Foundations of Discrete Mathematics

Spring 2022

Tuomas Sahlsten

Based on Ragnar Freij-Hollanti's materials

Version 1.0 (March 31, 2022)

Department of Mathematics and Systems Analysis, Aalto University

Contents

Welcome!

These are the lecture notes for the Foundations of Discrete Mathematics (MS-A0402) is given in Period IV on Spring 2022 in Aalto University. Discrete Mathematics is the mathematics of finite and countable structures, or loosely speaking the mathematics of sets where there is no notion of "convergence". Methods from discrete mathematics play a large role in many other subjects, in particular in computer engineering and data science. In this course we cover the foundations of discrete mathematics (graphs, enumeration, modular arithmetic) as well as as the foundations of all mathematics on university level (set logic and proof techniques). We also study some modern applications of the theory, in cryptography and networks theory.

Course content is roughly outlined as:

- Set theory and formal logic
- Relations and equivalence
- Enumerative combinatorics
- Graph theory
- Modular arithmetics

But more importantly:

- The fundamental notions and methods of mathematics (definition, theorem, proof, example...)

For learning, I recommend to look at the **Explorative exercises** (and additional exercises) from the assignment sheets: Updated on course homepage every Friday.

Here is some extra supporting literature for the course (in addition to these lecture notes, contain more details and proofs):

- Kenneth Rosen: *Discrete Mathematics and its Applications*, physical book
- Kenneth Bogart: *Combinatorics Through Guided Discovery.*, Freely available, `https://math.dartmouth.edu/news-resources/electronic/kpbogart/ComboNoteswHints11-06-04.pdf`
- Richard Hammack: *Book of Proof*, Freely available, `http://www.people.vcu.edu/%7Erhammack/BookOfProof/BookOfProof.pdf`

Good luck with the course!

- Tuomas

Chapter 1

Sets and formal logic

Set theory and formal logic form the foundation of all modern mathematics and the universal language used to describe and model phenomena. Here *sets* form some way to talk about collections of objects, where as *formal logic* gives us way to talk about logical implications. We learn formal logic:

- To define *precise* meanings of "and", "not", "or",...
- To transform complicated statements to equivalent but easier statements.
- Because it is the glue that holds mathematical statements together.

We do **not** learn it in order to:

- Write all mathematics using the symbols $\vee, \wedge, \forall, \exists, \cdots$

Formal logic is in the background of all mathematics, not the forefront.

1.1 Sets

1.1.1 Definition

All mathematical structures are sets, and all statements about them can be described in terms of sets.

Example 1.1

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is the set of natural numbers.
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ is the set of integers.
- $\mathbb{Q} = \{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\}$ is the set of rational numbers.
- $\mathbb{R}$ is the set of real numbers.
- $\{\Delta ABC : A, B, C \in \mathbb{R}^2\}$ is the set of triangles in the plane.
- The members (*elements*) of a set can be whatever:

  $$A = \{\text{skateboard}, \text{paperclip}, 16, \pi, \text{infinity}\}$$

  is a set.

The most important notion in set theory is the symbol $\in$.

- $x \in A$ if "the element x belongs to the set A".
- $x \notin A$ if "the element x does not belong to the set A".

Example 1.2

- my car $\in \{\text{cars}\}$.
- $5 \in \mathbb{Z}$.
- $5 \in \mathbb{R}$.
- $5 \notin \mathbb{R}^2$.
- $\pi \in \mathbb{R}$.
- $\pi \notin \mathbb{Z}$.

We can *define the set* in the following ways:

- Listing elements: $\{2, 4, 5, 7\}$ is a set whose elements are 2, 4, 5, 7.
- Writing

  $$\{\texttt{expression} : \texttt{condition}\},$$

  which is a set containing all elements described by the `expression`, if the `condition` is satisfied.
  - $\{x^2 : x \in \mathbb{Z}, 2 < x < 10\} = \{9, 16, 25, 36, 49, 64, 81\}$.
  - $\{x \in \mathbb{R} : -1 \leq x \leq 1\} = [-1, 1]$.
- Futhermore, *empty set* $\emptyset = \{\}$ is a set that has no elements.

1.1.2 Equality and subsets

Definition 1.3 (Equality)

We say that two sets are the *same* $=$ if they contain the same elements.

Example 1.4

$\{2, 3, 4\} = \{4, 2, 4, 3\}$.

Sets do not have "order", nor "multiplicity". Thus, there is only one "empty set" $\emptyset$.

Definition 1.5 (Subsets)

We define $A \subseteq B$ ("A is a *subset* of B") if all elements of A are also in B.

Subsets can be visualised with a *Venn diagram:*

Example 1.6

- $$\emptyset \subseteq \{1, 2, 3\} \subseteq \mathbb{Z} \subseteq \mathbb{R}.$$
- $\emptyset$ is a subset of every set.
- Every set is a subset of itself.

Thus, $A = B$ if

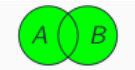
$$A \subseteq B \text{ and } B \subseteq A.$$

If $A \subseteq B$ and $A \neq B$, then A is a *proper* subset of B. Denoted $A \subsetneq B$, or sometimes $A \subset B$.

1.1.3 Set operations

In set theory we will commonly use the following set operations, which we can visualise with Venn diagrams.

- Union: $x \in A \cup B$ if $x \in A$ *or* $x \in B$.



- Intersection: $x \in A \cap B$ if $x \in A$ *and* $x \in B$.

- Set difference: $x \in A \setminus B$ if $x \in A$ but $x \notin B$.

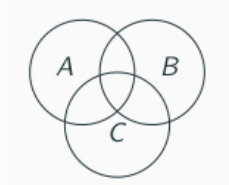
- Complement: $x \in A^c = \Omega \setminus A$ if $x \notin A$
  (but x is in the "universe" Ω, which is understood from context).

Then the set operations satisfy the following *laws*

Theorem 1.7

- Commutative laws:
  - $A \cap B = B \cap A$
  - $A \cup B = B \cup A$
- Associative laws:
  - $(A \cap B) \cap C = A \cap (B \cap C)$
  - $(A \cup B) \cup C = A \cup (B \cup C)$
- Distributive law:
  - $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$
  - $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

Proof
These can be proven using Venn diagrams:



□

1.1.4 Cartesian product

Cartesian products are used to construct "higher dimensional" sets from lower dimensions. For example, the Euclidean plane of vectors $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$:

Definition 1.8 (Cartesian product)

The *Cartesian product* $A \times B$ is the set of ordered pairs

$$\{(a, b) : a \in A, b \in B\}.$$

- $\{a, b, c\} \times \{1, 2\} = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$.
- $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ ("the xy-plane")

Definition 1.9 (Power set)

The *power set*: $P(A)$ is the set of all subsets of A.

Example 1.10

- $P(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.
- $P(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.
- $P(\emptyset) = \{\emptyset\} \neq \emptyset$.

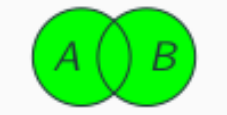
Definition 1.11 (Cardinality)

- $|A|$ denotes the number of elements in a finite set A.
- This is called the *cardinality* of A.
- If $S \subseteq T$, then $|S| \leq |T|$.

Example 1.12

- $|\emptyset| = 0$
- $|\{\emptyset\}| = 1$
- $|\{a, b, c\}| = |\{a, c, c, b, a, c, b, b, a\}| = 3$.

- If $|A| = 9$ and $|B| = 5$, what can we say about $|A \cup B|$?



  - $9 \leq |A \cup B|$.
  - $|A \cup B| \leq 14$.
  - $|A \cup B| \in \mathbb{N}$.
- In general, $|A \cup B| = |A| + |B| - |A \cap B|$.
- If $S \subseteq T$, then $|S| \leq |T|$.

Thus we have

Theorem 1.13

$$\max(|S|, |T|) \leq |S \cup T| \leq |S| + |T|.$$

1.1.5 Enumeration

Next we will go to the idea of *cardinality*, and counting the number of elements in a set. We will denote $|A|$ or $\sharp A$ as the number of elements in A.

- Let $|S| = n$ and $|T| = m$.
- An ordered pair (s, t), where $s \in S$ and $t \in T$, can be chosen in nm ways.
- So $|S \times T| = nm = |S| \cdot |T|$.

Theorem 1.14

Let $A_1, \ldots, A_k$ be finite sets. Then

$$|A_1 \times \cdots \times A_k| = |A_1| \cdot \cdots \cdot |A_k|.$$

- A subset A of $\{1, 2, \cdots, n\}$ is determined by, for each $1 \leq i \leq n$, whether or not $i \in A$.
- So a subset of $\{1, 2, \cdots, n\}$ can be described by a string of n symbols 0 ("out") and 1 ("in").
- Example: The string 001101 corresponds to the set

$$\{3, 4, 6\} \subseteq \{1, \ldots, 6\}.$$

- A subset of $\{1, 2, \cdots, n\}$ corresponds to a string of n symbols 0/1, which is the same as an element of
$$\{0,1\}^n = \underbrace{\{0,1\} \times \cdots \times \{0,1\}}_{n \text{ factors}}$$
- It follows that
$$|P(\{1,\ldots,n\})| = |\{0,1\}^n| = |\{0,1\}|^n = 2^n.$$

Theorem 1.15

Let A be a finite set. Then
$$|P(A)| = 2^{|A|}.$$

1.1.6 Indexing a family of sets and set operations

We can also have multiple sets, which we can index using some sets. Usually they are indexed with natural numbers (finite or infinite subsets), but they can be indexed over any set, like the reals.

Definition 1.16 (Indexed family of sets over finitely many indices)

Let $A_1, A_2, A_3, \cdots A_k \subseteq \Omega$ be sets. We say that
$$\{A_i : 1 \leq i \leq k\}$$
is an *indexed family of sets*. Then
$$\bigcup_{i=1}^{k} A_i = \{x \in \Omega : x \in A_i \text{ for some } 1 \leq i \leq k\}.$$
$$\bigcap_{i=1}^{k} A_i = \{x \in \Omega : x \in A_i \text{ for every } 1 \leq i \leq k\}.$$
This is union and intersection of more than two sets.

Example 1.17

Let $A_1 = \{0, 2, 5\}$, $A_2 = \{1, 2, 5\}$, $A_3 = \{2, 5, 7\}$.
$$\bigcup_{k=1}^{3} A_k = \{0, 1, 2, 5, 7\}.$$
$$\bigcap_{k=1}^{3} A_k = \{2, 5\}.$$

Definition 1.18 (Indexed family over countable index set)

We can do the same for infinitely large families of sets. Let $A_1, A_2, A_3, \cdots \subseteq \Omega$ be sets. We say that

$$\{A_i : i \geq 1\}$$

is an *indexed family of sets*. Then we can define the unions and intersections as follows:

$$\bigcup_{i=1}^{\infty} A_i = \{x \in \Omega : x \in A_i \text{ for some } i \in I\}.$$

$$\bigcap_{i=1}^{\infty} A_i = \{x \in \Omega : x \in A_i \text{ for every } i \in I\}.$$

Example 1.19

Let $\Omega = \mathbb{R}$, and let A_k be the closed interval $A_k = [0, \frac{1}{k}]$ for $k \geq 1$.

$$\bigcup_{k=1}^{\infty} A_k = [0, 1].$$

$$\bigcap_{k=1}^{\infty} A_k = \{0\}.$$

Definition 1.20 (Indexed family over general index set)

We can do the same for other indexing sets as well. Let I be a set. Let $A_i \subseteq \Omega$ be a set, for each $i \in I$. Then

$$\{A_i : i \in I\}$$

is an *indexed family of sets*. We can then define the unions and intersections over this family as follows:

$$\bigcup_{i \in I} A_i = \{x \in \Omega : x \in A_i \text{ for some } 1 \leq i\}.$$

$$\bigcap_{i \in I} A_i = \{x \in \Omega : x \in A_i \text{ for every } 1 \leq i\}.$$

1.1.7 Russel's paradox

"A male barber in the village shaves the beards of precisely those men, who do not shave their own beard."

Does the barber shave his own beard? Whether he does or does not, we get a contradiction. This is an instance of the problem of *self-reference* in set theory.

- For every man x in the village, there is a set S_x consisting of all the men whose beards he shaves.
- For the barber B,
$$S_B = \{x : x \notin S_x\}.$$
- In particular,
$$B \in S_B \Leftrightarrow B \notin S_B,$$
which is a contradiction! We are not allowed to use the set S in the formula that defines S!

For every "universe" Ω and every statement P (without self-reference),

$$\{x \in \Omega : P(x)\} \subseteq \Omega$$

is a set. Let Ω be "the set of all sets", and let

$$S = \{A \in \Omega : A \notin A\}.$$

Is S an element of itself? Again we get a contradiction.

To avoid this kind of contradictions, we decide:

- The "set of all sets" does not exist.
- No set is allowed to be an element of itself.
- All sets must be constructed from "safe and well-understood sets" (like $\mathbb{R}$) by taking
  - Subsets.
  - Cartesian products.
  - Power sets.
  - Unions.

1.2 Formal logic

1.2.1 Statements, closed- and open sentences

We will now move to the concept of formal logic to discuss about statements, their truth values and truth tables, and we will relate these to set theor.

Definition 1.21 (Statement)

A *statement* is a sentence that is either true or false.

Example 1.22

- Statements:
  - $2 \in \mathbb{Z}$
  - $2 = 5$
  - The millionth decimal of π is 7.
  - All mathematicians are bald.
- Not statements:
  - Is $2 + 2 = 4$?
  - This sentence is false.
  - x is an integer.
- Also not a statement:
  - This sentence is true.

Statements are also called *closed sentences*. An *open sentence* is a sentence containing a variable x, that *would have* a truth value of x had a given value. Open sentences are also called *predicates*.

Example 1.23

- Open sentences:
  - NN is the president of Finland.
  - $-1 \leq y \leq 1$.
  - The millionth decimal of π is n.
  - NN is bald.
  - x is an integer.
- Also an open sentence:
  - $1 \leq y \leq -1$.

- There are two ways to make a statement out of an open sentence (like "$-1 \leq y \leq 1$"):
- Assign a value to the variable.
  - "$-1 \leq 0 \leq 1$" is a TRUE statement.
  - "$-1 \leq 19 \leq 1$" is a FALSE statement.
- Quantify.
  - "There exists a real number y, such that $-1 \leq y \leq 1$" is a TRUE statement.
  - "For every real number y, $-1 \leq y \leq 1$" is a FALSE statement.

1.2.2 Quantifiers

Quantifiers are crucial way to discuss about existence and non-existence, and they relate closely to set theory. They are defined as follows

Definition 1.24 ($\forall$ and $\exists$ quantifiers)

- "For every $x \in A$, $P(x)$ holds" is denoted formally

$$\forall x \in A : P(x).$$

- "There is some $x \in A$, for which $P(x)$ holds" is denoted formally

$$\exists x \in A : P(x).$$

Example 1.25

- Which of the following statements are true?
  - $\forall x \in \mathbb{R} : x^2 > 0$.
  - $\exists a \in \mathbb{R} : \forall x \in \mathbb{R} : ax = x$.
  - $\forall n \in \mathbb{Z} : \exists m \in \mathbb{Z} : m = n + 5$.
  - $\exists n \in \mathbb{Z} : \forall m \in \mathbb{Z} : m = n + 5$.
  - On every party, there are two guests who know the same number of other guests.
- 2 and 3 are true, 1 and 4 are false.
- We will revisit 5 later in the course.

1.2.3 Connectives and truth tables

Statements can be connected by logical connectives:

negation	$\neg$	"not"
conjunction	$\wedge$	"and"
disjunction	$\vee$	"or"
implication	$\rightarrow$	"implies", "if ... then ..."
equivalence	$\leftrightarrow$	"if and only if"

- Statements can be quantified:

$\forall$	"for all"
$\exists$	"exists"

- Natural language has many more quantifiers: "many", "five", "infinitely many", "a few", "more than I thought"...

The meaning of connectives are *defined* via *truth tables*. In the following A and B denote statements, and T and F denote the truth values "True" and "False":

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

A	$\neg A$
T	F
F	T

A	B	$A \leftrightarrow B$
T	T	T
T	F	F
F	T	F
F	F	T

The least intuitive connective is implication $\rightarrow$. $A \rightarrow B$ should certainly be False if A is True but B is False. What about the other rows?

A	B	$A \rightarrow B$
T	T	?
T	F	F
F	T	?
F	F	?

A statement like

$$(a > 3) \rightarrow (a^2 > 9)$$

"should be" True for any number a.If $a = 4$, this means that $T \rightarrow T$ should be True. If $a = 0$, this means that $F \rightarrow F$ should be True. If $a = -4$, this means that $F \rightarrow T$ should be True.

A	B	$A \rightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

We *define* the connective $\rightarrow$ by the truth table

A	B	$A \rightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

A False statement implies everything! For example,

$$\forall x \in \mathbb{R} : (x^2 < 0) \rightarrow (x = 23)$$

is a True statement. Silly, I know. But that's how it has to be. Live with it.

1.2.4 Tautologies

Definition 1.26

A *tautology* is a (composed) statement that is True regardless of the truth values of the elementary statements that it is composed of.

Example 1.27

The following statements are tautologies:

- $(\neg\neg P) \to P$ (double negation)
- $P \vee (\neg P)$ (excluded middle)
- $(P \to Q) \leftrightarrow (\neg Q \to \neg P)$ (contrapositive)
- $(P \leftrightarrow Q) \leftrightarrow ((P \to Q) \wedge (Q \to P))$ (equivalence law)
- These can be *proven* via truth tables.

If $A \to B$ is a tautology (where A and B are composed statements), then we write

$$A \Rightarrow B.$$

This gives us a way to "calculate" with statements. If $A \iff B$ (ie $A \leftrightarrow B$ is a tautology), then we can replace A by B everywhere in our logical reasoning. Often useful in math to replace an implication $P \to Q$ by its *contrapositive* $(\neg Q) \to (\neg P)$.

Example 1.28

- The contrapositive (for $x \in \mathbb{R}$) of

$$\text{if } x > 0 \text{ then } x^3 \neq 0$$

is

$$\text{if } x^3 = 0 \text{ then } x \leq 0.$$

1.2.5 Treasures example

Example 1.29

- Before you are three chests. They all have an inscription.
  - **Chest 1**: Here is no gold.
  - **Chest 2**: Here is no gold.
  - **Chest 3**: Chest 2 contains gold.

- We know that one of the inscriptions is true. The other two are false.
- If we can only open one chest, which one should we open?

Solution.

- **Axiom:** One of the inscriptions is true. The other two are false.
- Let P_i be the statement *"Chest i contains gold"*.
  - **Chest 1:** Here is no gold. $Q_1 := \neg P_1$
  - **Chest 2:** Here is no gold. $Q_2 := \neg P_2$
  - **Chest 3:** Chest 2 contains gold. $Q_3 := P_2$
- The axiom says

$$[Q_1 \wedge (\neg Q_2) \wedge (\neg Q_3)] \vee [(\neg Q_1) \wedge Q_2 \wedge (\neg Q_3)] \vee [(\neg Q_1) \wedge (\neg Q_2) \wedge Q_3]$$

$$\iff$$

$$[(\neg P_1) \wedge (\neg\neg P_2) \wedge (\neg P_2)] \vee [(\neg\neg P_1) \wedge (\neg P_2) \wedge (\neg P_2)] \vee [(\neg\neg P_1) \wedge (\neg\neg P_2) \wedge P_2]\,.$$

$$\iff$$

$$[\neg P_1 \wedge P_2 \wedge \neg P_2)] \vee [P_1 \wedge \neg P_2 \wedge \neg P_2] \vee [P_1 \wedge P_2 \wedge P_2]\,.$$

$$\iff$$

$$[P_1 \wedge \neg P_2] \vee [P_1 \wedge P_2]\,.$$

$$\iff$$

$$P_1$$

- The axiom "One of the inscriptions is true. The other two are false." $\iff$ *"Chest 1 contains gold"*.

- **Lesson 1**: Open the first chest.
- **Lesson 2**: Manipulating propositional statements (by the tautology rule) is "mechanical". Mathematical reasoning *without quantifiers* can be automated.

1.2.6 Negations of quantifiers

What is the negation (opposite) of

$$\forall x \in A : P(x)?$$

Example 1.30

- $A = \{\text{mathematicians}\}$, $P(x) =$"x is bald".
- $\forall x \in A : P(x)$ means "all mathematicians are bald".
- The opposite is "some mathematicians are not bald".

So

$$\neg \forall x \in A : P(x)$$

is equivalent to

$$\exists x \in A : \neg P(x).$$

1.2.7 Computing with logical symbols

We can perform computations with logical symbols, which have consequences also for number theory later on. For example, the first one here is a bit like $-(-1) = 1$:

$$\begin{aligned} (\neg\neg P) &\iff P \\ (P \to Q) &\iff (\neg Q \to \neg P) \\ \exists x \in \Omega : \neg P(x) &\iff \neg \forall x \in \Omega : P(x) \end{aligned}$$

In *constructive mathematics*, one only has the right implication

$$\exists x \in \Omega : \neg P(x) \Rightarrow \neg \forall x \in \Omega : P(x)$$

in the last line. This is philosophically interesting, and also interesting in some algorithmic applications, but will not be relevant in this course.

1.2.8 Sets and predicate logic

Finally we relate sets A and predicates $P(x)$ as follows:

- To any predicate $P(x)$ corresponds a set $\{x \in \Omega : P(x)\}$.

- To the set $S \subseteq \Omega$ corresponds the predicate $x \in S$.
- Sometimes mathematical statements are easier to think about in terms of sets, sometimes in terms of logical symbols.
- To any predicate $P(x)$ corresponds a set $S_P = \{x \in \Omega : P(x)\}$.
- To the predicate $P(x) \wedge Q(x)$ corresponds the set

$$\begin{aligned} S_{P \wedge Q} &= \{x \in \Omega : P(x) \text{ and } Q(x)\} \\ &= \{x \in \Omega : P(x)\} \cap \{x \in \Omega : Q(x)\} = S_P \cap S_Q. \end{aligned}$$

- To the predicate $P(x) \vee Q(x)$ corresponds the set

$$\begin{aligned} S_{P \vee Q} &= \{x \in \Omega : P(x) \text{ or } Q(x)\} \\ &= \{x \in \Omega : P(x)\} \cup \{x \in \Omega : Q(x)\} = S_P \cup S_Q. \end{aligned}$$

1.3 Proof techniques

In mathematics *proofs* are used to verify if a statement is true or not. In this section we will learn about various techniques to prove a statement. If you have not encountered proofs before, this can be quite challenging initially, and it is good to practise first with simple statements with the techniques presented here.

1.3.1 Proof and overview of the proof techniques

In the most abstract version, a mathematical theorem has an *axiom* (or conjunction of axioms) P, and a conclusion Q. A *proof* consists of a sequence of statements such that each row is either

- An axiom or a definition.
- Tautologically implied by the previous rows.
  if previous rows say $p_1, \ldots, p_k$, and $(p_1 \wedge \cdots \wedge p_k) \to q$
  is a tautology, then the next row may say q.
- Obtained from previous lines by "quantor calculus":

$$\begin{aligned} \forall x : \neg P(x) &\Leftrightarrow \neg \exists x : P(x) \\ \exists x : \neg P(x) &\Leftrightarrow \neg \forall x : P(x) \end{aligned}$$

- A special case of a previous row.
  if one row says $\forall x P(x)$, then the next row may say $P(c)$.
- An existential consequence of previous rows.
  if one row says $P(c)$, then the next row may say $\exists x : P(x)$.

Most mathematical proofs uses one of the following tautologies:

Definition 1.31 (Proof techniques)

- $(P \wedge (P \to Q)) \Rightarrow Q$ (Direct proof)
- $(P \wedge (\neg Q \to \neg P)) \Rightarrow Q$ (Contrapositive proof)
- $(P \wedge ((P \wedge \neg Q) \to False) \Rightarrow Q$ (Proof by contradiction)
- $((P_1 \vee P_2) \wedge (P_1 \to Q) \wedge (P_1 \to Q)) \Rightarrow Q$ (Proof by cases)

...and / or the following ways to prove existence:

- $P(c) \Rightarrow \exists x : P(x)$ (Constructive proof)
- $(\neg P(c) \to \exists x : P(x)) \Rightarrow \exists x : P(x)$ (Nonconstructive proof)

Next, we will see examples of all these proof techniques.

1.3.2 Direct proof

Example 1.32

For all odd integers n, then n^2 is also odd.

Proof

- Let n be an *arbitrary* odd integer.
- That means $n = 2k + 1$ for some integer k.
- Then
$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$
- Since $2k^2 + 2k$ is an integer, this means that n^2 is odd.

□

1.3.3 Contrapositive proof

Example 1.33

For all integers n, if n^2 is odd, then n is also odd.

Proof

- First attempt (direct proof):
- $n^2 = 2k + 1$ for some integer k.
- So $n = \pm\sqrt{2k+1}$, and n is an integer.
- No obvious way to write $n = 2\ell + 1$.

□

Example 1.34

For all integers n, if n^2 is odd, then n is also odd.

Proof
New attempt (contrapositive proof): Need to prove that if n is **not** odd, then n^2 is **not** odd. So assume $n = 2k$ even. Then $n^2 = 4k^2 = 2(2k^2)$ is even, so not odd. Thus, if n were odd, then n^2 must also be odd. □

1.3.4 Proof by contradiction

Example 1.35

$\sqrt{2} \notin \mathbb{Q}$.

Proof
Assume the claim was not true, so $\sqrt{2} \in \mathbb{Q}$. Then we could write $\sqrt{2} = \frac{p}{q}$, where p and q are integers with no common divisor. Then $2q^2 = p^2$, so p^2 is even. So p is even, and we can write $p = 2r$, $r \in \mathbb{Z}$ So $q^2 = \frac{p^2}{2} = 2r^2$ is even. Now p and q are both even. But this contradicts our assumption that they had no common divisor. Thus the assumption was false, so $\sqrt{2} \notin \mathbb{Q}$. □

1.3.5 Proof by cases

Recall:

$$|a| = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases}$$

Example 1.36

For all real numbers x, y, it holds that $|xy| = |x||y|$.

Proof

- Three cases:
  - Both numbers ≥ 0, so $xy \geq 0$: $|xy| = xy = |x||y|$.
  - Both numbers < 0, so $xy > 0$: $|xy| = xy = (-x)(-y) = |x||y|$.
  - The numbers have different sign, so $xy \leq 0$. Without loss of generality (WLOG) $x < 0 \leq y$:
$$|xy| = -xy = (-x)y = |x||y|.$$
- These cases cover all possibilities, so the claim is true for all $x, y \in \mathbb{R}$.

□

1.3.6 Constructive existence proof

Example 1.37

There exist integers that can be written as a sum of two cubes in more than one way.

Proof

$$12^3 + 1^3 = 1728 + 1 = 1729 = 1000 + 729 = 10^3 + 9^3$$

□

1.3.7 Nonconstructive existence proof

Example 1.38

There exist irrational numbers $x, y \notin \mathbb{Q}$ such that $x^y \in \mathbb{Q}$.

Proof

- The number $a = \sqrt{2}^{\sqrt{2}}$ is of the form x^y, where $x = y = \sqrt{2} \notin \mathbb{Q}$.
- If a is not rational, then $a^{\sqrt{2}}$ is also of the form x^y, where $x = a \notin \mathbb{Q}$ and $y = \sqrt{2} \notin \mathbb{Q}$.
- But
$$a^{\sqrt{2}} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} = \sqrt{2}^2 = 2 \in \mathbb{Q}.$$
- So either $x = y = \sqrt{2}$ is an example of numbers with the desired property, or $x = a$, $y = \sqrt{2}$ is.
- So some irrational numbers with this desired property exist.

□

1.3.8 Induction proofs

This proof technique is very useful for number sequences (but also in many other parts of mathematics)

- **Goal:** Prove a statement $P(n)$ for all natural numbers $n \in \mathbb{N}$.
- **Technique:**
  - First (base case) prove the first case $P(0)$.
  - Then (induction step) prove that, for an arbitrary $m \in \mathbb{N}$,
    IF $P(m)$ holds, THEN $P(m+1)$ also holds.
  - These two steps together prove that the statement $P(n)$ holds for any $n \in \mathbb{N}$.

$$P(0) \Rightarrow P(1) \Rightarrow P(2) \Rightarrow P(3) \Rightarrow P(4) \Rightarrow \cdots .$$

Example 1.39

Let a_n be recursively defined by $a_0 = 0$ and $a_{n+1} = 2a_n + 1$. Then $a_n = 2^n - 1$ for all $n \in \mathbb{N}$.

Proof

- Base case: $a_0 = 0 = 1 - 1 = 2^0 - 1$, so the statement is true for $n = 0$.
- Induction step: Assume (*induction hypothesis*) that $a_m = 2^m - 1$. Then

$$a_{m+1} \overset{def}{=} 2a_m + 1 \overset{IH}{=} 2 \cdot (2^m - 1) + 1 = 2^{m+1} - 2 + 1 = 2^{m+1} - 1,$$

  so the statement is also true for $n = m + 1$.
- It follows that the statement $a_n = 2^n - 1$ is true for all $n \in \mathbb{N}$.

□

Example 1.40

Prove that, for every $n \in \mathbb{N}$,

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

Proof

- Base case ($n = 0$):

$$\sum_{i=1}^{0}(2i-1) = \sum_{i\in\emptyset}(2i-1) = 0 = 0^2.$$

- Induction step: Assume (*IH*) that $\sum_{i=1}^{m}(2i-1) = m^2$. Then

$$\begin{aligned}\sum_{i=1}^{m+1}(2i-1) &\overset{def}{=} (2(m+1)-1) + \sum_{i=1}^{m}(2i-1)\\ &\overset{IH}{=} m^2 + 2(m+1) - 1 = m^2 + 2m + 1 = (m+1)^2,\end{aligned}$$

  so the statement is also true for $n = m + 1$.

□

There is also a more general version of the induction proof, which can be useful for certain situations that involve e.g. sequences. The goal is the same:

- **Goal:** Prove a statement $P(n)$ for all natural numbers $n \in \mathbb{N}$.
- **More general technique:**
  - First (base case) prove the k first cases $P(0), \ldots, P(k)$.
  - Then (induction step) prove that, for an arbitrary $m \in \mathbb{N}$,
    IF $P(m-k), \ldots, P(m)$ holds, THEN $P(m+1)$ also holds.
  - These two steps together prove that the statement $P(n)$ holds for any $n \in \mathbb{N}$.

    $$(P(0) \wedge \cdots \wedge P(k)) \Rightarrow (P(1) \wedge \cdots \wedge P(k+1)) \Rightarrow (P(2) \wedge \cdots \wedge P(k+2)) \Rightarrow \cdots .$$

  - How large k needs to be, may depend on the problem.

Example 1.41

The Fibonacci numbers are defined by $f_0 = 0$, $f_1 = 1$ and $f_n = f_{n-1} + f_{n-2}$. For all $n \in \mathbb{N}$ holds $f_n < 2^n$.

Proof

- Base case: $f_0 = 0 < 1 = 2^0$ and $f_1 = 1 < 2 = 2^1$.
- Induction step: Assume (*induction hypothesis*) that $f_m < 2^m$ and $f_{m-1} < 2^{m-1}$. Then

$$f_{m+1} \overset{def}{=} f_m + f_{m-1} \overset{IH}{<} 2^m + 2^{m-1} < 2 \cdot 2^m = 2^{m+1},$$

  so the statement is also true for $n = m + 1$.
- It follows that the statement $f_n < 2^n$ is true for all $n \in \mathbb{N}$.

□

1.4 Relations

Next, we will move to the topic of *relations*. Relations are used in all parts of mathematics, and we can consider them as generalisations of *functions* $f : A \to B$ you may have seen before (we will talk about functions specifically a bit later!), but also have important applications outside of mathematics: Relational databases, automated translation,...

Example 1.42

• $y = x^2$.	$x, y \in \mathbb{R}$.
• $S \subseteq T$.	$S, T \in P(\Omega)$.
• $5 \mid x - y$, *i.e.* $x \equiv y \mod 5$.	$x, y \in \mathbb{Z}$.
• x and y are siblings.	$x, y \in \{\text{humans}\}$.
• $x \leq y$.	$x, y \in \mathbb{R}$.
• $x \mid y$, *i.e.* y is divisible by x.	$x, y \in \mathbb{Z}$.

1.4.1 Definition and different types of relations

Definition 1.43

A *relation* can be defined in any of two different ways (which we will use interchangably):

- A relation on a set A is a subset $R \subseteq A \times A$.
- A relation is an open statement $R(x, y)$ that has a truth value for every $x, y \in A$.

Recall: To the *predicate* $R(x, y)$ corresponds the *set*

$$\{(x, y) \in A^2 : R(x, y)\}.$$

This set is sometimes also denoted R.

Example 1.44

- Let $A = \{1, 2, 3, 4\}$.
- The equality relation $x = y$ on A is given by the set

$$\{(1,1), (2,2), (3,3), (4,4)\} \subseteq A^2.$$

- The order relation $x < y$ on A is given by the set

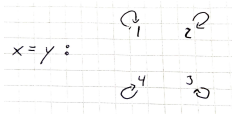
$$\{(1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\} \subseteq A^2.$$

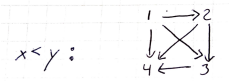
- The divisibility relation $x|y$ on A is given by the set

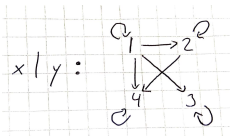
$$\{(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)\} \subseteq A^2.$$

A relation R on A can also be represented by a *directed graph*.

- *Nodes* corresponding to the elements $x \in A$.
- *Arcs* $x \to y$ if $R(x, y)$ holds.







Example 1.45

If

$$|A| = n,$$

how many relations are there on A? Recall a relation on a set A is a subset $R \subseteq A^2 = A \times A$.

Answer: $|P(A^2)| = 2^{|A \times A|} = 2^{|A| \cdot |A|} = 2^{n^2}$ different relations.

- We can also define a relation "from a set A to a set B":
  - As a subset $R \subseteq A \times B$.
  - As an open statement $R(x, y)$ that has a truth value for every $x \in A, y \in B$.

Example 1.46

- $x \in S$. $x \in \Omega$, $S \in P(\Omega)$.
- x has shoes in size y. $x \in \{\text{humans}\}$, $y \in \mathbb{R}$.
- x is born in year n. $x \in \{\text{humans}\}$, $n \in \mathbb{N}$.

Definition 1.47

A relation $\sim$ on A is called:

- *reflexive* if
$$\forall x \in A : x \sim x.$$
- *symmetric* if
$$\forall x, y \in A : x \sim y \leftrightarrow y \sim x.$$
- *antisymmeric* if
$$\forall x, y \in A : (x \sim y \wedge y \sim x) \rightarrow x = y.$$
- *transitive* if
$$\forall x, y, z \in A : (x \sim y \wedge y \sim z) \rightarrow x \sim z.$$

Example 1.48

- reflexive: $x \leq y$ on $\mathbb{R}$
- reflexive: $x|y$ on $\mathbb{Z}$
- reflexive: $x = y$ on any set
- reflexive: $x \equiv y \mod n$ on $\mathbb{Z}$
- NOT reflexive: $x < y$ on $\mathbb{R}$
- NOT reflexive: x is a father of y on $\{\text{humans}\}$

Example 1.49

- symmetric: x and y are siblings on $\{\text{humans}\}$
- symmetric: $|x - y| \leq 1$ on $\mathbb{R}$
- NOT symmetric: $x - y \leq 1$ on $\mathbb{R}$

Example 1.50

- antisymmeric: $x \leq y$ $x, y \in \mathbb{R}$
- antisymmeric: $S \subseteq T$ $S, T \in P(\Omega)$

Example 1.51

- transitive: $x - y \in \mathbb{Z}$ $x, y \in \mathbb{R}$
- transitive: $x \leq y$ $x, y \in \mathbb{R}$
- NOT transitive: x and y have a parent in common. $x, y \in \{\text{Humans}\}$.

1.4.2 Equivalence relations

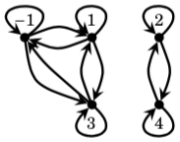
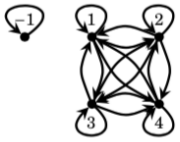
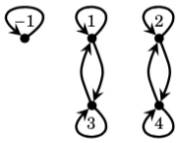
An equivalence relation usually describes "sameness" in some sense.

Definition 1.52

A relation $\sim$ is an *equivalence relation* if it is reflexive, symmetric, and transitive.

Example 1.53

- $x = y$ on any set.
- $x \equiv y \mod n$ $x, y \in \mathbb{Z}$.
- $x - y \in \mathbb{Z}$ $x, y \in \mathbb{R}$.
- $|S| = |T|$ $S, T \in P(\Omega)$.
- x and y have the same biological mother $x, y \in \{\text{Humans}\}$.
- NOT an equivalence relation: $x \leq y$ $x, y \in \mathbb{R}$.
- NOT an equivalence relation: $|x - y| \leq 1$. $x, y \in \mathbb{R}$.

Relation R	Diagram	Equivalence classes (see next page)
"is equal to" (=) $R_1 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4)\}$		$\{-1\}$, $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$
"has same parity as" $R_2 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4),$ $(-1,1),(1,-1),(-1,3),(3,-1),$ $(1,3),(3,1),(2,4),(4,2)\}$		$\{-1,1,3\}$, $\{2,4\}$
"has same sign as" $R_3 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4),$ $(1,2),(2,1),(1,3),(3,1),(1,4),(4,1),(3,4),$ $(4,3),(2,3),(3,2),(2,4),(4,2),(1,3),(3,1)\}$		$\{-1\}$, $\{1,2,3,4\}$
"has same parity and sign as" $R_4 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4),$ $(1,3),(3,1),(2,4),(4,2)\}$		$\{-1\}$, $\{1,3\}$, $\{2,4\}$

Every equivalence relation on A divides A into disjoint *equivalence classes* of elements that are "same".

Definition 1.54 (Equivalence classes)

- Let $\sim$ be an equivalence relation on A.
- The equivalence class of $a \in A$ is

$$[a] = [a]_\sim = \{x \in A : x \sim a\}.$$

Example 1.55

- Let $\sim$ be congruence modulo 2, on $\mathbb{Z}$.
- $x \equiv y$ if $2|x - y$.
- Then

$$[0] = \{\ldots, -4, -2, 0, 2, 4, \ldots\} \text{ and } [1] = \{\ldots, -3, -1, 1, 3, \ldots\}.$$

Theorem 1.56

- Let $\sim$ be an equivalence relation on A, and let $x, y \in A$.
- If $x \sim y$, then $[x] = [y]$.
- If $x \not\sim y$, then $[x] \cap [y] = \emptyset$.

This shows that the equivalence classes form a *partition* of A: Every element in A is in exactly one equivalence class.

Definition 1.57

A partition of a set A is a collection of subsets $A_i \subseteq A$, $i \in I$ such that:

- $A = \bigcup_{i \in I} A_i$.
- $A_i \cap A_j = \emptyset$ for all $i \neq j$.

How many equivalence relations are there on a set with n elements? This is the *Bell number* B_n. (outside the scope of this course). The first few Bell numbers are

$$B_0 = 1, B_1 = 1, B_2 = 2, B_3 = 5, B_4 = 15, B_5 = 52, B_6 = 203, B_7 = 877.$$

The numbers can be computed recursively in a *Bell triangle*. No "closed formula" known.

1.4.3 Partial orders

Remember that in real line, we can talk about some numbers being bigger than others, like $2 < 5$, $2 \leq 2$ or $3 < \pi < 4$. This idea can be introduced as a structure to sets as well, as a relation:

Definition 1.58 (Partial order)

A relation $\preceq$ on A is an *order relation* if it is reflexive, antisymmetric, and transitive.

Example 1.59

- $x \leq y$ on $\mathbb{R}$
- $x|y$ on $\mathbb{N}$
- $S \subseteq T$ on $P(\Omega)$.

An order relation is sometimes called a *partial order*. If $a \preceq b$ and $a \neq b$, then we write $a \prec b$.

Definition 1.60 (Covering relation)

- Let $\preceq$ be an order relation on A.
- Let $a, b \in A$ be elements such that:
  - $a \prec b$
  - $\neg\exists x \in A : a \prec x \prec b$.
- Then we say that b *covers* a, written $a \lessdot b$.

Example 1.61

- $18 \lessdot 19$ in the order $(\mathbb{Z}, \leq)$.
- $3 \lessdot 6$ in the order $(\mathbb{Z}, |)$.
- $\{a, b, c\} \lessdot \{a, b, c, d\}$ in the order $(P(\Omega), \subseteq)$.
- In the order $(\mathbb{R}, \leq)$, there are no covering pairs $a \lessdot b$.

Theorem 1.62

- Let $\preceq$ be an order relation on a *finite* set A, $a, b \in A$.
- $a \prec b$ if and only if there exist $a_1, a_2, \ldots, a_n \in A$ such that

$$a \lessdot a_1 \lessdot a_2 \lessdot \cdots \lessdot a_n \lessdot b.$$

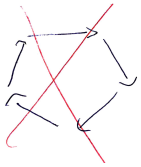
In other words, the order relation is uniquely defined if we know the corresponding covering relation. Note: This is not true if A is infinite.

1.4.4 Hasse diagram

So we can represent a finite order relation $(A, \preceq)$ as a directed graph where we only draw the arcs corresponding to covering pairs:

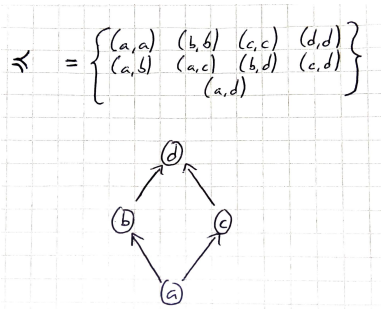
- Nodes are elements of A.
- Arc $a \to b$ if $a \lessdot b$.

Because of antisymmetry, this graph has no *directed cycles*:



When there are no directed cycles, we can draw the directed graph so that all arcs point upwards. This representation of a finite order relation is called its *Hasse diagram*.

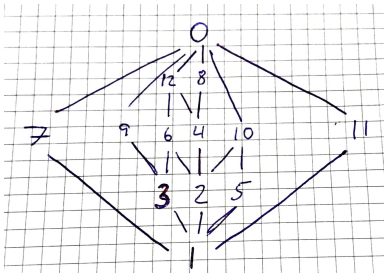
Example 1.63



The head of the arcs are usually not drawn in the Hasse diagram, as we already know that the arcs point upwards.

Example 1.64

The divisibility relation on $\{0, 1, 2, \ldots, 12\}$.



1.4.5 Linear extensions

Definition 1.65 (Linear relations and chains)

An order relation is called *linear*, or *total*, if for every x, y holds that $x \leq y$ or $y \leq x$. A totally ordered set is also called a *chain*.

Example 1.66

- The ordinary order relation $(\mathbb{N}, \leq)$ is linear, because for every two integers, if they are not the same, then one is smaller than the other.
- The divisibility relation $(\mathbb{N}, |)$ is not linear, because (for example) $5 \not| 7$ and $7 \not| 5$.

Definition 1.67 (Compatible linear relations)

A linear relation $\leq$ on a set P is *compatible* with a partial order $\preceq$ on the same set, if for every $x, y \in P$ such that $x \preceq y$, also holds that $x \leq y$. We say that $\leq$ is a *linear extension* of $\preceq$

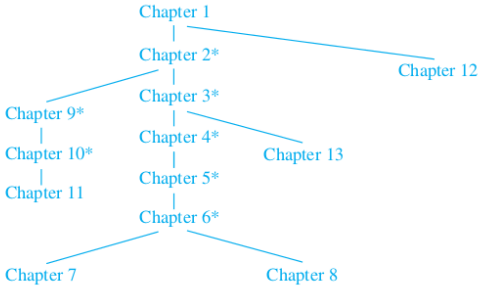
Example 1.68

- The ordinary order relation on $\{1, 2, 3, 4\}$ is a linear extension of the partial order
$$1 \preceq 2, 1 \preceq 3, 1 \preceq 4, 2 \preceq 4, 3 \preceq 4.$$
- Another linear extension of the same partially ordered set would be
$$1 \leq 3 \leq 2 \leq 4.$$

Example 1.69

- The ordinary order relation on $\mathbb{N} \setminus \{0\} = \{1, 2, 3, 4, \dots\}$ is a linear extension of the divisibility relation.
  - A positive integer can never be divisible by any larger integer
- The ordinary order relation on $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is **not** a linear extension of the divisibility relation.
- Zero is divisible by any positive integer n (because $0 = 0 \cdot n$), although $0 \leq n$.

A partial order $\preceq$ can describe the dependencies of tasks. (Task T $\preceq$ Task S if the outcome of S is needed in order to begin T.) Then, a linear extension of $\preceq$ is an order in which the tasks can be performed.



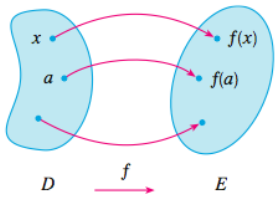
1.5 Functions

Functions are a special class of relations that describe a rule how an element is mapped into another element.

1.5.1 Definition and graphs

Definition 1.70 (Functions)

A *function* $f : A \to B$ is a relation "$f(x) = y$", such that for each element $a \in A$, there is a *unique* element $b \in B$ for which $f(a) = b$ holds.

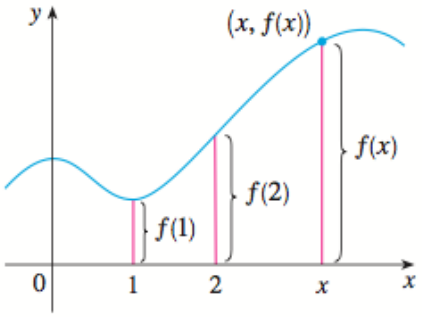


The set A is the *domain* of the function, and B is the *codomain*. The *range* of f is the set $f(A) \stackrel{\text{def}}{=} \{f(x) : x \in A\} \subseteq B$.

Functions can thus be seen as a special case of relations: Every element in the domain is related with some element in the codomain. A function f from A to B is compactly denoted $f : A \to B$. Sometimes a function does not need a name; in such case we write $a \mapsto b$ ("a maps to b") rather than $f(a) = b$. When considering a relation as a subset of $D \times E$, the set corresponding to f is its *graph*

$$\{(x, f(x)) : x \in D\} \subseteq D \times E.$$

A function is often represented geometrically by its graph, especially when the domain and codomain are both (subsets of) $\mathbb{R}$.



Example 1.71

The function

$$\begin{aligned} f :&\mathbb{Z} \to \mathbb{Z} \\ &x \mapsto 4x + 5 \end{aligned}$$

(also written $f(x) = 4x + 5$) has:

- Domain (*määrittelyjoukko*) $\mathbb{Z}$.
- Codomain (*maalijoukko*) $\mathbb{Z}$.
- Range (*arvojoukko*)

$$\{4x + 5 : x \in \mathbb{Z}\} = \{\dots, -7, -3, 1, 5, 9, \dots\}.$$

- Graph (*kuvaaja*)

$$\{(x, y) : y = 4x + 5\} \subseteq \mathbb{Z}^2.$$

1.5.2 Composition of functions

Two functions $f : A \to B$ and $g : B \to C$ can be *composed* into a function $g \circ f : A \to C$, $g \circ f(x) = g(f(x))$.

Example 1.72

The function $h(x) = 2^{x^2+1}$ can be written as $g \circ f$, where $g(y) = 2^y$ and $f(x) = x^2 + 1$.

Example 1.73

- The function $h(x) = 2^{x^2+1}$ can be written as $g \circ f$, where $g(y) = 2^y$ and $f(x) = x^2 + 1$.
- $$x \overset{f}{\longmapsto} x^2 + 1 \overset{g}{\longmapsto} 2^{x^2+1}.$$
- This is **not** the same as the composition $f \circ g$:
$$x \overset{g}{\longmapsto} 2^x \overset{g}{\longmapsto} (2^x)^2 + 1 = 4^x + 1.$$

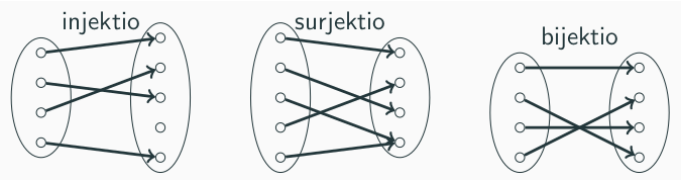
1.5.3 Injection, surjection, bijection

Next we will discuss three important notions of functions, which we will use later for example in checking whether two sets have same number of elements or not.

Definition 1.74

A function $f : A \to B$ is called

- *Injective* (or one-to-one) if
$$\forall x, y \in A : f(x) = f(y) \Rightarrow x = y.$$
- *Surjective* (or onto) if
$$\forall b \in B : \exists a \in A : f(a) = b.$$
- *Bijective* (or invertible) if it is injective and surjective.



injektio = injection, surjektio = surjection, bijektio = bijection

1.5.4 Inverse functions

Definition 1.75

The *inverse* of the bijective function $f : A \to B$ is the function $g = f^{-1} : B \to A$ such that

$$f(a) = b \iff g(b) = a.$$

This defines the inverse function f^{-1} uniquely. If $f : A \to B$ is not bijective, then it can not have an inverse $B \to A$. Warning: Do not mistake the *function* f^{-1} for the *number* $f(x)^{-1} = \frac{1}{f(x)}$.

1.6 Cardinalities

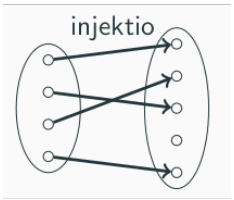
Next, we will apply the idea of injections, surjections and bijections to talk about *cardinalities* again and we can use them to formally define the cardinality of any set by using functions:

Theorem 1.76

Let A and B be finite sets. Then $A \to B$ injective $\Rightarrow n = |A| \leq |B|$.

Proof

If there is an injection $A = \{a_1, \ldots, a_n\} \to B$, then $f(a_1), \ldots, f(a_n)$ are all *different* elements of B.



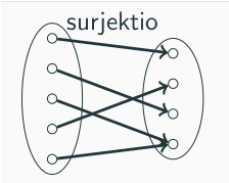
□

Theorem 1.77

Let A and B be finite sets. Then $A \to B$ surjective $|A| \geq |B| = m$.

Proof

If there is a surjection $A \to B = \{b_1, \ldots, b_m\}$, then there are *different* elements $a_1, \ldots a_m \in A$ such that $f(a_i) = b_i$ for $i = 1, \ldots, m$.



□

For finite sets, there is an injective map $A \to B$ precisely if B has at least as many elements as A. For general sets, we take this as the *definition* of cardinality (i.e. "number of elements")

Definition 1.78

Let A and B be sets. We say that:

- $|A| = |B|$ if there exists a bijection $A \to B$.
- $|A| \leq |B|$ if there exists an injection $A \to B$.

Fact (from exploratory exercises): There is a surjection $B \to A$ if and only if there is an injection $A \to B$. Assuming a technical axiom about sets, called the axiom of choice. Do not worry about this.

Definition 1.79 (Finite, countable and uncountable sets)

Note that $|A| = n$ if there is a bijection $A \to \{1, 2, \ldots, n\}$. The set A is *finite* if $|A| = n$ for some $n \in \mathbb{N}$. Otherwise it is *infinite*. For any infinite set A, there is an injection $\mathbb{N} \to A$. So $|\mathbb{N}| = \aleph_0$ is "the smallest infinite cardinality". The set A is *countable* if $|A| = |\mathbb{N}|$. If $|A| > |\mathbb{N}|$, then we say that A is *uncountable*.

Theorem 1.80

$|\mathbb{N}| = |\{0, 2, 4, 6, 8, \ldots\}|$

Proof

- Define $f : \mathbb{N} \to \{0, 2, 4, 6, 8, \ldots\}$ by $f(n) = 2n$ for all $n \in \mathbb{N}$.
- Then f is a bijection.
- Inverse function $m \mapsto \frac{m}{2} \in \mathbb{N}$ for $m \in \{0, 2, 4, 6, 8, \ldots\}$.

□

Note: for infinite sets A, B, it is very possible that $|A| = |B|$ even when $A \subsetneq B$.

1.6.1 Infinite cardinalities

Example 1.81 (Hilbert's hotel)

- David Hilbert is checking in to a hotel with infinitely many rooms (numbered $0, 1, 2, \dots$)
- Unfortunately, every room is already occupied.
- Solution: All guests move rooms: The guest who used to stay in room k moves to room $k + 1$ for all $i \in \mathbb{N}$.
- Now, Hilbert can move into room 0.

Example 1.82 (Hilbert's hotel, infinitely many new guests)

- The next day a bus arrives to the hotel, bringing infinitely (but countably) many new guests.
- Unfortunately, every room is already occupied.
- Solution: All guests move rooms: The guest who used to stay in room k moves to room $2k$ for all $i \in \mathbb{N}$.
- Now, the bus tourists can move into all odd numbered rooms.

Example 1.83 (Hilbert's hotel, infinite number of new buses!)

- The next day, **infinitely** many buses (numbered $1, 2, 3, \dots$) arrive to the hotel, all bringing infinitely (but countably) many new guests.
- Solution: All previous guests move to odd numbered rooms.
- Now, the passengers on bus number k can move into rooms numbered $2^k, 2^k \cdot 3, 2^k \cdot 5, 2^k \cdot 7, \dots$.

Theorem 1.84

The relation $|A| = |B|$ (between pairs of sets) is an equivalence relation (on $P(\Omega)$).

Proof

- Reflexivity: The identity map $\iota : A \to A$ is a bijection.
- Symmetry: If $f : A \to B$ is a bijection, then $f^{-1} : B \to A$ is a bijection.
- Transitivity: If $f : A \to B$ and $g : B \to C$ are bijections, then $g \circ f : A \to C$ is a bijection.

□

Theorem 1.85

- $|\mathbb{N}| = |\mathbb{Z}|$

Proof

- Define $f : \mathbb{N} \to \mathbb{Z}$ by

$$f(0) = 0, f(2k) = k \text{ and } f(2k-1) = -k \text{ for } k \geq 1.$$

- Then f is a bijection.

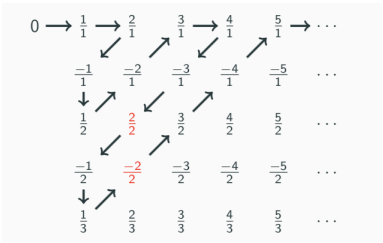
□

Theorem 1.86

- $|\mathbb{N}| = |\mathbb{Q}|$

Proof

- Order the numbers $\frac{p}{q}$, $p, q \in \mathbb{Z}$, $q > 0$, as in the figure:



- Let $f(n)$ be the n^{th} "new" number in the sequence, for $n \in \mathbb{N}$.
- Then $f : \mathbb{N} \to \mathbb{Q}$ is a bijection.

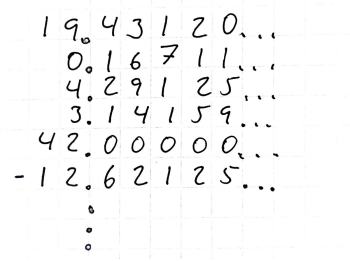
□

Theorem 1.87

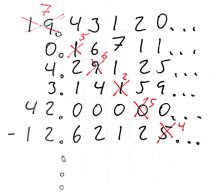
- $|\mathbb{N}| \neq |\mathbb{R}|$

Proof

- Assume for a contradiction that we can "list" the real numbers as in the figure



- Change the i^{th} decimal digit of the i^{th} number, in any way you want.



- The "diagonal number" (in the example $7.56254\ldots$) was not in the original list.
- Contradiction, so $|\mathbb{N}| \neq |\mathbb{R}|$.

□

Recall: $|A| \leq |B|$ if there exists an injection $A \to B$.

Theorem 1.88

- $|A| \leq |B| \leq |C| \implies |A| \leq |C|$.

Proof

- If $f : A \to B$ and $g : B \to C$ are injections, then $g \circ f : A \to C$ is an injection.

□

Theorem 1.89 (Not proved in this course)

- If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.
  - This is a nice and challenging problem - Try it at home!
- For any sets A and B holds that $|A| \leq |B|$ or $|B| \leq |A|$.
  - This is a deep fact, and not true in *constructive mathematics* - Do not try it at home!

Chapter 2

Combinatorics

2.1 Enumerative combinatorics

2.1.1 Principles of counting

We have already encountered some basic techniques to count the elements of a set. The *addition principle* says that, if $A_1, \ldots, A_k$ are pairwise disjoint, then

$$|A_1 \cup \cdots \cup A_k| = |A_1| + \cdots + |A_k|.$$

The *multiplication principle* says that

$$|A_1 \times \cdots \times A_k| = |A_1| \cdots |A_k|.$$

Recall that $|A| = m$ means (by definition) that there is a bijection $A \to \{1, 2, \ldots, m\}$. In this light, the addition and multiplication principles are (easy, but not trivial) *theorems*.

Example 2.1

- A bookshelf contains five physics books, seven chemistry books, and ten mathematics books. In how many ways can you choose two books about different subjects from the shelf?

Example 2.2

- Let P, C, M be the sets of physics, chemistry, and math books respectively. $|P| = 5$, $|C| = 7$, $|M| = 10$.
- A pair of two books about different subjects is an element of

$$(P \times C) \cup (P \times M) \cup (C \times M).$$

- The number of choices is

$$\begin{aligned} &|(P \times C) \cup (P \times M) \cup (C \times M)| \\ =&|P||C| + |P||M| + |C||M| \\ =&5 \cdot 7 + 5 \cdot 10 + 7 \cdot 10 \\ =&155. \end{aligned}$$

2.1.2 Counting linear orders

In how many ways can we order the letters a,b,c in a linear order?

- abc, acb, bac, bca, cab, cba.
- The first letter could be chosen in 3 ways.
- Regardless of the first letter, the second letter can be chosen in 2 ways, and after this, the third letter can be chosen in only one way. So the number of linear orders is $3 \cdot 2 \cdot 1 = 6$

In how many ways can we order n objects $a_1, a_2, \cdots, a_n$ in a linear order?

- The first object could be chosen in n ways.
- Regardless of the first i objects, the $(i+1)^{\text{th}}$ object can be chosen in $(n-i)$ ways, $0 \leq i \leq n-1$.
- So the number of linear orders is $n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$.

This number is denoted $n!$, read "n factorial". By convention, $0! = 1$ ("the empty product")

2.2 Binomial coefficients

2.2.1 Counting combinations

In how many ways can we select a committee of 5 members from a party of 11? Call this number

$$\binom{11}{5}$$

(read: "11 choose 5"). If we also order the committee members, and order the non-members, we would get 11! possible orders total.

- First committee member can be chosen in 11 ways, second committee member i 10 ways, ... , last committee member in 7 ways, first non-member in 6 ways, second non-member in 5 ways and so on.

Every committee can be ordered in 5! ways, and the non-members can be ordered in 6! ways. We get $\binom{11}{5} \cdot 5! \cdot 6! = 11!$, so

$$\binom{11}{5} = \frac{11!}{6! \cdot 5!} = 462.$$

We can generalize this: How many "combinations" (subsets) of k elements are there in a set B of n elements? This number is denoted $\binom{n}{k}$. (read: "n choose k"). The number of ways to select a set A with k elements and then order both A and $B \setminus A$ is

$$\binom{n}{k} \cdot k! \cdot (n-k)!,$$

but it is also $n!$ by the same argument as on the last slide. We get

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

Example 2.3

How many sequences of five cards (drawn from an ordinary 52 card deck) are there, if we know that it contains exactly two kings?

- The word "sequence" impies that the order matters, so ♣3,♡5,♢K,♣K,♡Q is a different sequence than ♡Q, ♡5,♢K,♣3,♣K

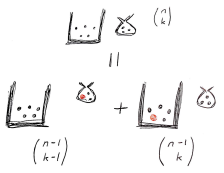
$$♣3, ♡5, ♢K, ♣K, ♡Q$$

The positions of the kings can be chosen in $\binom{5}{2}$ ways. The first king can be chosen in 4 ways, the second king in 3 ways. The first non-king can be chosen in 48 ways, the next in 47 ways, and the last in 46 ways. By the multiplication principle there are

$$\binom{5}{2} \cdot 4 \cdot 3 \cdot 48 \cdot 47 \cdot 46 = 12453120$$

possible sequences.

There are $\binom{n}{k}$ ways to choose k balls from a box containing n balls.



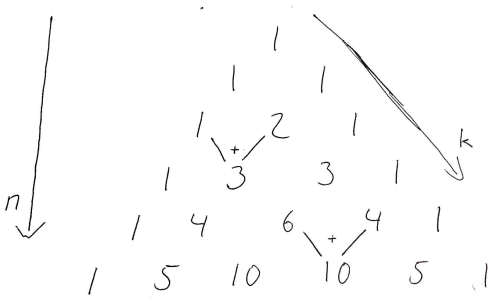
Refining according to whether or not our favourite (red) ball is chosen:

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

We can also prove the same identity "algebraically":

$$\begin{aligned}
\binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(n-k)!(k-1)!} + \frac{(n-1)!}{(n-1-k)!k!} \\
&= \frac{(n-1)!}{(n-1-k)!(k-1)!} \cdot \left[\frac{1}{n-k} + \frac{1}{k}\right] \\
&= \frac{(n-1)!}{(n-1-k)!(k-1)!} \cdot \frac{n}{(n-k)k} \\
&= \frac{n!}{(n-k)!k!} \\
&= \binom{n}{k}.
\end{aligned}$$

Clearly, $\binom{n}{0} = \binom{n}{n} = 1$. So the *binomial coefficients* $\binom{n}{k}$ are the entries in the recursively defined *Pascal's triangle:*



Recall that, if $|A| = n$, then $|P(A)| = 2^n$. Order $A = \{a_1, a_2, \ldots, a_n\}$. $\{0,1\}^n = \{0,1\} \times \cdots \times \{0,1\}$ is the set of length n bitstrings. Define $f : P(A) \to \{0,1\}^n$ by $f(S) = (f_1, \ldots, f_n)$, where

$$f_i = \begin{cases} 1 & \text{if } a_i \in S \\ 0 & \text{if } a_i \notin S \end{cases}$$

f is a bijection, so

$$|P(A)| = |\{0,1\}^n| = |\{0,1\}|^n = 2^n.$$

On the other hand, if $|A| = n$, then $P(A) = P_0 \cup P_1 \cup \cdots \cup P_n$, where

$$P_k = \{S \subseteq A : |S| = k\}.$$

$|P_k| = \binom{n}{k}$, so

$$2^n = |P(A)| = \sum_{k=0}^{n} |P_k| = \sum_{k=0}^{n} \binom{n}{k}.$$

2.2.2 Counting combinations with repetition

Example 2.4

A box contains (many) blue, red and green balls. In how many ways can I select 5 balls from this box, if the order does not matter? So ●●●●● is the same selection as ●●●●●.

Solution: Represent any selection by always lining up the balls blue first, then red, then green.

●●●●●　　●●●●●　　●●●●●

If we separate the different colours by bars, then we can reconstruct the colours from the position of the bars. The three selections above are now represented as

●●●|●|●　　●●||●●●　　|●●●●●|

A selection is given by placing bars in two out of 7 positions in a sequence, and placing balls in the other 5 positions. So there are $\binom{7}{2}$ different selections.

More generally, assume we have n different kinds of balls, and want to select k from these. Like in the previous example, this can be represented by a configuration of k balls and $n-1$ bars ordered in a sequence. So there are

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

different ways to select.

Note: This is also the number of non-negative integer solutions to the equation

$$x_1 + \cdots + x_n = k,$$

where x_i represents the number of balls of the i^{th} kind.

2.2.3 Binomial theorem

Theorem 2.5 (Binomial theorem)

For all $n \in \mathbb{N}$ and all $x, y \in \mathbb{R}$ holds

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Proof

[Combinatorial proof] Expand the product $(x+y)^n$ into a sum of 2^n monomial terms. Each

term corresponds to a way to select either x or y from each of the n parentheses. The monomial term $x^k y^{n-k}$ corresponds to selecting x from k of the parentheses, and y from $n-k$ of the parentheses. This can be done in $\binom{n}{k} = \binom{n}{n-k}$ ways. □

Proof
[Induction proof]

- Base case $n = 0$:
$$(x+y)^0 = 1 = \binom{0}{0} x^0 y^{0-0}.$$
- Base case $n = 1$:
$$(x+y)^1 = x + y = \sum_{k=0}^{1} \binom{1}{k} x^k y^{1-k}.$$
- Induction step: Assume true for $n = M$. Then

$$\begin{aligned}
(x+y)^{M+1} &= (x+y)(x+y)^M \\
&\overset{\text{IH}}{=} (x+y) \sum_{k=0}^{M} \binom{M}{k} x^k y^{M-k} \\
&= \sum_{j=0}^{M} \binom{M}{j} x^{j+1} y^{M-j} + \sum_{k=0}^{M} \binom{M}{k} x^k y^{M-k+1} \\
&= \sum_{k=1}^{M+1} \binom{M}{k-1} x^k y^{M-(k-1)} + \sum_{k=0}^{M} \binom{M}{k} x^k y^{M-(k-1)}
\end{aligned}$$

$$\begin{aligned}
&= x^{M+1} + \sum_{k=1}^{M} \left(\binom{M}{k-1} + \binom{M}{k} \right) x^k y^{M+1-k} + y^{M+1} \\
&= x^{M+1} + \sum_{k=1}^{M} \binom{M+1}{k} x^k y^{M+1-k} + y^{M+1} \\
&= \sum_{k=0}^{M+1} \binom{M+1}{k} x^k y^{M+1-k}.
\end{aligned}$$

By the induction principle,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \text{ for all } n \in \mathbb{N}.$$

□

Example 2.6

- This shows in a new way that

$$2^n = (1+1)^n = \sum_k \binom{n}{k} 1^k 1^{n-k} = \sum_k \binom{n}{k}.$$

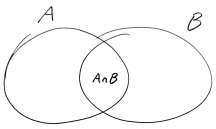
- Similarily,

$$3^n = (2+1)^n = \sum_k \binom{n}{k} 2^k 1^{n-k} = \sum_k 2^k \binom{n}{k}.$$

2.3 Inclusion exclusion principle

The inclusion exclusion principle for two sets says the following:

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



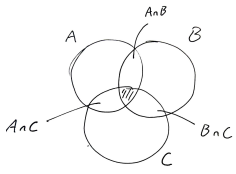
Example 2.7

How many 8 bit strings start or end with two zeroes?

Answer: $2^6 + 2^6 - 2^4 = 112$.

The inclusion exclusion principle for three sets:

$$\begin{aligned} |A \cup B \cup C| = \quad & |A| + |B| + |C| \\ & - |A \cap B| - |A \cap C| - |B \cap C| \\ & + |A \cap B \cap C|. \end{aligned}$$



Example 2.8

A martial arts club has courses in aikido, boxing and capoeira. There are 30 aikido students, 25 boxers and 35 capoeira dancers. 5 people do both aikido and boxing, 19 do both aikido and capoeira, and 7 boxers also do capoeira. One student (Chuck Norris) studies all martial arts at once. How many martial artists does the club have?

Solution. Let A, B and C be the sets of students of the respective martial arts.

- $|A| = 30$, $B = 25$, $|C| = 35$.
- $|A \cap B| = 5$, $|A \cap C| = 19$, $|B \cap C| = 7$
- $|A \cap B \cap C| = |\{\text{Chuck Norris}\}| = 1$

The total number of martial artists is

$$\begin{aligned} |A \cup B \cup C| = & \quad |A| + |B| + |C| \\ & - |A \cap B| - |A \cap C| - |B \cap C| \\ & + |A \cap B \cap C| \\ = & \quad 30 + 25 + 35 - 5 - 19 - 7 + 1 \\ = & \quad 60. \end{aligned}$$

Example 2.9

How many permutations a_1a_2, a_3, a_4 of the set $\{1, 2, 3, 4\}$ are such that $a_{i+1} \neq a_i + 1$ for all $i \in \{1, 2, 3\}$?

In other words, the string a_1a_2, a_3, a_4 must not contain "12", "23", or "34". For example, the permutation 1432 satisfies the property, but the permutation 1423 does not. A permutation containing "12" can be thought of as a permutation of $\{`12', 3, 4\}$. There are $3! = 6$ such permutations. Similarily, there are $3! = 6$ permutations that contain "23", and $3! = 6$ permutations that contain "34". Permutations that contain both "12" and "23" correspond to permutations of $\{`123', 4\}$. There are $2! = 2$, such permuations, namely 1234 and 4123. Similarily, there are 2 permutations that contain both "23" and "34", and 2 permutations that contain both "12" and "34". The only permutations that contains all the "forbidden pairs" is 1234. So there are

$$4! - 3 * 3! + 3 * 2! - 1 = 24 - 18 + 6 - 1 = 7$$

permutations with the desired property.

In the three set case, denote

- $s_1 = |A_1| + |A_2| + |A_3|$
  "count elements that are in one of the sets, one set at a time".

- $s_2 = |A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|$
  "count elements that are in two sets, one pair of sets at a time".
- $s_3 = |A_1 \cap A_2 \cap A_3|$
  "count elements that are in three sets, (one triple of sets at a time)".

Then the inclusion exclusion principle says

$$|A_1 \cup A_2 \cup A_3| = s_1 - s_2 + s_3 = \sum_{k=1}^{3} (-1)^{k-1} s_k.$$

For a collection of finite sets $A_1, \ldots, A_n$, let

$$s_k = \sum_{|B|=k} \left| \bigcap_{i \in B} A_i \right|,$$

where the sums are taken over subsets of $\{1, \ldots, n\}$.

Theorem 2.10

If $A_1, \ldots, A_n$ are finite sets, and $s_1, \ldots, s_k$ are as above, then

$$|A_1 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k-1} s_k.$$

Proof
Let $x \in A_1 \cup \cdots \cup A_n$, and let

$$I_x = \{i : x \in A_i\} \subseteq \{1, \ldots, n\}$$

be the indices of the sets containing x. Let $m = |I_x|$. Then x belongs to the set $\bigcap_{i \in B} A_i$ if and only if $B \subseteq I_x$. So on the right hand side, x is counted

$$\begin{aligned} \sum_{k=1}^{m} \binom{m}{k} (-1)^{k-1} &= -\sum_{k=1}^{m} \binom{m}{k} (-1)^{k} \\ &= 1 - \sum_{k=0}^{m} \binom{m}{k} (-1)^{k-1} \\ &= 1 - (1-1)^m = 1 \text{ times.} \end{aligned}$$

Hence each element $x \in A_1 \cup \cdots \cup A_n$ is counted exactly once on each side of the equation

$$|A_1 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k-1} s_k.$$

□

Example 2.11 (Counting surjections)

In how many ways can n balls be placed in m bins, so that no bin is left empty? In other words, how many maps

$$X \to \{1, \ldots, m\}$$

are surjective, if $|X| = n$?
Solution: For $i = 1, \ldots, m$, let A_i be the set of maps

$$\varphi : X \to \{1, \ldots, m\}$$

that "miss i", i.e. $\varphi(x) \neq i$ for all $x \in X$. Then $A_{i_1} \cap \cdots \cap A_{i_k}$ is the set of maps

$$X \to \{1, \ldots, m\} \setminus \{i_1, \ldots, i_k\}.$$

We have

$$|A_{i_1} \cap \cdots \cap A_{i_k}| = (m-k)^n.$$

and

$$s_k = \sum_{|B|=k} \left| \bigcap_{i \in B} A_i \right| = \binom{m}{k} (m-k)^n.$$

The number of maps $X \to \{1, \ldots, m\}$ is m^n. The number of non-surjections is

$$\begin{aligned} |A_1 \cup \cdots \cup A_m| &= \sum_{k=1}^{m} (-1)^{k-1} s_k \\ &= \sum_{k=1}^{m} (-1)^{k-1} \binom{m}{k} (m-k)^n. \end{aligned}$$

So the number of surjections is

$$\begin{aligned} S(n,m) &= m^n - \sum_{k=1}^{m} (-1)^{k-1} \binom{m}{k} (m-k)^n \\ &= \sum_{k=0}^{m} (-1)^k \binom{m}{k} (m-k)^n. \end{aligned}$$

Example 2.12

A secret Santa has brought 6 gifts to a christmas party with 4 guests. In how many ways can the gifts be distributed, so that all guests get at least one gift?
Solution: This is the number of surjections from the set of gifts to to the set of guests. The number of such maps is the *Stirling number*

$$\begin{aligned} S(6,4) &= \sum_{k=0}^{4} (-1)^k \binom{4}{k} (4-k)^6 \\ &= 4^6 - 4 \cdot 3^6 + 6 \cdot 2^6 - 4 \cdot 1^6 \\ &= 1560. \end{aligned}$$

The number of surjective maps $\{1,2,3,4,5,6\} \to \{1,2,3,4\}$ is the *Stirling number*

$$S(6,4) = 1560 = 24 \cdot 65.$$

Is it a coincidence that $S(6,4)$ is divisible by $4! = 24$? To put 6 balls in 4 bins so that no bin is left empty, we can first divide them into 4 non-empty piles (in $P(6,4) = 65$ of ways). Then we can pair up the 4 piles with the 4 bins in $24 = 4!$ ways. In general,

$$S(n,m) = m!P(n,m),$$

where $P(n,m)$ is the number of partitions of an n-element set into m parts.

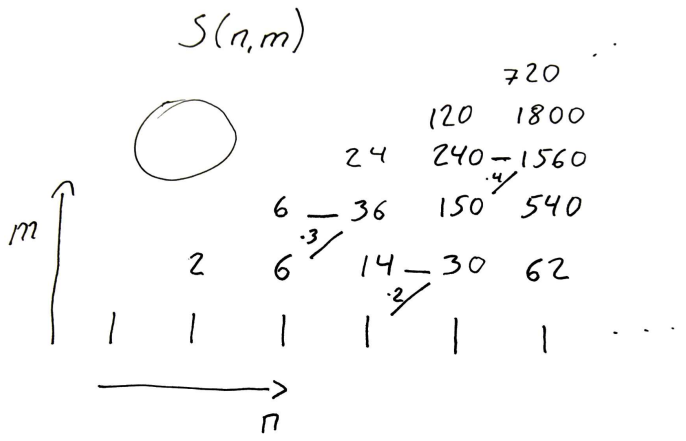
No "good" closed formula is known for

$$S(n,m) = \sum_{k=0}^{m} (-1)^k \binom{m}{k} (m-k)^n.$$

But $S(n,m)$ can also be computed recursively in a "triangle", like the binomial coefficients.

In how many ways can n balls be placed in m bins, so that no bin is left empty? Our favourite ball $\star$ can be placed in any of m different bins. The n other balls are either placed surjectively into all m bins, or surjectively into the $m-1$ bins not containing $\star$. So $S(n,m)$ can be computed recursively by.

$$\begin{aligned} S(n,m) &= 0 && n < m. \\ S(n,1) &= 1 && n \geq 1. \\ S(n+1,m) &= m\left(S(n,m) + S(n,m-1)\right) && n \geq m \geq 2. \end{aligned}$$



2.4 Permutations and group theory

2.4.1 Permutation group

Definition 2.13

A bijection $\pi : A \to A$ from a set to itself is called a *permutation*.

Example 2.14

- Let $\pi : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ be defined by:

$$\pi_1 = 3, \pi_2 = 2, \pi_3 = 4, \pi_4 = 1.$$

- In *two line notation* this is denoted:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 1 & 3 & 2 \\ 1 & 3 & 4 & 2 \end{pmatrix} = \cdots .$$

As a permutation is a bijection, it also has an inverse. In the two line notation, the inverse of a permutation is obtained by changing the place of the first and second row (and reordering the columns according to the first row).

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}.$$

$$\pi^{-1} = \begin{pmatrix} 3 & 2 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}.$$

Permutations can be composed as functions. Let

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix},$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

The two line notation of the permutation $\sigma \circ \pi$ is computed as follows:

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

The first two rows are aligned according to π; The last two rows according to σ.

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

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

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

Thus **"Multiplication"** $\pi\sigma = \pi \circ \sigma$ of permutations is **not** commutative ($\pi\sigma \neq \sigma\pi$).

Permutations form also an algebraic structure called a **group** as we will see now. The set of permutations of $\{1, 2, \ldots n\}$ is denoted S_n. Note: $|S_n| = n!$.

- The *identity permutation*
$$\iota = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$
is such that $\iota\pi = \pi\iota = \pi$ holds for all $\pi \in S_n$.

- *associativity:*
$$\pi^{-1}\pi = \pi\pi^{-1} = \iota.$$
$$(\pi\sigma)\tau = \pi(\sigma\tau)$$
holds for all $\pi, \sigma, \tau \in S_n$

We often write $\pi \in S_n$ using *one line notation* (without parentheses):

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi_1 & \pi_2 & \cdots & \pi_n \end{pmatrix} = \pi_1\pi_2\cdots\pi_n$$

Definition 2.15 (Group)

Let G be a set, and $\cdot : G \times G \to G$. The pair $(G, \cdot)$ is called a *group*, if the following holds:

- Associativity:
$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \text{ for all } a, b, c \in G.$$
- Neutral element: There exists $e \in G$ such that $e \cdot a = a \cdot e = a$ for all $a \in G$.
- Inverse: For every $a \in G$, there exists $a^{-1} \in G$ such that
$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$

The *permutation group* (or symmetric group) $(S_n, \circ)$ is a group, whose neutral element is the identity permutation ι.

2.4.2 Cycle notation

Permutations can be represented by **cycle notation**. Consider

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 1 & 3 & 5 & 7 & 6 \end{pmatrix}.$$

Here, $1 \mapsto 2 \mapsto 4 \mapsto 3 \mapsto 1$. This is a *cycle*, which is denoted (1243). Because $\alpha_5 = 5$, there is also a cycle (5). Finally, $6 \mapsto 7 \mapsto 6$, so there is a cycle (67) .On cycle notation we get

$$\alpha = (1243)(67) = (4312)(76) = (5)(1243)(67) = \cdots$$

The inverse of a cyclic permutation is easy to compute:

$$(a_1 \cdots a_k)^{-1} = (a_k \cdots a_1).$$

In any group it holds that

$$(\pi \cdot \sigma)^{-1} = \sigma^{-1}\pi^{-1}.$$

So for example, when

$$\pi = (145)(27)(3698),$$

we can compute

$$\pi^{-1} = (8963)(72)(541) = (154)(27)(3896).$$

Example 2.16

All permutations in S_3 can be represented by a single cycle (together with some trivial cycles):

$$\begin{aligned} 123 &= (1)(2)(3) = \iota \\ 132 &= (1)(23) = (23) \\ 213 &= (12)(3) = (12) \\ 231 &= (123) \\ 312 &= (132) \\ 321 &= (13)(2) = (13) \end{aligned}$$

All permutations in S_n can be written as a product of *disjoint* cycles. If $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_\ell)$ are disjoint, then

$$(a_1, \ldots, a_k)(b_1, \ldots, b_\ell) = (b_1, \ldots, b_\ell)(a_1, \ldots, a_k)$$

Example 2.17

The permutations in S_4 are:

ι							
(12)	(13)	(14)	(23)	(24)	(34)		
(123)	(132)	(124)	(142)	(134)	(143)	(234)	(243)
(12)(34)	(13)(24)	(14)(23)					
(1234)	(1243)	(1324)	(1342)	(1423)	(1432)		

2.4.3 Conjugates

In any group G, two elements $\pi, \sigma \in G$ are *conjugates* if $\pi = \tau\sigma\tau^{-1}$ for some $\tau \in G$. The conjugate relation is an equivalence relation

Example 2.18

(1234) and (1243) are conjugates in S_4, because

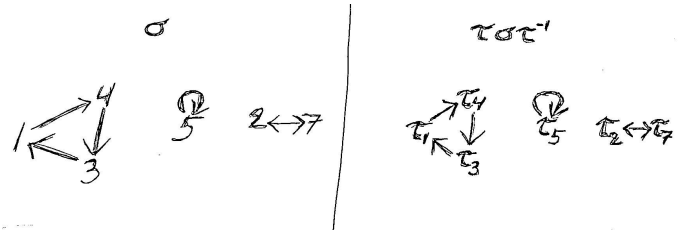
$$(1234) = (123)(1243)(132) = (123)(1243)(123)^{-1}.$$

If $\tau \in S_n$ is a permutation and $(a_1, \ldots, a_k)$ is a cycle, then

$$\tau(a_1 \ \ldots \ a_k)\tau^{-1} = (\tau(a_1) \ \cdots \ \tau(a_k)).$$

If π and σ are conjugates, then they have the same number of cycles of length k. In the symmetric group S_n, the conjugate relation can thus be equivalently defined as follows: $\pi, \sigma \in S_n$ are conjugates, if and only if they have equally many k-cycles for each $k = 1, \ldots, n$.

The conjugates σ and $\tau\sigma\tau^{-1}$ in S_n have "the same structure", but the elements of the ground set $\{1, \ldots n\}$ are in different places in the cycles.



Example 2.19

The elements of S_4 are:

ι							
(12)	(13)	(14)	(23)	(24)	(34)		
(123)	(132)	(124)	(142)	(134)	(143)	(234)	(243)
(12)(34)	(13)(24)	(14)(23)					
(1234)	(1243)	(1324)	(1342)	(1423)	(1432)		

The conjugate classes are the rows of this table. The group S_4 has five conjugate classes. How many conjugate classes does S_n have? There is no known closed formula (in terms of n).

A cycle (ab) of length 2 is called a *transposition*.

Theorem 2.20

Every permutation $\pi \in S_n$ can be written as the product of transpositions.

Proof
It is enough to show that every cycle $(a_1 \ldots a_k)$ is the product of transpositions.

$$(a_1 a_2 \ldots, a_{k-1} a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_3)(a_1 a_2).$$

□

The same permutation can be written as a product of transpositions in many different ways.

Example 2.21

$$(1234) = (12)(23)(34) = (14)(13)(12) = (12)(24)(23) = \ldots.$$

Theorem 2.22

1. Every permutation $\pi \in S_n$ can be written as a product using the transpositions $(1\ 2), (1\ 3), \ldots, (1\ n)$.
2. Every permutation $\pi \in S_n$ can be written as a product using the transpositions $(1\ 2), (2\ 3), \ldots, (n-1\ n)$.

Proof
It is enough to write every *transposition* as such a product. $(k\ \ell) = (1\ k)(1\ \ell)(1\ k)$. This proves 1.

$$(1\ k) = (k-1\ k)(k-2\ k-1)\cdots(2\ 3)(1\ 2)(2\ 3)\cdots(k-2\ k-1)(k-1\ k).$$

This proves 2. □

2.4.4 Even and odd permutations

Theorem 2.23

For a permutation $\pi \in S_n$, its representations as a product of transpositions either all use an even number of transpositions, or they all use an odd number of transpositions.

If $\pi \in S_n$ is the product of an even number transpositions, then we say that π is an *even* permutation, and that it has *sign* $\epsilon(\pi) = +1$. If $\pi \in S_n$ is the product of an odd number of transpositions, then we say that π is an *odd* permutation, and that it has *sign* $\epsilon(\pi) = -1$.

Example 2.24

A transposition

$$(j\ k) = (1\ j)(1\ k)(1\ j) = (1\ 3)(3\ j)(1\ 3)(1\ 2)(2\ k)(1\ 2)(1\ j) = \cdots$$

is odd. The identity permutation $\iota = (j\ k)(j\ k)$ is even. The set of even permutations is denoted A_n.

Example 2.25

- A cycle
$$(a_1, a_2, \ldots, a_{k-1}a_k) = (a_1a_k)(a_1a_{k-1}) \cdots (a_1a_3)(a_1a_2)$$
is even if its length k is odd, and it is odd if its length is even. (ANNOYING!)
- $\epsilon(\sigma\pi) = \epsilon(\sigma)\epsilon(\pi)$
  - even $\cdot$ even $=$ odd $\cdot$ odd $=$ even.
  - even $\cdot$ odd $=$ odd $\cdot$ even $=$ odd.
- So compositions of permutations is a map
$$A_n \times A_n \to A_n,$$
and so the even permutations form a *subgroup* $A_n \subseteq S_n$. (the alternating group).

Theorem 2.26

For a permutation $\pi \in S_n$, its representations as a product of transpositions either all use an even number of transpositions, or they all use an odd number of transpositions.

For the proof, we need the following definition:

Definition 2.27

- An *inversion* in $\pi \in S_n$ is a pair $i < j$ such that $\pi_i > \pi_j$.
- $\operatorname{inv}\pi$ is the number of inversions in $\pi \in S_n$.

Example 2.28

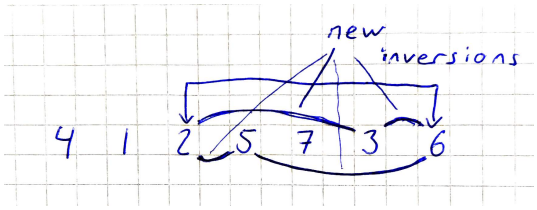
The inversions in $13542 \in S_5$ are $(2,5)$, $(3,4)$, $(3,5)$, $(4,5)$.

$$13542 \qquad 13542 \qquad 13542 \qquad 13542$$

Lemma 2.29

Let $\omega = (a\ b) \in S_n$ be a transposition, with $a < b$. Then $\operatorname{inv}\pi \circ \omega - \operatorname{inv}\pi$ is odd.

Proof



If $i, j \notin \{a, b\}$, then $(i\ j)$ is an inversion in π if and only if it is an inversion in $\pi\omega$. If $a < i < b$ and either $\pi_i \leq \min(\pi_a, \pi_b)$ or $\pi_i \geq \max(\pi_a, \pi_b)$, then exactly one of the pairs (a, i) and (i, b) is an inversion, both in π and in $\pi\omega$. Let $a < i < b$ and

$$\min(\pi_a, \pi_b) \leq \pi_i \leq \max(\pi_a, \pi_b).$$

Then the pairs (a, i) and (i, b) are both inversions in one of the permutations (either in π or in $\pi\omega$), and in the other one neither of them is an inversion. So the difference between the numbers of inversions

$$\begin{aligned} &|\{(i,j) : (i,j) \text{ inversion in } \pi \text{ but not in } \omega\pi, (i,j) \neq (a,b)\}| \\ -&|\{(i,j) : (i,j) \text{ inversion in } \omega\pi \text{ but not in } \pi, (i,j) \neq (a,b)\}| \end{aligned}$$

is even. (a, b) is an inversion in either π or $\pi\omega$, and not in the other. □

Lemma 2.30

$\operatorname{inv} \pi \circ \omega - \operatorname{inv} \pi$ is an odd number if ω is a transposition

Theorem 2.31

For a permutation $\pi \in S_n$, its representations as a product of transpositions either all use an even number of transpositions, or they all use an odd number of transpositions.

By the lemma, if π is the product of an odd (even)number of transpositions, then $\operatorname{inv} \pi$ is odd (even). But the number of inversions is well defined. So the parity of the permutation is also well defined.

2.4.5 Fixed points of permutations

Example 2.32

Each of n guests have brought gifts to a party, and these guests should be redistributed among the guests. Let $r(x)$ be the guest that gets the gift brought by x. We want

$$r : \{\text{Guests}\} \to \{\text{Guests}\}$$

to be surjectve (everyone should get a gift). We want $r(x) \neq x$ for all x (nobody should get back the same gift that they brought to the party). In how many ways can we redistribute the gifts with these rules?

Recall that a permutation is a bijection $X \to X$. The set of permutations of $X = \{1, \ldots, n\}$ is the *symmetric group* S_n. A *fixed point* of $\pi \in S_n$ is an element $x \in X$ such that $\pi(x) = x$. A permutation that has no fixed points is called a *derangement*. How many derangements are there in S_n?

Use the inclusion exclusion principle. For $i \in X$, let $A_i = \{\pi \in S_n : \pi(i) = i\}$. The number of permutations with k prescribed fixed points is

$$|A_{i_1} \cap \cdots \cap A_{i_k}| = (n-k)!,$$

because the $n-k$ other elements must be permuted internally. For $k = 1, \ldots, n$,

$$s_k = \sum_{|B|=k} \left| \bigcap_{i \in B} A_i \right| = \binom{n}{k} (n-k)! = \frac{n!}{k!}.$$

The number of non-derangements is

$$\begin{aligned} |A_i \cup \cdots \cup A_n| &= \sum_{k=1}^{n} (-1)^{k-1} s_k \\ &= \sum_{k=1}^{n} (-1)^{k-1} \frac{n!}{k!} \end{aligned}$$

So the number of derangements is

$$\begin{aligned} n! - |A_i \cup \cdots \cup A_n| &= \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} \\ &= n! \sum_{k=0}^{n} (-1)^k \frac{1}{k!} \end{aligned}$$

Fact from Calculus 1:

$$\sum_{k=0}^{\infty} t^k \frac{1}{k!} = \mathrm{e}^t.$$

So the number of derangements of n elements is

$$D_n = n! \sum_{k=0}^{n} (-1)^k \frac{1}{k!} = n! \mathrm{e}^{-1} - \sum_{k=n+1}^{\infty} (-1)^k \frac{n!}{k!}.$$

$$\left| D_n - \frac{n!}{\mathrm{e}} \right| = \left| \sum_{k=n+1}^{\infty} (-1)^k \frac{n!}{k!} \right| \leq \frac{n!}{(n+1)!} = \frac{1}{n+1} < \frac{1}{2}$$

So D_n is the closest integer to $n!/\mathrm{e}$.

Example 2.33

Each of n guests have brought gifts to a party, and put them in a pile on a table. Secret Santa comes and gives a (uniformly) random gift from the table to each guest. The probability that no guest gets her own gift back is (very very close to)

$$1/\mathrm{e} \approx 0.368$$

regardless of the number of guests!

Chapter 3

Graph theory

3.1 Basics on graphs

3.1.1 Motivation

"...networks may be used to model a huge array of phenomena across all scientific and social disciplines. Examples include the World Wide Web, citation networks, social networks (e.g., Facebook), recommendation networks (e.g., Netflix), gene regulatory networks, neural connectivity networks, oscillator networks, sports playoff networks, road and traffic networks, chemical networks, economic networks, epidemiological networks, game theory, geospatial networks, metabolic networks, protein networks and food webs, to name a few."

(Grady & Polimeni, Discrete Calculus, Springer 2010.)

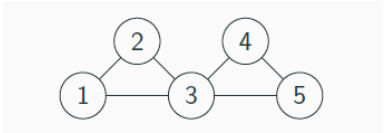
3.1.2 Graph

Definition 3.1

- A *graph* is a pair (V, E)
  - V is a set of *nodes* (or vertices, or points)
  - $E \subseteq \{\{u, v\} : u, v \in V\}$ is the set of *edges* (or links, or arcs).
  - Each edge is a "connection" between two nodes.
- A graph defined like this is *undirected*. One can also define directed graphs, whose edges are *ordered pairs* $(u, v) \in V^2$.
- If $u \neq v$ for each edge $\{u, v\} \in E$, then the graph is *simple*.

Example 3.2

If $V = \{1, 2, 3, 4, 5\}$ and $E = \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{3, 4\}, \{3, 5\}, \{4, 5\}\}$, then

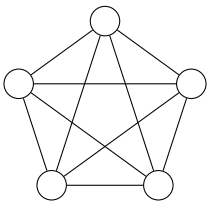


3.1.3 Complete graphs

A simple undirected graph with an edge $\{uv\}$ for every $u, v \in V$, $u \neq v$ called *complete*, or a *clique*. If it has $|V| = n$ nodes, it is denoted K_n. An edge in K_n is the same as a two element subset of V. So K_n has

$$\binom{n}{2} = \frac{n(n-1)}{2}$$

edges.

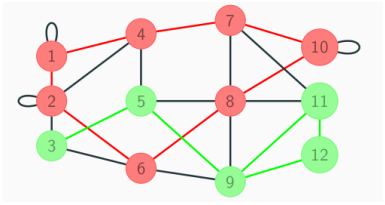


3.1.4 Paths and cycles

A *path* of length n in $G = (V, E)$ is a sequence $(v_0, v_1, \ldots, v_n)$ of nodes $v_i \in V$ where $\{v_{i-1}, v_i\}$ is an edge for every $i = 1, \ldots, n$. A *cycle* of length n in G is a path $(v_0, v_1, \ldots, v_n)$ where $v_0 = v_n$. The cycle is *simple* if $n \geq 3$ and $v_j \neq v_k$ for $1 \leq j < j \leq n$.

Note: This terminology is not entirely standard. Always check the definitions in the source before you cite any theorem about paths and cycles.

Example 3.3



- $(3, 5, 9, 11, 12, 9)$ is a (green) path.
- $(1, 4, 7, 10, 8, 6, 2, 1)$ is a (red) simple cycle.

3.1.5 Degree

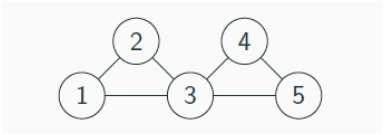
The *degree* $d(v)$ of a node v is the number of edges that have v as one of their endpoints.

Example 3.4

- In the graph below,

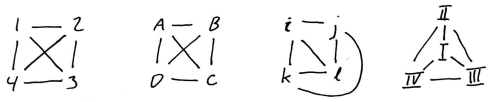
$$d(1) = d(2) = d(4) = d(5) = 2,$$

$$d(3) = 4.$$



3.1.6 Isomorphism

When are two graphs "the same"?



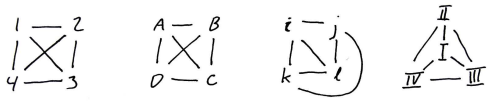
The four graphs above look different, still they are all "complete on 4 vertices", and share the "same structure". The following definition describes "sameness" of graphs.

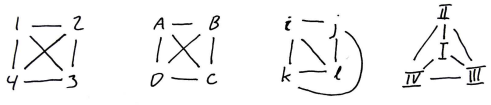
An isomorphism is a bijection between two sets, that preserve some "structure" on the set. For example graph structure, or group structure.

Definition 3.5

The graphs $G = (V, E)$ and $G' = (V', E')$ are *isomorphic*, if there is a bijection *(isomorphism)* $f : V \to V'$ such that

$$\{u, v\} \in E \iff \{f(u), f(v)\} \in E'.$$



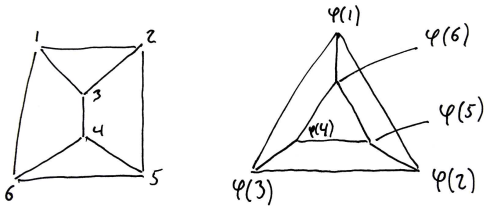


Isomorphic graphs are "the same, except for their representation".

- The number of nodes is the same.
- The number of edges is the same.
- The degrees of the nodes are the same.
- The lengths of the cycles are the same.
- The sizes of the complete subgraphs are the same.
- ...

Example 3.6

- All complete graphs on n nodes are isomorphic.
- The graphs below are isomorphic. An isomorphism is for example φ.



3.2 Adjacency matrix

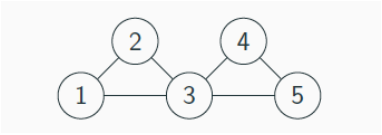
Let $G = (V, E)$ be a graph, and $V = \{v_1, \ldots, v_n\}$. The *adjacency matrix* of G is the $n \times n$ matrix A with

$$A(j,k) = \begin{cases} 1 & \text{if } \{v_j, v_k\} \in E \\ 0 & \text{otherwise} \end{cases}$$

So the adjacency matrix has an entry 1 in the i^{th} row and j^{th} column if the v_i and v_j are neighbours.

Example 3.7

The adjacency matrix of the graph



is

$$A = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

As in Matrix Algebra, the product of two $n \times n$ matrices A and B is the $n \times n$ matrix AB with

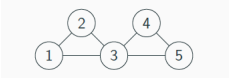
$$AB(i,j) = \sum_{k=1}^{n} A(i,k)B(k,j).$$

In other words, $AB(i,j)$ is the *scalar product* of the i^{th} row of A and the j^{th} column of B. The product of adjacency matrices can be interpreted combinatorially.

Theorem 3.8

Let A be the adjacency matrix of the graph G, with nodes $v_1, \ldots, v_n$. Then $A^k(i,j)$ is the number of paths of length k from v_i to v_j in G, for $k \in \mathbb{N}$.

Example 3.9



$$A = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \qquad A^2 = \begin{pmatrix} 2 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 & 1 \\ 1 & 1 & 4 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 2 \end{pmatrix} \qquad A^3 = \begin{pmatrix} 2 & 3 & 5 & 2 & 2 \\ 3 & 2 & 5 & 2 & 2 \\ 5 & 5 & 4 & 5 & 5 \\ 2 & 2 & 5 & 2 & 3 \\ 2 & 2 & 5 & 3 & 2 \end{pmatrix}$$

The entry $A^3(2,3) = 5$ tells us that there are five paths of length 3 from node 2 to node 3.

Theorem 3.10

Let A be the adjacency matrix of the graph G, with nodes $v_1, \ldots, v_n$. Then $A^k(i,j)$ is the number of paths of length k from v_i to v_j in G, for $k \in \mathbb{N}$.

Proof
By induction:

Base case $n = 0$: A^0 is the identity matrix $A^0 = I_n$, with

$$I_n(i,j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases}$$

The only paths of length 0 in G go from a node v_i to itself, so the number of such paths is $I_n(i,j)$.

Induction step: Assume $A^m(i,j)$ is the number of paths of length m from v_i to v_j in G. A path of length $m+1$ in G from v_i to v_j is a path of length m from v_i to some node v_ℓ, together with an edge from v_ℓ to v_j. So the number of such paths is

$$\sum_{\substack{\ell \in \{1,\dots n\} \\ \{v_\ell, v_j\} \in E}} A^m(i,\ell) = \sum_{\substack{\ell \in \{1,\dots n\} \\ A(\ell,j)=1}} A^m(i,\ell) = \sum_{\ell=1}^{n} A^m(i,\ell)A(\ell,j) = A^{m+1}(i,j).$$

By the induction principle, $A^k(i,j)$ is the number of paths of length k from v_i to v_j in G, for all $k \in \mathbb{N}$. □

3.3 Spanning trees

3.3.1 Trees

A graph is *connected* if there is a path between any pair of nodes. A connected graph without cycles is a *tree*. A node is a *leaf* if it only has one neighbour. A *rooted tree* is a tree with a distinguished node v_0 that is called the root.

If v_0 is the root, then the *level* of the node v is the length of the path $(v_0, \dots, v)$. The root is not called a leaf, even if it would only have one neighbour.

Example 3.11

Family trees, database trees, decision trees...

3.3.2 Spanning trees

A connected graph without cycles is a *tree*. In other words, a tree is a graph in which there is a *unique* path between any two nodes. A *spanning tree* in the graph (V, E) is a tree (V, E') that contains all the nodes and some of the edges $E' \subseteq E$ of the graph.

Notice: the spanning tree is not unique.

A spanning tree exists in any connected graph: Delete one edge from some cycle at a time. A spanning tree can also be constructed as follows: Start from one node, and add an edge at a time between a node contained in the tree and the node not contained in the tree.

Lemma 3.12

A tree with n nodes has exactly $n - 1$ edges.

Lemma 3.13

A tree with n nodes has at least two leaves.

Proof
By induction. □

3.3.3 Weighted graphs

Definition 3.14

A weighted graph is a graph $G = (V, E)$ together with a weight function $w : E \to \mathbb{R}$. To total weight of the graph is

$$w(G) = \sum_{e \in E} w(E).$$

Example 3.15

- Cities connected by data cables; $w(e)$ is the price of the cable e.
- Cities connected with highways; $w(e)$ is the length of the road e.
- Electricity networks; $w(e)$ is the resistance of the conductor e.

3.3.4 Minimal spanning tree

Many important optimization problems are of the form: find a subgraph with property X, of as small total weight as possible.

Examples: minimal spanning tree, shortest path, Travelling Salesman (shortest cycle through all nodes), etc.

Definition 3.16

A minimal spanning tree in the weighted graph (G, w) is a spanning tree T of G such that $w(T) \leq w(U)$ for any spanning tree U of G.

A minimal spanning tree can be found using *Prim's algorithm* (greedy algorithm).

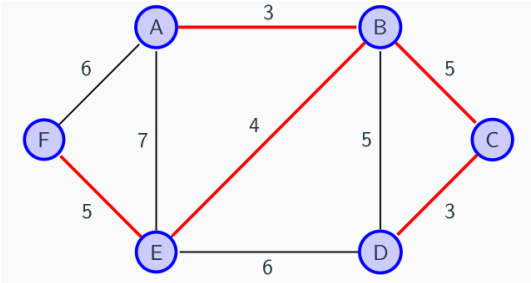
Prim's algorithm

- Choose an edge e_1 of minimal weight.
- Choose a edge e_2 that is incident to (shares an endpoint with) e_1 , whose weight is minimal among all edges incident to e_1.
- Continue: in each step we choose an edge of minimal weight that is incident to some previously chosen edge, such that the tree structure (no cycles) remains.
- The resulting spanning tree T, with edges $\{e_1, \ldots, e_n\}$, is minimal.

Example 3.17

Prim's algorithm on the graph below adds the red edges in the order

$$AB, BE, BC, CD, EF.$$



Theorem 3.18

The tree T obtained by Prim's algorithm is minimal.

Proof

Let the edge set of T be $\{e_1, \ldots, e_n\}$, where $e_i = \{u_i, v_i\}$. Let $U \neq T$ be another spanning tree. We want to show that $w(T) \leq w(U)$. If e_1 is an edge in U, let $U_1 = U$. Otherwise, let e be the first edge in the (unique) path from u_1 to v_1 in U. By the greedy algorithm, $w(e_1) \leq w(e)$. Replace e by the link e_1 in U. We get another spanning tree U_1 with

$$w(U_1) = w(U) - w(e) + w(e_1) \leq w(U).$$

Follow the unique path from u_2 to v_2 in the tree U_1. If this path only uses edges in T, then let $U_2 = U_1$. Otherwise, ley e be the first edge in the path. By the greedy algorithm, $w(e_2) \leq w(e)$. Replace e by the edge e_2 in U_1. We get a new spanning tree U_2 , with

$$w(U_2) = w(U_1) - w(e) + w(e_2) \leq w(U).$$

Continuing the same way, we get a sequence $U, U_1, \ldots, U_{n-1} = T$ of spanning trees such that

$$w(T) = w(U_n) \leq w(U_{n-1}) \leq \cdots \leq w(U_1) \leq w(U).$$

□

3.4 Graph colouring

3.4.1 Vertex colouring

Definition 3.19

- A *(vertex) k-colouring* of the graph $G = (V, E)$ is a function

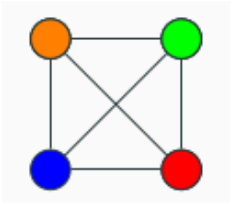
$$\gamma : V \to \{1, 2, \ldots, k\}$$

such that

$$\text{if } \{u, v\} \in E \text{ then } \gamma(u) \neq \gamma(v).$$

- The *chromatic number* $\chi(G)$ of G is the smallest number k such that there is a k-colouring of G.

We often think about, and refer to, $\{1, 2, \ldots k\}$ as "colours".



Example 3.20

- The complete graph K_n has $\chi(K_n) = n$.
- $\chi(G) = 1 \Leftrightarrow E = \emptyset$
- $\chi(G) = 2 \Leftrightarrow G$ is *bipartite*.

If $\chi(G) > 2$, there is no efficient algorithm known to compute $\chi(G)$ exactly. One can define *edge colourings* analogously, but the results discussed here hold only for vertex colourings.

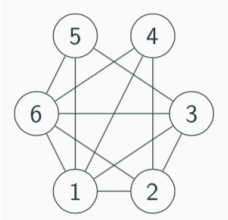
3.4.2 Conflict graphs

Example 3.21

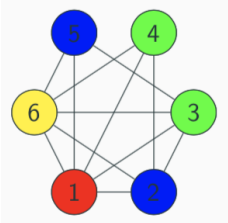
Six students Alice, Bob, Camilla, David, Erika, Fred are doing six different projects in the following groups:

1. A,B,C,F
2. B,D,E
3. C,F
4. B,E
5. A,C,F
6. D,E,F

Each project requires one day to complete, which the participants have to spend together. In how many days can all the projects be completed?
Solution: Construct the *conflict graph*, $G = (V, E)$ whose nodes are the tasks, and whose edges represent pairs of tasks that can not be completed on the same day.



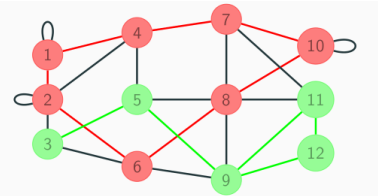
If $\gamma : V \to \{1, \ldots, k\}$ is a graph colouring, then we can complete each task v on day number $\gamma(v)$. So the smallest number of days needed is $\chi(G)$. We can colour the graph with 4 colours as below, so $\chi(G) \leq 4$.



On the other hand, the nodes $\{1, 2, 3, 6\}$ are pairwise connected, so need four different colours. Thus, $\chi(G) = 4$.

3.4.3 Subgraphs

The graph $G' = (V', E')$ is a *subgraph* of $G = (V, E)$ if $V' \subseteq V$ and $E' \subseteq E$.



The largest n for which K_n is (isomorphic to) a subgraph of G is called the *clique number* $\omega(G)$.

Theorem 3.22

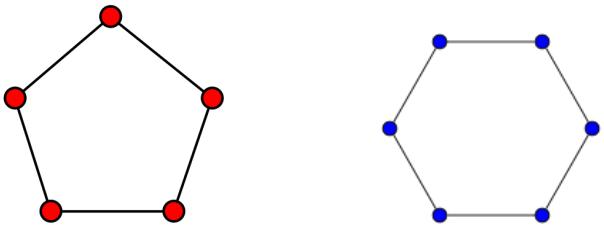
If G' is a subgraph of G, then $\chi(G') \leq \chi(G)$.

In particular, if G contains K_n as a subgraph, then $\chi(G) \geq n$. We have shown $\omega(G) \leq \chi(G)$ for any graph G. Are there graphs for which $\omega(G) < \chi(G)$?

There are many graphs for which $\omega(G) < \chi(G)$.

Example 3.23

Let $n > 3$, and let C_n be the cycle of length n



$$\omega(C_n) = 2 \text{ and } \chi(C_n) = \begin{cases} 2 & \text{if } n \text{ is even} \\ 3 & \text{if } n \text{ is odd.} \end{cases}$$

3.4.4 Greedy algorithm

Finding the chromatic number of a graph is a difficult problem. There is no known algorithm whose complexity grows polynomially with the number of vertices. Any colouring gives an upper bound of $\chi(G)$. The following *greedy algorithm* often gives useful upper bounds. Requires an ordering $\{v_1, \ldots, v_n\}$ of the vertices of V. The number of colours needed depends on the ordering.

Definition 3.24 (Greedy algorithm for graph colouring)

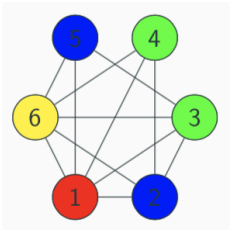
Let $G = (V, E)$ be a graph and write $V = \{v_1, \ldots, v_n\}$.

1. Initiation: Fix an order for the vertices: $(v_1, \ldots, v_n)$ and let $\gamma(v_1) = 1$
2. Iterate until halts: If $v_1, \ldots, v_{k-1}$ have already been coloured, let

$$\gamma(v_k) = \min\{i \geq 1 : \gamma(v_j) \neq i \text{ for all } j < k \text{ for which } \{v_j, v_k\} \in E\}.$$

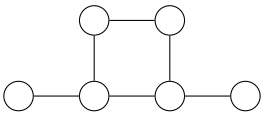
Example 3.25

Let us colour the previous conflict graph with the greedy algorithm. The vertices are already labelled $1, \ldots 6$. Visualize the "colours" $1, 2, 3, 4$ as red, blue, green, yellow, in that order.

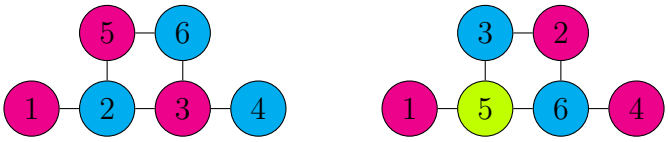


Example 3.26

Colour the following graph with the greedy algorithm.



Depending on how you order the nodes, you need either two or three colours.



Theorem 3.27

Let $G = (V, E)$ be a graph with $\chi(G) = k$. Then there exists an ordering $v_1, v_2, \ldots, v_n$ of the vertices such that the greedy algorithm colours the graph with k colours, if colouring the vertices in this order.

So if we can perform the greedy algorithm for all possible orderings of V, we can compute the chromatic number *exactly*. But there are $n!$ possible ways to order V, so this is not an efficient algorithm.

Proof
[Sketch of proof] Let $\gamma : V \to \{1, 2, \ldots, k\}$ be some colouring of G with $\chi(G) = k$ colours. Let $V_i \subseteq V$ be the set of vertices with $\gamma(v) = i$. So there are no edges between two nodes in V_i. Order the vertices such that all nodes in V_1 come first, then all nodes in V_2, and so on. Let $\delta : V \to \{1, 2, \ldots, k\}$ be a greedy graph colouring with respect to this ordering. By induction: $\delta(v) \leq i$ for all $v \in V_i$. So the greedy algorithm colours $V = V_1 \cup V_2 \cup \cdots \cup V_k$ with k colours. □

Theorem 3.28

Let G be a graph, where all nodes have degree $\leq d$. Then $\chi(G) \leq d + 1$.

Proof
Order the vertices arbitrarily, and colour the graph using the greedy algorithm. For each vertex v_k, the set $\{v_j : j < k, \{j, k\} \in E\}$ has size $\leq d$, so at most d colours are used for those vertices. So v_k can be coloured with at least one of the colours $1, 2, \ldots, d + 1$. So the greedy algorithm requires at most $d + 1$ colours, so $\chi(G) \leq d + 1$. □

Finally, there is a rigidity theorem by Brooks on the structure of graphs which achieve the value $\chi(G) = d + 1$:

Theorem 3.29 (Brooks' Theorem, 1941)

Let G be a graph, where all nodes have degree $\leq d$. If $\chi(G) = d+1$, then G is either a complete graph K_n or an odd cycle.

Chapter 4

Number theory

4.1 Divisibility

A number $n \in \mathbb{Z}$ is *divisible* by $m \in \mathbb{Z}$ if there exists $k \in \mathbb{Z}$ such that

$$mk = n.$$

Then we also say that m *divides* n, or in formulas $m|n$.

Example 4.1

- $2|4$.
- $6|12$
- $6 \not| 9$
- $0 \not| n$, $n \neq 0$.
- $1|n$, $n \in \mathbb{Z}$.
- $n|0$, $n \in \mathbb{Z}$.
- $n \not| 1$, $n \neq 1$.

If $m|n_1$ and $m|n_2$, then $m|(a_1n_1 + a_2n_2)$ for all integers a_1, a_2.

Example 4.2

Since $3|9$ and $3|15$, it follows that $3|4 \cdot 15 - 2 \cdot 9 = 42$.

So the set of common divisors of n_1 and n_2 is the same as the set of common divisors of n_2 and $n_1 - an_2$. In particular, the *greatest common divisor* satisfies

$$\gcd(n_1, n_2) = \gcd(n_1 - an_2, n_2) \text{ for all } a.$$

Example 4.3

$$\begin{aligned} \gcd(162, 114) &= \gcd(48, 114) & &= \gcd(48, 18) \\ &= \gcd(12, 18) & &= \gcd(12, 6) \\ &= \gcd(6, 6) & &= 6. \end{aligned}$$

This illustrates the *Euclidean algorithm* for computing the greatest common divisor of two numbers.

4.1.1 Euclidean division

Theorem 4.4 (Euclidean division)

Let $a, b \in \mathbb{Z}$, with $b > 0$. Then there exist unique numbers $q, r \in \mathbb{Z}$ with $0 \leq r < b$ and

$$a = qb + r.$$

Here

- q is called the *quotient* of a when divided by b.
- r is called the *remainder* of a when divided by b (or *modulo* b).

So $\frac{a}{b} = q + \frac{r}{b}$.

Example 4.5

- When dividing $a = 19$ by $b = 7$, the quotient is $q = 2$ and the remainder is $r = 5$.
- When dividing $a = -19$ by $b = 7$, the quotient is $q = -3$ and the remainder is $r = 2$.

The proof of Euclidean division is simple but tedious. Idea: r is the smallest non-negative number in $S\{a - kb : k \in \mathbb{Z}\}$. Show that this r is the only element in S with $0 \leq r < b$.

4.2 Diophantine equations

4.2.1 Euclidean algorithm

Euclidean algorithm is a method to compute the *greatest common divisor*:

Definition 4.6 (Euclidean algorithm)

Let $a, b \in \mathbb{Z}$.

- Let $r = a - qb$ be the remainder of a modulo b.
- Then $\gcd(a, b) = \gcd(r, b) = \gcd(b, r)$.
- $\gcd(b, 0) = b$ for all integers $b \neq 0$.

This gives an *algorithm* for computing the greatest common divisor

$$\gcd(a, b)$$

of two numbers $a \geq b$ in $O(\log a)$ steps.

Example 4.7

Compute $\gcd(162, 114)$.
Solution:

$$\begin{aligned} 162 &= 1 \cdot 114 + 48 \\ 114 &= 2 \cdot 48 + 18 \\ 48 &= 2 \cdot 18 + 12 \\ 18 &= 1 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 + 0 \end{aligned}$$

The greatest common divisor is the last non-zero remainder:

$$\gcd(162, 114) = 6.$$

4.2.2 Extended Euclidean algorithm

In each iteration of the Euclidean algorithm, the remainder is written as an integer combination of previous remianders:

Example 4.8

$$\begin{aligned} 48 &= 162 - 1 \cdot 114 \\ 18 &= 114 - 2 \cdot 48 \\ 12 &= 48 - 2 \cdot 18 \\ 6 &= 18 - 1 \cdot 12 \end{aligned}$$

This can be used to write the final remainder $\gcd(a, b)$ as an integer combination $xa + yb$, where $x, y \in \mathbb{Z}$.

Example 4.9

$$\begin{aligned} 48 &= 162 - 1 \cdot 114 \\ 18 &= 114 - 2 \cdot 48 \\ 12 &= 48 - 2 \cdot 18 \\ 6 &= 18 - 1 \cdot 12 \end{aligned}$$

- We use this to write $6 = \gcd(114, 162)$ as an integer combination

$$114x + 162y, \text{ where } x, y \in \mathbb{Z}.$$

$$\begin{aligned} 6 &= 18 - 12 \\ &= 18 - (48 - 2 \cdot 18) && = 3 \cdot 18 - 48 \\ &= 3(114 - 2 \cdot 48) - 48 && = 3 \cdot 114 - 7 \cdot 48 \\ &= 3 \cdot 114 - 7(162 - 114) && = 10 \cdot 114 - 7 \cdot 162. \end{aligned}$$

4.2.3 Linear Diophantine equations in two variables

An equation where the variables are integer valued is called a *Diophantine* equation. The extended Euclidean algorithm gives a solution (x_B, y_B) to the Diophantine equation

$$\gcd(a, b) = ax + by.$$

The integers (x_B, y_B) are the *Bézout coefficients* of a and b:

$$\gcd(a, b) = ax_B + by_B.$$

If $\gcd(a, b)|c$, then the pair

$$(x_0, y_0) = \frac{c}{\gcd(a, b)}(x_B, y_B)$$

is an integer solution to the equation $c = ax + by$. If $\gcd(a, b) \not| c$, can there still be integer solutions to the equation

$$c = ax + by?$$

No! Because $\gcd(a, b)|ax + by$ for all integers x, y.

Theorem 4.10

The Diophantine equation

$$c = ax + by$$

has integer solutions if and only if $\gcd(a, b)|c$.
If $\gcd(a, b)|c$, then one *particular* solution (x_0, y_0) is given by Euclid's extended algorithm. Let $a' = \frac{a}{\gcd(a,b)}$ and $b' = \frac{b}{\gcd(a,b)}$. Then *all* integer solutions to the equation are

$$(x_0 + nb', y_0 - na')\,,\ n \in \mathbb{Z}.$$

To prove this, we first must address the issue of *unique factorization*.

4.2.4 Dividing a product

Lemma 4.11

if $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

If $\gcd(a, b) = 1$, then $1 = xa + yb$ holds for some $x, y \in \mathbb{Z}$, so

$$c = xca + ybc.$$

Since a divides

$$xca + ybc$$

, it also divides c.

4.2.5 Unique factorization

So if p is a prime (only divisible by 1 and itself) such that $p|bc$, then either $p|b$ or $p|c$. It follows that every number can be written as a product of primes *in a unique way*.

$$210 = 7 \cdot 30 = 10 \cdot 21 = 6 \cdot 35 = \cdots = 2 \cdot 3 \cdot 5 \cdot 7$$

can not be written as a product of *primes* in any other way.

We want to divide a large number N into prime factors First, we find a prime p that divides N. Then we factorize the smaller number N/p.

Example 4.12

$$\begin{aligned} 10452 &= 2 \cdot 5226 \\ &= 2^2 \cdot 2613 \\ &= 2^2 \cdot 3 \cdot 871 \\ &= 2^2 \cdot 3 \cdot 13 \cdot 67. \end{aligned}$$

We see that 67 is a prime, because it is not divisible by any prime $\leq \sqrt{67} < 9$.

4.2.6 Linear Diophantine equations in two variables

We are now ready to prove the following theorem.

Theorem 4.13

The Diophantine equation

$$c = ax + by$$

has integer solutions if and only if $\gcd(a, b)|c$.
If $\gcd(a, b)|c$, then one *particular* solution (x_0, y_0) is given by Euclid's extended algorithm. Let $a' = \frac{a}{\gcd(a,b)}$ and $b' = \frac{b}{\gcd(a,b)}$. Then all integer solutions to the equation are

$$(x_0 + nb', y_0 - na')\,,\ n \in \mathbb{Z}.$$

Proof

$$a' = \frac{a}{\gcd(a, b)} \text{ and } b' = \frac{b}{\gcd(a, b)}.$$

$$\begin{aligned} a(x_0 + nb') + b(y_0 - na') &= ax_0 + by_0 + (nab' - nba') \\ &= c + 0, \end{aligned}$$

so $(x_0 + nb', y_0 - na')$ is a solution. If (x, y) is an arbitrary solution, then

$$a(x - x_0) + b(y - y_0) = c - c = 0.$$

$\gcd(a', b) = \gcd(a, b') = 1$, so

$$a'|y - y_0 \text{ and } b'|x - x_0.$$

So $x = x_0 + mb'$ ja $y = y_0 - na'$ holds for some $n, m \in \mathbb{Z}$.

$$ax_0 + by_0 = c = ax + by \Longrightarrow m = n.$$

□

Example 4.14

Solve the Diophantine equation

$$514x + 387y = 2.$$

Solution: First find $\gcd(514, 387)$ by the Euclidean algorithm:

$$\begin{aligned} 514 &= 387 + 127 \\ 387 &= 3 \cdot 127 + 6 \\ 127 &= 21 \cdot 6 + 1 \\ 6 &= 6 \cdot 1 + 0. \end{aligned}$$

This shows $\gcd(514, 387) = 1|2$, so the equation has solutions.
Now solve

$$514x + 387y = \gcd(514, 387) = 1$$

by the extended Euclidean algorithm:

$$\begin{aligned} 1 &= 127 - 21 \cdot 6 \\ &= 127 - 21 \cdot (387 - 3 \cdot 127) && = 64 \cdot 127 - 21 \cdot 387 \\ &= 64 \cdot (514 - 387) - 21 \cdot 387 && = 64 \cdot 514 - 85 \cdot 387. \end{aligned}$$

So

$$2 = 2(64 \cdot 514 - 85 \cdot 387) = 128 \cdot 514 - 170 \cdot 387.$$

Answer: The Diophantine equation

$$514x + 387y = 2$$

has infinitely many solutions,

$$(x, y) = (128, -170) + n(387, -514).$$

Example 4.15

Solve the Diophantine equation

$$112x + 49y = 2.$$

Solution: First find $\gcd(112, 49)$ by the Euclidean algorithm:

$$\begin{aligned} 112 &= 2 \cdot 49 + 14 \\ 49 &= 3 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0. \end{aligned}$$

This shows $\gcd(112, 49) = 7 \not| 2$, so the equation has no integer solutions.

4.3 Modular arithmetic

4.3.1 Congruence classes

Definition 4.16

Let n be a positive integer. If $n|(a-b)$, then we say $a \equiv b \mod n$.
In words: a and b are *congruent* modulo n.

Congruence modulo n is an **equivalence relation** on $\mathbb{Z}$:

- Reflexive: $\forall a \in \mathbb{Z} : n|0 = a - a$.
- Symmetric: $\forall a, b \in \mathbb{Z}$: If $n|a-b$ then $n| - (a-b) = b - a$.
- Transitive:

$$\forall a, b, c \in \mathbb{Z} : \text{ If } n|a-b \text{ and } n|b-c, \text{ then } n|(a-b)+(b-c) = a-c.$$

Notice that $a \equiv b \mod n$ if and only if a and b have the same remainder when divided by n.

Example: $4 \equiv 16 \mod 12$; The clock hands are in the same position at 4:00 and 16:00.

Definition 4.17

The *congruence class* of $a \in \mathbb{Z}$ modulo n is

$$[a]_n = \{b \in \mathbb{Z} : a \equiv b \mod n\} \subseteq \mathbb{Z}.$$

Example 4.18

$[4]_{12} = \{\ldots, -20, -8, 4, 16, 28, \ldots\}$

The elements of a congruence class are *representatives* of that class. Each congruence class has precisely one representative in$\{0, 1, \ldots, n-1\}$. Note: $[n]_n = [0]_n$.

Example 4.19

The smallest non-negative representative of $[27]_{11}$ is $5 = 27 - 2 \cdot 11$.

Definition 4.20

The set of congruence classes modulo $n \in \mathbb{Z}$ modulo n is denoted $\mathbb{Z}_n$ (or $\mathbb{Z}/n\mathbb{Z}$).

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \cdots, [n-1]_n\}.$$

4.3.2 Addition and multiplication of congruence classes

For $n \in \mathbb{N} \setminus \{0\}$ and $a, b \in \mathbb{Z}$, define:

$$[a]_n + [b]_n = [a+b]_n$$
$$[a]_n[b]_n = [ab]_n$$

Note: If $a = pn + r$, $b = qn + s$, then

$$[a+b]_n = [(p+q)n + r + s]_n = [r+s]_n$$
$$[ab]_n = [pnqn + pns + qnr + rs]_n = [rs]_n,$$

so the sum and product really only depend on the congruence classes of a and b modulo n. Example: $[4]_3 + [5]_3 = [9]_3 = [3]_3 = [1]_3 + [2]_3$.

Example 4.21

We get addition and multiplication tables as follows in

$$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\} :$$

$+_3$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\times_3$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Theorem 4.22

The following laws hold for $a, b, c \in \mathbb{Z}_n$:

- $a + b = b + a$ and $ab = ba$ *(commutativity)*
- $a + (b + c) = (a + b) + c$ and $a(bc) = (ab)c$ *(associativity)*
- $a + 0 = a$ and $a \cdot 1 = a$ *(neutral elements)*
- For each a there exists $-a$ s.t. $a + (-a) = 0$. *(additive inverse)*
- $a(b + c) = ab + ac$ *(distributivity)*

Note: $a, b, 0, 1$ are *congruence classes*; not integers. These are the axioms of a *commutative ring with a unit*. In some sources, this is called a *commutative ring*, or even just a *ring*. The set $\mathbb{Z}_n$ is called the *ring of integers modulo n*.

4.3.3 Differences between $\mathbb{Z}$ and $\mathbb{Z}_n$

The table did not talk about *multiplicative* inverses. b is a multiplicative inverse of a if $ab = ba = 1$. In $\mathbb{Z}$, only ± 1 have multiplicative inverses. In $\mathbb{Z}_n$, other elements can have inverses too.

Example: $[2]_5 \cdot [3]_5 = [1]_5$, so $[2]_5$ and $[3]_5$ are inverses in $\mathbb{Z}_5$.

A commutative ring with a unit, where all non-zero elements have an inverse, is called a *field*.

Example: $\mathbb{R}$ and $\mathbb{Q}$ are fields.

Theorem 4.23

Let p be a prime. Then $\mathbb{Z}_p$ is a field.

Proof
Let $0 < a < p$, so $[a]_p \neq [0]_p$. Then $\gcd(p, a) = 1$. By Bezout's identity, $xp + ya = 1$ has an integer solution. Then $ya \equiv 1 \mod p$, so $[y]_p$ is an inverse of $[a]_p$. □

In $\mathbb{Z}_n$ it is not true that $ab = ac \Rightarrow b = c$. In fact, this is true if and only if a is invertible. $[x]$ is invertible in $\mathbb{Z}_n$ if and only if $\gcd(x, n) = 1$.

Example 4.24

In $\mathbb{Z}_6$, $[2] \cdot [4] = [2] \cdot [1]$, but $[4] \neq [1]$.

4.3.4 Congruence equations

When does $b \equiv ax \mod n$ have a solution? If $\gcd(a, n) \neq 1$, then we must have $\gcd(a, n) | b$. In such case, divide the equation by $\gcd(a, n)$.

Theorem 4.25

Assume $\gcd(a, n) = 1$. Then $ax \equiv b \mod n$ has a unique (modulo n solution).

Proof
$[a]$ has an inverse $[a]^{-1}$ in $\mathbb{Z}_n$. Thus $[a][x] = [b] \Rightarrow [x] = [a]^{-1}[a][x] = [a]^{-1}[b]$. □

Example 4.26

The invertible elements in $\mathbb{Z}_{10}$ are $[1], [3], [7], [9]$. Their inverses are

$$[1]^{-1} = [1],\ [3]^{-1} = [7],\ [7]^{-1} = [3],\ [9]^{-1} = [9]$$

respectively. Notice: $[9] = -[1]$.

Example 4.27

The invertible elements in $\mathbb{Z}_{12}$ are $[1], [5], [7], [11]$. They are all their own inverses. We can solve the congruence

$$7x \equiv 9 \mod 12$$

by multiplying with the inverse of 7 modulo 12.

$$x \equiv 7 \cdot 7x \equiv 7 \cdot 9 \equiv 63 \equiv 3 \mod 12.$$

4.4 Computing exponents modulo n

What is the remainder of 3^{13} when divided by 100? Using division algorithm: $3^{13} = 100q + r$, so $[r]_{100} = [3^{13}]_{100}$. However, we save time by not computing 13 multiplications, but doing *repeated squaring* in $\mathbb{Z}_{100}$:

$$\begin{aligned} [3]^2 &= [9] \\ [3]^4 = [9]^2 &= [81] \\ [3]^8 = [81]^2 = [6561] &= [61] \\ [3]^{13} = [3]^8 \cdot [3]^4 \cdot [3]^1 = [61][81][3] = [14823] &= [23]. \end{aligned}$$

Thus the remainder is 23. However, if the exponent is very large, then even repeated squaring is inconvenient.

Example 4.28

- Can we compute $[3]_{13}^{100}$?
- Yes, because we are lucky! $[3]^3 = [27] = [1]$.

$$[3]^{100} = ([3]^3)^{33} \cdot [3] = [1]^{33} \cdot [3] = [3]$$

- So the remainder is 3.

It would help if we had a *systematic* way to find a number k such that

$$a^k \equiv 1 \mod n.$$

(if $\gcd(a, n) = 1$). For thus purpose we have the useful Fermat's little theorem:

Theorem 4.29 (Fermat's little theorem)

Let p be a prime and $a \not\equiv 0 \mod p$. Then $a^{p-1} \equiv 1 \mod p$.

Proof
Each $[a][x] = [b]$ has a unique solution if $[b] \neq [0]$. So

$$\{[1], [2], \dots [p-1]\} = \{[a][1], [a][2], \dots [a][p-1]\}.$$

Thus

$$[(p-1)!] = \prod_{i=1}^{p-1} [i] = \prod_{i=1}^{p-1} [a][i] = [a]^{p-1}[(p-1)!].$$

But $p \not| (p-1)!$, so $(p-1)!$ is invertible modulo p. It follows that $[1]_p = [a]_p^{p-1}$. □

Example 4.30

We check Fermat's little theorem in $\mathbb{Z}_7$:

- $1^6 = 1$
- $2^6 = (2^3)^2 = 1^2 = 1$
- $3^6 = (3^3)^2 = (-1)^2 = 1$
- $4^6 = (-3)^6 = 3^6 = 1$
- $5^6 = (-2)^6 = 2^6 = 1$
- $6^6 = (-1)^6 = 1^6 = 1$

4.4.1 Euler's φ function and Euler's theorem

How do we compute powers modulo a non-prime n? The proof of Fermat's little theorem suggests a generalization. Let us first define:

Definition 4.31 (Euler's φ function)

We say that two integers a, b are called **relatively prime** if $\gcd(a, b) = 1$. Let $n \in \mathbb{N}$. The **Euler's φ function** $\varphi(n)$ is the number of elements

$$0 \leq i < n \text{ such that } \gcd(n, i) = 1.$$

I.e. it counts the number of relatively prime non-negative integers less than n.

Note: $\varphi(n) = n - 1$ if and only if n is prime. Equivalently, $\varphi(n)$ is the number of invertible elements in $\mathbb{Z}_n$.

If $n = p^k$ is a power of a prime, then

$$\begin{aligned}\varphi(n) &= |\{0 \le i < n : \gcd(n, i) = 1\}| \\ &= p^k - \{pj : 0 \le j < p^{k-1}\}| \\ &= (p-1)p^{k-1}.\end{aligned}$$

If $\gcd(a, b) = 1$, then $\varphi(ab) = \varphi(a)\varphi(b)$. (Proof omitted.) Thus,

$$\varphi(p_1^{k_1} \cdots p_r^{k_r}) = (p_1 - 1) \cdots (p_r - r) \cdot p_1^{k_1 - 1} \cdots p_r^{k_r - 1}$$

Example 4.32

How many integers in $[0, 10200]$ are relatively prime to 10200?
Solution: First factorize

$$\begin{aligned}10200 &= 2 \cdot 5100 &&= 2^2 \cdot 2550 &&= 2^3 \cdot 1275 \\ &= 2^3 \cdot 3 \cdot 425 &&= 2^3 \cdot 3 \cdot 5 \cdot 85 &&= 2^3 \cdot 3 \cdot 5^2 \cdot 17.\end{aligned}$$

Thus we get

$$\begin{aligned}\varphi(10200) &= (2-1)2^2 \cdot (3-1) \cdot (5-1)5 \cdot (17-1) \\ &= 2^{2+1+2+4} \cdot 5 \\ &= 528 \cdot 5 = 2640.\end{aligned}$$

Thus the answer is 2640.

Now, Euler's φ function provides a powerful tool to compute powers modulo n due to **Euler's theorem**:

Theorem 4.33 (Euler's theorem)

Let $n \in \mathbb{N}$, and $\gcd(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \mod n$.

The proof closely follows that of Fermat's little theorem. It follows that, if $b = q\varphi(n) + r$, then $a^b \equiv a^r \mod n$. Note that in the above example, by Euler's theorem,

$$a^{2640} \equiv 1 \mod 10200$$

for all a with $\gcd(10200, a) = 1$. In general, if $m \equiv 1 \mod \varphi(n)$ and $\gcd(a, n) = 1$, then $a^m \equiv a \mod n$. Thus, if we can factorise n, this provides a more efficient tool to compute powers modulo n than before.

4.5 Application to RSA cryptography

In 1978, Ron Rivest, Adi Shamir and Leonard Adleman demonstrated the RSA cryptography scheme. It allows anybody with a *public* key to send messages to Alice. Alice has a *private* key, with which she can read the secret message. RSA cryptograpy is considered secure in practice. Breaking the crypto (i.e. reading the message without the private key) is equally difficult as computing $\varphi(n)$ for a large number n.

Anybody with a *public* key (k, n), can transmit a message $s \in \mathbb{Z}_n$ to Alice, by sending the message $s^k \in \mathbb{Z}_n$. This is easy to compute. Alice can compute

$$s = s^{k\ell} = (s^k)^\ell,$$

if $k\ell \equiv 1 \mod \varphi(n)$. Here ℓ is the inverse of k modulo $\varphi(n)$, **and Alice knows $\varphi(n)$.** Alice generates two large primes p and q secretly. She computes $n = pq$ (public knowledge) and $\varphi(n) = (p-1)(q-1)$. Alice chooses a number k (public) with $\gcd(k, \varphi(n)) = 1$, and in secret computes its inverse d in $\mathbb{Z}_{\varphi(n)}$. Public key: (k, n). Alice trusts that the number d remains secret. Computing d from the public key would require first computing $\varphi(n)$, *i.e.* factorizing the large number n.

Mathematical essence:

$$(s^k)^d = s^{kd} = s^{r\varphi(n)+1} = s.$$

This is a consequence of Euler's theorem.

- Computational essence 1: It is **easy** to compute s^k from s.
- Computational essence 2: It is **easy** to compute $s = (s^k)^d$ from s^k if you know d.
- Computational essence 3: It is **difficult** to compute s from s^k if you do not know d.

A user Bob who wants to send a message to Alice, first writes that message using the "alphabet" $[0], [1], [2], \ldots, [n-1]$. In our example, Bob uses the translation $A = 1, B = 2, C = 3, \ldots$. If n is really large, he can translate more efficiently by encoding more than one letter per symbol, like $AA = 1, AB = 2, \ldots$. To avoid "frequency attacks", Bob might encode common strings into a single symbol. Encoding: If Bob wants to communicate the symbol $s \in \mathbb{Z}_n$ to Alice, he instead sends the symbol $s^k \in \mathbb{Z}_n$. Encoding: If Bob wants to communicate the symbol $s \in \mathbb{Z}_n$ to Alice, he instead sends the symbol $s^k \in \mathbb{Z}_n$. Decoding: If Alice receives the symbol $t \in \mathbb{Z}_n$, she knows that the sent symbol was

$$t^d = (s^k)^d = s^{kd} = s^{r\varphi(n)+1} = s.$$

Cracking the crypto: If we can factorize n, then we can compute $\varphi(n)$, and then compute d from k by solving the diophantine equation

$$1 = kd + \varphi(n)y.$$

Example 4.34 (Spying example)

 .

Public key: $(5, 2021)$. (We pretend that it were difficult to factor $2021 = 43 \cdot 47$).
Secret message: `"The cats' names are`

$$1698\ \ 1500\ \ 1954\ \ 1450\ \ 1104\ \ 1671\ \ 0757\ \ 0001\ \ 1954\ \ 0440$$

`and`

$$0432\ \ 1104\ \ 1450\ \ 1681\ \ 0249\ \ 0440.\text{"}$$

So we have seen that computing $\varphi(n)$ for a large number n is equivalent to prime factorizing n. However, **no efficient algorithm is known for this *on a classical computer*.** Peter Shor showed in 1993, that primes can in principle be efficiently factorized on a ***quantum computer***. *If* quantum computers actually start working on a big scale, RSA will be outdated. To date, Shor's algorithm has managed to factorize $21 = 7 \times 3$.