structural induction** to prove that every formula contains an equal number of left and right parentheses.

4.3 More exercises

Exercise 4.10. Consider an infinite sequence of integers $(A_0, A_1, A_2, A_3, \dots)$, whose members are defined recursively as follows:

$$A_{n+3} = A_{n+2} + 5 \cdot A_{n+1} + 3 \cdot A_n, \quad \forall n \in \mathbb{N}_0$$

and $A_0 = 1$, $A_1 = -2$, and $A_2 = 3$. Prove by mathematical induction that for all $n \in \mathbb{N}_0$,

$$A_n = (-1)^n(n+1).$$

Exercise 4.11. Consider a set S defined inductively using the rules below:

(R0) $1 \in S$,

(R1) If $n \in S$ then $3n + 2 \in S$ and $n^2 \in S$.

Use structural induction to prove that $\forall n \in S$, we have $4|(n-1)$.

Exercise 4.12. Consider the matrix $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ with $a, b \in \mathbb{R}$. Prove that $A^n = \begin{pmatrix} a^n & 0 \\ 0 & b^n \end{pmatrix}$ for any integer $n \geq 1$.

Exercise 4.13. Consider the matrix $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Prove that $A^n = \begin{pmatrix} f(n+1) & f(n) \\ f(n) & f(n-1) \end{pmatrix}$ for any integer $n \geq 1$, where $f(n)$ denotes n-th Fibonacci number defined in Exercise 4.5.

Exercise 4.14. Prove that

a) $A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ for any $n \geq 1$, where $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

b) (*) $A^n = \begin{pmatrix} \cos(n\varphi) & -\sin(n\varphi) \\ \sin(n\varphi) & \cos(n\varphi) \end{pmatrix}$ for any $n \geq 1$, where $A = \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}$, $\varphi \in \mathbb{R}$.