Discrete mathematics

Petr Kovář & Tereza Kovářová
petr.kovar@vsb.cz

VŠB – Technical University of Ostrava

Winter Term 2022/2023
DiM 470-2301/02, 470-2301/04, 470-2301/06

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

The translation was co-financed by the European Union and the Ministry of Education, Youth and Sports from the Operational Programme Research, Development and Education, project "Technology for the Future 2.0", reg. no. CZ.02.2.69/0.0/0.0/18_058/0010212.

About this file

This file is meant to be a guideline for the lecturer. Many important pieces of information are not in this file, they are to be delivered in the lecture: said, shown or drawn on board. The file is made available with the hope students will easier catch up with lectures they missed.

For study the following resources are better suitable:

- Meyer: Lecture notes and readings for an http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-042j-mathematics-for-computer-science-fall-2005/readings/"(weeks 1-5, 8-10, 12-13), MIT, 2005.
- Diestel: Graph theory http://diestel-graph-theory.com/ (chapters 1-6), Springer, 2010.

See also http://homel.vsb.cz/~kov16/predmety_dm.php

Lecture overview

Chapter 0. Review

- sets, subsets and set operations
- inclusion-exclusion principle
- relations
- proof techniques

Sets and set operations

Set

is a collection of distinct objects. Sets are usually denoted by capital letters $A, B, X, M, \ldots$

Elements are denoted by lowercase letters $a, b, x, \ldots$

Empty set $\emptyset$ not $\{\emptyset\}$!

Described by

- specifying members: $M = \{a, b, c, d\}$,
  (it holds $a \in M$, $d \in M$, but $e \notin M$)
- intensional definition (describing a property): $N = \{x \colon x \in \mathbb{N}, x > 5\}$.

Cardinality of a set M

is the number of members in M, denoted by $|M|$.

Subset

A is a subset of B, if for every $a \in A$ is also $a \in B$. We write $A \subseteq B$.

Set operations

Union of sets $A \cup B = \{x : x \in A \text{ or } x \in B\}$
Intersection of sets $A \cap B = \{x : x \in A \text{ and } x \in B\}$
Difference of sets $A \setminus B = \{x : x \in A \text{ and } x \notin B\}$
Symmetric difference of sets $A \Delta B = (A \setminus B) \cup (B \setminus A)$

Examples

$$A = \{a, b, c\},\ \ B = \{c, d\}$$

$$A \cup B = \{a, b, c, d\}, \quad A \cap B = \{c\}, \quad A \setminus B = \{a, b\}, \quad A \Delta B = \{a, b, d\}$$

Questions

Can you find such two sets A, B that $A \setminus B = B \setminus A$?
Can you find such two *distinct* sets A, B that $A \setminus B = B \setminus A$?

Generalized unions and intersections

Generalized union $\bigcup_{i=1}^{n} X_i$ and intersection $\bigcap_{i=1}^{n} X_i$ of sets.

Given a set J, we can write $\bigcup_{j \in J} X_j$ and $\bigcap_{j \in J} X_j$.

Examples

$$A_i = \{1, 2, \ldots, i\}$$

$$\bigcup_{i=1}^{5} A_i = \{1, 2, 3, 4, 5\}, \quad \bigcap_{i=1}^{5} A_i = \{1\}, \quad \bigcap_{i=1}^{\infty} A_i = \{1\}$$

Questions

What is $\bigcap_{j \in J} A_j$ for $J = \{2, 5\}$?

What is $\bigcup_{j \in J} A_j$ for $J = \mathbb{N}$?

Cartesian product and Cartesian power

Cartesian product of two sets $A \times B = \{(a, b) : a \in A,\ b \in B\}$ is the set of all ordered pairs (a, b) such that $a \in A$ and $b \in B$ in this order.
$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_i \in A_i,\ i = 1, 2, \ldots, n\}$
For $A_1 = A_2 = \ldots = A_n$ we get the Cartesian power A^n.
We define $A^0 = \{\emptyset\}$, $A^1 = A$.

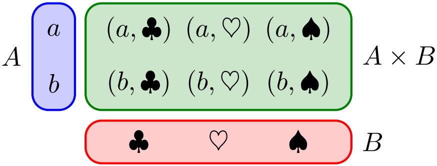
Example

$$A = \{a, b\},\ B = \{\clubsuit, \heartsuit, \spadesuit\}$$

$$A \times B = \{(a, \clubsuit), (a, \heartsuit), (a, \spadesuit), (b, \clubsuit), (b, \heartsuit), (b, \spadesuit)\}$$

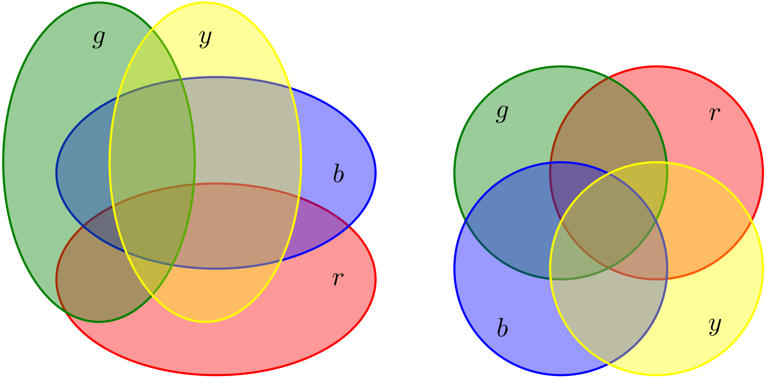
A classical example

Cartesian coordinates (x, y) in $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ and (x, y, z) in $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$.



A	$A \times B$		
a	$(a, \clubsuit)$	$(a, \heartsuit)$	$(a, \spadesuit)$
b	$(b, \clubsuit)$	$(b, \heartsuit)$	$(b, \spadesuit)$
B	$\clubsuit$	$\heartsuit$	$\spadesuit$

Cartesian product of sets $A \times B = \{a, b\} \times \{\clubsuit, \heartsuit, \spadesuit\}$.



All subsets of the set of colors $C = \{r, g, b, y\}$.

Power set of A

is the set of all subsets of A

$$2^A = \{X : X \subseteq A\}.$$

A family of sets over A

or a family of subsets of A is some $\mathcal{T} \subseteq 2^A$.

We prefer the term "family of sets" to "set of sets".

Examples

$$A = \{a, b\} \qquad 2^A = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$

$$\left|2^A\right| = 2^{|A|}$$

Complement of a set on given universe

Universe contains all possible elements.

Given a set A the complement $\overline{A}$ contains elements which are not in A.

Questions

$$B \times A \times B = ?, \quad A \times \emptyset = ?, \quad \emptyset \times \emptyset = ?, \quad \emptyset^0 = ?, \quad \emptyset^\emptyset = ?$$

Which set operations are

- commutative?
- associative?

Questions

$$|A \times B| = ?, \quad |2^A| \overset{?}{=} |A^2|, \quad |2^A| \overset{?}{<} |A^2|, \quad |2^A| \overset{?}{\leq} |A^2|$$

Questions

Set S contains all even numbers.
What is $\overline{S}$ in the universe $\mathbb{Z}$? What is $\overline{S}$ in the universe $\mathbb{R}$?

Numbers and interval of integers

Natural numbers and integers

Natural numbers are denoted by $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$
notice! zero is not among them
Natural numbers with zero included denoted by $\mathbb{N}_0 = \{0, 1, 2, 3, 4, 5, \ldots\}$
Integers are denoted by $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$

Intervals of integers between a and b

is the set $\{a, a+1, \ldots, b-1, b\}$
we denote it by: $[a, b] = \{a, a+1, \ldots, b-1, b\}$

Compare to the notation used for an interval of real numbers (a, b).

Examples

$[3, 7] = \{3, 4, 5, 6, 7\}$ $\quad [-2, -2] = \{-2\}$
$[5, 0] = \emptyset$ (the empty set)

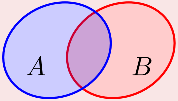
Inclusion exclusion principle

For small n we use it often intuitively:

Theorem

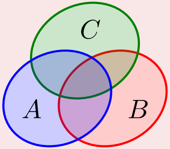
The number of elements in a union of two sets is:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$



The number of elements in a union of three sets is:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|.$$



General form of the inclusion exclusion principle

The number of elements in a union of n sets is:

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{\substack{J\subseteq\{1,\ldots,n\}\\ J\neq\emptyset}} (-1)^{|J|-1} \cdot \left|\bigcap_{i\in J} A_i\right|.$$

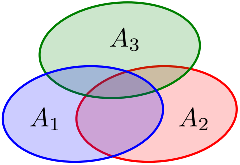
To count the cardinality of a union, we

- sum the cardinalities of all sets,
- subtract the cardinalities of intersections of all pairs of sets,
- add the cardinalities of intersections of all triples of sets,
- subtract the cardinalities of intersections of all quadruples of sets,
- ...

Size of the union of three sets

For example for $n = 3$ we get

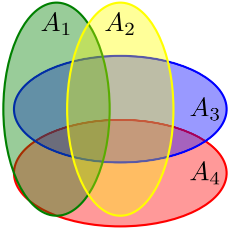
$$
\begin{aligned}
\left|\bigcup_{i=1}^{3} A_i\right| &= \sum_{\substack{J\subseteq\{1,2,3\}\\ J\neq\emptyset}} (-1)^{|J|-1}\cdot\left|\bigcap_{i\in J} A_i\right| = \\
&= |A_1| + |A_2| + |A_3| - \\
&\quad - |A_1\cap A_2| - |A_1\cap A_3| - |A_2\cap A_3| + \\
&\quad + |A_1\cap A_2\cap A_3|.
\end{aligned}
$$



Size of the union of four sets

for $n = 4$ we get

$$
\begin{aligned}
& \left|\bigcup_{i=1}^{4} A_i\right| = \sum_{\substack{J\subseteq\{1,2,3,4\}\\ J\neq\emptyset}} (-1)^{|J|-1} \cdot \left|\bigcap_{i\in J} A_i\right| = \\
= \quad & |A_1| + |A_2| + |A_3| + |A_4| - \\
- \quad & |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| - |A_1 \cap A_4| - |A_2 \cap A_4| - |A_3 \cap A_4| \\
+ \quad & |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| - \\
- \quad & |A_1 \cap A_2 \cap A_3 \cap A_4|.
\end{aligned}
$$



Special case of inclusion exclusion principle

A simpler form (with fewer summands), if the intersections of i sets have always the same cardinality:

$$\left|\bigcup_{j=1}^{n} A_j\right| = \sum_{i=1}^{n} (-1)^{i-1} \cdot \binom{n}{i} \cdot \left|\bigcap_{j=1}^{i} A_j\right|.$$

To count the cardinality of a union, we

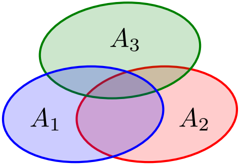
- take the number of one-element sets × size of A_1,
- subract number of two-element sets × size of pair-set intersections,
- add number of three-element sets × size of tripple-set intersections,
- subract number of four-element sets × size of quadruple-set intersections,
- . . .

Size of the union of three set where all sets and their intersection have same sizes

For $n = 3$ we get

$$\left|\bigcup_{i=1}^{3} A_i\right| = \sum_{k=1}^{3} (-1)^{k-1} \cdot \binom{3}{k} \cdot \left|\bigcap_{j=1}^{k} A_j\right| =$$

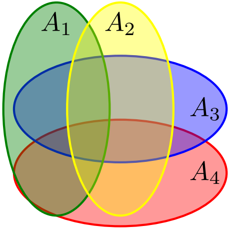
$$= \binom{3}{1} \cdot |A_1| - \binom{3}{2} \cdot |A_1 \cap A_2| + \binom{3}{3} \cdot |A_1 \cap A_2 \cap A_3|.$$



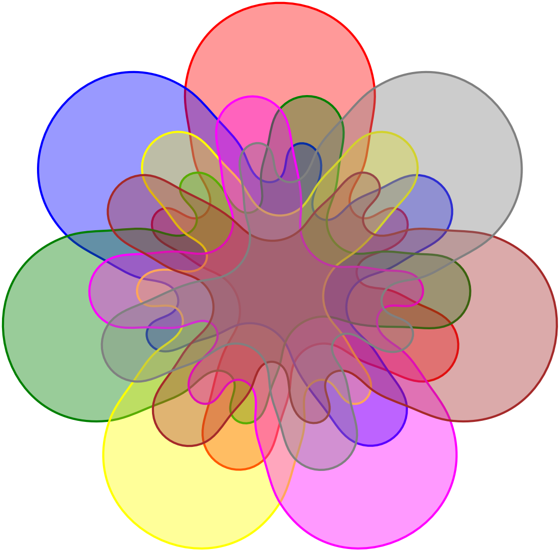
Size of the union of four set where all sets and their intersection have same sizes

For $n = 4$ we get

$$\begin{aligned}
\left|\bigcup_{i=1}^{4} A_i\right| &= \sum_{k=1}^{n} (-1)^{k-1} \cdot \binom{n}{k} \cdot \left|\bigcap_{j=1}^{k} A_j\right| = \\
&= \binom{4}{1} \cdot |A_1| - \binom{4}{2} \cdot |A_1 \cap A_2| + \\
&+ \binom{4}{3} \cdot |A_1 \cap A_2 \cap A_3| - \binom{4}{4} |A_1 \cap A_2 \cap A_3 \cap A_4|.
\end{aligned}$$



Venn diagram for seven sets – Adelaide



Example

There are 25 students in a class. 17 study English and 10 German. 4 study English and German, 4 English and French, 2 German and French and one all three languages. How many students study only French?

We denote the sets by E, G a F. We know

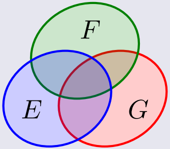
$$|E| = 17,\ |G| = 10,\ |E \cap G| = |E \cap F| = 4,\ |G \cap F| = 2,\ |E \cap G \cap F| = 1$$

From the equation

$$|E \cup G \cup F| = |E| + |G| + |F| - |E \cap G| - |G \cap F| - |E \cap F| + |E \cap G \cap F|$$

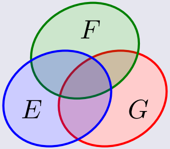
it follows

$$|F| = |E \cup G \cup F| - |E| - |G| + |E \cap G| + |G \cap F| + |E \cap F| - |E \cap G \cap F|$$
$$|F| = 25 - 17 - 10 + 4 + 4 + 2 - 1 = 7.$$



Example (continued)

But some of these 7 students study also other languages!



Just French

$$x = |F| - |E \cap F| - |G \cap F| + |E \cap G \cap F|$$
$$x = 7 - 4 - 2 + 1 = 2 \text{ students.}$$

2 students study just French.

0.3. Relations and mappings

While studying Discrete mathematics we need precise definitions of the terms function, ordering, or to be equivalent. All are built upon the concept of relations.

The importance of equivalence and function definitely outreaches Discrete mathematics.

In the next chapter we mention the inclusion exclusion principle, which has many nice applications.

Overview

- notion of a relation
- ordering and equivalence
- function and mapping
- composition of relations

0.3.1. Binary and *n*-ary relations (on a set and between sets)

Recall that a Cartesian product of sets $A \times B = \{(a, b) : a \in A, b \in B\}$ is a set of all ordered pairs taken component-wise from the sets A and B (in this order).

Definition

(Heterogenous) binary relation R between sets A and B is a subset of the Cartesian product $A \times B$, i.e.

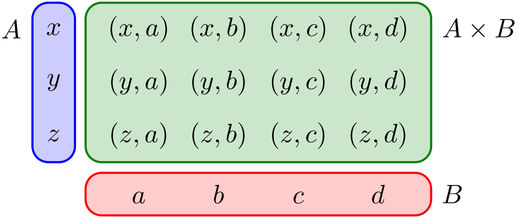
$$R \subseteq A \times B.$$

We say "element $x \in A$ is/is not related to $y \in B$" (in this order).
We write $(x, y) \in R$ or $(x, y) \notin R$, often just xRy.
(e.g. $x = y$, $x < y$ instead of $(x, y) \in =$, $(x, y) \in <$)

Definition – more general

(Heterogenous) n-ary relation S between the sets $A_1, A_2, \ldots, A_n$ is a subset of the Cartesian product $A_1 \times A_2 \times \cdots \times A_n$, i.e.

$$S \subseteq A_1 \times A_2 \times \cdots \times A_n.$$



$$\begin{array}{cccccccc} A & x & (x,a) & (x,b) & (x,c) & (x,d) & A \times B \\ & y & (y,a) & (y,b) & (y,c) & (y,d) & \\ & z & (z,a) & (z,b) & (z,c) & (z,d) & \\ & & a & b & c & d & B \end{array}$$

cartesian product of set $A \times B = \{x, y, z\} \times \{a, b, c, d\}$.

Example

Typically, a database entry represents an element of a relation. For example exam results in Edisonu:

$$\text{(name, ID, date, points)}$$

Element of the product $\mathit{Names} \times \mathit{IDs} \times \mathit{Dates} \times \mathit{Points}$

In the database we can look up entries with given parameters:

- students, taking exam in a particular day,
- pairs of students, taking same exams,
- point scores for a given day,
- . . .

The query result may determine a relationship (relation) between elements of the *same* set:

- relation between students,
- relation between exam scores.

Definition

(Homogenous) binary relation R on the set A is a subset of the Cartesian product $A \times A = A^2$, i.e.

$$R \subseteq A^2.$$

Definition

(Homogenous) n-ary relation S on the set A is a subset of the Cartesian power $A \times A \times \cdots \times A = A^n$, i.e.

$$S \subseteq A^n.$$

Example

- Relation between students, with the same grade in DiM.
- Relation between pairs of students, who has a higher score.
- Relation between documents with similar terms (plagiarism)...

Binary relation is a special case of an n-ary relation. (unary, ternary, ...). (Homogenous) relations on a given set are special case of (heterogenous) relation between sets. In greater detail in another course.

Definition

(Binary) relation R on the set A is

- *reflexive* if $(x, x) \in R$ for all $x \in A$,
- *symmetric* if $(x, y) \in R \Leftrightarrow (y, x) \in R$ for all $x, y \in A$,
- *antisymmetric* if $(x, y), (y, x) \in R \Rightarrow x = y$ for all $x, y \in A$,
- *transitive* if $(x, y), (y, z) \in R \Rightarrow (x, z) \in R$ for all $x, y, z \in A$.
- *linear* (or *total*) if $(x, y) \in R$ or $(y, x) \in R$ for all $x, y \in A$

Examples

- equality relation "$=$" is reflexive, transitive, symmetric, and antisymmetric
- relation "$<$" is transitive a antisymmetric, "$\leq$" is also reflexive
- divisibility relation "$|$" on $\mathbb{N}$ (and $\mathbb{N}_0$) is reflexive, transitive, and antisymmetric
- "kindred" relation surely is symmetric, transitive, and reflexive
- relation of "subordinality" is antisymmetric and transitive
- relation of "understanding" is usually symmetric, generally not transitive

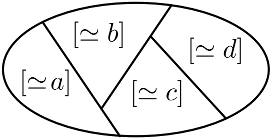
0.3.2. Equivalence relation

Definition

Equivalence on the set A is a *reflexive, symmetric, and transitive* binary relation on the set A. We denote it by $\simeq$.

Definition

Let $\simeq$ be an equivalence relation on the set A. An equivalence class of x (denoted by $[\simeq x]$) is the subset of A defined by $[\simeq x] = \{z \in A : z \simeq x\}$.



Equivalence relation expresses "having the same property".

Examples

- congruence relation $\equiv$ (same remainder after division by n)
- relation among students "having the same grade in DIM"
- relation "synonyms in a language" is (often) an equivalence

Definition of a set partition

We say the subsets $X_1, X_2, \ldots, X_m$ of the set Y form a partition of Y if

- $X_1, X_2, \ldots, X_m$ are pairwise disjoint: $X_i \cap X_j = \emptyset$ for $\forall i \neq j$
- their union gives the entire set: $X_1 \cup X_2 \cup \cdots \cup X_m = Y$

Questions

- find a partition with finitely many infinite classes
- find a partition with infinitely many classes
- find a partition with infinitely many infinite classes

There is a connection between equivalence relation on the set A and partition of the set A:

Theorem

The set of all different equivalence classes of $\simeq$ on the set A forms a partition of A.

The opposite is also true: a partition of the set A defines an equivalence relation on A.

Theorem

The set of different equivalence classes of $\simeq$ on A forms a partition of A.

Proof Notice, that every pair $a \simeq b$ has the same equivalence $[\simeq a] = [\simeq b]$ even if the notation is different, since for all $x \in [\simeq a]$ is $x \simeq a$, by transitivity $x \simeq b$, thus $x \in [\simeq b]$.

- $\bigcup_{x \in A} [\simeq x] = A$
  this follows by reflexivity of the $\simeq$ relation, since $x \in [\simeq x]$.
- $[\simeq x] \cap [\simeq y] = \emptyset$ for all $x \not\simeq y$
  We give an indirect proof: $[\simeq x] \cap [\simeq y] \neq \emptyset \Rightarrow [\simeq x] = [\simeq y]$.
  Taking some $u \in [\simeq x] \cap [\simeq y]$, then by the definition of an equivalence class is $u \simeq x$ and $u \simeq y$, which by transitivity and symmetry yields $x \simeq y$. So every $u \in [\simeq x]$ is in $[\simeq y]$ and vice versa, thus $[\simeq x] = [\simeq y]$. □

Examples

- partition of the set of all natural numbers by congruence relation modulo n
- partition of the set of all students according the relation "having the same grade in DIM"

0.3.3. Partial ordering

Ordering and equivalence are among the most common relations.

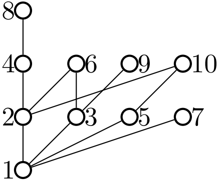
Definition

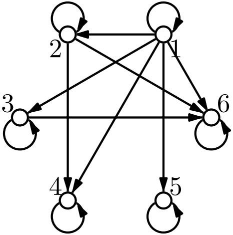
Partial ordering $\preceq$ on the set A is *reflexive, antisymmetric, and transitive* binary relation on the set A. The set with the relation is called a poset.

The word *partial* emphasizes the fact, that the relation does not have to be *linear* relation on A, i.e. not every pair of elements has necessarily to be related. Neither xRy nor yRx.

Partial orderings can be illustrated by a Hasse diagram

- if $x \preceq y$, then the element y will be drawn higher than x,
- elements x and y will be connected by a line if $x \preceq y$. We omit all lines that follow from transitivity.





Examples

- The relation of inclusion $\subseteq$ (to be a subset). Two sets can easily be not in relation $\subseteq$, for example $\{1,2\}$ and $\{1,3,4\}$.
- divisibility relation $|$ on $\mathbb{N}$ (previous figure)
- round robin tournament after first round — some players did not meet yet, we do not know "who is better"

Definition

We say a is smaller than b in a partial ordering $\preceq$ if $a \preceq b$. Moreover a and b are incomparable if neither $a \preceq b$ nor $b \preceq a$ hold.

We say the sequence $a_1, a_2, \ldots, a_n$ forms a path (or chain) in a poset with relation $\preceq$ if $a_1 \preceq a_2 \preceq \cdots \preceq a_n$.

An element m is called maximal in a partial ordering $\preceq$ on A if there is not element $x \in A$ greater than m, i.e. $\forall x \in A : m \preceq x \Rightarrow x = m$.

An element m is called maximum (or greatest) in a partial ordering $\preceq$ on A if every other element $x \in A$ is smaller than m, i.e. $\forall x \in A : x \preceq m$.

Minimal and minimum (or smallest) elements are defined analogously.

Examples

- 1 is the smallest positive natural number in the ordering “smaller” $\leq$
- the set $\{2, 3, 4, 5, 6\}$ with the divisibility relation does not have a smallest element, 2, 3, and 5 are minimal; elements 4 and 6 are not minimal, since $2|4$ and $2|6$ (thus “2 is smaller than 4 and 6”)
- natural numbers without zero do not have a maximal nor a greatest element in the ordering “smaller”
- positive rational numbers do not have a smallest nor a minimal element
- non-negative rational numbers have the smallest element 0 (it is also minimal)

The partial ordering $\preceq$ is called linear (or total) on the set A, if it does not have incomparable elements.

Having a total ordering of A, we can order the elements of A to one path.

Examples

- well known ordering of integers, rational, and real numbers “smaller”
- alphabetical (lexicographic) ordering of words; like in a dictionary

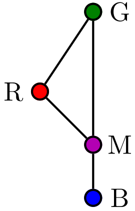
Example

There were four cars in the race: red, blue, green and magenta car. Red car arrived before magenta car. Green car arrived before red car. Magenta car arrived before blue car. Green car arrived before magenta car. Which car was last to arrive?

Let us introduce a partial ordering on the set of cars. Car x is smaller than car y (in this order), if x arrived later than car y.

This is a partial ordering: transitivity and antisymmetry are obvious. It is not reflexive! Make it reflexive ba taking rather "car x arrived before or at the same time as x".

We can draw a hasse diagram, cars that arrived earlier are depicted higher.



0.3.4. Mappings (functions)

Definition

Let $f \subseteq A \times B$ be a binary relation in which for each $x \in A$ exists *exactly one* ordered pair $(x, y) \in f$, where $y \in B$. Then relation f we call a mapping of set A to set B; we write $f : A \to B$.

In DiM we call the mapping of set A to set B a function.

The (unique) second element of the pair we denote for simplicity $y = f(x)$ instead of $(x, y) \in f$.

Note

In literature functions are considered to be a special case of mappings, when $A = B \subseteq \mathbb{R}$ (or $\mathbb{C}$). In this course we consider the terms *function* and *mapping* equivalent.

Examples

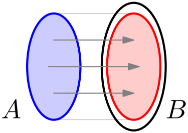
- in analysis $f : \mathbb{R} \to \mathbb{R}$, or a multi-variable function $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$
- the mapping $f : A \to B$, which assigns memory blocks in B to the pointers in A

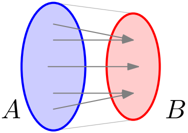
Certain significant properties of mappings have their own names:

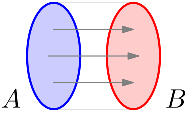
Definition

Function $f : A \to B$ is called

- one-to-one (injective) if any two distinct elements in A have distinct images in B, i.e. $x \neq y \Rightarrow f(x) \neq f(y)$ (or $f(x) = f(y) \Rightarrow x = y$)
- onto (surjective) if every element in B is the image of some element in A, i.e. $\forall y \in B$ there exists $x \in A$ such that $f(x) = y$
- bijective if f is "one-to-one" and "onto"





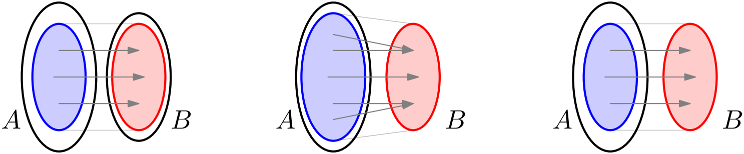


Examples

- Let $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$. Then f is not one-to-one nor onto.
- Let $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^3$. Then f is bijective.
- Let $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \sqrt{x}$. Then f is not a function ($\sqrt{-3} = ?$).

In UTI course there will be additional concepts:

- total function
  Let $f \subseteq A \times B$ be a binary relation in which for each $x \in A$ exists *exactly* one ordered pair $(x, y) \in f$, where $y \in B$.
- partial function
  Let $f \subseteq A \times B$ be a binary relation in which for each $x \in A$ exists *at most* one ordered pair $(x, y) \in f$, where $y \in B$.



Mapping and function form previous slides correspond to total functions. Partial functions are not “functions” in the given sense.

Beware: A (partial) bijection is defined only for total mappings, injectivity and surjectivity is not enough.

Composition of mapping

Definition: composition of mapping

Take two mappings $f : A \to B$ and $g : B \to C$.
Their composition is a mapping $(g \circ f) : A \to C$ (read "g after f") defined as

$$(g \circ f)(x) = g(f(x)).$$

In the composition of mappings $(g \circ f) : A \to C$ first f maps the pre-image $x \in A$ to its image $f(x) \in B$ and then g maps the pre-image $f(x) \in B$ to its image $g(f(x)) \in C$.

Note

Notice: the set of images (co-domain) of the first mapping f has to be a subset in the domain of the second mapping g.
If this is not true, no composed mapping exists!

Isomorphisms

Often we encounter structures which come from different concepts, have different names and are denoted differently though their structure is analogous. The elements of one structure can be relabeled using a *bijection* as in the second structure while its "properties" are preserved. This is the state of being isomorphic.

Examples

- the powerset of the set $\{a, b\}$ with the "subset" relation is isomorphic to the set $\{1, 2, 3, 6\}$ with divisibility relation
- the set $\{1, 2, \ldots, n\}$ has a similar subset system as $\{n + 1, n + 2, \ldots, 2n\}$; there is an obvious bijection $b(i) = i + n$; the partial orderings are isomorphic: bijection $b^*(X) = \{i + n : i \in X\}$
- divisibility relation on the set $\{1, 2, 3, 4, 6, 9, 12, 18, 36\}$ is isomorphic to the divisibility relation on $\{1, 2, 4, 5, 10, 20, 25, 50, 100\}$; bijection p in the prime factorization maps 3 to 5,
  i.e. $p(1) = 1$, $p(3) = 5$, $p(6) = 10$, $p(9) = 25$, $\ldots$
- Take (A, ρ), (B, σ). $(A, \rho) \simeq (B, \sigma)$ if there exists a bijection $f : A \to B$ s.t. $x \rho y \Leftrightarrow f(x) \sigma f(y)$

5.0.3. Permutations on a finite set

A permutation (without repetition) on set A can be considered as a mapping $\pi : A \to A$.

Take $A = [1, n]$.
Permutation on A is given by an arrangement $(p_1, p_2, \ldots, p_n)$. A mapping π we define by $\pi(i) = p_i$.

Examples

Permutations can be denoted by a matrix

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 2 & 6 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 3 & 1 & 6 \end{pmatrix}.$$

Now we can make a compound permutations

$$\sigma \circ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 3 & 5 & 6 \end{pmatrix}, \quad \pi \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 3 & 6 \end{pmatrix}.$$

One can think of the examples above as shuffling a deck of 6 cards.

Notes

- All permutations of the set $[1, n]$ along with the composition operation form a group called symmetric. We denote it by S_n.
- Each group is isomorphic to some subgroup of a symmetric group.
- Notice! There may be a different notation used for permutations!

By writing permutations we can omit the first (ordered) line $1, 2, \ldots, n$. We introduce the cycle notation used to specify permutations.

Definition

Let π be a permutation of the set A. By a cycle in π we understand such a sequence $(a_1, a_2, \ldots, a_k)$, that

$$\pi(a_i) = a_{i+1} \text{ for } i = 1, 2, \ldots, k-1 \text{ and } \pi(a_k) = a_1.$$

Examples

- $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 2 & 6 \end{pmatrix}$ in cycle notation $\pi = (1, 3, 5, 2)(4)(6)$
- $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 3 & 1 & 6 \end{pmatrix}$ in cycle notation $\sigma = (1, 2, 5)(3, 4)(6)$

Cycle notation of permutations

It is not specified by which element we start a cycle, usually we start by the "lowest".

Theorem

Each permutation of a finite set A can be written as a product of disjoint cycles.

Proof Take any (e.g. the smallest) element $a_1 \in A$ and iterate the mapping $a_2 = \pi(a_1)$, $a_3 = \pi(a_2), \dots,$ until we get a_1 (the process is finite, since A is finite). In this way we obtain the first cycle $(a_1, \dots, a_k)$. We continue by constructing cycles in the set $A \setminus \{a_1, \dots, a_k\}$ (e.g. from the lowest element), until we have used all elements of A. □

- a drawback of cycle notation lies in compositions of permutations
- an advantage is that the order of a permutation is easily found (the least number of compositions until we obtain identity)

Definition

Let $n \in \mathbb{N}$. Then n-th power of the permutation π is defined by the recurrence:
$\pi^1 = \pi$ for $n = 1$ and $\pi^n = \pi^{n-1} \circ \pi = \pi \circ \pi^{n-1}$ for $n > 1$.

Definition

Let k be the smallest $k \in \mathbb{N}$ for which $\pi^k = \mathrm{id}$, where π is a permutation. The number k is the order of the permutation π.

Example

Permutation $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$ is of order 6.
It is easy to verify, that $\tau \circ \tau \circ \tau \circ \tau \circ \tau \circ \tau = \mathrm{id}$ and that fewer than 6 compositions do not yield identity.

Theorem

The order of a permutation is the least common multiple of cycle lengths of all disjoint cycles of the permutation.

Example

Composition of permutations in cycle notation

We have the permutations

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 2 & 6 \end{pmatrix} = (1, 3, 5, 2)(4)(6),$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 3 & 1 & 6 \end{pmatrix} = (1, 2, 5)(3, 4)(6).$$

We know

$$\sigma \circ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 3 & 5 & 6 \end{pmatrix}, \quad \pi \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 3 & 6 \end{pmatrix}.$$

We compose the permutations in cycle notation:

$$\sigma \circ \pi = (1, 2, 5)(3, 4)(6) \circ (1, 3, 5, 2)(4)(6) = (1, 4, 3)(2)(5)(6).$$

Similarly

$$\pi \circ \sigma = (1, 3, 5, 2)(4)(6) \circ (1, 2, 5)(3, 4)(6) = (1)(2)(3, 4, 5)(6).$$

Example

We have a card shuffling machine for n cards.
It always performs the same permutation of the deck $\{1, 2, \ldots, n\}$.

- after using the machine k-times (k being the order of the permutation), the deck will be as before shuffling
- it is easy to prove, that for $n > 2$ we cannot obtain all possible shufflings by one machine

Example

Elegant explanation, why it is not possible to solve Loyd's fifteen is based on permutations.

Example

German cipher machine Enigma was cracked by the Alies during WWII. Major breakthrough was done by a Polish mathematician Marian Rejewski in 1932 based on the analysis of permutations. He was able to reconstruct the wiring without seeing the machine.

Example

The key for hints in the geocaching game is described by

```
A|B|C|D|E|F|G|H|I|J|K|L|M
-------------------------
N|O|P|Q|R|S|T|U|V|W|X|Y|Z
```

This is a permutation of order 2, same algorithm for encryption/decription.

Example

Random number generators in many programming languages are usually *not random*, but give elements from a permutation of high order.
Not obvious on the first sight, since we list (rounded) integers or elements from a specific list of numbers.

Questions

- What is the difference between a bijection and surjection?
- How do you show two sets have the same number of elements?
- How do you show two sets with an operation are “same”?
- How to compare sizes of sets using mappings?
- How to compare sizes of infinite sets using mappings?
- How many different shufflings a machine can make for 10 cards?
- How many different shufflings a machine can make for 32 cards?

0.4. Proof techniques in Discrete Mathematics

A typical attribute of mathematics is precision.
By this we mean the ability to prove a claim beyond any doubt.

The notion of a mathematical proof developed through centuries. Among the most famous proofs (based on historical evidence) are:

- visual proofs of Pythagorean theorem (claim: Babylonian script c. 1900–1600 BC., "Rhind Papyrus" Egypt 1788–1580 BC., proof: Pythagoreans c. 560–480 BC., China c. 500–200 BC.)
- Euklid's "Elements" c. 300 BC.

In modern mathematics: the understanding of a proof is a sequence of elementary verifiable steps leading from a known or assumed facts to a new claim.

Discrete mathematics is based on axioms, called "Peano axioms" or "Peano postulates" (i.e. well known facts about natural numbers along with the mathematical induction principle).

0.4.1. Basic logic and symbols

Known concepts:

- A proposition is a declarative sentence that is either true or false
- Truth value: 1/0, True/False
- Logical operators: "NOT" $\neg X$, "AND" $X \wedge Y$, "OR" $X \vee Y$
- Implication: "if X (is true), then Y (must be true)" $X \Rightarrow Y$
- Equivalence: "X (is true), if and only if Y (is true)" $X \Leftrightarrow Y$

Negation $\neg$ is an unary operator, $\wedge, \vee, \Rightarrow, \Leftrightarrow$ are binary operators.

Further operators can be obtained as combinations:
$A \text{ XOR } B$ is the same as $\neg(A \Leftrightarrow B)$.

Questions

- How many different logic binary operators are there?
- Is " ? : " a full ternary operator?

Quantifiers

Universal quantifier “For all $x \in M$ the statement $P(x)$ (is true)”
we write: $\forall x \in M : P(x)$
Existential quantifier “There exists $x \in M$, for which $P(x)$ (is true)”
we write: $\exists x \in M : P(x)$
We can omit the set M if it is clear what it stands for.

How to find a negation of a statement with a quantifier in general?

Example

Find the negation of $\forall x \in M : P(x)$?
$\exists x \in M : \neg P(x)$

Example

Find the negation of $\exists x \in M : P(x)$?
$\forall x \in M : \neg P(x)$

General setting for all particular examples in class. . .

0.4.2. Concept of a mathematical proof

Theorem (claims) in mathematics are usually of the form of a conditional statement: $P \Rightarrow C$

Precisely formulated premise (or hypothesis) P, under which the conclusion (consequence) C holds.

Detailed description how to obtain the conclusion from the premises is called a proof.

Mathematical proof

of some statement C is a finite sequence of steps including:

- axioms – or postulates that are considered true (the set of postulates differs for various disciplines*),
- hypothesis P is an assumption on which we work,
- statement derived from previous by some correct rule (depends on logic used).

The last step is a conditional statement with *conclusion* C.

* Discrete mathematics relies on Peano axioms, geometry is build upon five Euklid's postulates, ...

What could I need a proof for?

“What is the use of a newborn?”

- correctly understand the limitations of various method
- arguments for/against a presented solution
- comparison of quality of different solutions
- 100% validity of an algorithm may be required
  (autopilot, intensive care unit)

Example

About the inverse element We prove, that in any (even non-commutative!) algebraic group multiplication "by the inverse element" is commutative. I.e. if $A \cdot B = E$, then $B \cdot A = E$.
Recall multiplication of regular matrices: the unit matrix is defined only for regular matrices, the inverse matrix exists.

The group $(G, \cdot)$ is a set of elements with such an operation defined, that the so called *group axioms* hold. We need only three of them

1. the operation is associative
2. there exists a "unit element"
3. to every element there exists its inverse

Note

In the proof we can skip or shorten some elementary step. But we cannot omit any premise, that would violate the correctness. What can be omitted depends also on the "average reader".

The group $(G, \cdot)$ is a set of elements with such an operation defined, that the so called *group axioms* hold. We need only three of them

1. the operation is associative:
   $\forall A, B, C \in G : (A \cdot B) \cdot C = A \cdot (B \cdot C)$
2. there exists a "unit element":
   $\exists E \in G : E \cdot A = A \cdot E = A$ for $\forall A \in G$
3. to every element there exists its inverse:
   $\forall A \in G \ \exists A^{-1} : A \cdot A^{-1} = E \ \wedge \ A^{-1} \cdot A = E.$

Proof:

$$\begin{array}{rcll}
A \cdot B & = & E & \text{by assumption} \\
A^{-1} \cdot (A \cdot B) & = & A^{-1} \cdot E & \text{by 3rd axiom there exists } A^{-1} \\
(A^{-1} \cdot A) \cdot B & = & A^{-1} & \text{by 1st and 2nd axioms} \\
E \cdot B & = & A^{-1} & \text{by 3rd axiom} \\
B & = & A^{-1} & \text{by 2nd axiom} \\
B \cdot A & = & A^{-1} \cdot A & \\
B \cdot A & = & E & \text{by 3rd axiom}
\end{array}$$

0.4.3. Basic proof techniques

- direct proof: $A \Rightarrow B$
- indirect proof: $\neg B \Rightarrow \neg A$
- by contradiction: $A \wedge \neg B \Rightarrow$ *contradiction* (both T and $\neg T$ are true)
- proof by mathematical induction (weak and strong)

Example

Every odd number can be written as a difference of two squares.

We give a direct proof. Let $2k+1$, where $k \in \mathbb{Z}$, be any odd number, then $2k+1 = k^2+2k+1-k^2 = (k+1)^2-k^2$.

Example

There are infinitely many primes.

We know, that any positive natural number can be written as a product of primes. Proceed by contradiction:

Assume that there exist only finitely many primes $p_1, p_2, \ldots, p_n$ (*the complete list*). But the number $x = p_1 \cdot p_2 \cdots p_n + 1$ is not divisible by any prime in the list! We have a contradiction. Thus the assumption is not true – there are infinitely many primes.

0.4.4.Mathematical induction

Mathematical induction is a common proof technique used to prove propositional functions with a natural parameter n, denoted by $P(n)$.

Mathematical induction

Let $P(n)$ be a propositional function with an integer parameter n.
Suppose:

- *Basis step:*
  The proposition $P(n_0)$ is true, where $n_0 = 0$ or 1, or some integer.
- *Inductive step:*
  Assume the Inductive hypothesis: $P(n)$ holds for some n.
  Show, that for all $n > n_0$ if $P(n)$ holds, then also $P(n+1)$ holds.

Then $P(n)$ is true for all integers $n \geq n_0$.

Mathematical induction can be used also to prove validity of algorithms.

A few examples follow. . .

Wait a minute!

But. . .

- we verify the Basis step,
- we verify the Inductive step (using the Inductive hypothesis),

. . . how come this implies the validity for infinity many values!?!

Example

How high can you climb a ladder?

Suppose we can

- mount the first step,
- standing on rung n climb the rung $n + 1$.

. . . thus, we can reach any rung of the ladder!

Theorem

The sum of the first n even natural numbers is $n(n+1)$.

$2+4+6=12=3\cdot 4$

$2+4+6+8+10+12+14+16+18+20=110=10\cdot 11$

Proof by mathematical induction based on n:

We prove $\forall n \in \mathbb{N}$ the following holds $\sum_{i=1}^{n} 2i = n(n+1)$.

- *Basis step:* For $n=1$ claim P(1) gives "$2=1\cdot 2$".
- *Inductive step:* Does $P(n)$ imply $P(n+1)$?

  I.e. does $\sum_{i=1}^{n} 2i = n(n+1)$, imply $\sum_{i=1}^{n+1} 2i = (n+1)(n+2)$?

  We state *Inductive hypothesis* P(n):
  Suppose $\exists n \in \mathbb{N} : \sum_{i=1}^{n} 2i = n(n+1)$.
  Now
  $\sum_{i=1}^{n+1} 2i = \sum_{i=1}^{n} 2i + 2(n+1) \overset{IH}{=} n(n+1)+2(n+1) = (n+1)(n+2)$.
  We have shown the correctness of the formula for the sum of the first $n+1$ evens using the formula for the sum of the first n evens.

By mathematical induction the claim holds $\forall n \in \mathbb{N}$. □

A template for proofs by mathematical induction

One can use the following template:

1. State, that the proof technique will be mathematical induction: "$\forall n \in \mathbb{N}, n \geq n_0$ prove P(n)."

2. Verify the *Basis step:* Prove claim $P(n_0)$.

3. State the *Inductive hypothesis*: $\exists n \in \mathbb{N}, n \geq n_0$ for which P(n) holds.

4. Show the *Inductive step:*
   Using the Inductive hypothesis show the claim P(n+1).
   (We know how the statement P(n+1) is formulated!)

5. Invoke mathematical induction; state that P(n) holds for all $n \geq n_0$ by the induction principle.

Another example (on divisibility):

Theorem

For every natural number n is the expression $n^3 + 2n$ divisible by 3.

We say "a divides b" if $\exists k \in \mathbb{Z} : b = ka$. We write $a \mid b$.

Proof by mathematical induction based on n:
Prove that $\forall n \in \mathbb{N}$ the number 3 divides $n^3 + 2n$.

- *Basis step:* For $n = 1$ claim P(1) gives "3 divides $1^3 + 2 \cdot 1$".
- *Inductive step:* Prove that $P(n)$ implies $P(n+1)$ for every n.

  I.e., 3 divides $n^3 + 2n$, implies 3 divides $(n+1)^3 + 2(n+1)$.

  State *Inductive hypothesis* P(n):
  Suppose $\exists n \in \mathbb{N} : 3 \mid n^3 + 2n$, thus $\exists k \in \mathbb{Z} : n^3 + 2n = 3k$.

  Now $(n+1)^3 + 2(n+1) = (n^3 + 3n^2 + 3n + 1) + (2n + 2) =$
  $(n^3 + 2n) + (3n^2 + 3n + 3) \overset{IH}{=} 3k + 3(n^3 + n + 1)$.
  Obviously, 3 divides the last expression, therefore 3 divides $(n+1)^3 + 2(n+1)$.

By mathematical induction the claim holds $\forall n \in \mathbb{N}$. □

Yet another example (inequality):

Theorem

For every natural number $n \geq 4$ holds $n! > 2^n$.

The factorial $n!$ grows (super)exponentially with respect to n.

Proof by mathematical induction based on n:

We show, that $\forall n \in \mathbb{N}, n \geq 4$ the inequality $n! > 2^n$ holds.

- *Basis step:* For $n = 4$ the claim $P(4)$ gives "$4! > 2^4$", $24 > 16$.
- *Inductive step:* Does $P(n)$ imply $P(n+1)$?
  I.e., we show, that if $n! > 2^n$, then also $(n+1)! > 2^{n+1}$.

  State the *Inductive hypothesis* $P(n)$:
  Suppose, that $\exists n \in \mathbb{N}, n \geq 4$, for which $n! > 2^n$.

  Now $(n+1)! = (n+1) \cdot n! \overset{IH}{>} (n+1)2^n > 2 \cdot 2^n = 2^{n+1}$.

  We proved using the Inductive hypothesis, that $(n+1)! > 2^{n+1}$.

By mathematical induction the claim holds $\forall n \in \mathbb{N}$, $n \geq 4$. □

More examples:

Theorem

The number of all mappings of a b-element set to an a-element set is a^b.

Proof by induction on b:

- *Basis step:*
  For $b = 0$ we have only one choice (how *not* to assign: $a^b = a^0 = 1$).
  For $b = 1$ we have a possible images of one element ($a^b = a^1 = a$).
- *Inductive step:*
  IH: Suppose for some b the number of $B \to A$ mappings is a^b.

  Take any set B on $b + 1 > 0$ elements. Pick any element $x \in B$ and denote $B' = B \setminus \{x\}$, $|B'| = b$. There are a^b mappings from B' to A by Inductive hypothesis. Moreover, for x there are a (independent) choices of its image. There is a total of $a \cdot a^b = a^{b+1}$ different mappings from B to A.

By mathematical induction the number of distinct mappings from B to A is a^b for all $b \in \mathbb{N}_0$. □

Strong mathematical induction compared to mathematical induction

Mathematical induction

Let $P(n)$ be a propositional function with an integer parameter n.
Suppose:

- *Basis step:*
  The proposition $P(n_0)$ is true, where $n_0 = 0$ or 1, or some integer n_0.
- *Inductive step:*
  Assume the Inductive hypothesis: $P(n)$ holds for some n.
  Show, that for all $n > n_0$ if $P(n)$ holds, then also $P(n+1)$ holds.

Then $P(n)$ is true for all integers $n \geq n_0$.

Strong mathematical induction

- *Basis step:* The proposition $P(n_0)$ is true.
- *Inductive step:*
  Inductive hypothesis: Assume $P(k)$ holds for all $n_0 \leq k < n$.
  Show, that also $P(n)$ is true.

Then $P(n)$ is true for all integers $n \geq n_0$.

Example

There are always $pr-1$ breaks necessary to split a chocolate bar of $p \times r$ squares.

By *strong* induction on $n = pr$:

- *Basis step:*
  For $n_0 = 1$ we have a bar with only one square, there are no breaks necessary $(pr - 1 = 0)$.
- *Inductive step:*
  Suppose now the claim holds for *any* chocolate bars with less than n squares. Take any bar with n squares. We break this bar into two parts of s or t squares, respectively, where $1 \leq s, t < n$ and $s + t = n$. By Inductive hypothesis we can break each part by $s-1$ or $t-1$ breaks, respectively. There is a total of $(s-1)+(t-1)+1 = s+t-1 = n-1$ breaks necessary.

The proof is complete by strong induction for all positive p, r. □

Example

We have a stack of n boxes. We play the following game (for one/many players):

In one round we always unstack a stack with z boxes ($z \geq 2$) into two smaller stacks with x and y boxes each. For this unstacking we get points, the number of points is given by the product $x \cdot y$.

Game ends, if we obtain n stacks with one box each. We start with zero points and we want to get as many points as possible.

- Suggest a strategy that gives the highest score possible.
- Prove that no strategy gives a higher score that the one you suggested.

0.4.5. Combinatorial identities

For binomial coefficients we can derive many interesting formulas. There is an entire part of Discrete mathematics dealing with them.

Fact (an obvious statement)

For all $n \geq 0$ the following holds

$$\binom{n}{0} = \binom{n}{n} = 1.$$

Lemma (supporting statement)

For all $n \geq k \geq 0$ the following holds

$$\binom{n}{k} = \binom{n}{n-k}.$$

Statement, proof of which is just a substitution and one or two simple steps we consider as obvious and their proof we do not write down. On the other hand if the proof requires some elaborate step, "trick", or genuine derivation, it is customary to give some explanation.

Lemma

For all $n \geq k \geq 0$ the following holds

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

Proof (direct by substitution and derivations)

$$\binom{n}{k} + \binom{n}{k+1} = \frac{n!}{k! \cdot (n-k)!} + \frac{n!}{(k+1)! \cdot (n-k-1)!} =$$

$$= \frac{n! \cdot (k+1) + n! \cdot (n-k)}{(k+1)! \cdot (n-k)!} = \frac{n! \cdot (n+1)}{(k+1)! \cdot (n-k)!} =$$

$$= \frac{(n+1)!}{(k+1)! \cdot ((n+1)-(k+1))!} = \binom{n+1}{k+1}.$$

□

These formulas are an *alternative definition of binomial coefficients*.

$$\binom{n}{0} = \binom{n}{n} = 1 \qquad \binom{n}{k} = \binom{n}{n-k} \qquad \binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

Pascal's triangle

$$\binom{0}{0} = 1$$

$$\binom{1}{0} = 1 \quad \binom{1}{1} = 1$$

$$\binom{2}{0} = 1 \quad \binom{2}{1} = 2 \quad \binom{2}{2} = 1$$

$$\binom{3}{0} = 1 \quad \binom{3}{1} = 3 \quad \binom{3}{2} = 3 \quad \binom{3}{3} = 1$$

$$\binom{4}{0} = 1 \quad \binom{4}{1} = 4 \quad \binom{4}{2} = 6 \quad \binom{4}{3} = 4 \quad \binom{4}{4} = 1$$

$$\binom{5}{0} = 1 \quad \binom{5}{1} = 5 \quad \binom{5}{2} = 10 \quad \binom{5}{3} = 10 \quad \binom{5}{4} = 5 \quad \binom{5}{5} = 1$$

. . . .

All border elements are 1, all inner elements equal the sum of two elements immediately above.

Binomial Theorem

For all $n > 0$ the following holds

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n-1}x^{n-1} + \binom{n}{n}x^n.$$

Proof The proof can run by induction, but there is a nice argument. Multiplying through we use the rule "multiply each element with each other". Thus in $\underbrace{(1+x)(1+x)\dots(1+x)}_{n}$ each product x^k appears as many times as there are k-element selections from n parentheses. There are $\binom{n}{k}$ such different k-element subsets. □

From the Binomial theorem we have (first for $n \geq 0$, second for $n > 0$)

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n\,,$$

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \ldots - (-1)^n\binom{n}{n-1} + (-1)^n\binom{n}{n} = 0\,.$$

0.4.6. Proofs for the selection and arrangement formulas

In the following proofs we use mathematical induction and double counting.

Theorem

The number of all permutations of an n-element set is $n!$, for all $n \geq 0$.

By induction on n:

Basis step: The statement is true for $n = 0$, since there is only one way how to arrange an empty set. (Same is true for one-element sets.)

Inductive step: Suppose $n \geq 0$ and take any set P on $n + 1$ elements. Suppose for simplicity $P = \{1, 2, \ldots, n + 1\}$. Choose any element $p \in P$, there are $n + 1$ possibilities to do so. For any of the choices we then continue by constructing permutations of $P \setminus \{p\}$.
(Formally, these are always arrangements of a *different set*, but WLOG we can "relabel" the elements of $P \setminus \{p\}$ to get $\{1, 2, \ldots, n\}$.)

Now, by Inductive hypothesis there are $n!$ permutations of an n-element set $\{1, 2, \ldots, n\}$, thus there are $(n + 1) \cdot n! = (n + 1)!$ permutations of P. By mathematical induction this completes the proof $\forall n \in \mathbb{N}_0$. □

Theorem

The number of all k-permutations of an n-element set is $\dfrac{n!}{(n-k)!}$, for all $n \geq k \geq 0$.

By double counting:

We count the number of permutations of an n-element set in two ways. We know that there are $n!$ different permutations of the entire set. On the other hand we can take any k-permutation (a k-element sequence) and *the remaining $n-k$ elements order arbitrarily* after the sequence in one of the $(n-k)!$ different ways. From every k-permutation we obtain different permutations and every n-permutation can give a k permutation.

We denote by x the total number of all k-permutations on an n-element set. By the method above we obtain all $x \cdot (n-k)!$ different permutations of the n-element set. Thus

$$\begin{aligned} x \cdot (n-k)! &= n! \\ x &= \frac{n!}{(n-k)!}. \end{aligned}$$

Theorem

The number of all k-combinations of an n-element set is $\binom{n}{k}$, for all $n \geq k \geq 0$.

By double counting:

Now we count all k-permutations of an n-element set in two ways. First we know that there are $\frac{n!}{(n-k)!}$ such k-permutations. Second *from every k-combination we can obtain $k!$ different k-permutations* by arranging its elements into a sequence. We denote by x the number of k-combinations on an n-element set and similarly as in the previous proof we have,

$$\begin{aligned} x \cdot k! &= \frac{n!}{(n-k)!} \\ x &= \frac{n!}{k! \cdot (n-k)!} \\ x &= \binom{n}{k}. \end{aligned}$$

□

0.4.7. Proofs “by counting”

Sometimes we have to show that there exists an element with a certain property, but we cannot find/construct one. Such proofs are called non-constructive.

Instead to “construct” a solution, we show by “counting” there has to be at least one.

The pigeon-hole principle (Dirichlet’s principle)

When distributing $\ell + 1$ (or more) objects into ℓ boxes, there has to be a box with at least two objects.

Proofs by counting

The existence of a possibility will follow from the fact that there are too few cases in which the possibility does not occur.

Example

We see three cars entering a tunnel, but only two cars leaving the tunnel. This means there is one car left in the tunnel (though we do not see it).

Example

8 friends went on a 9 day vacation. Each day some triple of them went for a trip. Show, that at least one pair of friends didn't go together on a trip.

Proof Checking of all possibilities would take long…

The proof by counting is easy: In one triple there are 3 pairs, thus after 9 days there was *at most* $9 \cdot 3$ *pairs* on trips. But $9 \cdot 3 = 27 < \binom{8}{2} = 28$, thus at least one pair is missing.

Question

Are there two people on Earth with the same number of hair?

Example

In a drawer there are 30 pairs of black socks, 10 pairs of brown socks, and 3 pairs of white socks. How many socks we have to take (without light or looking) to guarantee, that we have at least one pair of the same color?

"Boxes" in the Pigeon-hole principle are the three colors. While taking four socks (not distinguishing the right or left sock), at least two of them have to be of the same color.

Question

We have four natural numbers. Show, that among them there are two numbers difference of which is divisible by 3.

Question

We have 3 natural numbers. Show, that among them there are two numbers difference of which is divisible by some prime.

Handshaking problem

There are n people in the room, some of them shook hands. Show that there are always at least two people who performed the same number of handshakes.

Example

We have five natural numbers. Show that there are always two among them, such that their sum is divisible by 9.

Proof (incorrect!) We have a total of 9 different classes modulo 9. Among five numbers we obtain 10 different sums. Surely, there has to be at least one sum in each class, in some class there will be at least two sums. Thus the pair which is in class "0", has its sum divisible by 9. □

Question

Why is the proof not correct?

Hint: try to verify the argument for the following set of five numbers: $\{0, 2, 4, 6, 8\}$.

Next lecture

Chapter 1. Sequences

- sequences
- sums and products
- arithmetic progression
- geometric progression
- ceiling and floor functions