

Diskrete Mathematik für Informatik (SS 2018)

Martin Held

FB Computerwissenschaften
Universität Salzburg
A-5020 Salzburg, Austria
held@cosy.sbg.ac.at

1. März 2018



LVA-Leiter (VO+PS): Martin Held.

Email-Adresse: held@cs.sbg.ac.at.

Basis-URL: <https://www.cosy.sbg.ac.at/~held>.

Büro: Universität Salzburg, Computerwissenschaften, Zi. 1.20,
Jakob-Haringer Str. 2, 5020 Salzburg-Itzling.

Telefonnummer (Büro): (0662) 8044-6304.

Telefonnummer (Skr.): (0662) 8044-6328.



LVA-Leiter (PS): Peter Palfrader.

Email-Adresse: palfrader@cs.sbg.ac.at.

Büro: Universität Salzburg, Computerwissenschaften, Zi. 0.28,
Jakob-Haringer Str. 2, 5020 Salzburg-Itzling.

Telefonnummer (Büro): (0662) 8044-6326.

Telefonnummer (Skr.): (0662) 8044-6328.

LVA-Leiter (PS): Ana Sokolova.

Email-Adresse: anas@cs.uni-salzburg.at.

Büro: Universität Salzburg, Computerwissenschaften, Zi. 2.17,
Jakob-Haringer Str. 2, 5020 Salzburg-Itzling.

Telefonnummer (Büro): (0662) 8044-6417.

Telefonnummer (Skr.): (0662) 8044-6404.

LVA-URL (VO+PS): [Basis-URL/teaching/diskrete_mathematik/dm.html](https://www.univ-salzburg.at/teaching/diskrete_mathematik/dm.html).

Allg. Information: [Basis-URL/for_students.html](https://www.univ-salzburg.at/for_students.html).

Abhaltezeit der VO: Donnerstag 8^{00} – 10^{55} , mit etwa 20 Minuten Pause.

Abhalteort der VO: T01, Computerwissenschaften, Jakob-Haringer Str. 2.

Abhaltezeit des PS: Freitag 8^{00} – 9^{45} .

Abhalteort des PS: T01+T02+T03, Computerwissenschaften, Jakob-Haringer Str. 2.

Tutorium: Philipp Mayer:
Mittwoch 13^{00} – 15^{00} im T04,
Donnerstag 13^{00} – 15^{00} im T02,
Computerwissenschaften, Jakob-Haringer Str. 2.

Achtung — das Proseminar ist prüfungsimmanent!

In addition to these slides, you are encouraged to consult the WWW home-page of this lecture:

https://www.coby.sbg.ac.at/~held/teaching/diskrete_mathematik/dm.html.

In particular, this WWW page contains up-to-date information on the course, plus links to online notes, slides and (possibly) sample code.



A Few Words of Warning

I hope that these slides will serve as a practice-minded introduction to various aspects of discrete mathematics which are of importance for computer science. I would like to warn you explicitly not to regard these slides as the sole source of information on the topics of my course. It may and will happen that I'll use the lecture for talking about subtle details that need not be covered in these slides! In particular, the slides won't contain all sample calculations, proofs of theorems, demonstrations of algorithms, or solutions to problems posed during my lecture. That is, by making these slides available to you I do not intend to encourage you to attend the lecture on an irregular basis.



Acknowledgments

These slides are a revised and extended version of a draft prepared by Kamran Safdar. Included is material written by Christian Alt, Caroline Atzl, Michael Burian, Peter Gintner, Bernhard Guillon, Yvonne Höller, Stefan Huber, Sandra Huemer, Christian Lercher, Sebastian Stenger, Alexander Zrinyi. I also benefited from comments and suggestions made by Stefan Huber and Peter Palfrader.

This revision and extension was carried out by myself, and I am responsible for all errors.

Salzburg, February 2018

Martin Held



Legal Fine Print and Disclaimer

To the best of our knowledge, these slides do not violate or infringe upon somebody else's copyrights. If copyrighted material appears in these slides then it was considered to be available in a non-profit manner and as an educational tool for teaching at an academic institution, within the limits of the "fair use" policy. For copyrighted material we strive to give references to the copyright holders (if known). Of course, any trademarks mentioned in these slides are properties of their respective owners.

Please note that these slides are copyrighted. The copyright holder(s) grant you the right to download and print it for your personal use. Any other use, including non-profit instructional use and re-distribution in electronic or printed form of significant portions of it, beyond the limits of "fair use", requires the explicit permission of the copyright holder(s). All rights reserved.

These slides are made available without warrant of any kind, either express or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. In no event shall the copyright holder(s) and/or their respective employers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, arising out of or in connection with the use of information provided in these slides.



Recommended Textbooks I



S. Maurer, A. Ralston.

Discrete Algorithmic Mathematics

A.K. Peters, 3rd edition, Jan 2005; ISBN 978-1-56881-166-6



K. Rosen.

Discrete Mathematics and Its Applications

McGraw-Hill, 7th edition, June 2011; ISBN 9780073383095



B. Kolmann, R.C. Busby, S.C. Ross.

Discrete Mathematical Structures

Pearson India, 6th edition, 2015; ISBN 978-9332549593.



K.A. Ross, C.R.B. Wright.

Discrete Mathematics

Pearson Prentice Hall, 5th edition, Aug 2002; ISBN 9780130652478




K. Bogart, C. Stein, R.L.S. Drysdale.

Discrete Mathematics for Computer Science

Addison-Wesley, March 2010; ISBN 978-0132122719.

Recommended Textbooks II

 J. O'Donnell, C. Hall, R. Page.
Discrete Mathematics Using a Computer
Springer, 2nd edition, 2006; ISBN 978-1-84628-241-6

 N.L. Biggs.
Discrete Mathematics
Oxford University Press, 2nd edition, Feb 2003, reprinted (with corrections) 2008;
ISBN 978-0-19-850717-8

 M. Smid.
Discrete Structures for Computer Science: Counting, Recursion, and Probability
[http://glab.ca/~michiell/DiscreteStructures/](http://glab.ca/~michiell/DiscreteStructures/DiscreteStructures.pdf)
[DiscreteStructures.pdf](http://glab.ca/~michiell/DiscreteStructures/DiscreteStructures.pdf), 2017

Table of Content

- 1 Introduction
- 2 Formalism: Definitions and Theorem Proving
- 3 Numbers and Basics of Number Theory
- 4 Principles of Elementary Counting and Combinatorics
- 5 Complexity Analysis and Recurrence Relations
- 6 Graph Theory
- 7 Cryptography

1 Introduction

- What is Discrete Mathematics?
- Motivation

What is Discrete Mathematics?

- No universally accepted definition of the scope of DM exists . . .
- Typically, objects studied in DM can only assume discrete, separate values rather than values out of a continuum; sets of such objects are countable.
- The term “discrete” is often used in contrast to “continuous”, where the values of objects may vary smoothly.
- Calculus does not belong to DM, but to “continuous mathematics”.

Typical Topics of Discrete Mathematics

- Depending on what is covered in other courses a variety of topics tends to be studied within a course on DM:
 - Logic and Boolean algebra,
 - Mathematical language,
 - Algebraic structures,
 - Set theory,
 - Functions and relations;
 - Formal languages,
 - Automata theory;
 - Number theory,
 - Proofs and mathematical reasoning,
 - Counting and elementary combinatorics,
 - Graph theory,
 - Complexity theory,
 - Encoding and cryptography;
 - Computability theory,
 - Elementary probability theory.

- DM forms the mathematical language of computer science.
- Thus, its importance has increased significantly in recent years.
- In any case, DM is at the very heart of several other disciplines of computer science.
- Applications of DM include — but are not limited to —
 - Algorithms and data structures,
 - Automated programming,
 - Automated theorem proving,
 - Combinatorial geometry,
 - Computational geometry,
 - Cryptography and cryptanalysis,
 - Discrete simulation,
 - Game theory,
 - Operations research and combinatorial optimization,
 - Theory of computing,
 - Queuing theory.
- We start with a set of sample problems; solutions for all problems will be worked out or, at least, sketched during this course.

Sample Problem: Summation Formula

- Suppose that an algorithm needs $1 + 2 + 3 + \dots + (n - 1) + n$ many computational steps (of unit cost) to handle an input of size n .
- Question: Can we express this sum by means of a closed formula?
- Basic math:

$$1 = 1 = 1 \cdot 2 / 2$$

$$1 + 2 = 3 = 2 \cdot 3 / 2$$

$$1 + 2 + 3 = 6 = 3 \cdot 4 / 2$$

$$1 + 2 + 3 + 4 = 10 = 4 \cdot 5 / 2$$

$$1 + 2 + 3 + 4 + 5 = 15 = 5 \cdot 6 / 2$$

$$1 + 2 + 3 + 4 + 5 + 6 = 21 = 6 \cdot 7 / 2$$

$$1 + 2 + 3 + 4 + 5 + 6 + 7 = 28 = 7 \cdot 8 / 2$$

- An inspection of the numbers on the right-hand side *might* let us suspect that

$$1 + 2 + 3 + \dots + (n - 1) + n = \frac{n(n + 1)}{2}.$$

- But is this indeed correct? And, by the way, what do the dots in this equation really mean??



Sample Problem: Summation Formula

- An answer can be established by means of number theory (natural numbers, induction). And we get indeed

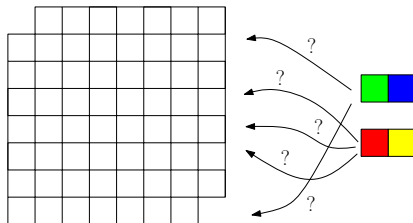
$$1 + 2 + 3 + \cdots + (n - 1) + n = \frac{n(n + 1)}{2}$$

for all “natural numbers” n .

- Caution: Even after calculating this sum for all values of n between 1 and 500 one can not legitimately claim to know the sum for, say, $n = 1000$.
- Note: It would constitute a horrendous waste of CPU time to let a computer compute $1 + 2 + 3 + \cdots + (n - 1) + n$ by successively adding numbers if we could simply obtain the result by evaluating $\frac{n(n+1)}{2}$.

Sample Problem: Chessboard Tilings

- Consider an 8×8 chessboard with the upper-left and lower-right cells removed, and assume that we are given red/yellow and green/blue domino blocks whose sizes match the size of two adjacent squares of the chessboard.
- Question: Can this chessboard be covered completely by 31 domino blocks of arbitrary color combinations?

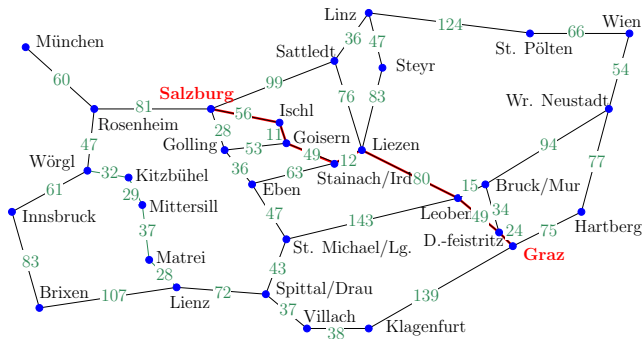


- We consult counting principles and obtain the answer: No!
- Caution: Simply trying out *all* possible placements of domino blocks hardly is an option for an 8×8 chessboard — and definitely no option for an $n \times n$ board!



Sample Problem: Route Calculation

- Question: What is the shortest route for driving from Salzburg to Graz?
- Answer provided by computing a shortest path in a weighted graph: Salzburg → Bad Ischl → Bad Goisern → Stainach/Irdning → Liezen → Leoben → Deutschfeistritz → Graz.

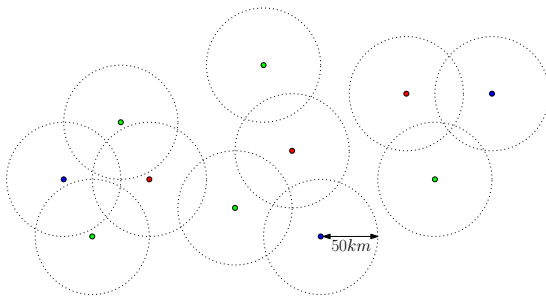


- Note: Simply trying all possible routes gets tedious! (How would you even guarantee that all possible routes have indeed been checked?)



Sample Problem: Channel Assignment

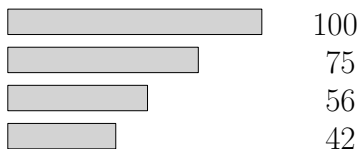
- Suppose that frequencies out of a set of m frequencies are to be assigned to n broadcast stations within Austria. We are told that the area serviced by a station lies within a disk with radius 50 kilometers. Obviously, no two different stations whose broadcast areas overlap may use the same frequency.
- Question: Do we have enough frequencies? What is the minimum number of frequencies needed?



- The solution can be obtained by using techniques of computational geometry combined with graph coloring.

Sample Problem: Complexity of an Algorithm

- Suppose that an algorithm is given n numbers as input and that it solves a problem by proceeding as follows: During one round of computation, it performs n computational steps. Further we know that during each round it discards at least 25% of the numbers. The algorithm executes one round after the other until only one number is left.

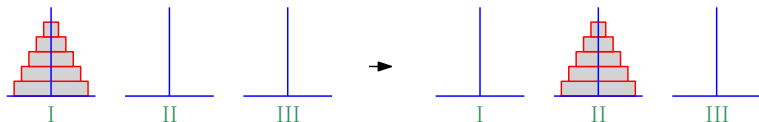


- Question: How many rounds does the algorithm run in the worst case (depending on the input size n)? How many computational steps are carried out in the worst case?
- Answer provided by the theory of recurrence relations: The number of computational steps is linear in n , and the number of rounds is logarithmic in n .
- In asymptotic notation: $O(n)$ and $O(\log n)$.



Sample Problem: Optimality of an Algorithm

- Tower-of-Hanoi Problem (ToH): Given three poles (labeled I,II,III) and a stack of n disks arranged on Pole I from largest at the bottom to smallest at the top, we are to move all disks to Pole II such that only one disk is moved at a time and such that no larger disk ever is placed on a smaller disk.
- Attributed to Édouard Lucas [1883]. Supposedly based on an Indian legend about Brahmin priests moving 64 disks in the Great Temple of Benares; once they are finished, life on Earth will end.
- Goal: Find an algorithm that uses the minimum number of moves.



- One can prove: A (straightforward) recursive algorithm needs $2^n - 1$ moves.
- One can also prove: Every(!) algorithm that solves ToH needs at least $2^n - 1$ moves.
- Thus, the solution achieved by the recursive algorithm is optimal as far as the number of moves is concerned.
- Note, though, that there exists a simple iterative solution due to Buneman&Levy [1980] which avoids an exponential-sized stack!

Sample Problem: The Power of Exponential Growth

- According to legend, the power of exponential growth was already known by the Brahmin Sissa ibn Dahir (ca. 300-400 AD): As a reward for the invention of the game of chess (or its Indian predecessor Chaturanga) he asked his king to place one grain of rice in the first square of a chessboard, two in the second, four in the third, and so on, doubling the amount of rice up to the 64-th square.
- So, how many grains of rice did Sissa ask for?
- Let $R(64)$ denote the number of rice grains for 64 squares. We get

$$R(64) = 1 + 2 + 4 + \dots + 2^{63}$$

and, in general, using the capital-sigma notation and geometric series,

$$R(n) = 1 + 2 + 4 + \dots + 2^{n-1} = \sum_{i=1}^n 2^{i-1} = \sum_{i=0}^{n-1} 2^i = \frac{2^n - 1}{2 - 1} = 2^n - 1.$$

- Hence, Sissa asked for

$$2^{64} - 1 = 18\,446\,744\,073\,709\,551\,615$$

grains of rice. This is about 1 000 times the current global yearly production!

- The “*second half of the chessboard*” is a phrase, coined by Kurzweil in 1999, to refer to the point where exponential growth begins to have a significant impact.
- [Sagan 1997]: “Exponentials can’t go on forever, because they will gobble up everything”.



Sample Problem: Hairy Siblings?

- Apparently, every human has a certain number of hairs on her/his body.
- Question: Is it correct that there live at least two Austrians who have precisely the same number of hairs on their bodies?
- A combinatorial argument (pigeon hole principle) provides an affirmative answer: Yes, this is correct!
- Note: This is not a trick question — mild assumptions on the maximum number of hairs per square centimeter on a human's body will allow us to come up with a rigorous mathematical argument.

Formalism: Definitions and Theorem Proving

- Definitions
- Syntactical Proof Techniques
- Types of Proofs
- Pigeonhole Principle

How to Deal with Formal Statements ...

- Experience tells me that students find it difficult
 - to parse and understand formal statements,
 - to formulate meaningful definitions,
 - to write clean and mathematically correct proofs.
- Hence, prior to diving into other areas of Discrete Mathematics, we start with taking a practical look at the formal nuts and bolts of mathematical reasoning.
- In the following slides on definitions and theorem proving we pre-suppose an “intuitive” understanding of natural numbers, integers, reals, etc.; e.g., as taught in school.
- We will later on put these number systems on slightly more formal grounds.

Definitions

- We distinguish between *explicit* and *recursive* definitions.
- An explicit definition relates an entity that is to be specified (“*definiendum*”) to an already known entity (“*definiens*”).
- Explicit definition of an n -ary function f :

$$f(x_1, x_2, \dots, x_n) := t,$$

where the term t (normally) contains x_1, x_2, \dots, x_n as free variables.

- E.g., $f(x, y) := \sqrt{x^2 + y^2}$.
- Explicit definition of an n -ary predicate P :

$$P(x_1, x_2, \dots, x_n) :\Leftrightarrow A,$$

where the statement A (normally) contains x_1, x_2, \dots, x_n as free variables.

- E.g., $P(x, y) :\Leftrightarrow (x < y)$.

Warning

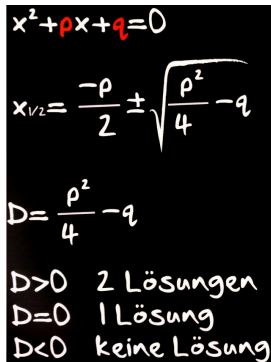
The definiendum does not occur in the definiens of an explicit definition of a function f or predicate P ! That is, the symbols f and P do not appear on the right-hand side.

Definitions: The Symbols “:=” and “:⇔”

- It is common to use the special symbols $:=$ and $:⇔$ for definitions, where the symbol “:” appears on the side of the definiendum.
- Thus, one can also write $=:$ or $⇔:$ to indicate that the definiendum is on the right-hand side.
- This is very good practice since
 - it makes it immediately obvious to the reader that what follows constitutes a definition rather than some lemma or claim,
 - it shows beyond doubt what is the definiens and what is the definiendum, and
 - it forces the author to decide whether or not something is a consequence of prior knowledge or some newly introduced entity.
- However, if “:=” or “:⇔” are used once in a text then they have to be used for absolutely all definitions in that text!!

Definitions: The Symbols “:=” and “:⇔”

- Poster seen in a tutoring institute at Salzburg:



A handwritten poster on a black background. At the top, the equation $x^2 + px + q = 0$ is written, with p and q in red. Below it, the quadratic formula is written: $x_{1/2} = \frac{-p}{2} \pm \sqrt{\frac{p^2}{4} - q}$. Then, the discriminant is defined: $D = \frac{p^2}{4} - q$. Finally, three cases are listed: $D > 0$ 2 Lösungen, $D = 0$ 1 Lösung, and $D < 0$ keine Lösung.

- Can $x_{1/2}$ be derived?
- Can D be derived?

- Better formalism:

- The roots x_1, x_2 of the second-degree polynomial equation $x^2 + px + q = 0$, with $p, q \in \mathbb{R}$, are obtained as follows:

$$x_{1/2} := -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$

- With $D := p^2 - 4q$ we get

$$D \begin{cases} > \\ = \\ < \end{cases} 0 \begin{cases} 2 \text{ distinct real roots,} \\ 1 \text{ real root,} \\ 0 \text{ no real roots.} \end{cases}$$

Recursive Definitions

- Aka: *Inductive* definition.

- How can we state

x is ancestor of y if x is parent of y, or if x is parent of parent of y, or if x is parent of parent of parent of y, or if ...

in a form that does not need to resort to an ellipsis "...” ?

- Recursive definitions (typically) consist of two parts:
 - a *basis* in which the definiendum does not occur in the definiens, and
 - an *inductive step* in which the definiendum does occur.
- E.g.,

x is an ancestor of y if x is parent of y or x is ancestor of parent of y.

Warning

To avoid infinite circles, the definiendum must not occur in the basis!



Recursive Definitions: Sum and Product

- Consider k real numbers $a_1, a_2, \dots, a_k \in \mathbb{R}$, together with some $m, n \in \mathbb{N}$ such that $1 \leq m, n \leq k$.

$$\sum_{i=m}^n a_i := \begin{cases} 0 & \text{if } n < m \\ a_m & \text{if } n = m \\ (\sum_{i=m}^{n-1} a_i) + a_n & \text{if } n > m \end{cases}$$

$$\prod_{i=m}^n a_i := \begin{cases} 1 & \text{if } n < m \\ a_m & \text{if } n = m \\ (\prod_{i=m}^{n-1} a_i) \cdot a_n & \text{if } n > m \end{cases}$$

- Consider a real number $a \in \mathbb{R}$ and a natural number $n \in \mathbb{N}_0$.

$$a^n := \begin{cases} 1 & \text{if } n = 0 \text{ and } a \neq 0 \\ a & \text{if } n = 1 \\ a^{n-1} \cdot a & \text{if } n > 1 \end{cases}$$

Recursive Definitions: Factorial and Fibonacci

Definition 1 (Factorial, Dt.: Fakultät, Faktorielle)

For $n \in \mathbb{N}_0$,

$$n! := \begin{cases} 1 & \text{if } n \leq 1, \\ n \cdot (n-1)! & \text{if } n > 1. \end{cases}$$

n	0	1	2	3	4	5	6	7	8	9	10
$n!$	0	1	2	6	24	120	720	5040	40320	362880	3628800

Definition 2 (Fibonacci numbers)

For $n \in \mathbb{N}_0$,

$$F_n := \begin{cases} 0 & \text{if } n = 0, \\ 1 & \text{if } n = 1, \\ F_{n-1} + F_{n-2} & \text{if } n \geq 2. \end{cases}$$

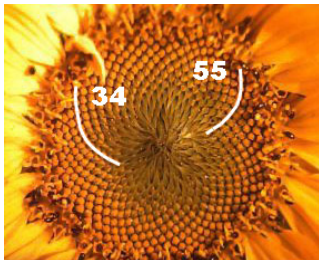
n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
F_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610

Fibonacci Numbers

- The Fibonacci numbers are named after Leonardo da Pisa (1180?–1241?), aka “figlio di Bonaccio”.
- The Fibonacci numbers have been studied extensively; they exhibit lots of interesting mathematical properties. For instance,

$$\lim_{n \rightarrow \infty} \frac{F_{n+1}}{F_n} = \phi.$$

- The Fibonacci numbers may also be found in nature: The numbers of spirals of sunflower heads are given by subsequent Fibonacci numbers.



[Image credit: [Wikipedia.](#)]

Caveats When Formulating Definitions

- Definitions like

$$P(x) :\Leftrightarrow (x < 2y) \quad \text{or} \quad P(x, y, z) :\Leftrightarrow (x < 2y)$$

can be seen as syntactically correct but they are semantically problematic!

Rule of thumb

All arguments of the definiendum have to appear as free variables in the definiens, and vice versa!

Warning

An entity introduced in a definition has to be free of internal inconsistencies and free of contradictions with prior facts.

- E.g., assume that for $\frac{m}{n}, \frac{p}{q} \in \mathbb{Q}$, with $m, p \in \mathbb{N}$ and $n, q \in \mathbb{N} \setminus \{0\}$, we define

$$\frac{m}{n} \# \frac{p}{q} := \frac{m+p}{n+q}.$$

- Then $\frac{1}{1} \# \frac{2}{3} = \frac{3}{4}$, but $\frac{2}{2} \# \frac{2}{3} = \frac{4}{5}$.
- Since $\frac{1}{1} = \frac{2}{2}$, we conclude $\frac{4}{5} = \frac{3}{4}$, and, thus, $0 = 1$. Yikes!



Definition 3 (Proof, Dt.: Beweis)

To *prove* a statement means to derive it from axioms (or postulates) and other previously established theorems by means of rules of logic.

- Common symbols to mark the end of a proof: \square , *qued* or *qed* (as an abbreviation for the Latin words “*quod erat demonstrandum*”, i.e., for “what was to be shown”).
- Note the difference between the English words “the proof” and “to prove”.

Definition 4 (Theorem, Dt.: Satz, Theorem)

A statement is a *theorem* if it has been proved. If the statement is of the form $H \Rightarrow C$ then we call H the *hypothesis* and C the *conclusion*.

- Of course, a theorem may involve quantifiers. E.g., $\forall x \ H(x) \Rightarrow C(x)$.
- Depending on the importance of the result, terms like *lemma* (Dt.: Lemma, Hilfssatz) or *corollary* (Dt.: Korollar) are also used instead of “theorem”.
- A *conjecture* is a statement which has not yet been proved or disproved.
- The status of a conjecture may remain unknown for decades or even centuries: Fermat’s Last Theorem was stated by Pierre de Fermat in 1637 and proved by Andrew Wiles (with the help of Richard Taylor) in 1993–1995.

Syntactical Proof Techniques

- *Syntactical proof techniques* are proof techniques based on the analysis of the syntactical structure of a statement.
- Syntactical proof techniques allow us to reason about statements and to simplify statements with no or very little “understanding” of their mathematical meaning.
- In particular, syntactical proof techniques allow us to split complicated proofs into simpler proofs, without any need for an ingenious idea for how to carry out a specific proof.
- On the next slides we will study the standard proof situation $H \Rightarrow C$, and formulate rules which depend on the syntax of H and/or C .
- Recall the truth table for “ \Rightarrow ”:

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

$H \Rightarrow C$

... is true if either H is false (and C arbitrary) or if C is true for H being true.

Syntactical Proof Techniques for $H \Rightarrow C$

- If conclusion C is of the form $(A \wedge B)$:
 - Prove A under the assumption H ; and
 - Prove B under the assumption H .
- If conclusion C is of the form $(A \vee B)$:
 - Add $\neg A$ to the assumption H and prove B . That is, assume both H and $\neg A$ to be true and use this to prove B .
 - Alternatively, add $\neg B$ to the assumption H and prove A .
- If conclusion C is of the form $(A \Rightarrow B)$:
 - Add A to the assumption H and prove B .
- If conclusion C is of the form $(A \Leftrightarrow B)$:
 - Prove $A \Rightarrow B$ under the assumption H ; and
 - Prove $B \Rightarrow A$ under the assumption H .

Warning

In all the rules on this slide, A and B must not be part of a quantified formula. (Otherwise, get rid of the quantifier first!)

Syntactical Proof Techniques for $H \Rightarrow C$

- If conclusion C is of the form $(\forall x \ A)$:
 - Proof technique: Let x_0 be arbitrary but fixed (Dt.: “beliebig aber fix”). From now on, x_0 can be treated as a constant!
 - It remains to prove $A[x_0/x]$ under the assumption H .
 - Often one does not trouble to explicitly label the particular arbitrary-but-fixed choice of x as, say, x_0 but only states that x is now regarded to be fixed.

Warning

The crucial point is that x_0 has to be arbitrary, and the proof may not depend on the particular choice of x_0 !

- The symbol x_0 may not occur anywhere in A , in the hypothesis H , or in some other part of the conclusion.
- We are not allowed to make any assumptions on x_0 except for those that hold for all x in the universe of discourse.

- If conclusion C is of the form $(\exists x \ A)$:
 - *Constructive Proof* (Dt.: konstruktiver Beweis):
 - It “suffices” to find a suitable x_0 such that $A[x_0/x]$ if H .
 - Such an x_0 is called the “solving term”.
 - *Existential Proof* (Dt.: Existenzbeweis):
 - Prove that some suitable x_0 exists.
 - No need to “construct” x_0 explicitly.
- E.g., suppose that we want to prove the following claim: The polynomial $p(x) := x^3 - x^2 + x - 1$ has a real root over \mathbb{R} .

Proof (constructive): Factoring $p(x)$ yields $p(x) = (x - 1)(x^2 + 1)$. Thus, we learn that $x = 1$ is a real root. □

Proof (existential): We have $p(2) = 5 > 0$ and $p(0) = -1 < 0$. Since p is continuous on the closed interval $[0, 2]$, the Intermediate Value Theorem tells us that there exists a real number x strictly between 0 and 2 such that $p(x) = 0$. □

- If conclusion C is of the form $(\exists!x \ A)$:
 - Prove that such an x exists.
 - Prove its uniqueness.
- If hypothesis H is of the form $(\exists x \ A)$:
 - Let x_0 such that $A[x_0/x]$.
 - Add $A[x_0/x]$ to knowledge.
 - Again: x_0 must not occur anywhere else in H or C !

- On many occasions a conjecture will not be stated in formal terms but by using a natural language.
- Then one has to *decode* the natural-language formulation and *translate* it into formal terms!
- Natural-language synonyms for $A \Rightarrow B$:
 - B if A ,
 - A only if B ,
 - If A then B ,
 - A is sufficient for B ,
 - B is necessary for A .
- Natural-language synonyms for $A \Leftrightarrow B$:
 - A if and only if B , A genau dann wenn B ,
 - A is necessary and sufficient for B , A ist notwendig und hinreichend für B .

Equivalence Transformations

- First attempt to prove $(\forall n \in \mathbb{N} \quad \frac{2n+1}{n+1} \geq \frac{3}{2})$:

$$\begin{aligned}\frac{2n+1}{n+1} &\geq \frac{3}{2} \\ 2(2n+1) &\geq 3(n+1) \\ 4n+2 &\geq 3n+3 \\ n &\geq 1\end{aligned}$$

- Second refined attempt to prove $(\forall n \in \mathbb{N} \quad \frac{2n+1}{n+1} \geq \frac{3}{2})$:

$$\begin{aligned}\frac{2n+1}{n+1} &\geq \frac{3}{2} && | \cdot 2(n+1) \\ \Rightarrow 2(2n+1) &\geq 3(n+1) \\ \Rightarrow 4n+2 &\geq 3n+3 && | - (3n+2) \\ \Rightarrow n &\geq 1\end{aligned}$$

- Correct proof of $(\forall n \in \mathbb{N} \quad \frac{2n+1}{n+1} \geq \frac{3}{2})$:

$$\begin{aligned}\frac{2n+1}{n+1} &\geq \frac{3}{2} && | \cdot 2(n+1) \\ \Leftrightarrow 2(2n+1) &\geq 3(n+1) \\ \Leftrightarrow 4n+2 &\geq 3n+3 && | - (3n+2) \\ \Leftrightarrow n &\geq 1\end{aligned}$$

- Another way to prove ($\forall n \in \mathbb{N} \quad \frac{2n+1}{n+1} \geq \frac{3}{2}$): We start with the term $\frac{2n+1}{n+1}$ and construct a series of inequalities that ends in $\frac{3}{2}$.

We get for all $n \in \mathbb{N}$

$$\frac{2n+1}{n+1} = \frac{2(n+1)}{n+1} - \frac{1}{n+1} = 2 - \frac{1}{n+1} \geq 2 - \frac{1}{2} = \frac{3}{2}.$$

- Similarly we can prove ($\forall n \in \mathbb{N} \setminus \{1, 2\} \quad 2n^2 \geq (n+1)^2$):

$$2n^2 = n^2 + n^2 \stackrel{n \geq 3}{\geq} n^2 + 3n \geq n^2 + 2n + 1 = (n+1)^2$$

Equivalence Transformations: Caveats

- Let $a, b \in \mathbb{N}$ be equal natural numbers. We “prove” that $1 = 2$:

$$\begin{array}{lll} & a = b & | \cdot a \\ \Leftrightarrow & a^2 = ab & | - b^2 \\ \Leftrightarrow & a^2 - b^2 = ab - b^2 & \\ \Leftrightarrow & (a - b) \cdot (a + b) = b \cdot (a - b) & | \div (a - b) \\ \Leftrightarrow & (a + b) = b & | a = b \\ \Leftrightarrow & (b + b) = b & \\ \Leftrightarrow & 2b = b & | \div b \\ \Leftrightarrow & 2 = 1 & \end{array}$$

- And here comes a “proof” of $4 = 5$: Let $x := 4$ and $y := 5$. Then

$$\begin{array}{lll} & x + y = 9 & | \cdot (x - y) \\ \Leftrightarrow & x^2 - y^2 = 9x - 9y & | + \frac{81}{4} - 9x + y^2 \\ \Leftrightarrow & x^2 - 9x + \frac{81}{4} = y^2 - 9y + \frac{81}{4} & \\ \Leftrightarrow & (x - \frac{9}{2})^2 = (y - \frac{9}{2})^2 & | \sqrt{} \\ \Leftrightarrow & x - \frac{9}{2} = y - \frac{9}{2} & | + \frac{9}{2} \\ \Leftrightarrow & x = y & \\ \Leftrightarrow & 4 = 5 & \end{array}$$

Equivalence Transformations: Caveats

- In the same way we can “prove” that $0 = 2$. We start with the well-known identity $\cos^2 x = 1 - \sin^2 x$, which holds for all $x \in \mathbb{R}$:

$$\begin{array}{lll} \cos^2 x = 1 - \sin^2 x & & | \sqrt{} \\ \iff \cos x = \sqrt{1 - \sin^2 x} & & | + 1 \\ \iff 1 + \cos x = 1 + \sqrt{1 - \sin^2 x} & & | x := \pi \\ \iff 1 - 1 = 1 + \sqrt{1 - 0} & & \\ \iff 0 = 2 & & \end{array}$$

- Playing with square roots also allows to “prove” that $1 = -1$:

$$1 = \sqrt{1} = \sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1} = i \cdot i = i^2 = -1.$$

- We attempt to solve the equation $\sqrt{x^2 - 1} = \sqrt{x - 1}$ over \mathbb{R} :

$$\begin{array}{lll} \sqrt{x^2 - 1} = \sqrt{x - 1} & & |^2 \\ \iff x^2 - 1 = x - 1 & & | + 1 - x \\ \iff x^2 - x = 0 & & \\ \iff x(x - 1) = 0 & & \end{array}$$

Hence, we seem to get $\{0, 1\}$ as set of solutions.
However, the equation is not even defined for $x < 1$.

Advice and Warnings

- Squaring is not an equivalence transformation!
- If squaring is applied for solving an equation then all candidate solutions found need to be tested with the original equation.
- Taking a square root is only permissible if both signs are considered. That is, $\sqrt{x^2}$ yields $\pm x$ or $|x|$.
- A division by x is only permissible if $x \neq 0$ can be assured.
- Multiplication by a negative number is not an equivalence transformation for inequalities.
- In general, a relation $a \circ b$ may only be replaced by a new relation $a' \circ b'$ if one can argue that $(a \circ b) \Leftrightarrow (a' \circ b')$.
- It is advisable to prove $a \circ b$, where $\circ \in \{=, <, >, \leq, \geq\}$, by constructing a chain $a_0 \circ a_1 \circ a_2 \circ \dots \circ a_n$, with $a_0 = a$ and $a_n = b$, for some $n \in \mathbb{N}$.

- “W.l.o.g.” for avoiding similar cases.
- Direct enumeration.
- Case analysis.
- Direct proof.
- Proof by contrapositive.
- Proof by contradiction.
- Indirect proof.
- Disproving conjectures.

- “W.l.o.g., A ” means “Without loss of generality, we assume A ”.
- Dt.: O.B.d.A. (“Ohne Beschränkung der Allgemeinheit”).
- This means that we could also carry on without the particular assumption A , and would either
 - have to consider cases that are handled very similarly, or
 - could easily convert the general case to this special case.
- That is, a “w.l.o.g.” assumption allows us to save space/paper by avoiding to replicate portions of a proof that differ only in trivial aspects.

Warning

Do not use “w.l.o.g.” unless *you could* indeed *explain* explicitly how to carry on without that assumption!

- *Direct Enumeration*

- E.g.: The conjecture

$$2p + 1 \text{ is prime for all } p \in \{2, 3, 5\}$$

can be proved by considering all finitely many possible values for p .

- Note: Direct enumeration only works if the set given is finite!

Types of Proofs: Case Analysis

- Aka *Proof by Exhaustion*.
- Dt.: Fallunterscheidung.
- In order to prove $H \Rightarrow C$, it suffices to prove

$$A_1 \vee A_2 \vee \dots \vee A_k$$

for some statements A_1, A_2, \dots, A_k , and to prove

$$(H \wedge A_1) \Rightarrow C,$$

$$(H \wedge A_2) \Rightarrow C,$$

$$\vdots$$

$$(H \wedge A_k) \Rightarrow C.$$

Warning

It is essential to guarantee that $A_1 \vee A_2 \vee \dots \vee A_k$ holds, i.e., that no case is missing!

Types of Proofs: Sample Case Analysis

- Suppose that we want to prove the following claim: For all $n \in \mathbb{N}_0$ the number 7 divides $n^7 - n$ without remainder. E.g., for $n = 3$, we get $3^7 - 3 = 2184 = 7 \cdot 312$.

Proof: Factoring $n^7 - n$ yields

$$n^7 - n = n(n^6 - 1) = n(n^3 - 1)(n^3 + 1) = n(n - 1)(n^2 + n + 1)(n + 1)(n^2 - n + 1).$$

Let $n = 7q + r$ with $q, r \in \mathbb{N}_0$ and $0 \leq r \leq 6$. We consider seven cases, depending on whether $r = 0, 1, 2, 3, 4, 5$ or 6 .

Case $n = 7q$: Then the factor n of $n^7 - n$ is divisible by 7.

Case $n = 7q + 1$: Then the factor $n - 1 = 7q$ of $n^7 - n$ is divisible by 7.

Case $n = 7q + 2$: Then $n^2 + n + 1 = (7q + 2)^2 + (7q + 2) + 1 = 49q^2 + 35q + 7$ is divisible by 7.

Case $n = 7q + 3$: Then $n^2 - n + 1 = (7q + 3)^2 - (7q + 3) + 1 = 49q^2 + 35q + 7$ is divisible by 7.

Case $n = 7q + 4$: Then $n^2 + n + 1 = (7q + 4)^2 + (7q + 4) + 1 = 49q^2 + 63q + 21$ is divisible by 7.

Case $n = 7q + 5$: Then $n^2 - n + 1 = (7q + 5)^2 - (7q + 5) + 1 = 49q^2 + 63q + 21$ is divisible by 7.

Case $n = 7q + 6$: Then $n + 1 = 7q + 7$ is divisible by 7.



Types of Proofs: Direct Proof

- Dt.: direkter Beweis.
- We want to prove $H \Rightarrow C$:
 - We build a chain of reasoning that starts at H and ends in C .
 - This approach is the classical example of deductive reasoning, where a logically valid sequence of steps establishes the truth of C under the assumption of H .
- Suppose we want to prove $(\forall x, y \in \mathbb{R}^+ \ (x < y) \Rightarrow (x^2 < y^2))$.

Proof: (Direct Proof)

Let $x_0, y_0 \in \mathbb{R}^+$ be arbitrary but fixed, with $x_0 < y_0$.

We have $x_0 < y_0$, and therefore $x_0^2 = x_0 \cdot x_0 < y_0 \cdot x_0$. Since $x_0 < y_0$ we know $y_0 \cdot x_0 < y_0^2$, and obtain $x_0^2 < y_0 \cdot x_0 < y_0^2$, which finally establishes $x_0^2 < y_0^2$. □

Types of Proofs: Proof by Contrapositive

- Dt.: Umkehrschluss, Kontraposition.
- We want to prove $H \Rightarrow C$:
 - In order to prove $H \Rightarrow C$ we build a (direct) proof for $(\neg C \Rightarrow \neg H)$.
- Again, suppose we want to prove $(\forall x, y \in \mathbb{R}^+ (x < y) \Rightarrow (x^2 < y^2))$.
Proof: Let $x_0, y_0 \in \mathbb{R}^+$ be arbitrary but fixed. We prove $(x_0^2 \geq y_0^2) \Rightarrow (x_0 \geq y_0)$ similar to the direct proof before. We get

$$0 \leq x_0^2 - y_0^2 = (x_0 - y_0)(x_0 + y_0),$$

which implies $y_0 \leq x_0$ since we may divide by the positive number $x_0 + y_0$. □

- Suppose we want to prove $H \Rightarrow (\exists x \ A)$.

Proof: Prove $(\forall x \ (\neg A)) \Rightarrow \neg H$. □

Warning

Make sure that the statements are negated correctly!



Types of Proofs: Proof by Contradiction

- Dt.: Widerspruchsbeweis.
- We want to prove $H \Rightarrow C$:
 - Formally, $(H \Rightarrow C) \equiv ((H \wedge \neg C) \Rightarrow \neg H)$.
 - Thus, assume $(H \wedge \neg C)$ and prove $\neg H$.
- Warning: As when proving the contrapositive it is essential to check twice that the statements are indeed negated correctly!

Types of Proofs: Indirect Proof

- Aka *Reductio ad absurdum*.
- Dt.: indirekter Beweis.
- We want to prove $H \Rightarrow C$.
 - Consider a statement R that is known to be true, like $0 \neq 1$.
 - Now assume $(H \wedge \neg C)$ and deduce $\neg R$, i.e., $0 = 1$.
 - This is absurd, and we conclude that $\neg C$ is false.
 - Formally, $(H \wedge \neg C \wedge R) \Rightarrow \neg R$.
 - This is of the form $(A \Rightarrow B)$, and we have $(A \Rightarrow B) \equiv T$, where $B \equiv F$. Thus, $A \equiv F$.

Note

Since an indirect proof is similar to a proof by contradiction, many textbooks treat it as one proof technique, or use the terms “reductio ad absurdum”, “indirect proof”, and “proof by contradiction” as synonyms.

- In a nutshell: If we manage to prove $\neg C \Rightarrow F$ to be true, then we have $\neg C \equiv F$ and, thus, $C \equiv T$.



Types of Proofs: Sample Indirect Proof

- Suppose that we want to prove that the polynomial equation $x^3 + x + 1 = 0$ has no rational solution.

Proof: Assume to the contrary that there exists a rational number $\frac{p}{q}$ which is a root of that polynomial. W.l.o.g., we may assume $\frac{p}{q}$ to be irreducible. (A rational number $\frac{p}{q}$ is irreducible if there exists no integer other than ± 1 that divides both p and q .) We get

$$0 = \frac{p^3}{q^3} + \frac{p}{q} + 1 = p^3 + pq^2 + q^3.$$

As statement R we take “0 is even”.

We do a case analysis, depending on whether p, q are even or odd:

Case p, q odd: Then $p^3 + pq^2 + q^3$ is odd, but 0 is even, yielding a contradiction to R .

Case p odd, q even: Then again $p^3 + pq^2 + q^3$ is odd; contradiction.

Case p even, q odd: Then again $p^3 + pq^2 + q^3$ is odd; contradiction.

Case p, q even: This is not possible since we assumed (rightfully) that $\frac{p}{q}$ is irreducible.



Disproving Conjectures

- Sometimes conjectures are false . . .
- If the conjecture is of the form $(\forall x \ A)$:
 - Then we can disprove this conjecture by showing $(\exists x \ \neg A)$.
 - The latter is proved if we can come up with a *counterexample* (Dt.: Gegenbeispiel) to the original claim.
 - E.g., the claim $\forall p \in \mathbb{P} \ (2p + 1) \in \mathbb{P}$ is shown to be false by testing $p := 7$. (Note, though, that it is true for $p = 2, 3, 5, 11, 23, \dots$)
 - Similarly, numbers of the form $2^{2^n} + 1$, for $n \in \mathbb{N}$, were once assumed to be primes. Indeed, this is correct for $n = 1, 2, 3, 4$ but $n := 5$ yields a counterexample:

$$2^{2^5} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417.$$

- If, however, the conjecture is of the form $(\exists x \ A)$:
 - Then a counterexample does not suffice!
 - Rather, to disprove this conjecture, we'd have to prove formally $(\forall x \ \neg A)$.

Caveat: Ex Falso Quodlibet!

- Consider the following lemma: Let $x \in \mathbb{R}$. If $\frac{x}{x^2+1} > 2$ then $x < \frac{1}{2}$.
- Formally: $\forall x \in \mathbb{R} \quad \left(\frac{x}{x^2+1} > 2 \right) \implies \left(x < \frac{1}{2} \right)$.

Proof: Let $x \in \mathbb{R}$ arbitrary but fixed and suppose that $\frac{x}{x^2+1} > 2$. This implies $x > 0$ and we get

$$\frac{1}{x} = \frac{x}{x^2} > \frac{x}{x^2+1} > 2, \quad \text{thus } \frac{1}{x} > 2 \text{ and, therefore, } x < \frac{1}{2}.$$



- Note, though, that this lemma is of little use for mathematics: The hypothesis is never true! We have

$$\frac{x}{x^2+1} > 2 \iff 0 > 2x^2 - x + 2 \iff 2x^2 - x + 2 < 0.$$

However, by a simple case analysis,

$$\text{if } x \leq 1 \text{ then } 2x^2 - x + 2 = 2x^2 + 1 + (1 - x) \geq 2x^2 + 1 > 0,$$

$$\text{if } x > 1 \text{ then } 2x^2 - x + 2 = x^2 + 2 + x(x - 1) \geq x^2 + 2 > 0.$$



The Pigeonhole Principle

- If n letters are posted to m pigeonholes, then
 - at least one pigeonhole receives more than one letter if $n > m$.
 - at least one pigeonhole remains empty if $n < m$.
 - each pigeonhole might receive exactly one letter if $n = m$.

Theorem 5 (Pigeonhole Principle, Dt.: Schubfachschluss)

Consider two finite sets A and B . There is a bijection between A and B if and only if A and B have the same number of elements. If A has more elements than B then every mapping from A to B will cause at least one element of B to be the target of two or more elements of A .

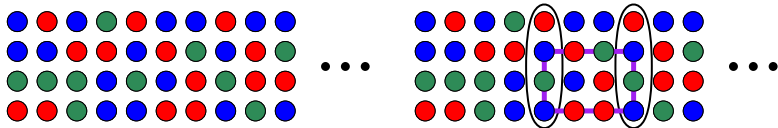
Corollary 6

For $n \in \mathbb{N}$ let $\mathcal{A}_n := \{1, 2, 3, \dots, n-1, n\} \subset \mathbb{N}$, and let \mathcal{B}_n denote an arbitrary set of n elements. Then, for all $n \in \mathbb{N}$ and all sets \mathcal{B}_n , no mapping from \mathcal{A}_{n+1} to \mathcal{B}_n is injective.

The Pigeonhole Principle: Sample Application

Lemma 7

Consider a rectangular grid of points which consists of four rows and 100 columns. Each point is colored with a color which is picked randomly among red, green and blue. Prove that there always exist four points of the same color that form the corners of a rectangle (with sides parallel to the grid), no matter how the coloring is done.



Proof: A column pattern is the top-to-bottom sequence of colors assigned to the points of a column of the grid. There are exactly $3^4 = 81$ different column patterns. Since there are more than 81 columns, we are guaranteed to have at least two columns with the same column pattern. Consider two such columns. Since there are four rows but only three colors, we conclude that two of the rows have the same color, thus giving us the four corners of the rectangle sought. \square

- Note: Just 19 columns suffice to guarantee the existence of such a rectangle.



The Pigeonhole Principle: A Hairy Application

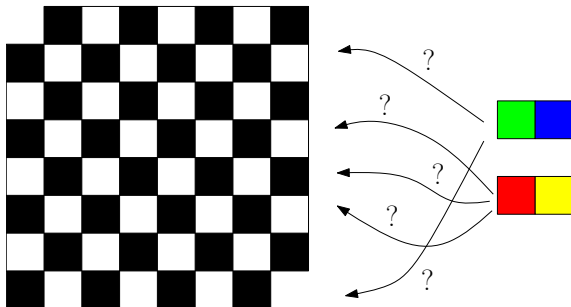
- Suppose there exists an upper limit for the number of hairs on the human skin per square centimeter, say 140 hairs.
- Taking 5 square meters as a reasonable upper limit for the skin area of a human, we conclude that a human has at most 7 000 000 hairs.
- Since Austria has (significantly) more than 7 000 001 inhabitants, we conclude that, by the *pigeonhole principle*, at least two inhabitants of Austria have exactly the same number of hairs.

#hairs	hairy ID numbers
0	1
1	2
\vdots	\vdots
7 000 000	7 000 001
	7 000 002
	7 000 003

It is impossible to map every inhabitant to his/her own "hair bin"!

Real-World Application: Chessboard Tilings Revisited

- Question: Can our modified chessboard be covered completely by 31 domino blocks of arbitrary color combinations?



- We observe that every permissible domino placement covers exactly one black square and one white square of the chessboard.
- Thus, all domino placements would establish a one-to-one mapping between black and white squares. However, there are 32 black squares and only 30 white squares! We conclude that our chessboard cannot be covered completely by domino blocks.

Real-World Application: Analysis of Lossless Data Compression

- Could one design an algorithm for lossless data compression that is guaranteed to compress every input data set to a truly smaller output? No!
- Assume that every file is represented as a string of bits of some arbitrary length. Suppose further that there exists a compression algorithm that transforms every file into a distinct file which is no longer than the original file, and that at least one file will be compressed into something that is shorter than itself.
- Let m be the least number such that there is a file f with length m bits that gets compressed to something shorter. Let n be the number of bits of the compressed version of f . Hence, $n < m$.
- Since $n < m$, every file of length n keeps its size during compression. There are 2^n many such files. Together with f we would have $2^n + 1$ files which all compress into one of the 2^n files of length n .
- By the pigeonhole principle there must exist some file f' of length n which is the output of the compression algorithm for two different inputs. That file f' cannot be decompressed reliably, which contradicts the assumption that the algorithm is lossless.
- Hence, no compression algorithm exists that compresses every input to a file of truly smaller size.



Numbers and Basics of Number Theory

- Natural Numbers
- Integers
- Rational Numbers
- Real Numbers
- Well-founded Induction

How Shall We Define Natural Numbers or Real Numbers?

- Three options:
 - 1 Ignore all formal details and presuppose an “intuitive” understanding of reals, integers, . . .
 - 2 Introduce the natural numbers, \mathbb{N} , and then construct a hierarchy of number systems: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.
 - 3 Set up the reals, \mathbb{R} , axiomatically and then define proper subsets for \mathbb{N} , \mathbb{Z} , \mathbb{Q} .
- What is the best approach for a course on (applied) discrete mathematics? Much scholarly debate — no consensus!
- We will start with introducing the natural numbers. However, since the gory details result in a lengthy discussion which provides little additional insight in \mathbb{N} — and this is no course on number theory — we base our introduction of \mathbb{N} on a simplified treatment of the so-called Peano axioms; see a book on number theory for a more formalized introduction of \mathbb{N} .
- Note: Make sure to recall algebraic structures if you are not (or no longer) familiar with them. (See, e.g., the course “Formale Systeme”).

Natural Numbers: \mathbb{N}

- Intuitively, the natural numbers \mathbb{N} are given by $\{1, 2, 3, 4, 5, \dots\}$ or by $\{0, 1, 2, 3, 4, 5, \dots\}$.
- Unfortunately, there is no general agreement on whether or not to include 0 . . .
- Paulo Ribenboim (1996): "Let P be a set of natural numbers; whenever convenient, it may be assumed that 0 is an element of P ."

Convention

In this course we adopt the following convention:

$$\mathbb{N} := \{1, 2, 3, 4, 5, \dots\} \quad \text{and} \quad \mathbb{N}_0 := \{0, 1, 2, 3, 4, 5, \dots\}.$$

- Caution: Read a text carefully to learn what an author means by "natural number". In particular, watch for clues such as terms like "positive natural numbers" (which indicates that zero is included) or statements like " n is a natural number, so it must be greater than zero" (which indicates that zero is not included).
- If one treats 0 as an element of \mathbb{N} then $\{1, 2, 3, 4, 5, \dots\}$ is often denoted by \mathbb{N}^* .



Definition 8 (Partial order, Dt.: Halbordnung)

A *partial order* on a set S is a binary relation \preceq , i.e., a subset of $S \times S$, such that the following three properties hold for all $a, b, c \in S$:

- 1 Reflexivity: $a \preceq a$.
- 2 Anti-symmetry: $(a \preceq b \wedge b \preceq a) \Rightarrow a = b$.
- 3 Transitivity: $(a \preceq b \wedge b \preceq c) \Rightarrow a \preceq c$.

If \preceq is a partial order on S then (S, \preceq) is called a *partially ordered set*, aka a *poset*.

Definition 9 (Strict partial order, Dt.: strikte Halbordnung)

A binary relation \prec on a set S forms a *strict partial order* on S if the following two properties hold for all $a, b, c \in S$:

- 1 Irreflexivity: $\neg(a \prec a)$.
- 2 Transitivity: $(a \prec b \wedge b \prec c) \Rightarrow a \prec c$.

- A strict partial order is always *asymmetric*: If $a \prec b$ then $\neg(b \prec a)$.

$a \prec b \wedge b \prec a \xrightarrow{\text{trans.}} a \prec a$, in contradiction to the irreflexivity: $\neg(a \prec a)$



Theorem 10

There is a one-to-one correspondence between non-strict and strict partial orders. Let S be a set and $a, b \in S$.

- 1 If \preceq is a non-strict partial order on S then the corresponding strict partial order " \prec " on S is the *reflexive reduction* given by

$$a \prec b \quad :\Leftrightarrow \quad a \preceq b \text{ and } a \neq b.$$

- 2 If, on the other hand, \prec is a strict partial order on S then the corresponding non-strict partial order " \preceq " on S is the *reflexive closure* given by

$$a \preceq b \quad :\Leftrightarrow \quad a \prec b \text{ or } a = b.$$

- As a notational convention, we omit the indication of an equality sign if we refer to a strict order, e.g., we write \prec rather than \preceq or \subset rather than \subseteq .

- E.g., (\mathbb{Z}, \supseteq) with (the non-strict order) \supseteq as defined below forms a poset:

if a and b are even: $a \supseteq b \Leftrightarrow a \geq b$

if a and b are odd: $a \supseteq b \Leftrightarrow a \leq b$

- The subset relation, \subset , on the powerset $\mathcal{P}(X)$ of a set X is a strict partial order.

Definition 11 (Dual order, Dt.: duale Ordnung)

Let (S, \preceq) resp. $(S, <)$ be a (strict) poset. The *dual order* (or *reverse order*) on S , \succeq resp. \succ , is defined as follows for $a, b \in S$:

$$a \succeq b \Leftrightarrow b \preceq a \qquad a \succ b \Leftrightarrow b < a.$$

Definition 12 (Minimal element, Dt.: minimales Element)

Let (S, \preceq) be a poset and $T \subseteq S$. An element $a \in T$ is a *minimal element* of T if no $b \in T \setminus \{a\}$ exists such that $b \preceq a$.

Definition 13 (Least element, Dt.: kleinstes Element, Minimum)

Let (S, \preceq) be a poset and $T \subseteq S$. An element $a \in T$ is a *least element* (or *minimum*) of T if $\forall b \in T \setminus \{a\} \quad a \preceq b$.

Definition 14 (Maximal element, Dt.: maximales Element)

Let (S, \preceq) be a poset and $T \subseteq S$. An element $a \in T$ is a *maximal element* of T if no $b \in T \setminus \{a\}$ exists such that $a \preceq b$.

Definition 15 (Greatest element, Dt.: Maximum)

Let (S, \preceq) be a poset and $T \subseteq S$. An element $a \in T$ is a *greatest element* (or *maximum*) of T if $\forall b \in T \setminus \{a\} \quad b \preceq a$.

- Note: If a minimum or maximum exists then the anti-symmetry ensures that it is unique. Minimal or maximal elements need not be unique, though.

Definition 16 (Total order, Dt.: totale Ordnung)

A binary relation \preceq on a set S forms a *total order* (or *linear order*) on S if the following three statements hold for all $a, b, c \in S$:

- 1 Totality: $a \preceq b \vee b \preceq a$.
- 2 Anti-symmetry: $(a \preceq b \wedge b \preceq a) \Rightarrow a = b$.
- 3 Transitivity: $(a \preceq b \wedge b \preceq c) \Rightarrow a \preceq c$.

If \preceq is a total order on S then (S, \preceq) is called a *totally ordered set*.

- Note that (1) in Def. 16 implies reflexivity: $a \preceq a$ for all $a \in S$.
- That is, a total order on S is a (non-strict) partial order such that every pair of elements of S is comparable.

Definition 17 (Well-order, Dt.: Wohlordnung)

A total order \preceq on a set S forms a *well-order* if every non-empty subset of S has a least element.

Natural Numbers and Peano's Axioms

- The following definition of \mathbb{N} is based on a simplified version of Peano's Axioms, as proposed by Giuseppe Peano (1858–1932) in 1889.

Definition 18 (Natural numbers, Dt.: natürliche Zahlen)

The set of all *natural numbers*, \mathbb{N} , together with an order relation \leq , is a totally ordered set defined as follows:

- (N1) $1 \in \mathbb{N}$.
- (N2) $\forall n \in \mathbb{N} \quad n + 1 \in \mathbb{N} \quad \wedge \quad n < n + 1$.
- (N3) $\forall n \in \mathbb{N}, n \neq 1 \quad \exists m \in \mathbb{N} \quad n = m + 1$.
- (N4) Every non-empty subset of \mathbb{N} has a least element.

The number $n + 1$ is called the *successor* of n , and sometimes denoted by $\text{succ}(n)$.

- **N1** together with **N2** establish the infinite sequence $1 < 2 < 3 < \dots$
- **N3** guarantees that every $n \in \mathbb{N}$ (except 1) is the successor of some number in \mathbb{N} .
- The so-called *well-ordering principle*, **N4**, weeds out numbers like $\frac{1}{2}$ or π .
- One can show that the standard algebraic rules are compatible with the conditions imposed on \mathbb{N} , and that algebra and order interact smoothly within \mathbb{N} .
- One can also show that (up to a renaming of elements) there is only one set that fulfills all conditions of Def. 18. Hence, \mathbb{N} is uniquely defined.



The Principle of Mathematical Induction

- Franciscus Maurolicus (1494–1575), an abbot of Messina, seems to have been first to use induction for proving a theorem. (He proved $\sum_{i=1}^n (2i - 1) = n^2$.)
- Blaise Pascal (1623–1662) used induction to prove a relation among binomial coefficients.
- Augustus de Morgan (1806–1871) was the first to use the term “induction”.
- Today’s view of induction is based on the work of Giuseppe Peano (1858–1932).

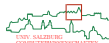
Theorem 19

Consider a set $K \subseteq \mathbb{N}$ and assume that it is *inductive*, i.e., that

- 1 $1 \in K$,
- 2 $\forall k \in K \ (k + 1) \in K$.

Then $K = \mathbb{N}$.

Proof: Suppose that $K \neq \mathbb{N}$, i.e., $K \subset \mathbb{N}$. Hence, $K' := \mathbb{N} \setminus K$ is not empty. By the well-ordering principle, (N4), K' has a least element, n . Since $n \neq 1$ there exists a number $k \in \mathbb{N}$ such that $k + 1 = n$. As n is the least element of K' , we have $k \in K$. Applying modus ponens yields $k + 1 = n \in K$, i.e., a contradiction.



Theorem 20 (Weak Principle of Induction (W.P.I.))

Consider a predicate P over \mathbb{N} .

If

$$P(1)$$

and if

$$\forall k \in \mathbb{N} \quad (P(k) \Rightarrow P(k+1))$$

then

$$\forall n \in \mathbb{N} \quad P(n).$$

Proof: Define $K := \{n \in \mathbb{N} : P(n)\}$. We have

- 1 $1 \in K$, and
- 2 $\forall k \in K \quad (k+1) \in K$.

Thus, Thm. 19 is applicable and we conclude $K = \mathbb{N}$. That is, the predicate P holds for all natural numbers. □



Three Main Steps of a Proof by Induction

- Suppose that we want to prove

$$\forall n \in \mathbb{N} \quad P(n),$$

for some predicate P over \mathbb{N} .

- We proceed as follows:

- 1 *Induction basis* (“IB”): A basis step is done, i.e., $P(1)$ is proved to be true.
- 2 *Induction hypothesis* (“IH”): We assume $P(k)$ to be true for an arbitrary but fixed $k \in \mathbb{N}$.
- 3 *Inductive step* (“IS”): We prove $P(k + 1)$ based on the knowledge that $P(k)$ is true.

Gauß' Problem Revisited: Sample Inductive Proof

- We claim that $\sum_{i=1}^n i = \frac{n \cdot (n+1)}{2}$ holds for all $n \in \mathbb{N}$.

Proof: We use induction to prove our claim as follows:

- We define a suitable predicate P :

$$\forall n \in \mathbb{N} \quad \left(P(n) :\Leftrightarrow \sum_{i=1}^n i = \frac{n \cdot (n+1)}{2} \right).$$

- *Induction basis (IB):* We establish the truth of $P(1)$:

$$\sum_{i=1}^1 i = 1 = \frac{1 \cdot 2}{2}.$$

- *Induction hypothesis (IH):* Assume $P(k)$ true for an arbitrary but fixed $k \in \mathbb{N}$. That is, we assume

$$\sum_{i=1}^k i = \frac{k \cdot (k+1)}{2}.$$

Proof (cont'd):

- *Inductive step (IS):* We have to prove $P(k + 1)$ based on the induction hypothesis. That is, we have to prove

$$\sum_{i=1}^{k+1} i = \frac{(k+1) \cdot (k+2)}{2}.$$

We get

$$\begin{aligned}\sum_{i=1}^{k+1} i &= \sum_{i=1}^k i + (k+1) \\ &\stackrel{\text{I.H.}}{=} \frac{k \cdot (k+1)}{2} + (k+1) \\ &= \frac{k \cdot (k+1) + 2(k+1)}{2} \\ &= \frac{(k+1) \cdot (k+2)}{2}.\end{aligned}$$



Theorem 21 (Strong Principle of Induction (S.P.I.))

Consider a predicate P over \mathbb{N} .

If

$$P(1)$$

and if

$$\forall k \in \mathbb{N} \quad [(P(1) \wedge P(2) \wedge \dots \wedge P(k)) \Rightarrow P(k+1)]$$

then

$$\forall n \in \mathbb{N} \quad P(n).$$

- Obviously, all theorems that can be proved by W.P.I. can also be proved by S.P.I., and one can actually show the equivalence of W.P.I. and S.P.I.

Theorem 22 (S.P.I. with Larger Base)

Consider a predicate P over \mathbb{N} , and let $m \in \mathbb{N}$.

If

$$P(m)$$

and if

$$\forall(k \in \mathbb{N}, k \geq m) [(P(m) \wedge P(m+1) \wedge \dots \wedge P(k)) \Rightarrow P(k+1)]$$

then

$$\forall(n \in \mathbb{N}, n \geq m) P(n).$$

Proof: We define a new predicate P' over \mathbb{N} with

$$P'(n) \quad :\Longleftrightarrow \quad P(m-1+n) \quad \text{for all } n \in \mathbb{N},$$

and apply the standard S.P.I. □

- We could also carry out induction for smaller base values. That is, induction works for claims over \mathbb{N}_0 . (And even for negative base values!)



Mathematical Induction: Caveats

- We may not assume anything in the inductive step $n \rightarrow n + 1$ besides that $P(n)$ holds and, of course, the standard properties of \mathbb{N} .
- The inductive step alone does not suffice! By carrying out only the inductive step one can “prove” that $\forall n \in \mathbb{N} \ n = n + 5$. Let $k \in \mathbb{N}$ be arbitrary but fixed and assume as I.H. that $k = k + 5$:

$$k + 1 \stackrel{\text{I.H.}}{=} (k + 5) + 1 = (k + 1) + 5.$$

Thus, proving the base is mandatory!

- Several base cases alone do not suffice! E.g., consider

$$\forall n \in \mathbb{N} \ (n^2 - n + 41 \text{ is a prime}).$$

For n up to 20, the number $n^2 - n + 41$ actually is a prime, but this is not true for $n = 41$. Thus, proving the inductive step is mandatory!



Mathematical Induction: Caveats

- George Pólya (1887–1985): "All cats have the same color", or $\forall n \in \mathbb{N}$ (for all sets S of n cats (all cats of S have the same color)).
- We use induction to prove this claim.
 - IB $k = 1$: obviously true.
 - IH: For all sets S of k cats, all cats of S have the same color, for k arbitrary but fixed.
 - IS from k to $k + 1$: Consider a set S of $k + 1$ cats, and let A and B be two subsets of S such that

$$|A| = |B| = k \quad \text{and} \quad A \cup B = S.$$

Using the induction hypothesis and the transitivity of the equivalence, we conclude that all cats of the set S have the same color!

As nature shows, this "proof" is seriously flawed . . .



Mathematical Induction: Caveats

- We claim that $2 \cdot n = 0$ for all $n \in \mathbb{N}_0$.
- We use induction to prove this claim:
 - IB $k = 0$: obviously true.
 - IH: Suppose that the claim holds for all $k \in \mathbb{N}_0$ with $k \leq n$, for some arbitrary but fixed $n \in \mathbb{N}_0$.
 - IS from n to $n + 1$: We write $n + 1$ as $n + 1 = k_1 + k_2$, where $k_1, k_2 \in \mathbb{N}_0$ with $k_1, k_2 \leq n$. Then

$$2 \cdot (n + 1) = 2 \cdot (k_1 + k_2) = 2 \cdot k_1 + 2 \cdot k_2 \stackrel{I.H.}{=} 0 + 0 = 0,$$

thus finishing the inductive “proof” . . .

Real-World Application: Fair Resource Distribution

- Suppose that some limited and non-uniform resource has to be distributed fairly among n receivers, for some $n \in \mathbb{N}$ with $n > 1$.
- E.g., a cake (with fruits, whipped cream, chocolate crumbs, icing, etc.) might have to be distributed fairly among n kids. Aka: “Cake Cutting Problem”.
- To make the situation worse, each kid might value different portions of the cake differently. (Bob likes fruits, Alice hates them; Alice likes whipped cream, but Bob hates it.)
- The distribution should involve all kids such that each kid has to agree that it received a fair share of the cake by his/her preferences.

Definition 23 (Fair distribution protocol)

A protocol for the distribution of a resource among n receivers is considered *fair* if each receiver gets at least $1/n$ -th of the resource (by his/her preferences), no matter what the preferences of the other receivers are and what the other receivers get.

- How can we come up with a fair distribution protocol? Is there a general algorithm for fair cake cutting in the presence of n kids??



Real-World Application: Fair Resource Distribution

If $n = 2$: Cut-and-choose distribution protocol.

- 1 Alice cuts the cake into two equal pieces (equal by her preferences).
- 2 Bob chooses whichever piece seems larger (by his preferences).
- 3 Alice takes the remaining piece.

If $n > 2$: Recursive application of the cut-and-choose distribution protocol.

- 1 The first $n - 1$ kids cut the cake into $n - 1$ pieces by applying the cut-and-choose distribution protocol recursively to $n - 2$, $n - 3$ etc. kids, thus each obtaining (hopefully) at least a fair $1/(n-1)$ portion of the cake.
- 2 The n -th kid asks all other $n - 1$ kids to cut his/her portion of the cake into n pieces such that the cutting is fair according to his/her preferences. (That is, according to each kid's preferences, each of the n pieces of his/her portion is equally desirable, for all of the first $n - 1$ kids.)
- 3 The n -th kid walks around and collects one piece — the most desirable piece according to his/her preferences! — from all the other $n - 1$ kids.

Theorem 24

The recursive cut-and-choose distribution protocol is fair.

Real-World Application: Fair Resource Distribution

Proof of Thm. 24 by induction: Assume that the total cake is worth 1 for each kid.

I.B.: $n = 2$ Alice cut the cake into two pieces that are equally desirable (according to her preferences) and, thus, both worth $1/2$. Hence, she will get one half of the cake (by her preferences), no matter how Bob behaves.

Bob sees two pieces, one worth w_1 and the other one worth $1 - w_1$ (by his preferences). Trivially, either $w_1 \geq 1/2$ or $1 - w_1 \geq 1/2$.

Hence, Bob can choose at least one half of the cake (according to his preferences), and both kids have no reason to complain about an unfair cutting.

I.H.: Assume that the recursive cut-and-choose cake cutting has been considered fair by the first $k - 1$ kids, for $k \geq 3$ arbitrary but fixed. Hence, each of the first $k - 1$ kids got a portion that is at least worth (according to the kid's preferences) $\frac{1}{k-1}$.

I.S.: After the cuts for the k -th kid were made, each kid has k pieces each worth $\frac{1}{(k-1) \cdot k}$. After the k -th kid took one piece from each of them, each of the first $k - 1$ kids is left with $k - 1$ pieces each worth $\frac{1}{(k-1) \cdot k}$, i.e., with a total worth of $\frac{1}{k}$. Suppose that the k -th kid values the portion of the i -th kid with w_i , for $i \in \{1, 2, \dots, k - 1\}$. Of course, $w_1 + w_2 + \dots + w_{k-1} = 1$. Since the k -th kid gets at least w_i/k from the i -th kid, the k -th kid gets in total at least

$$\frac{w_1}{k} + \frac{w_2}{k} + \dots + \frac{w_{k-1}}{k} = \frac{1}{k}(w_1 + w_2 + \dots + w_{k-1}) = \frac{1}{k}.$$



Cardinality of \mathbb{N}

- Intuitively, the cardinality of a set A specifies the number of elements of A .
- It is common to write $|A|$ to denote the cardinality of A . E.g., $|\{1, 2, 4, 8, 16\}| = 5$.
- The notion of cardinality becomes tricky for “infinite” sets, where the cardinality is not simply given by the number of elements.

Definition 25 (Comparing cardinality)

The sets A, B have the *same cardinality*, denoted by $|A| = |B|$, if there exists a bijection from A to B .

The set A is of *strictly smaller cardinality* than B , denoted by $|A| < |B|$, if there exists an injective function but no bijective function from A to B .

Definition 26 (Finite, countably infinite, uncountable, Dt: endlich, abzählbar unendlich, überabzählbar unendlich)

The set A is a *finite set* if $|A| < |\mathbb{N}|$.

The set A is a *countably infinite set* if $|A| = |\mathbb{N}| =: \aleph_0$.

The set A is an *uncountable set* if $|A| > |\mathbb{N}|$.

Theorem 27

A subset of a countably infinite set is a finite or a countably infinite set itself.

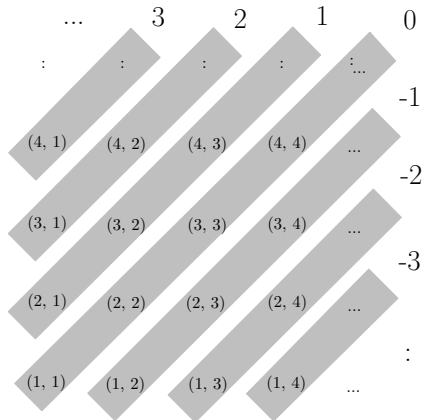
- Intuitive way to define the integers: $\mathbb{Z} := \mathbb{N}_0 \cup \{-n : n \in \mathbb{N}\}$.
- Thus, $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \dots\}$.
- $\mathbb{Z}^+ := \mathbb{N}$ and $\mathbb{Z}_0^+ := \mathbb{N}_0$.
- The blackboard-bold letter \mathbb{Z} stands for the German word “Zahlen”.
- But what are the properties of the elements $-n$??
- And how could we define $a + b$ and $a \cdot b$ for $a, b \in \mathbb{Z}$??
- In order to put \mathbb{Z} on a more solid basis, we “extend” \mathbb{N} to obtain \mathbb{Z} .

Construction of \mathbb{Z} Based on \mathbb{N}

- Let \cong_Z be a relation on $\mathbb{N}_0 \times \mathbb{N}_0$ such that

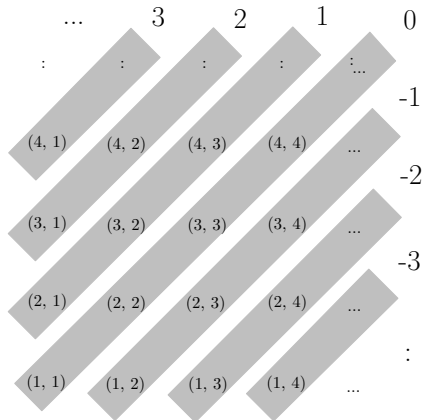
$$(a, b) \cong_Z (c, d) \quad :\Leftrightarrow \quad a + d = c + b.$$

- Easy to show: \cong_Z is an equivalence relation on $\mathbb{N}_0 \times \mathbb{N}_0$, with the equivalence classes shown below.



Construction of \mathbb{Z} Based on \mathbb{N}

- We interpret $[(a, b)]_{\cong_{\mathbb{Z}}}$ as $a - b$.
- For $n \in \mathbb{N}$, the equivalence classes $[(n, 0)]_{\cong_{\mathbb{Z}}}$ form the natural numbers, while $[(0, n)]_{\cong_{\mathbb{Z}}}$ form the negative integers.
- Zero is given by $[(0, 0)]_{\cong_{\mathbb{Z}}}$.



Construction of \mathbb{Z} Based on \mathbb{N}

- It remains to define addition, multiplication and order. For $a, b, c, d \in \mathbb{N}_0$ we define an addition $+_{\mathbb{Z}}$, a multiplication $\cdot_{\mathbb{Z}}$ and an order $\leq_{\mathbb{Z}}$ as follows:

$$\begin{aligned} [(a, b)]_{\cong_{\mathbb{Z}}} +_{\mathbb{Z}} [(c, d)]_{\cong_{\mathbb{Z}}} &:= [(a + c, b + d)]_{\cong_{\mathbb{Z}}} \\ [(a, b)]_{\cong_{\mathbb{Z}}} \cdot_{\mathbb{Z}} [(c, d)]_{\cong_{\mathbb{Z}}} &:= [(a \cdot c + b \cdot d, a \cdot d + b \cdot c)]_{\cong_{\mathbb{Z}}} \\ [(a, b)]_{\cong_{\mathbb{Z}}} \leq_{\mathbb{Z}} [(c, d)]_{\cong_{\mathbb{Z}}} &\Leftrightarrow a + d \leq b + c \end{aligned}$$

- It is easy to show that
 - addition, multiplication and order are well-defined,
 - the standard rules of arithmetic hold, with $[(0, 0)]_{\cong_{\mathbb{Z}}}$ as zero element (“zero”),
 - $\leq_{\mathbb{Z}}$ defines a total order on $\mathbb{N}_0 \times \mathbb{N}_0$.

Definition 28 (Positive/negative)

An integer is *positive* if it is greater than zero and *negative* if it is less than zero; zero is neither positive nor negative.

Theorem 29

\mathbb{Z} is a countably infinite set.

Definition 30 (Divisor, Dt.: Teiler, Faktor)

Let $a, b \in \mathbb{Z}$ with $a \neq 0$. Then a *divides* b , denoted by $a \mid b$, if there exists $c \in \mathbb{Z}$ such that $b = ca$.

$$a \mid b \quad :\Leftrightarrow \quad \exists c \in \mathbb{Z} \quad b = ca.$$

In this case, we also say that b is a *multiple* of a , or a is a *divisor* or *factor* of b , or b is *divisible* by a . Otherwise we have $a \nmid b$.

Lemma 31

- 1 $\forall a \in \mathbb{Z} \setminus \{0\} \quad a \mid a.$
- 2 $\forall a \in \mathbb{Z} \setminus \{0\} \quad \forall b \in \mathbb{Z} \quad a \mid b \Rightarrow (\forall c \in \mathbb{Z} \quad a \mid bc).$
- 3 $\forall a, b \in \mathbb{Z} \setminus \{0\} \quad \forall c \in \mathbb{Z} \quad (a \mid b \wedge b \mid c) \Rightarrow a \mid c.$
- 4 $\forall a \in \mathbb{Z} \setminus \{0\} \quad \forall b, c \in \mathbb{Z} \quad (a \mid b \wedge a \mid c) \Rightarrow [\forall s, t \in \mathbb{Z} \quad a \mid (bs + ct)].$
- 5 $\forall a, c \in \mathbb{Z} \setminus \{0\} \quad \forall b \in \mathbb{Z} \quad a \mid b \Leftrightarrow ac \mid bc.$
- 6 $\forall a, b \in \mathbb{Z} \setminus \{0\} \quad (a \mid b \wedge b \mid a) \Rightarrow (a = b \vee a = -b).$

Lemma 32

A number $a \in \mathbb{N}$ is divisible by

- 2 if its last digit is even;
- 3 if the sum of its digits is divisible by three;
- 4 if its last two digits form a number that is divisible by four;
- 5 if its last digit is 0 or 5;
- 6 if it is divisible by two and three;
- 7 if the hundreds digit is even and the number formed by the last two digits is divisible by eight, or if hundreds digit is odd and the number formed by the last two digits plus four is divisible by eight;
- 8 if the sum of its digits is divisible by nine;
- 9 if its last digit is 0;
- 10 if the alternating sum of its digits is divisible by eleven;
- 11 if it is divisible by three and four.

Divisibility Rules

Proof of Lem. 32: We prove only the divisibility by three. Let $n \in \mathbb{N}$ and $a_0, a_1, \dots, a_n \in \{0, 1, \dots, 9\}$ such that

$$a = \sum_{i=0}^n a_i \cdot 10^i.$$

We get

$$a = \sum_{i=0}^n a_i \cdot 10^i = \sum_{i=0}^n a_i \cdot (10^i - 1) + \sum_{i=0}^n a_i.$$

Since

$$3 \mid \left(\sum_{i=0}^n a_i \cdot (10^i - 1) \right),$$

the number a is divisible by three if and only if

$$3 \mid \left(\sum_{i=0}^n a_i \right).$$



Divisibility and the Pigeonhole Principle: Sample Application

Lemma 33

For any $n \in \mathbb{N}$ and any set of n distinct natural numbers $\{a_1, a_2, \dots, a_n\} \subset \mathbb{N}$, the sum of a (suitable) subset of these numbers is divisible by n .

Proof: Let n be arbitrary but fixed and consider n arbitrary (but fixed and distinct) natural numbers a_1, a_2, \dots, a_n . We define n numbers $b_1, b_2, \dots, b_n \in \mathbb{N}_0$ as follows:

$$b_k := \left(\sum_{j=1}^k a_j \right) \bmod n \quad \text{for } k = 1, 2, \dots, n.$$

If one of the numbers b_k is zero then we are done. Otherwise, we have

$$\{b_1, b_2, \dots, b_n\} \subseteq \{1, 2, \dots, n-1\}.$$

By the pigeonhole principle, there exist $i \neq j$ with $1 \leq i, j \leq n$ such that $b_i = b_j$. W.l.o.g. $i < j$. However, then

$$(a_{i+1} + a_{i+2} + \dots + a_j) \bmod n = 0, \quad \text{i.e., } (a_{i+1} + a_{i+2} + \dots + a_j) \equiv_n 0,$$

thus settling our claim.



Definition 34 (Prime, Dt.: Primzahl)

A natural number $p \in \mathbb{N}$ is a *prime number*, or is *prime*, if $p \geq 2$ and if p is divisible only by 1 and p itself. All other numbers $p \geq 2$ are called *composite*.

- The number 1 is no prime number!
- The only even prime number is 2.
- All primes greater than 2 are odd numbers.
- The set of all prime numbers is frequently (but not always) denoted by \mathbb{P} .

Definition 35 (Prime factor, Dt.: Primfaktor)

A natural number $p \in \mathbb{N}$ is a *prime factor* of $n \in \mathbb{N}$ if p is prime and $p \mid n$. If p is a prime factor of n then its *multiplicity* (Dt.: Vielfachheit) is the largest exponent k for which $p^k \mid n$.

Lemma 36

Let $a_1, a_2, \dots, a_k \in \mathbb{Z}$ and $p \in \mathbb{P}$. Then

$$p \mid a_1 \cdot a_2 \cdot \dots \cdot a_k \Leftrightarrow (\exists (1 \leq j \leq k) \ p \mid a_j).$$

Corollary 37

If two products of primes are identical then the primes are identical up to the order in which they appear in the products.

Theorem 38

Every natural number $n > 1$ is representable uniquely in the form

$$n = p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_k^{m_k},$$

where $p_1 < \dots < p_k$ are primes and $m_j \in \mathbb{N}$ are multiplicities for every $j = 1, \dots, k$.

Corollary 39

There are infinitely many prime numbers.

Proof attributed to Euclid of Alexandria: Suppose that $p_1 < p_2 < \dots < p_k$ are all the primes. Let

$$n := p_1 \cdot p_2 \cdot \dots \cdot p_k + 1.$$

We have $n \in \mathbb{N}$ and $n > 1$. By Thm. 38, $p_j \mid n$ for some $j = 1, \dots, k$. This implies $p_j \mid (n - p_1 \cdot p_2 \cdot \dots \cdot p_k)$, but $n - p_1 \cdot p_2 \cdot \dots \cdot p_k = 1$, and we get a contradiction. \square



Definition 40 (Mersenne prime)

A *Mersenne number* is of the form $2^n - 1$ for $n \in \mathbb{N}$. A *Mersenne prime* is a Mersenne number which is prime.

- Several unsolved problems related to Mersenne numbers:
 - Note that $2^{11} - 1 = 2047 = 23 \cdot 89$. Thus, not all Mersenne numbers are primes!
 - Are there infinitely many Mersenne primes? As of January 2018, only 50 Mersenne primes are known, with $2^{77232917} - 1$ being the largest known prime. (It was discovered by the “Great Internet Mersenne Prime Search”.)
 - What is a sufficient condition on n for $2^n - 1$ to be prime?

Lemma 41

If $2^n - 1$ is prime for some $n \in \mathbb{N}$ then n is prime.

Chances to Become Famous: Conjectures About Primes

Conjecture 42 (Goldbach 1742, “weak version” or “ternary conjecture”)

Every odd natural number greater than 5 can be written as the sum of three primes.

Conjecture 43 (Goldbach-Euler 1742, “strong version”)

Every even natural number greater than 3 can be written as the sum of two primes.

- Christian Goldbach (1690–1764), Leonhard Euler (1707–1783).
- The strong version of this conjecture implies the weak version: If $n \in \mathbb{N}$, with $n \geq 7$, is odd then $n' := n - 3$ is even with $n' > 3$. Hence, if n' can be written as the sum of two primes, then n can be written as the sum of three primes.
- By means of distributed computer search, as of Dec 2012, Tomás Oliveira e Silva verified the strong version of Goldbach's conjecture up to $4 \cdot 10^{18}$.
- Also by distributed computing, in 2013 Harald Helfgott and David Platt verified the weak Goldbach conjecture up to (roughly) $8 \cdot 10^{30}$.
- In 1937, Vinogradov proved the weak version for "sufficiently large numbers", and later on his student Borozdin proved $3^{3^{15}}$ to be sufficiently large.
- In 2013, Harald Helfgott released papers that, if accepted as correct, yield a formal proof of the weak conjecture for all natural numbers greater than $\approx 10^{30}$.

Conjecture 44 (Polignac, 1849)

For every natural number k there exist infinitely many numbers p such that p and $p + 2k$ are primes.

- For $k := 1$, the conjecture by Alphonse de Polignac (1817–1890) is known as the *twin prime conjecture*. As of 25-Dec-2011, the largest known twin primes are $3\,756\,801\,695\,685^{2\,666\,669} \pm 1$; these numbers have 200 700 digits.
- In April 2013, Yitang Zhang proved that there exist infinitely many prime numbers p_{n+1} and p_n such that $p_{n+1} - p_n < 7 \cdot 10^7$.
- In November 2013, James Maynard reduced this bound to 600.
- This bound seems to have been further reduced to 246 by the Polymath project led by Terence Tao.

A Chance Missed to Become Famous: Fermat's Last Theorem

Theorem 45 (Wiles&Taylor, 1995)

For every natural number $n > 2$, the Diophantine equation $a^n + b^n = c^n$ has no solution over \mathbb{N} .

- Dt.: Großer Satz von Fermat.
- A Diophantine equation is an equation for which only integer solutions are sought.
- E.g., $(3, 4, 5)$ is an integer solution triple for $a^2 + b^2 = c^2$.
- Stated in 1637 by Pierre de Fermat (1607(?)–1665) without proof, but with a famous side remark: "Cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet."
- Proved for $n = 4$ by Fermat himself.
- Finally proved by Andrew Wiles in 1993; a gap in the proof was fixed by Wiles and his former student Richard Taylor; the full proof was published in 1995.

Quotient and Remainder

Lemma 46

Let $a \in \mathbb{N}$ and $b \in \mathbb{Z}$. Then there exist a unique *quotient* $q \in \mathbb{Z}$ and a unique *remainder* $r \in \mathbb{N}_0$ such that

$$b = aq + r \quad \text{and} \quad 0 \leq r < a.$$

- We will use the operators `div` and `mod` for computing the divisor and remainder. That is, q and r of Lemma 46 are given by $q := b \text{ div } a$ and $r := b \text{ mod } a$.
- The modulo of powers of 2 can be expressed as a bitwise AND operation: $b \text{ mod } 2^n == b \& (2^n - 1)$.
- In many programming languages the remainder r can be obtained by means of the *modulo* operator. See, e.g., the operator `%` in C, C++, C#, Java, and Perl.

Warning

If one or both of a and b are allowed to be negative integers then the sign of the remainder may differ among different implementations!



Real-World Application: Base Conversion

- We know that $25 = (11001)_2$, i.e., $(11001)_2$ is the base-two representation of $25 = (25)_{10}$. (After all, $25 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$.)
- How can we represent an integer relative to an arbitrary base $b \in \mathbb{N} \setminus \{1\}$?
- Lemma 46 tells us that there exist unique $q_0, r_0 \in \mathbb{N}_0$ such that

$$n = bq_0 + r_0 \quad \text{with} \quad 0 \leq r_0 < b.$$

- The number r_0 becomes the rightmost digit of the base- b representation of n , and we seek q_1, r_1 such that

$$q_0 = bq_1 + r_1 \quad \text{with} \quad 0 \leq r_1 < b,$$

and so on until some $q_i = 0$.

- E.g.,

$$\begin{array}{rcl} 25 & = & 12 \cdot 2 + 1 \\ 12 & = & 6 \cdot 2 + 0 \\ 6 & = & 3 \cdot 2 + 0 \\ 3 & = & 1 \cdot 2 + 1 \\ 1 & = & 0 \cdot 2 + 1 \end{array}$$

and therefore $25 = (11001)_2$.



- Introduced by Carl Friedrich Gauss (1777–1855) in 1801.

Definition 47 (Congruence, Dt.: Kongruenz)

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$. We say that a is *congruent* to b modulo m , and write

$$a \equiv_m b,$$

if $a - b$ is divisible by m . The term $a \equiv_m b$ is called a *congruence*.

- Hence: $a \equiv_m b :\Leftrightarrow m \mid (a - b)$.
- If $a \equiv_m b$ then a and b have the same remainder after dividing by m .
That is, $a \bmod m = b \bmod m$.
- Note: Some authors prefer to write $a \equiv b (m)$ or $a \equiv b \bmod m$ for $a \equiv_m b$.

Definition 48 (Even/odd, Dt.: gerade/ungerade)

A number $n \in \mathbb{Z}$ is said to be *odd* if and only if $n \equiv_2 1$; otherwise, n is *even*.

$$38 \equiv_{12} 2$$

$$-3 \equiv_5 2$$

$$0 \equiv_3 3$$

$$8 \equiv_3 2$$

$$7 \equiv_3 1$$

$$7 \equiv_3 -8$$

$$\text{even} + \text{even} \equiv_2 \text{even}$$

$$\text{even} + \text{odd} \equiv_2 \text{odd}$$

$$\text{odd} + \text{odd} \equiv_2 \text{even}$$

$$\text{even} \cdot \text{even} \equiv_2 \text{even}$$

$$\text{even} \cdot \text{odd} \equiv_2 \text{even}$$

$$\text{odd} \cdot \text{odd} \equiv_2 \text{odd}$$

Lemma 49

For $m \in \mathbb{N}$, the relation \equiv_m is an equivalence relation on \mathbb{Z} , i.e., for all $a, b, c \in \mathbb{Z}$,

reflexivity $a \equiv_m a$,

symmetry if $a \equiv_m b$ then $b \equiv_m a$, and

transitivity if $a \equiv_m b$ and $b \equiv_m c$ then $a \equiv_m c$

hold.

Lemma 50

For $m \in \mathbb{N}$, the relation \equiv_m is a congruence relation on \mathbb{Z} , i.e., it respects addition, subtraction, and multiplication: Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{N}$, and suppose that

$$a \equiv_m b \quad \text{and} \quad c \equiv_m d.$$

Then

$$a + c \equiv_m b + d \quad \text{and} \quad a - c \equiv_m b - d \quad \text{and} \quad a \cdot c \equiv_m b \cdot d.$$

Definition 51 (Residue, Dt.: Residuum, Restklasse)

Let $m \in \mathbb{N}$ with $m \geq 2$. The equivalence classes of \mathbb{Z} modulo m are called *residues* (or remainders) modulo m . For $a \in \mathbb{Z}$, its equivalence class modulo m is denoted by $[a]_m$. The set of residues modulo m is denoted by \mathbb{Z}_m or $\mathbb{Z}/m\mathbb{Z}$.

Lemma 52

Let $m \in \mathbb{N}$ with $m \geq 2$. Then $\mathbb{Z}_m = \{[a]_m : a \in \mathbb{N}_0 \wedge a < m\}$.

Definition 53 (Arithmetic on \mathbb{Z}_m)

Let $m \in \mathbb{N}$ with $m \geq 2$, and $[a]_m, [b]_m \in \mathbb{Z}_m$. On \mathbb{Z}_m we define an addition $+_m$ and a multiplication \cdot_m as follows.

$$[a]_m +_m [b]_m := [a + b]_m$$

$$[a]_m \cdot_m [b]_m := [a \cdot b]_m$$

Lemma 54

Let $m \in \mathbb{N}$ with $m \geq 2$. Then addition $+_m$ and multiplication \cdot_m on \mathbb{Z}_m are well-defined. Furthermore, $(\mathbb{Z}_m, +_m, \cdot_m)$ forms a commutative ring.

- Note: Often the notation $[a]_m$ is simplified by omitting the modulus m , i.e., by writing $[a]$, or even by simply writing a if it is clear that $a \in \mathbb{Z}_m$.

Real-World Application: Pseudo-Random Numbers

- Since computers cannot flip a coin to obtain a random result, one resorts to algorithms that generate “random” numbers: pseudo-random number generators.
- *Linear congruential generators* (LCG, [Lehmer 1954]) have been well studied, are easy to implement and used frequently.
- They generate a sequence of non-negative integers less than some specified modulus $m \in \mathbb{N}$ according to the following recursive definition:

$$x_{n+1} := (a \cdot x_n + c) \bmod m,$$

where

$m \in \mathbb{N}$	with	$m > 1$	modulus,
$a \in \mathbb{N}$	with	$a < m$	multiplier,
$c \in \mathbb{N}_0$	with	$c < m$	increment,
$x_0 \in \mathbb{N}_0$	with	$x_0 < m$	seed.

- E.g., $m := 15$, $a := 1$, $c := 4$ and $x_0 := 2$ yields the following sequence of numbers:

2 6 10 14 3 7 11 0 4 8 12 1 5 9 13 2 ...

- GCC/glibc: $m := 2^{31} - 1$, $a := 1103515245$, $c := 12345$. More advanced pseudo-random number generators exist, e.g., Mersenne twister.



Greatest Common Divisor

Lemma 55

Let $a, b \in \mathbb{N}$. Then there exists a unique $n \in \mathbb{N}$ such that

- 1 $n \mid a$ and $n \mid b$, and
- 2 for all $m \in \mathbb{N}$, if $m \mid a$ and $m \mid b$ then $m \leq n$.

Definition 56 (Greatest common divisor, Dt.: größter gemeinsamer Teiler (ggT))

Let $a, b \in \mathbb{N}$. The unique number $n \in \mathbb{N}$ that exists according to Lem. 55 is called *greatest common divisor* of a and b , and is denoted by $\gcd(a, b)$. Conventionally, $\gcd(a, 0) = \gcd(0, a) := a$, since 0 is divisible by all natural numbers.

Definition 57 (Relatively prime, Dt.: teilerfremd, relativ prim)

The numbers $a, b \in \mathbb{N}$ are *relatively prime*, or *coprime*, if $\gcd(a, b) = 1$.

Definition 58 (Pairwise relatively prime)

A set S of natural numbers is called *pairwise relatively prime* (or *pairwise coprime* or *mutually coprime*) if all pairs of numbers a and b in S , with $a \neq b$, are relatively prime.

Lemma 59 (Bézout's Identity)

Let $a, b \in \mathbb{N}$. Then there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$. Conversely, the smallest positive number $ax + by$, for all $x, y \in \mathbb{Z}$, equals $\gcd(a, b)$.

- Lemma 59 was first stated by Étienne Bézout (1730–1783), and numbers $x, y \in \mathbb{Z}$ with $\gcd(a, b) = ax + by$ are called Bézout numbers.
- Note: Bézout numbers are not unique! For instance, $\gcd(10, 15) = 5$, and $10x + 15y = 5$ has the solutions $x = -1$ and $y = 1$, and $x = 2$ and $y = -1$.
- For $a, b, d \in \mathbb{Z}$ given, the identity $d = ax + by$ over $\mathbb{Z} \times \mathbb{Z}$ is called a *linear Diophantine equation* in x and y .

Corollary 60

The numbers $a, b \in \mathbb{N}$ are relatively prime if and only if the linear Diophantine equation $ax + by = 1$ has a solution, i.e., if and only if there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

Theorem 61 (Euclidean Algorithm)

The following algorithm computes $\gcd(a, b)$ for $a, b \in \mathbb{N}_0$ with $a > b$.

function $\gcd(a, b)$

precondition: $a, b \in \mathbb{N}_0$ with $a > b$.

postcondition: $t = \gcd(a, b)$

while $b > 0$ **do**

$t \leftarrow b$

$b \leftarrow a \bmod b$

$a \leftarrow t$

end while

$t \leftarrow a$

Euclidean Algorithm for GCD Computation: Sample Run

```
function gcd( $a, b$ )  
precondition:  $a, b \in \mathbb{N}_0$  with  $a > b$ .  
postcondition:  $t = \text{gcd}(a, b)$   
  while  $b > 0$  do  
     $t \leftarrow b$   
     $b \leftarrow a \bmod b$   
     $a \leftarrow t$   
  end while  
   $t \leftarrow a$ 
```

- We want to compute the gcd of 78 and 99. Hence, $b := 78$ and $a := 99 = 1 \cdot 78 + 21$. We get after different passes through the loop:

after 1st pass:	$t = 78,$	$b = 21,$	$a = 78 = 3 \cdot 21 + 15$
after 2nd pass:	$t = 21,$	$b = 15,$	$a = 21 = 1 \cdot 15 + 6$
after 3rd pass:	$t = 15,$	$b = 6,$	$a = 15 = 2 \cdot 6 + 3$
after 4th pass:	$t = 6,$	$b = 3,$	$a = 6 = 2 \cdot 3 + 0$
after 5th pass:	$t = 3,$	$b = 0,$	$a = 3$

- Hence, $t = 3 = \text{gcd}(78, 99)$.



Does $(\mathbb{Z}_m, +_m, \cdot_m)$ Form a Field?

Theorem 62

Let $m \in \mathbb{N}$ with $m \geq 2$. An element $[a]_m \in \mathbb{Z}_m$ has a multiplicative inverse if and only if a is relatively prime to m .

Corollary 63

Let $m \in \mathbb{N}$ with $m \geq 2$. The ring $(\mathbb{Z}_m, +_m, \cdot_m)$ forms a (finite) field if and only if m is prime.

Lemma 64

Let $m \in \mathbb{N}$ with $m \geq 2$ and $[a]_m \in \mathbb{Z}_m$ such that m and a are relatively prime. Let $x, y \in \mathbb{Z}$ such that $ax + my = 1$. Then $[a]_m \cdot_m [x]_m = [1]_m$, i.e., $[x]_m$ is the multiplicative inverse element for $[a]_m$.

Theorem 65 (Extended Euclidean Algorithm)

The following algorithm computes $x, y \in \mathbb{Z}$ and $d \in \mathbb{N}$ such that $\gcd(a, b) = d = ax + by$ for $a, b \in \mathbb{N}$ with $a > b$.

function gcd_extended(a, b)

precondition: $a, b \in \mathbb{N}_0$ with $a > b$.

postcondition: $(d, x, y) \in \mathbb{N} \times \mathbb{Z} \times \mathbb{Z}$ such that $\gcd(a, b) = d = ax + by$

if $(a \bmod b) = 0$ **then**

return $(b, 0, 1)$

else

$(d, x, y) \leftarrow \text{gcd_extended}(b, a \bmod b)$

return $(d, y, x - y \cdot (a \text{ div } b))$

end if

Extended Euclidean Algorithm for GCD Computation: Sample Run

```
function gcd_extended( $a, b$ )  
postcondition:  $(d, x, y) \in \mathbb{N} \times \mathbb{Z} \times \mathbb{Z}$  such that  $\gcd(a, b) = d = ax + by$   
  if  $(a \bmod b) = 0$  then  
    return  $(b, 0, 1)$   
  else  
     $(d, x, y) \leftarrow \text{gcd\_extended}(b, a \bmod b)$   
    return  $(d, y, x - y \cdot (a \text{ div } b))$   
  end if
```

- We want to compute $x, y \in \mathbb{Z}$ and $d \in \mathbb{N}$ such that $\gcd(99, 78) = d = 99x + 78y$.

a	b	$a \text{ div } b$	$a \bmod b$	d	x	y
99	78	1	21	3	-11	14
78	21	3	15	3	3	-11
21	15	1	6	3	-2	3
15	6	2	3	3	1	-2
6	3	-	0	3	0	1

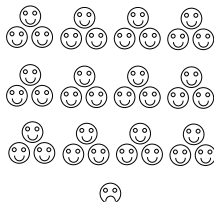
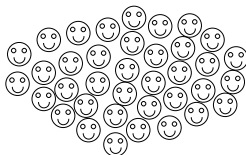
- Hence, $\gcd(99, 78) = -11 \cdot 99 + 14 \cdot 78 = -1089 + 1092 = 3$.



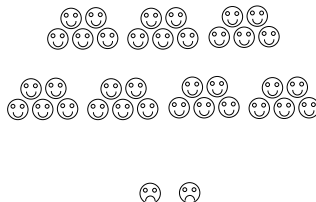
Chinese Remainder Theorem

- Old Chinese folk tale: A Chinese Emperor used to count his army after a battle by ordering them to form groups of different sizes:
 - 1 The soldiers should form groups of 3 and report back the number of soldiers that could not join a group consisting of 3 soldiers.
 - 2 Then the soldiers should form groups of 5 and report back the number of soldiers that could not join a group consisting of 5 soldiers.
 - 3 Then the soldiers should form groups of 7 and report back the number of soldiers that could not join a group consisting of 7 soldiers.
 - 4 Then the soldiers should form groups of 11 and report back the number of soldiers that could not join a group consisting of 11 soldiers.
 - 5 ...
- Based on this information he was able to figure out the number n of soldiers in his army.
- Indeed, a mathematical solution was provided by the Chinese mathematician Sun Tzu sometime in the third to fifth century, and republished by Qin Jiushao in 1247!

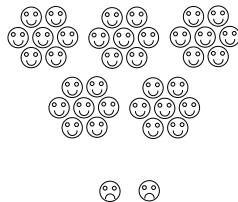
Chinese Remainder Theorem



$$n \bmod 3 = 1$$



$$n \bmod 5 = 2$$



$$n \bmod 7 = 2$$

Theorem 66 (Chinese Remainder Theorem, Dt.: Chinesischer Restsatz)

If, for some $k \in \mathbb{N}$, the numbers $m_1, m_2, \dots, m_k \in \mathbb{N}$ are pairwise relatively prime, then the following system of simultaneous congruences has an integer solution b for $a_1, a_2, \dots, a_k \in \mathbb{Z}$ given:

$$\left. \begin{array}{l} b \equiv_{m_1} a_1 \\ b \equiv_{m_2} a_2 \\ \vdots \\ b \equiv_{m_k} a_k \end{array} \right\} (*)$$

Furthermore, all solutions of $(*)$ are congruent modulo $m := \prod_{i=1}^k m_i$. That is, the solution is unique if constrained to $\{1, 2, \dots, m\}$.

Constructive Proof of Chinese Remainder Theorem 66

Proof: We show the existence of an integer solution. Consider $i \in \mathbb{N}$ with $1 \leq i \leq k$. Since m_1, m_2, \dots, m_k are pairwise relatively prime, $\gcd(\frac{m}{m_i}, m_i) = 1$. Using the extended Euclidean algorithm (Thm. 65), we can find integers x_i and y_i such that

$$x_i \cdot m_i + y_i \cdot \frac{m}{m_i} = 1. \quad (\star)$$

Let $b_i := y_i \cdot \frac{m}{m_i}$. Equation (\star) guarantees that the remainder of b_i when divided by m_i is 1. On the other hand, for $i \neq j$ every m_j divides b_i evenly. Thus,

$$b_i \equiv_{m_i} 1 \quad \text{and} \quad b_i \equiv_{m_j} 0 \quad \text{for all } j \text{ with } i \neq j, \quad 1 \leq j \leq k.$$

Since congruences respect multiplication, we get

$$a_i \cdot b_i \equiv_{m_i} a_i \quad \text{and} \quad a_i \cdot b_i \equiv_{m_j} 0 \quad \text{for all } j \text{ with } i \neq j, \quad 1 \leq j \leq k.$$

Thus, one solution of the simultaneous congruences is given by

$$b := \sum_{i=1}^k a_i b_i.$$



- The Emperor collected the following information:
 - When the soldiers formed groups of 3, one soldier was left out.
 - When the soldiers formed groups of 5, two soldiers were left out.
 - When the soldiers formed groups of 7, again two soldiers were left out.
- That is, since $a_1 = 1$, $a_2 = 2$, $a_3 = 2$ and $m_1 = 3$, $m_2 = 5$, $m_3 = 7$ and $m = 3 \cdot 5 \cdot 7 = 105$:

$$n \equiv_3 1 \quad n \equiv_5 2 \quad n \equiv_7 2$$

- Hence, we are to find $x_1, x_2, x_3, y_1, y_2, y_3 \in \mathbb{Z}$ such that

$$3x_1 + 35y_1 = 1 \quad 5x_2 + 21y_2 = 1 \quad 7x_3 + 15y_3 = 1.$$

- We have $x_1 := 12$, $y_1 := -1$, $x_2 := -4$, $y_2 := 1$, $x_3 := -2$, $y_3 := 1$ and, thus,

$$n = (35 \cdot (-1) \cdot 1 + 21 \cdot 1 \cdot 2 + 15 \cdot 1 \cdot 2) \bmod 105 = 37 \bmod 105 = 37.$$

Real-World Application: Secret Sharing

- Secret sharing refers to the distribution of information related to a secret (e.g., a number) among a group of receivers such that the secret can only be reconstructed if all or, at least, a large percentage of the receivers cooperate.
- Ideally, the information received by one individual receiver shall be of no (or very little) help for the receiver to obtain the secret without the help of the others.
- A secret sharing scheme is called a (t, n) threshold scheme, or t -out-of- n scheme, if at least t of the n receivers have to cooperate. (Of course, $t \leq n$.)
- Typically, t is large relative to n but not identical to n .
- Several different variants of schemes for secret sharing are used in practice.
- At least two published schemes rely on the Chinese Remainder Theorem 66.
- We sketch the very basic idea of a scheme based on the Chinese Remainder Theorem 66. (In our simple scheme we have $t = n$.)

Real-World Application: Secret Sharing

- Suppose that the number 1234 is the secret to be shared by five receivers.
- We choose

$$m_1 := 2, \quad m_2 := 3, \quad m_3 := 5, \quad m_4 := 7, \quad m_5 := 11.$$

- Note that

$$m := \prod_{i=1}^5 m_i = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310 > 1234.$$

- Now consider $a_i := 1234 \bmod m_i$, for $1 \leq i \leq 5$. This gives us the numbers

$$a_1 = 0, \quad a_2 = 1, \quad a_3 = 4, \quad a_4 = 2, \quad a_5 = 2.$$

- The numbers m_i and a_i are passed to the i -th receiver.
- Note that each individual receiver has gained little information about the original secret.
- Rather, in our simple approach, all five receivers need to cooperate in order to recover the secret: They have to solve the following set of five congruences:

$$b \equiv_2 0 \quad b \equiv_3 1 \quad b \equiv_5 4 \quad b \equiv_7 2 \quad b \equiv_{11} 2$$



Real-World Application: Secret Sharing

- The five receivers have to solve the following set of five congruences:

$$b \equiv_2 0 \quad b \equiv_3 1 \quad b \equiv_5 4 \quad b \equiv_7 2 \quad b \equiv_{11} 2$$

- Since $a_1 = 0$, we need to solve only four congruences and get the following four Diophantine equations.

$$3x_2 + 770y_2 = 1 \quad 5x_3 + 462y_3 = 1 \quad 7x_4 + 330y_4 = 1 \quad 11x_5 + 210y_5 = 1$$

- Solving these equations yields the following solutions:

$$x_2 = 257, y_2 = -1 \quad x_3 = 185, y_3 = -2 \quad x_4 = -47, y_4 = 1 \quad x_5 = -19, y_5 = 1$$

- Hence, the secret sought is recovered as

$$b = (-1) \cdot 770 \cdot 1 - 2 \cdot 462 \cdot 4 + 1 \cdot 330 \cdot 2 + 1 \cdot 210 \cdot 2 = -3386 \equiv_{2310} 1234.$$

Real-World Application: Arithmetic with Large Integers

- Standard integer arithmetic cannot handle arbitrarily large integers.
- One way to carry out complex integer arithmetic with large integers is to apply modulo arithmetic and the Chinese Remainder Theorem 66:
 - 1 Select k modules $m_1, m_2, \dots, m_k \in \mathbb{N} \setminus \{1\}$ which are relatively prime, for some $k \in \mathbb{N}$.
 - 2 Let $m := m_1 \cdot m_2 \cdot \dots \cdot m_k$.
 - 3 Represent an integer $n < m$ by its k remainders n_1, n_2, \dots, n_k upon division by m_1, m_2, \dots, m_k .
 - 4 Perform the arithmetic operations of your algorithm on these remainders, with the calculations involving n_i being carried out modulo m_i .
 - 5 Recover the actual result by applying the Chinese Remainder Theorem 66.
- This approach works as long as all intermediate results are less than m .
- Advantages:
 - One can use (mostly) standard arithmetic to handle integers larger than those normally handled.
 - One can run the computations for the different remainders in parallel, thus speeding up the computation.
- Standard choices for the modules are numbers of the form $2^i - 1$:
 - One can prove $\gcd(2^i - 1, 2^j - 1) = 2^{\gcd(i,j)} - 1$, which makes it easy to ensure that the modules are relatively prime.

Real-World Application: Arithmetic with Large Integers

- Suppose that we want to limit our arithmetic operations to numbers less than 12.
- We choose the five modules

$$m_1 := 2, \quad m_2 := 3, \quad m_3 := 5, \quad m_4 := 7, \quad m_5 := 11.$$

and remember that $m := m_1 \cdot m_2 \cdot m_3 \cdot m_4 \cdot m_5 = 2310$.

- Hence, we can deal with numbers less than 2310.
- Recall that $n := 1234$ can be represented by the five remainders $(0, 1, 4, 2, 2)$.
- Similarly, 1000 can be represented by the five remainders $(0, 1, 0, 6, 10)$.
- We get

$$\begin{aligned} (0, 1, 4, 2, 2) + (0, 1, 0, 6, 10) &= (0, 2 \bmod 3, 4 \bmod 5, 8 \bmod 7, 12 \bmod 11) \\ &= (0, 2, 4, 1, 1). \end{aligned}$$

- Thus, $b := 1234 + 1000$ is uniquely determined as the solution of the following set of five congruences:

$$b \equiv_2 0 \quad b \equiv_3 2 \quad b \equiv_5 4 \quad b \equiv_7 1 \quad b \equiv_{11} 1$$



Definition 67 (Rational equivalence)

On $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ we define the binary relation \cong_Q as follows:

$$(p_1, q_1) \cong_Q (p_2, q_2) \quad :\Leftrightarrow \quad p_1 q_2 = p_2 q_1.$$

Lemma 68

The relation \cong_Q is an equivalence relation on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.

Definition 69 (Rational numbers)

The *rational numbers* \mathbb{Q} are defined as

$$\mathbb{Q} := \{[(p, q)]_{\cong_Q} : p \in \mathbb{Z}, q \in \mathbb{Z} \setminus \{0\}\}.$$

The *canonical representative* of $[(p, q)]_{\cong_Q}$ is denoted by $\frac{p'}{q'}$, where $p' := p \operatorname{div} \operatorname{gcd}(p, q)$ and $q' := q \operatorname{div} \operatorname{gcd}(p, q)$.

- We have $\mathbb{N} \subset \mathbb{Q}$, since for every $n \in \mathbb{N}$ the fraction $\frac{n}{1}$ belongs to \mathbb{Q} .
- It is easy to define an addition $+$, multiplication \cdot and order \leq on \mathbb{Q} that turns $(\mathbb{Q}, +, \cdot)$ into a totally ordered field. E.g.,

$$[(p, q)]_{\cong_Q} +_{\cong_Q} [(m, n)]_{\cong_Q} := [(pn + qm, qn)]_{\cong_Q}$$

- Of course, it is standard to simplify the notation and write

$$\frac{p}{q} \quad \text{instead of} \quad [(p, q)]_{\cong_Q}.$$

But keep in mind that fractions are equivalence classes. Thus,

$$\frac{1}{3} \cong_Q \frac{2}{6} \cong_Q \frac{3}{9} \cong_Q \frac{2000}{6000}.$$

- In the sequel we resort to standard knowledge and deal with rational numbers as we learned in school. (However, this could be formalized, based on Def. 69!)

\mathbb{Q} Is Dense in \mathbb{R} But Still Countably Infinite!

Lemma 70

There exists a rational number between any two distinct rational numbers.

Theorem 71

\mathbb{Q} is everywhere dense in \mathbb{R} . That is, for every $x \in \mathbb{R}$, every arbitrarily small neighborhood of x contains a rational number.

Theorem 72

The equation $x^2 = 2$ has no solution over \mathbb{Q} .

Proof: Suppose that there exist $x \in \mathbb{Q}$ such that $x^2 = 2$. Hence, there exist $p \in \mathbb{Z}$ and $q \in \mathbb{Z} \setminus \{0\}$ such that

$$\gcd(p, q) = 1 \quad \text{and} \quad 2 = \left(\frac{p}{q}\right)^2 = \frac{p^2}{q^2}.$$

This equation is equivalent to $2q^2 = p^2$, implying that $p^2 \equiv_2 0$, and, thus, also $p \equiv_2 0$. This in turn implies $q^2 \equiv_2 0$, and, therefore, also $q \equiv_2 0$. We have a contradiction to $\gcd(p, q) = 1$.



- Intuitively, the reals comprise both rational and irrational numbers like $\sqrt{2}$ or π .
- A formal introduction of the reals based on \mathbb{N} and \mathbb{Q} — e.g., based on Dedekind cuts or on equivalence classes of Cauchy sequences — is beyond the scope of this lecture.
- Convenient notations for intervals of real numbers:
 $\forall a, b \in \mathbb{R} \quad [a, b] := \{x \in \mathbb{R} : a \leq x \leq b\};$
 $\forall a, b \in \mathbb{R} \quad]a, b[:= \{x \in \mathbb{R} : a < x < b\};$
 $\forall a, b \in \mathbb{R} \quad [a, b[:= \{x \in \mathbb{R} : a \leq x < b\};$
 $\forall a, b \in \mathbb{R} \quad]a, b] := \{x \in \mathbb{R} : a < x \leq b\}.$
- Note: Some authors prefer to denote the open interval $]a, b[$ by (a, b) .

Definition 74 (Decimal representation, Dt.: Dezimalzahl)

A real number $x \in \mathbb{R}_0^+$ is in *decimal representation* (or a *decimal number*) if it is represented as a sum of powers of ten:

$$x = x_0 + \sum_{i=1}^{\infty} \frac{x_i}{10^i}, \quad \text{with an integer part } x_0 \in \mathbb{N}_0 \text{ and with } 0 \leq x_i \leq 9 \text{ for all } i \in \mathbb{N}.$$

The decimal representation is *finite* if, for some $n_0 \in \mathbb{N}_0$, we have $x_i = 0$ for all $i \geq n_0$.

- By definition,

$$x = \lim_{n \rightarrow \infty} \sum_{i=0}^n \frac{x_i}{10^i}.$$

- It is straightforward to extend Def. 74 to negative reals.

Definition 75 (Decimal separator)

The decimal separator is a symbol which is used to mark the boundary between the integer part and the fractional part of a number in decimal representation.

Warning

A least two symbols are in wide-spread use for the decimal separator!

- Most of Europe, most of South America and French Canada use the comma, while the UK, USA, Australia, English Canada and several Asian countries use a dot (“period”, “full stop”). The dot also prevails in English-language publications.
- Dots or commas are frequently used to group three digits into groups within the integer part. However, this practice is discouraged by ISO!
- Note: The decimal representation is not unique: we have $1.0 = 0.9999\dots$, where the ellipsis “...” represents an infinite sequence of the digit 9.
- In fact, every non-zero, finitely represented decimal number has an alternate representation with trailing 9s, such as 123.4567 and 123.4566999...
- Of course, the finite representation is (almost) always the preferred representation.

Definition 76 (Recurring decimal, Dt.: periodische Dezimalzahl)

A decimal representation of a real number is a *recurring decimal* (or *repeating decimal*) if it becomes periodic at some point: a finite subsequence of the digits after the decimal separator is repeated indefinitely.

- *Recurring decimals*, e.g.,

$$\frac{1}{3} = 0.333 \dots$$

or

$$\frac{1}{7} = 0.142857142857142857 \dots$$

are written as $0.\overline{3}$ or $0.\dot{3}$, and $0.\overline{142857}$. (The horizontal line is known as *vinculum*.)

Lemma 77

A real number has a finite or recurring decimal representation if and only if it is a rational number.

Decimal Notation: Conversion to a Fraction

- We proceed as follows to convert $0.43\overline{21}$ to a rational number.
- Let $x := 0.00\overline{21}$. Then $100x = 0.\overline{21}$.
- This gives

$$99x = 100x - x = 0.\overline{21} - 0.00\overline{21} = 0.21 = \frac{21}{100}.$$

- We get

$$x = \frac{21}{9900} = \frac{7}{3300}.$$

- Hence,

$$0.43\overline{21} = 0.43 + x = \frac{43}{100} + \frac{7}{3300} = \frac{1426}{3300} = \frac{713}{1650}.$$

The Reals are Not Countable

Theorem 78

The real numbers are uncountable, i.e., there exists no bijection from \mathbb{N} onto \mathbb{R} .

Proof by Cantor (1891): Suppose to the contrary that there exists a bijection $a : \mathbb{N} \rightarrow \mathbb{R}$. We show that we can construct a number r which is not in the list a_1, a_2, a_3, \dots : For $k \in \mathbb{N}$ let d_k be the k -th digit after the decimal separator in a_k if a_k has at least k digits after the decimal separator, and $d_k := 0$ otherwise.

$$\begin{array}{rcl} a_1 & = & \text{---} . d_1 \text{ ---} \dots \\ a_2 & = & \text{---} . \text{---} d_2 \text{ ---} \dots \\ a_3 & = & \text{---} . \text{---} \text{---} d_3 \text{ ---} \dots \\ & \vdots & \end{array}$$

If $d_k = 1$ then $r_k := 2$ else $r_k := 1$. Now regard r_k as the k -th digit of a number $r \in \mathbb{R}$: we have $r = 0.r_1 r_2 r_3 r_4 \dots$. Since at least the k -th digit of r differs from the k -th digit of a_k , we conclude that $r \neq a_n$ for all $n \in \mathbb{N}$. □

- Arguments of this form are called *diagonal arguments*.
- Cantor proved $\mathfrak{c} := |\mathbb{R}| = 2^{\aleph_0} > \aleph_0 = |\mathbb{N}|$.
- *Continuum hypothesis*: There is no set with cardinality strictly between that of the integers and the reals. (This is a hypothesis, but not a theorem!)



Well-Ordering the Reals

- By definition, (\mathbb{N}, \leq) is well-ordered. And we have already hinted at well-orderings for \mathbb{Z} and \mathbb{Q} .
- Question: Can the reals be well-ordered?
- Answer: We don't know it for sure!
- In 1883, Georg Cantor stated that the Well-Order Theorem is a "fundamental law of thought". This statement started a mathematical flame war!

Well-Order "Theorem"

Every set can be well-ordered.

- It has also been proved that it is impossible to write down an explicit well-ordering for the reals.
- In any case, this "theorem" can only be taken as an axiom, since it has been proved that it does not follow from any of the other commonly accepted axioms of set theory.
- In first-order logic, the Well-Order Theorem is equivalent to the Axiom of Choice (Dt.: Auswahlaxiom) and to Zorn's Lemma, in the sense that either one of them together with the Zermelo-Fraenkel Axioms allows to deduce the other ones.



Definition 79 (Well-founded order, Dt.: wohlfundierte Ordnung)

A strict partial order \prec on M is called *well-founded* if every $X \subseteq M$, with $X \neq \emptyset$, has at least one minimal element relative to \prec . A poset (M, \prec) is called a *well-founded poset* if \prec is well-founded.

- Of course, $(\mathbb{N}, <)$ is well-founded.

Lemma 80

The poset (M, \prec) is well-founded if and only if no infinite strictly decreasing sequence in M exists, i.e., if an $a : \mathbb{N} \rightarrow M$ with $a_{i+1} \prec a_i$ for all $i \in \mathbb{N}$ does not exist.

- Some authors call a well-founded order also a *Noetherian order*, named after Emmy Noether (1882-1935).
- Not to be confused with a well-order (Dt.: Wohlordnung).

Definition 81

Let (M_1, \prec_1) and (M_2, \prec_2) be two posets. The *lexicographical ordering* $(\prec_1, \prec_2)_{lex}$ on $M_1 \times M_2$ is defined as

$$(a_1, b_1) (\prec_1, \prec_2)_{lex} (a_2, b_2) \quad :\Leftrightarrow \quad ((a_1 \prec_1 a_2) \vee ((a_1 = a_2) \wedge (b_1 \prec_2 b_2))),$$

where $(a_1, b_1), (a_2, b_2) \in M_1 \times M_2$.

Lemma 82

Let (M_1, \prec_1) and (M_2, \prec_2) be two posets. Then $M_1 \times M_2$ together with the lexicographical order $(\prec_1, \prec_2)_{lex}$ is a poset.

- Similarly for a non-strict partial order \preceq .

Lemma 83

The posets (M_1, \prec_1) and (M_2, \prec_2) are well-founded if and only if $(M_1 \times M_2, (\prec_1, \prec_2)_{lex})$ is well-founded.

- Consider a predicate P over \mathbb{N} and recall the Strong Induction Principle (Thm 21):
If $P(1)$ and if

$$\forall k \in \mathbb{N} \quad [(\forall (m \in \mathbb{N}, m \leq k) \ P(m)) \Rightarrow P(k+1)]$$

then

$$\forall n \in \mathbb{N} \quad P(n).$$

- And yet another version with “implicit” base:
If

$$\forall k \in \mathbb{N} \quad [(\forall (m \in \mathbb{N}, m < k) \ P(m)) \Rightarrow P(k)]$$

then

$$\forall n \in \mathbb{N} \ P(n).$$

- Note: The base case was not lost! Rather, it is included since we have to prove $P(1)$ using the “helpful knowledge” that $P(m)$ holds for all $m \in \mathbb{N}$ with $m < 1$.

Theorem 84 (Principle of Well-founded Induction, Dt.: wohlfundierte Induktion)

Let (M, \prec) be well-founded and P be a predicate on M .

If

$$\forall k \in M \ [(\forall (m \in M, m \prec k) \ P(m)) \Rightarrow P(k)]$$

then

$$\forall m \in M \ P(m).$$

- That is, as inductive step we have to prove that the predicate holds for k if it holds for all predecessors m of k relative to \prec .

Proof: Let $X := \{m \in M : P(m) \text{ is false}\}$, and suppose $X \neq \emptyset$. Since (M, \prec) is well-founded, X has a minimal element n . Thus, $\forall m \in M$ with $m \prec n$ the predicate $P(m)$ holds. The inductive step

$$\forall (m \in M, m \prec n) \ P(m) \Rightarrow P(n)$$

yields that $P(n)$ holds, in contradiction to $n \in X$.



Sample Well-founded Induction

- We give a proof of the existence claim made by the Fundamental Theorem of Arithmetic (Thm. 38): Every natural number $n > 1$ is either a prime number or has a prime factorization.

Proof: We begin with observing that the relation “is divisor of” (recall Def. 30) over $\mathbb{N} \setminus \{1\}$ is well-founded. The minimal elements relative to this relation are the primes.

We consider an arbitrary but fixed $k \in \mathbb{N} \setminus \{1\}$ and assume as inductive hypothesis that the claim holds for all $m \in \mathbb{N} \setminus \{1\}$ that are smaller than k relative to this order.

Of course, if k is prime then the claim given by the theorem holds.

So suppose that k is not prime. By definition of primality, this means that there exist $m_1, m_2 \in \mathbb{N} \setminus \{1\}$ such that $k = m_1 \cdot m_2$.

Now we have

$$m_1 \text{ is divisor of } k \quad \text{and} \quad m_2 \text{ is divisor of } k.$$

Hence, both m_1 and m_2 are predecessors of k . By the induction hypothesis, we know that m_1 is either prime or has a prime factorization; same for m_2 . Thus, also k has a prime factorization, which establishes the inductive step. □



Real-World Application: Functional Completeness of NAND

- A NAND gate is a logic gate which produces an output that is false only if all its inputs are true. That is, $(p \mid q) \equiv \neg(p \wedge q)$ for two Boolean variables p, q .

Theorem 85 (Functional completeness of NAND)

Every formula of propositional logic (that contains at least one junctor) can be implemented by using only a combination of NAND gates.

- Thus, any digital circuit can be realized by using only one type of gate: NANDs. (This is also true for the NOR inverter.)

Lemma 86

Let p, q denote two Boolean variables. The following logical equivalences hold:

$$\neg p \equiv (p \mid p) \quad (p \wedge q) \equiv ((p \mid q) \mid (p \mid q)) \quad (p \vee q) \equiv ((p \mid p) \mid (q \mid q))$$

$$(p \Rightarrow q) \equiv (\neg p \vee q) \quad (p \Leftrightarrow q) \equiv ((p \Rightarrow q) \wedge (q \Rightarrow p))$$

$$\top \equiv (p \mid (p \mid p)) \quad \perp \equiv (\top \mid \top)$$

Real-World Application: Functional Completeness of NAND

Proof of Thm. 85: Recall that propositional formulas (over some fixed set of n propositional variables p_1, p_2, \dots, p_n) follow a rigid construction scheme: A propositional formula over the n propositional variables p_1, p_2, \dots, p_n is constructed inductively from a set of

- junctors: $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$;
- parentheses: $(,)$;
- constants (truth values): \perp, \top (or F, T);

based on the following rules:

- A propositional variable is a propositional formula.
- The constants \perp and \top are propositional formulas.
- If ϕ_1 and ϕ_2 are propositional formulas then so are the following:

$$(\neg\phi_1), (\phi_1 \wedge \phi_2), (\phi_1 \vee \phi_2), (\phi_1 \Rightarrow \phi_2), (\phi_1 \Leftrightarrow \phi_2).$$

Real-World Application: Functional Completeness of NAND

Proof of Thm. 85 continued: On the set of of propositional formulas over p_1, p_2, \dots, p_n we define the following order \prec_{PL} :

$$\phi_1 \prec_{PL} \phi_0 \quad :\Longleftrightarrow \quad \left\{ \begin{array}{ll} \phi_0 =_{syn} (\neg \phi_1) & \text{or} \\ \phi_0 =_{syn} (\phi_1 \wedge \phi_2) & \text{for a suitable } \phi_2, \text{ or} \\ \phi_0 =_{syn} (\phi_2 \wedge \phi_1) & \text{for a suitable } \phi_2, \text{ or} \\ \phi_0 =_{syn} (\phi_1 \vee \phi_2) & \text{for a suitable } \phi_2, \text{ or} \\ \phi_0 =_{syn} (\phi_2 \vee \phi_1) & \text{for a suitable } \phi_2, \text{ or} \\ \phi_0 =_{syn} (\phi_1 \Rightarrow \phi_2) & \text{for a suitable } \phi_2, \text{ or} \\ \phi_0 =_{syn} (\phi_2 \Rightarrow \phi_1) & \text{for a suitable } \phi_2, \text{ or} \\ \phi_0 =_{syn} (\phi_1 \Leftrightarrow \phi_2) & \text{for a suitable } \phi_2, \text{ or} \\ \phi_0 =_{syn} (\phi_2 \Leftrightarrow \phi_1) & \text{for a suitable } \phi_2, \end{array} \right.$$

where $=_{syn}$ denotes syntactical equivalence, i.e., equivalence among strings of characters.

Easy to see: \prec_{PL} is a partial order. If $\phi_1 \prec_{PL} \phi_0$ then the number of junctors of ϕ_1 is one smaller than the number of junctors of ϕ_0 . Hence, the order \prec_{PL} is well-founded.

Real-World Application: Functional Completeness of NAND

Proof of Thm. 85 continued: We use a well-founded induction:

- 1 The minimal elements of \prec_{PL} are given by the variables p_1, p_2, \dots, p_n and the constants \perp and \top . Lem. 86 tells us that \perp and \top can be expressed using NANDs.
- 2 Consider an arbitrary but fixed propositional formula ϕ_0 that contains at least one junctor, and assume as inductive hypothesis that all formulas smaller than ϕ_0 relative to \prec_{PL} can be expressed using only NANDs (or are simply variables).

By the construction scheme of propositional formulas, the formula ϕ_0 is of the form $\phi_0 =_{syn} (\neg \phi_1)$ or $\phi_0 =_{syn} (\phi_1 \# \phi_2)$, for suitable ϕ_1, ϕ_2 and where $\#$ is one of the junctors $\wedge, \vee, \leftrightarrow, \Rightarrow$.

Since ϕ_1 (and ϕ_2) are smaller than ϕ_0 , the inductive hypothesis applies and ϕ_1 (and ϕ_2) can be expressed using only NANDs (or are simply variables).

By using the scheme outlined in Lem. 86, also ϕ_0 can be expressed using only NANDs.



Principles of Elementary Counting and Combinatorics

- Sum and Product Rule
- Inclusion-Exclusion Principle
- Binomial Coefficient
- Permutations
- Ordered Selection (Variation)
- Unordered Selection (Combination)

Sum and Product Rule

Theorem 87 (Sum rule, Dt.: Additionsprinzip)

Let A, B be two finite sets with $A \cap B = \emptyset$. Then

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

Corollary 88

For $n \in \mathbb{N}$, let A_1, A_2, \dots, A_n be n finite sets that are pairwise disjoint. Then

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{i=1}^n |A_i|.$$

Theorem 89 (Product rule, Dt.: Multiplikationsprinzip)

Let A, B be two finite sets. Then

$$|A \times B| = |A| \cdot |B|.$$

Sum and Product Rule

Proof of Theorem 89:

- We observe that

$$A \times B = \bigcup_{b \in B} (A \times \{b\}), \quad \text{with } (A \times \{b_1\}) \cap (A \times \{b_2\}) = \emptyset \text{ if } b_1 \neq b_2.$$

- Furthermore, there exists a bijective mapping between A and $A \times \{b\}$. Thus, $|A| = |A \times \{b\}|$, and the theorem is a consequence of Corollary 88.



Corollary 90

For $n \in \mathbb{N}$, let A_1, A_2, \dots, A_n be n finite sets. Then

$$|A_1 \times A_2 \times \dots \times A_n| = \prod_{i=1}^n |A_i|.$$

Corollary 91

For a propositional formula that contains n variables, 2^n evaluations are necessary in order to test all possible combinations of truth assignments to its variables.

Characteristic Function and Cardinality of Power Set

Definition 92 (Characteristic function, Dt.: Indikatorfunktion)

Let A be a finite set, and $B \subseteq A$. The *characteristic function* indicates membership of an element of A in B :

$$1_B : A \rightarrow \{0, 1\}, \quad 1_B(a) := \begin{cases} 1 & \text{if } a \in B, \\ 0 & \text{if } a \notin B. \end{cases}$$

Lemma 93

A finite set A has $2^{|A|}$ many different subsets. That is, $|\mathcal{P}(A)| = 2^{|A|}$.

Proof: We observe that every subset of A , including \emptyset and A itself, has a one-to-one correspondance to a characteristic function. Thus, every subset of A corresponds to a sequence of n 0's and 1's, where $n := |A|$. We conclude that the power set $\mathcal{P}(A)$ has 2^n members. □

Lemma 94

Let A be a finite set, and $B \subseteq A$. Then $|B| = \sum_{a \in A} 1_B(a)$.

Real-World Application: Counting Strings

- How many 3-element strings s can be formed over the standard alphabet — 26 lower-case letters — such that every string contains at least one x ?
- Obviously such an s is in exactly one of the following sets:

$$A_1 := \{s : \text{first } x \text{ in first place of } s\},$$

$$A_2 := \{s : \text{first } x \text{ in second place of } s\},$$

$$A_3 := \{s : \text{first } x \text{ in third place of } s\}.$$

- Applying the Product Rule 89 yields

$$|A_1| = |\{x\} \times \{a, b, \dots, z\} \times \{a, b, \dots, z\}| = 26 \cdot 26,$$

$$|A_2| = |(\{a, b, \dots, z\} \setminus \{x\}) \times \{x\} \times \{a, b, \dots, z\}| = 25 \cdot 26,$$

$$|A_3| = |(\{a, b, \dots, z\} \setminus \{x\}) \times (\{a, b, \dots, z\} \setminus \{x\}) \times \{x\}| = 25 \cdot 25.$$

- Since A_1, A_2, A_3 are pairwise disjoint, the Sum Rule 87 implies

$$|A_1 \cup A_2 \cup A_3| = 1951.$$



Real-World Application: Counting Passwords

- Suppose that passwords are limited to strings of six to eight characters, where each character is one of the 26 uppercase letters or a digit. Every password has to contain at least one digit.
- How many different passwords do exist under these restrictions?
- Let N be the total number of passwords, and let N_6, N_7, N_8 denote the number of passwords with six (seven, eight, resp.) characters.
- By the Product Rule 89, the total number of six-character strings (over the 26 letters and the 10 digits) is 36^6 , with 26^6 of them containing no digit at all. Hence,

$$N_6 = 36^6 - 26^6 = 1\,867\,866\,560.$$

- Similarly,

$$N_7 = 36^7 - 26^7 = 70\,332\,353\,920$$

and

$$N_8 = 36^8 - 26^8 = 2\,612\,282\,842\,880.$$

- Hence, by the Sum Rule 87,

$$N = N_6 + N_7 + N_8 = 2\,684\,483\,063\,360.$$



Theorem 95 (Inclusion-exclusion principle, Dt.: Siebprinzip, Poincaré-Formel)

Let A_1, A_2, \dots, A_n be finite sets. Then

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

• For $|I| = 1$:

$$\sum_{1 \leq i \leq n} (-1)^{1+1} |A_i| = \sum_{i=1}^n |A_i|.$$

• For $|I| = 2$:

$$\sum_{1 \leq i < j \leq n} (-1)^{2+1} |A_i \cap A_j| = - \sum_{1 \leq i < j \leq n} |A_i \cap A_j|.$$

• In particular:

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$



Real-World Application: Counting Bit Strings

- How many bit strings of length eight either start with 1 as first bit or end in 00 as the two last bits? (This is a non-exclusive or!)
- Let A_1 be the set of 8-bit strings that start with 1. Similarly, let A_2 be the set of 8-bit strings that end in 00.
- Then the number sought equals $|A_1 \cup A_2|$.
- By the Product Rule 89,

$$|A_1| = 2^7 = 128 \quad \text{and} \quad |A_2| = 2^6 = 64 \quad \text{and} \quad |A_1 \cap A_2| = 2^5 = 32.$$

- Hence, by the Inclusion-Exclusion Principle (Thm. 95),

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| = 128 + 64 - 32 = 160.$$



Definition 96 (Binomial coefficient, Dt.: Binomialkoeffizient)

Let $n \in \mathbb{N}_0$ and $k \in \mathbb{Z}$. Then the *binomial coefficient* $\binom{n}{k}$ of n and k is defined as follows:

$$\binom{n}{k} := \begin{cases} 0 & \text{if } k < 0, \\ \frac{n!}{k! \cdot (n-k)!} & \text{if } 0 \leq k \leq n, \\ 0 & \text{if } k > n. \end{cases}$$

- Recall $k! := 1$ for $k = 0$.
- The binomial coefficient $\binom{n}{k}$ is pronounced as “ n choose k ”; Dt.: “ n über k ”.

Lemma 97

Let $n \in \mathbb{N}_0$ and $k \in \mathbb{Z}$.

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

Binomial Coefficients

- The following table contains the non-zero values of $\binom{n}{k}$ for $0 \leq n, k \leq 6$.

n	k						
	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

- Trivial to observe:
 - Each row begins and ends with 1.
 - Initially each row contains increasing numbers till its middle but then the numbers start to decrease.
 - Each row's first half is exactly the mirror image of its second half.

Binomial Coefficients: Pascal's Triangle

- A simple rearrangement of the previous table yields what is known as *Pascal's Triangle* in the Western world (Blaise Pascal, 1623–1662). But it was already studied in India in the 10th century, and discussed by Omar Khayyam (1048–1131)!

						1						
					1		1		1			
				1		2		1				
			1		3		3		1			
		1		4		6		4		1		
	1		6		15		20		15		6	
1		6		15		20		15		6		1

- All entries in this triangle, except for the left-most and right-most entries per row, are the sum of the two entries above them in the previous row.

Theorem 98 (Khayyam, Yang Hui, Tartaglia, Pascal)

For $n \in \mathbb{N}$ and $k \in \mathbb{Z}$,

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

Binomial Theorem

- We know: $(a + b)^2 = a^2 + 2ab + b^2$ and $(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$.

Theorem 99 (Binomial Theorem, Dt.: Binomischer Lehrsatz)

For all $n \in \mathbb{N}_0$ and $a, b \in \mathbb{R}$,

$$(a + b)^n = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \cdots + \binom{n}{n} b^n$$

or, equivalently,

$$(a + b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i.$$

Corollary 100

For all $n \in \mathbb{N}$ and all $x \in \mathbb{R}$:

$$\sum_{i=0}^n \binom{n}{i} x^i = (1 + x)^n$$

$$\sum_{i=0}^n \binom{n}{i} = 2^n$$

$$\sum_{i=0}^n (-1)^i \binom{n}{i} = 0$$

Definition 101 (Permutation)

Let A be a finite set. A *permutation* of A is a bijective function from A to A . The set of all permutations of $I_n := \{1, 2, \dots, n\}$, for $n \in \mathbb{N}$, is denoted by S_n .

- A permutation on a finite set A of cardinality n can be regarded as an (ordered) sequence of length n in which every element of A appears exactly once.
- Standard notation for a permutation π of S_n :

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}$$

Definition 102 (Product of permutations)

Let A be a finite set together with two permutations α, β . Then the *product* (or *composition*) $\alpha \circ \beta$ is the function

$$\alpha \circ \beta : A \rightarrow A \quad \text{with} \quad (\alpha \circ \beta)(a) := \alpha(\beta(a)) \quad \text{for all } a \in A.$$

Warning

Some authors take $(\alpha \circ \beta)(a)$ as $(\beta(\alpha(a)))!$

Permutations

- Of course, the product of two permutations is itself a bijective function.
- Note: It is common to drop \circ in $\alpha \circ \beta$ and simply write $\alpha\beta$.
- The product of two permutations is not commutative.

$$\alpha := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \quad \beta := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \quad \beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

Lemma 103

For all $n \in \mathbb{N}$, the set of all permutations, S_n , over I_n together with \circ as operation forms a group, the so-called *symmetric group*.

Lemma 104

For all $n \in \mathbb{N}$, the set of all permutations, S_n , has exactly $n!$ members.

Definition 105 (Cycle, Dt.: Zyklus)

Let A be a finite set of cardinality n . A permutation π of A is a *cycle of length* $k \leq n$ if there exists a set $B \subseteq A$ with $|B| = k$ such that, with $B := \{b_1, b_2, \dots, b_k\}$,

$$\pi(b_1) = b_2, \quad \pi(b_2) = b_3, \quad \dots, \quad \pi(b_{k-1}) = b_k, \quad \pi(b_k) = b_1,$$

and $\pi(a) = a$ for all $a \in A \setminus B$. In this case this k -cycle is written as

$$(b_1 \ b_2 \ \dots \ b_k) \quad \text{or as} \quad b_1 \mapsto b_2 \mapsto \dots \mapsto b_k \mapsto b_1.$$

Definition 106 (Transposition)

A *transposition* is a 2-cycle.

Lemma 107

Every permutation can be written as

- (1) a product of cycles,
- (2) a product of transpositions.

Lemma 108

If two different products of transpositions correspond to the same permutation then both products consist of either an even or an odd number of transpositions.

Definition 109 (Signature, Dt.: Signum)

The *signature* of a permutation is $+1$, and the permutation is *even*, if it consists of an even number of transpositions. Otherwise, the signature is -1 and the permutation is *odd*.

Definition 110 (Derangement, Dt.: Permutation ohne Fixpunkt)

A permutation π of A is a *derangement* if $\pi(a) \neq a$ for all $a \in A$.

Ordered Selection

Definition 111 (Ordered selection without repetition, Dt.: Variation ohne Zurücklegen, Variation ohne Wiederholung)

Let $n \in \mathbb{N}$ and $k \in \mathbb{N}_0$, with $k \leq n$, and A be a finite set of cardinality n . An *ordered selection without repetition* of k elements from A is a k -tuple

$$(a_1, a_2, \dots, a_k) \quad \text{with } a_i \in A \text{ for } i = 1, 2, \dots, k \text{ and } a_i \neq a_j \text{ for } 1 \leq i < j \leq k.$$

Lemma 112

Let $n \in \mathbb{N}$ and $k \in \mathbb{N}_0$, with $k \leq n$, and A be a finite set of cardinality n . There exist

$$V_k^n := \frac{n!}{(n-k)!}$$

many different ordered selections without repetition of k elements from A .

- Convention: $V_k^n := 0$ for $k > n$.
- V_k^n is the number of injective functions from I_k to A .
- Sometimes, $V(n, k)$ is written instead of V_k^n . Also, English-language textbooks often speak of a k -permutation rather than of an ordered selection without repetition of k elements.



Definition 113 (Ordered selection with repetition, Dt.: Variation mit Zurücklegen)

Let $n \in \mathbb{N}$ and $k \in \mathbb{N}_0$, and A be a finite set of cardinality n . An *ordered selection with repetition* of k elements from A is a k -tuple

$$(a_1, a_2, \dots, a_k) \quad \text{with } a_i \in A \text{ for } i = 1, 2, \dots, k.$$

Lemma 114

Let $n \in \mathbb{N}$ and $k \in \mathbb{N}_0$, and A be a finite set of cardinality n . There exist

$${}_r V_k^n := n^k$$

many different ordered selections with repetition of k elements from A .

- Dt.: Auch *Variation mit Wiederholung*.
- Note: ${}_r V_k^n = |A^k|$.
- Sometimes, $V_r(n, k)$ is written instead of ${}_r V_k^n$.

Unordered Selection

Definition 115 (Unordered selection without repetition, Dt.: Kombination ohne Zurücklegen, Kombination ohne Wiederholung)

Let $n \in \mathbb{N}$ and $k \in \mathbb{N}_0$, with $k \leq n$, and A be a finite set of cardinality n . An *unordered selection without repetition* of k elements from A is a set B such that

$$B \subseteq A \quad \text{with} \quad |B| = k.$$

Lemma 116

Let $n \in \mathbb{N}$ and $k \in \mathbb{N}_0$, with $k \leq n$, and A be a finite set of cardinality n . There exist

$$C_k^n := \binom{n}{k}$$

many different unordered selections without repetition of k elements from A .

- Convention: $C_k^n := 0$ for $k > n$.
- Lemma 116 yields an alternate proof of $|\mathcal{P}(A)| = 2^n$. It also implies that there exist $\binom{n}{k}$ different binary sequences where exactly k elements are 1.
- Sometimes, $C(n, k)$ is written instead of C_k^n .



Definition 117 (Unordered selection w. repetition, Dt.: Kombination m. Zurücklegen)

Let $n \in \mathbb{N}$ and $k \in \mathbb{N}_0$, and A be a finite set of cardinality n . An *unordered selection with repetition* of k elements from A is a k -element *multiset*, i.e., a set B together with a *multiplicity function*, *mult*, such that

$$B \subseteq A \quad \text{and} \quad \text{mult} : B \rightarrow \mathbb{N} \quad \text{with} \quad \sum_{b \in B} \text{mult}(b) = k.$$

Lemma 118

Let $n \in \mathbb{N}$ and $k \in \mathbb{N}_0$, and A be a finite set of cardinality n . There exist

$${}_r C_k^n := \binom{n+k-1}{k}$$

many different unordered selections with repetition of k elements from A .

- Dt.: Auch *Kombination mit Wiederholung*.
- Sometimes, $C_r(n, k)$ is written instead of ${}_r C_k^n$.

Proofs of Lemmas 112–116

Proof of Lemma 112: We have n options for a_1 , leaving $n - 1$ options for a_2 , etc. Thus, we have $n \cdot (n - 1) \cdot \dots \cdot (n - k + 1) = \frac{n!}{(n-k)!}$ options. □

Proof of Lemma 114: We have n options for every selection. Thus, we have n^k options in total. □

Proof of Lemma 116: We know that $V_k^n = \frac{n!}{(n-k)!}$. There are $k!$ many different ordered selections that correspond to the same unordered selection. Thus, $C_k^n = V_k^n / k! = \frac{n!}{(n-k)!k!} = \binom{n}{k}$. □

Sample Unordered Selection With Repetition

- Suppose you are buying a 3-scoop icecream cup and that the flavor options are chocolate, vanilla, strawberry, and blackberry.
- You can also choose all the three scoops to be of the same flavor, say, vanilla.
- Hence, we have $A = \{\text{chocolate, vanilla, strawberry, blackberry}\}$ and $n = 4$ and $k = 3$.
- Using

$${}^r C_k^n = \binom{n+k-1}{k} = \frac{(n+k-1)!}{k!(n-1)!},$$

for our current example, we have 20 options to choose our icecream:

$${}^r C_3^4 = \binom{4+3-1}{3} = \frac{6!}{3!(4-1)!} = 20.$$

Sample Unordered Selection With Repetition

- What is the number of non-negative integer solutions of the Diophantine equation $x_1 + x_2 + x_3 + x_4 = 10$?
- Think of the variables x_i as four categories, x_1, x_2, x_3, x_4 , which are separated by three vertical bars. Let the number of crosses in each category indicate the value of x_i in the solution. Thus

$$\times_1 \times_1 || \times_3 \times_3 \times_3 \times_3 | \times_4 \times_4 \times_4 \times_4$$

represents the solution $x_1 = 2, x_2 = 0, x_3 = 4, x_4 = 4$.

- We have $A = \{\times_1, \times_2, \times_3, \times_4\}$ and $n = 4$. There must be 10 crosses in all, so $k = 10$. In all, there are ${}^rC_{10}^4 = 286$ different solutions.
- What if we want to count the number of solutions where each $x_i \geq 1$?
- One way to do this is to initially put one cross in each category. There are now $k = 10 - 4 = 6$ crosses remaining, and still 4 categories. So there are ${}^rC_6^4 = 84$ such solutions.

Real-World Application: Elementary Probability

- What is the probability to win in the Austrian “6-aus-45” lottery after choosing one set of six numbers?
- As usual, we define the probability of an event among equally-likely outcomes as the number of favorable outcomes divided by the total number of possible outcomes.
- Assuming that the lottery is fair and, thus, that all combinations are equally likely to win, we have

$$\frac{1}{C_6^{45}} = \frac{1}{\binom{45}{6}} = \frac{1}{8145060} \approx 1.22774 \cdot 10^{-7}.$$

Real-World Application: Elementary Probability

- A standard deck of cards contains 52 cards grouped into four suits (diamonds, clubs, hearts, and spades), with 13 cards in each suit (ace, 2, 3, 4, 5, 6, 7, 8, 9, 10, jack, queen, king).
- What is the probability that all hearts appear in consecutive order after a decent shuffling of the deck?
- There are $52!$ different permutations of the 52 cards.
- There are $40!$ different permutations of the 39 cards plus one block of 13 hearts, and $13!$ many permutations of the 13 hearts.
- Hence, the probability that all hearts are consecutive is given by

$$\frac{40! \cdot 13!}{52!} \approx 6.29908 \cdot 10^{-11}.$$

Real-World Application: Elementary Probability

- All 52 cards are distributed to four players. (Again we assume that the deck was shuffled decently.) What is the probability that one of the four players gets four aces?
- The possible outcomes are the positions of the four aces within the 52 cards. We have a total of C_4^{52} such outcomes.
- A distribution of the cards is favorable if all four aces are within the thirteen cards of one of the four players. We have a total of $C_1^4 \cdot C_4^{13}$ such favorable outcomes.
- Hence, the probability that one of the four players gets four aces is given by

$$\frac{C_1^4 \cdot C_4^{13}}{C_4^{52}} = \frac{\binom{4}{1} \cdot \binom{13}{4}}{\binom{52}{4}} \approx 0.010564$$

Complexity Analysis and Recurrence Relations

- Complexity of an Algorithm
- Asymptotic Analysis
- Recurrence Relations
- Master Theorem

Complexity of an Algorithm

- Typical kinds of complexities studied:
 - time complexity, i.e., a mathematical estimation of the running time independent of a particular implementation or platform;
 - space complexity, i.e., a mathematical estimation of the number of memory units consumer by the algorithm;
 - complexity of the output generated.
- We start with four (informal!) definitions that pertain to the complexity analysis of algorithms.

Definition 119 (Elementary Operation, Dt.: Elementaroperation)

An *elementary operation* is an operation whose running time is assumed not to depend on the specific values of its operands, such as the time for the comparison of two floating-point numbers.

Definition 120 (Input Size, Dt.: Eingabegröße)

The *size of the input* of an algorithm is a quantity that measures the number of input items relevant for elementary operations of the algorithm, such as the number of memory units needed to represent the input data, or the number of records to be sorted (if constant memory and comparison time per record may be assumed).

Complexity of an Algorithm

Definition 121 (Worst-Case Complexity, Dt.: Komplexität im schlimmsten Fall)

A *worst-case complexity* of an algorithm is a function $f: \mathbb{N} \rightarrow \mathbb{R}^+$ that gives an upper bound on the number of elementary operations of an algorithm with respect to the size of its input, for all inputs of the same size.

Definition 122 (Average-Case Complexity, Dt. Komplexität im durchschnittl. Fall)

An *average-case complexity* of an algorithm is a function $g: \mathbb{N} \rightarrow \mathbb{R}^+$ that models the average number of elementary operations of an algorithm with respect to the size of its input.

- It is common to denote the input size by the variable n .
- If m is the (finite!) number of inputs $\{l_1, l_2, \dots, l_m\}$ of size n and $h(l_k)$ denotes the number of elementary operations of an algorithm for input l_k , then

$$g(n) = \frac{1}{m} \sum_{k=1}^m h(l_k).$$

- The worst-case complexity is a pessimistic estimator; the average-case complexity often is more relevant if the worst case is encountered rarely.
- In any case, we seek sharp bounds.



Growth Rate of Functions

- Small input sizes can usually be computed instantaneously. Therefore we are most interested in how an algorithm performs as n gets large: *asymptotic complexity analysis*.
- We are interested in the growth of the complexity as a function of the input size n .
- Determine the dominating term in the complexity function – it gives the order of magnitude of the asymptotic behavior.

$$1, \log n, \log^2 n, \sqrt{n}, n, n \log n, n \log^2 n, n^{\frac{7}{6}}, n^2, n^3, \dots, 2^n, 3^n, 2^{(2^n)}, \dots$$

- Note: In this course, $\log n$ will always denote the logarithm of n to the base 2, i.e., $\log n := \log_2 n$. Recall that $\log_\alpha n = \frac{1}{\log_2 \alpha} \log_2 n$.

How Can We Compare the Growth Rate of Functions?

- Let's consider $f, g: \mathbb{N} \rightarrow \mathbb{R}^+$ with $f(n) := n$ and $g(n) := 9n + 20$.

- We get for all $n \in \mathbb{N}$ with $n \geq 20$

$$g(n) = 9n + 20 \leq 9n + n = 10n = 10f(n), \quad \text{that is } g(n) \leq 10f(n).$$

- Also for all $n \in \mathbb{N}$

$$f(n) \leq g(n).$$

Thus, we have

$$\underbrace{c_1 \cdot f(n) \leq g(n) \leq c_2 \cdot f(n)}_{\text{for all } n \geq n_0 \text{ where } n_0 := 20, \text{ } c_1 := 1, \text{ } c_2 := 10.}$$

g grows at least as fast as $c_1 \cdot f$
 f is an asymptotic lower bound on g
we'll say that $g \in \Omega(f)$

g grows at most as fast as $c_2 \cdot f$
 f is an asymptotic upper bound on g
we'll say that $g \in O(f)$

g has same growth rate as f
we'll say that $g \in \Theta(f)$



Asymptotic Notation: Big-O

$$c_1 \cdot f(n) \leq g(n) \leq c_2 \cdot f(n) \quad \left\{ \begin{array}{l} \text{for all } n \geq n_0 \text{ and} \\ \text{fixed } c_1, c_2 \in \mathbb{R}^+. \end{array} \right.$$

g grows at most as fast as $c_2 \cdot f$
 f is an asymptotic upper bound on g
we'll say that $g \in O(f)$

Definition 123 (Big-O, Dt.: Groß-O)

Let $f: \mathbb{N} \rightarrow \mathbb{R}^+$. Then the set $O(f)$ is defined as

$$O(f) := \{g: \mathbb{N} \rightarrow \mathbb{R}^+ \mid \exists c_2 \in \mathbb{R}^+ \exists n_0 \in \mathbb{N} \forall n \geq n_0 \quad g(n) \leq c_2 \cdot f(n)\}.$$

- Note: $O(f)$ is a set of functions!
- Definitions of the form

$O(f(n)) := \{g: \mathbb{N} \rightarrow \mathbb{R}^+ \mid \exists c_2 \in \mathbb{R}^+ \exists n_0 \in \mathbb{N} \forall n \geq n_0 \quad g(n) \leq c_2 \cdot f(n)\}$
are a (wide-spread) formal nonsense.

- Some authors prefer to use the symbol \mathcal{O} instead of O .

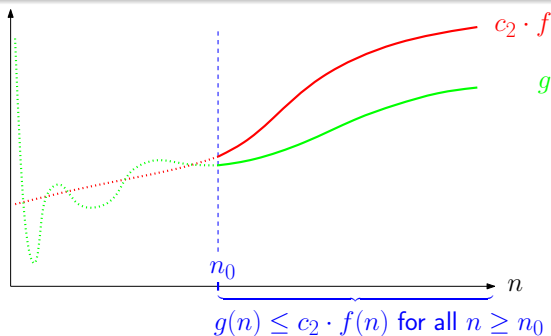


Graphical Illustration of $O(f)$

Definition 123 (Big-O, Dt.: Groß-O)

Let $f: \mathbb{N} \rightarrow \mathbb{R}^+$. Then the set $O(f)$ is defined as

$$O(f) := \{g: \mathbb{N} \rightarrow \mathbb{R}^+ \mid \exists c_2 \in \mathbb{R}^+ \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad g(n) \leq c_2 \cdot f(n)\}.$$



- Equivalent definition used by some authors:

$$O(f) := \left\{ g: \mathbb{N} \rightarrow \mathbb{R}^+ \mid \exists c_2 \in \mathbb{R}^+ \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad \frac{g(n)}{f(n)} \leq c_2 \right\}.$$



Why Don't We Care About Constants?

- Note that this notation hides all lower-order terms and multiplicative constants. Why don't we care?
- Since it doesn't matter for large values of n !
- Consider the following two nested for-loops:

```
for  $i = 1$  to  $n$  do
  for  $j = i$  to  $n$  do
    Compute( $i, j$ )
  end for
end for
```

- How often is Compute() being called?
Let $g: \mathbb{N} \rightarrow \mathbb{R}^+$ be the function that models the number of calls in dependence on n .
- We get

$$\begin{aligned} g(n) &= n + (n-1) + \dots + 2 + 1 \\ &= \frac{n(n+1)}{2} = \frac{1}{2}n^2 + \frac{1}{2}n. \end{aligned}$$

- Consider $f: \mathbb{N} \rightarrow \mathbb{R}^+$ with $f(n) := n^2$.
- Let's compare the growth rates of f and g when we double n :

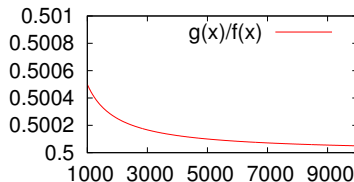
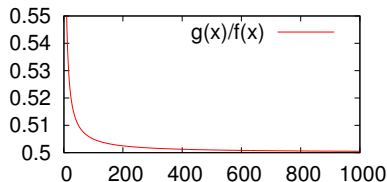
n	$g(n)$	$f(n)$
1	1	1
5	15	25
10	55	100
20	210	400
40	820	1600
80	3240	6400

- Doubling n causes both $f(n)$ and $g(n)$ to (roughly) quadruple!



Why Don't We Care About Constants?

- We plot the growth ratio $\frac{g(n)}{f(n)}$ for $f, g: \mathbb{N} \rightarrow \mathbb{R}^+$ with $f(n) := n^2$ and $g(n) := \frac{1}{2}n^2 + \frac{1}{2}n$.



- The plots suggest $\frac{g(n)}{f(n)} \leq 1$ for all $n \geq 200$, that is, $g(n) \leq f(n)$, which would imply $g \in O(f)$.
- More precisely, they suggest $\frac{g(n)}{f(n)} \leq \frac{1}{2} + \varepsilon$ for any positive ε and all sufficiently large values of n .
- The plots also suggest $\frac{g(n)}{f(n)} \geq \frac{1}{2}$, which would imply $g \in \Omega(f)$.
- Hence $g(n) \approx \frac{1}{2}f(n)$, which would imply $g \in \Theta(f)$.

Asymptotic Notation: Big-Omega

$$c_1 \cdot f(n) \leq g(n) \leq c_2 \cdot f(n)$$

$$\left\{ \begin{array}{l} \text{for all } n \geq n_0 \text{ and} \\ \text{fixed } c_1, c_2 \in \mathbb{R}^+. \end{array} \right.$$

g grows at least as fast as $c_1 \cdot f$

f is an asymptotic lower bound on g

we'll say that $g \in \Omega(f)$

Definition 124 (Big-Omega, Dt.: Groß-Omega)

Let $f: \mathbb{N} \rightarrow \mathbb{R}^+$. Then the set $\Omega(f)$ is defined as

$$\Omega(f) := \left\{ g: \mathbb{N} \rightarrow \mathbb{R}^+ \mid \exists c_1 \in \mathbb{R}^+ \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad c_1 \cdot f(n) \leq g(n) \right\}.$$

• Equivalently,

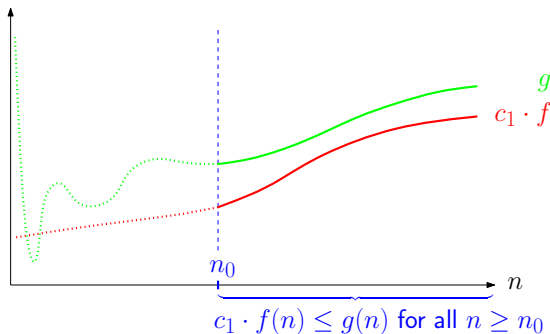
$$\Omega(f) := \left\{ g: \mathbb{N} \rightarrow \mathbb{R}^+ \mid \exists c_1 \in \mathbb{R}^+ \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad c_1 \leq \frac{g(n)}{f(n)} \right\}$$

Graphical Illustration of $\Omega(f)$

Definition 124 (Big-Omega, Dt.: Groß-Omega)

Let $f: \mathbb{N} \rightarrow \mathbb{R}^+$. Then the set $\Omega(f)$ is defined as

$$\Omega(f) := \{g: \mathbb{N} \rightarrow \mathbb{R}^+ \mid \exists c_1 \in \mathbb{R}^+ \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad c_1 \cdot f(n) \leq g(n)\}.$$



Asymptotic Notation: Big-Theta

$$\underbrace{c_1 \cdot f(n) \leq g(n) \leq c_2 \cdot f(n)}_{\substack{\text{for all } n \geq n_0 \text{ and} \\ \text{fixed } c_1, c_2 \in \mathbb{R}^+ .}}$$

g has same growth rate as f
we'll say that $g \in \Theta(f)$

Definition 125 (Big-Theta, Dt.: Groß-Theta)

Let $f: \mathbb{N} \rightarrow \mathbb{R}^+$. Then the set $\Theta(f)$ is defined as

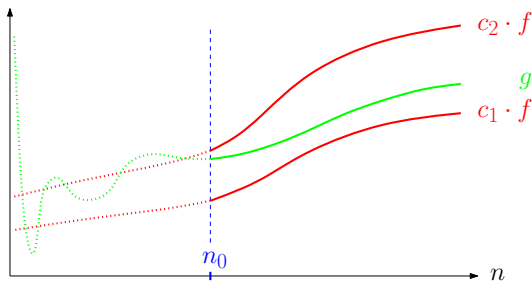
$$\Theta(f) := \left\{ g: \mathbb{N} \rightarrow \mathbb{R}^+ \mid \exists c_1, c_2 \in \mathbb{R}^+ \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \right. \\ \left. c_1 \cdot f(n) \leq g(n) \leq c_2 \cdot f(n) \right\} .$$

Graphical Illustration of $\Theta(f)$

Definition 125 (Big-Theta, Dt.: Groß-Theta)

Let $f: \mathbb{N} \rightarrow \mathbb{R}^+$. Then the set $\Theta(f)$ is defined as

$$\Theta(f) := \{g: \mathbb{N} \rightarrow \mathbb{R}^+ \mid \exists c_1, c_2 \in \mathbb{R}^+ \exists n_0 \in \mathbb{N} \forall n \geq n_0 \\ c_1 \cdot f(n) \leq g(n) \leq c_2 \cdot f(n)\}.$$



$$c_1 \cdot f(n) \leq g(n) \leq c_2 \cdot f(n) \text{ for all } n \geq n_0$$

which is equivalent to $c_1 \leq \frac{g(n)}{f(n)} \leq c_2$ for all $n \geq n_0$



Sample Proof of $g \in \Theta(f)$

- We prove $g \in \Theta(f)$ for $f(n) := n^2$ and $g(n) := \frac{1}{2}n^2 + \frac{1}{2}n$.

Proof:

- We get, for all $n \in \mathbb{N}$,

$$g(n) = \frac{1}{2}n^2 + \frac{1}{2}n \leq \frac{1}{2}n^2 + \frac{1}{2}n^2 = n^2 = f(n), \quad \text{that is } g(n) \leq f(n).$$

- Thus, $g \in O(f)$ with $c_2 := 1$ and $n_0 := 1$.
- Now we prove $g \in \Omega(f)$ and get, again for all $n \in \mathbb{N}$,

$$g(n) = \frac{1}{2}n^2 + \frac{1}{2}n \geq \frac{1}{2}n^2 = \frac{1}{2}f(n), \quad \text{that is } \frac{1}{2}f(n) \leq g(n).$$

- Thus, $g \in \Omega(f)$ with $c_1 := \frac{1}{2}$ and $n_0 := 1$. Lemma 128 implies $g \in \Theta(f)$. □
- There is no need to try to obtain the smallest-possible values for n_0 and c_1, c_2 !
- Can we also prove $h \in O(f)$ for $h: \mathbb{N} \rightarrow \mathbb{R}^+$ with $h(n) := n^3$? We get, for all $n \in \mathbb{N}$,

$$\frac{h(n)}{f(n)} = \frac{n^3}{n^2} = n.$$

- Thus, $\frac{h(n)}{f(n)}$ grows unboundedly as n grows, while it ought to be bounded by some constant c_2 for all $n \geq n_0$, for some fixed $n_0 \in \mathbb{N}$. We conclude that $h \notin O(f)$.



Definition 126 (Small-Oh, Dt.: Klein-O)

Let $f: \mathbb{N} \rightarrow \mathbb{R}^+$. Then the set $o(f)$ is defined as

$$o(f) := \{g: \mathbb{N} \rightarrow \mathbb{R}^+ \mid \forall c \in \mathbb{R}^+ \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad g(n) \leq c \cdot f(n)\}.$$

Mind the difference

$$O(f) := \{g: \mathbb{N} \rightarrow \mathbb{R}^+ \mid \exists c \in \mathbb{R}^+ \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad g(n) \leq c \cdot f(n)\}$$

$$o(f) := \{g: \mathbb{N} \rightarrow \mathbb{R}^+ \mid \forall c \in \mathbb{R}^+ \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad g(n) \leq c \cdot f(n)\}$$

- Similarly, $\omega(f)$ can be defined relative to $\Omega(f)$.
- It is trivial to extend Definitions 123–126 such that \mathbb{N}_0 rather than \mathbb{N} is taken as the domain (Dt.: Definitionsmenge).
- We can also replace the codomain (Dt.: Zielbereich) \mathbb{R}^+ by \mathbb{R}_0^+ (or even \mathbb{R}) provided that all functions are eventually positive.
- The same comments apply to the subsequent slides.

Asymptotic Notation: Basic Facts

Lemma 127

Let $f_1, f_2, g_1, g_2: \mathbb{N} \rightarrow \mathbb{R}^+$, and $c \in \mathbb{R}^+$. Then the following relations hold:

$$g_1 \in O(f_1) \wedge g_2 \in O(f_2) \Rightarrow g_1 + g_2 \in O(f_1 + f_2)$$

$$g_1 \in O(f_1) \wedge g_2 \in O(f_2) \Rightarrow g_1 \cdot g_2 \in O(f_1 \cdot f_2)$$

$$f_2 \cdot O(f_1) \subseteq O(f_1 \cdot f_2) \qquad g_1 \in \Theta(f_1) \Leftrightarrow f_1 \in \Theta(g_1)$$

$$O(c \cdot f_1) = O(f_1) \qquad g_1 \in O(f_1) \Rightarrow c \cdot g_1 \in O(f_1)$$

Lemma 128

Let $f, g: \mathbb{N} \rightarrow \mathbb{R}^+$. Then:

$$\Theta(f) = O(f) \cap \Omega(f),$$

and

$$g \in o(f) \Leftrightarrow \lim_{n \rightarrow \infty} \frac{g(n)}{f(n)} = 0.$$

Asymptotic Notation: Limit of a Sequence

Definition 129 (Sequence, Dt.: Folge)

A (real) *sequence*, $(x_n)_{n \in \mathbb{N}}$ or $\{x_n\}_{n \in \mathbb{N}}$, or simply (x_n) or $\{x_n\}$, is a function $x: \mathbb{N} \rightarrow \mathbb{R}$.

Definition 130 (Limit, Dt. Grenzwert)

The value $\bar{x} \in \mathbb{R}$ is the limit of the (real) sequence (x_n) , denoted by $\lim_{n \rightarrow \infty} x_n = \bar{x}$, if

$$\forall \varepsilon \in \mathbb{R}^+ \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad |x_n - \bar{x}| < \varepsilon.$$

Theorem 131 (Squeeze theorem, Dt.: Einschnürungssatz)

Consider three real sequences (x_n) , (y_n) , (z_n) and suppose that $x_n \leq y_n \leq z_n$ for all $n \geq n_0$ for some $n_0 \in \mathbb{N}$. If the limits of (x_n) and (z_n) exist such that

$$\lim_{n \rightarrow \infty} x_n = \lim_{n \rightarrow \infty} z_n,$$

then the limit of (y_n) exists with

$$\lim_{n \rightarrow \infty} x_n = \lim_{n \rightarrow \infty} y_n = \lim_{n \rightarrow \infty} z_n.$$

Asymptotic Notation: Limit of a Sequence

- The following theorem (by Guillaume de l'Hôpital, 1661–1704) allows to handle limits that involve indeterminate terms of the form

$$\frac{0}{0} \quad \text{or} \quad \frac{\infty}{\infty}.$$

Theorem 132 (L'Hôpital's rule)

Consider two real functions f and g and a real value c .

If

- 1 $\lim_{x \rightarrow c} f(x) = 0 = \lim_{x \rightarrow c} g(x)$ or $\lim_{x \rightarrow c} f(x) = \pm\infty = \lim_{x \rightarrow c} g(x)$,
- 2 f and g are differentiable in an open interval I with $c \in I$, except possibly at c itself,
- 3 $g'(x) \neq 0$ for all $x \in I \setminus \{c\}$, and if
- 4 $\lim_{x \rightarrow c} \frac{f'(x)}{g'(x)}$ exists,

then

$$\lim_{x \rightarrow c} \frac{f(x)}{g(x)} = \lim_{x \rightarrow c} \frac{f'(x)}{g'(x)}.$$

Asymptotic Notation: Wide-spread Notational Abuse

- It is common to write

$$g(n) = O(n^2) \quad \text{or} \quad g \in O(n^2)$$

as an informal short-hand notation for

$$g \in O(f) \quad \text{with } f: \mathbb{N} \rightarrow \mathbb{R}^+, n \mapsto n^2.$$

- Similarly,

$$g(n) = h(n) + O(n^3)$$

means

$$|g - h| \in O(f) \quad \text{with } f: \mathbb{N} \rightarrow \mathbb{R}^+, n \mapsto n^3.$$

- Furthermore,

$$g(n) = n^{O(1)}$$

indicates that

$$g \in O(f) \quad \text{with } f: \mathbb{N} \rightarrow \mathbb{R}^+, n \mapsto n^c$$

for some constant $c \in \mathbb{R}^+$.



Warning

- 1 In the equation-based notation the equality sign does not assert the equality of two functions or sets!
- 2 The property expressed by this equality sign is not symmetric! That is,

$$O(n^2) = O(n^3) \quad \text{but} \quad O(n^3) \neq O(n^2).$$

- 3 Stipulating

$$g(m) = O(m^n)$$

is not the same as stipulating

$$g(n) = O(m^n).$$

- It is convenient to be a bit sloppy and write, e.g., $n^2 = O(n^3)$, rather than to resort to the λ -quantifier and write $\lambda n. n^2 \in O(\lambda n. n^3)$. But keep in mind that an *is-element-of* or *subset relation* is meant even if an equality sign is used!
- Unfortunately, several textbooks are fuzzy about this important distinction



Some Growth Rates Arranged in Increasing Order

- $O(1)$ *constant*:
E.g., the time consumed by a basic arithmetic operation.
- $O(\alpha)$ *inverse Ackermann*:

$$A(m, n) := \begin{cases} n + 1 & \text{if } m = 0, \\ A(m - 1, 1) & \text{if } m > 0 \text{ and } n = 0, \\ A(m - 1, A(m, n - 1)) & \text{if } m > 0 \text{ and } n > 0. \end{cases}$$

The Ackermann function $A(m, n)$ grows extremely rapidly. E.g.,
 $A(4, 3) = 2^{2^{65536}} - 3$. Hence, the inverse of $A(n, n)$, the inverse Ackermann function $\alpha(n)$, grows extremely slowly; it is less than 5 for any input of practical relevance. But it does grow unboundedly as n grows, and $O(1) \subset O(\alpha)$!

- $O(\log^* n)$ *log star*:

$$\log^* n := \begin{cases} 0 & \text{if } n \leq 1, \\ 1 + \log^*(\log n) & \text{if } n > 1. \end{cases}$$

- $O(\log n)$ *logarithmic*:
E.g., the time consumed by a binary search in a sorted array of n numbers.



Some Growth Rates Arranged in Increasing Order

- $O(n)$ *linear*:
E.g., the time consumed by determining the minimum of n unsorted numbers.
- $O(n \log^* n)$ *n -log-star- n* :
E.g., in computational geometry, the randomized time consumed by computing the Delaunay triangulation of n points in the plane if their Euclidean minimum spanning tree is known.
- $O(n \log n)$ *n -log- n* :
E.g., the worst-case time consumed by running heapsort on n numbers; the average time consumed by quicksort for n numbers.
Note: We have $\Theta(\log n^n) = \Theta(n \log n)$. Also, Stirling's formula asserts

$$n! \approx \sqrt{2\pi n} \left(\frac{n}{e}\right)^n, \quad \text{thus, } \Theta(\log n!) = \Theta(n \log n).$$

- $O(n^2)$ *quadratic*:
E.g., the time consumed by adding two $n \times n$ matrices; the worst-case time of quicksort for n numbers.
- $O(n^3)$ *cubic*:
E.g., the time consumed by inverting a (dense) $n \times n$ matrix.
- $O(n^c)$, $c > 1$ *polynomial*.



Some Growth Rates Arranged in Increasing Order

- $O(c^n)$, $c > 1$ *exponential*:
E.g., the time consumed by the Tower-of-Hanoi problem (with $c := 2$).
Note: $c_1^n = o(c_2^n)$ for all $c_1, c_2 \in \mathbb{R}^+$ with $1 < c_1 < c_2$.
- $O(n!)$ *factorial*:
E.g., the time consumed by a brute-force solution of the traveling salesman problem. Note: $c^n = o(n!)$ for all $c \in \mathbb{R}^+$.
- $O(n^n)$ *n-power-n*:
Note $n! = o(n^n)$.

Definition 133 (Conditional Asymptotic Notation)

Consider a function $f: \mathbb{N} \rightarrow \mathbb{R}^+$ and a predicate $P: \mathbb{N} \rightarrow \{F, T\}$.

$$O(f \mid P) := \{g: \mathbb{N} \rightarrow \mathbb{R}^+ \mid \exists c \in \mathbb{R}^+ \exists n_0 \in \mathbb{N} \forall n \geq n_0 : \\ P(n) \Rightarrow g(n) \leq c \cdot f(n)\}.$$

$$\Omega(f \mid P) := \{g: \mathbb{N} \rightarrow \mathbb{R}^+ \mid \exists c \in \mathbb{R}^+ \exists n_0 \in \mathbb{N} \forall n \geq n_0 : \\ P(n) \Rightarrow g(n) \geq c \cdot f(n)\}.$$

$$\Theta(f \mid P) := \{g: \mathbb{N} \rightarrow \mathbb{R}^+ \mid \exists c_1, c_2 \in \mathbb{R}^+ \exists n_0 \in \mathbb{N} \forall n \geq n_0 : \\ P(n) \Rightarrow c_1 \cdot f(n) \leq g(n) \leq c_2 \cdot f(n)\}.$$

$$o(f \mid P) := \{g: \mathbb{N} \rightarrow \mathbb{R}^+ \mid \forall c \in \mathbb{R}^+ \exists n_0 \in \mathbb{N} \forall n \geq n_0 : \\ P(n) \Rightarrow g(n) < c \cdot f(n)\}.$$

- E.g., let $P(n) :\Leftrightarrow n \equiv_2 0$, or $P(n) :\Leftrightarrow (\exists k \in \mathbb{N}_0 \ n = 2^k)$.

Definition 134 (Eventually non-decreasing, Dt.: schlußendlich nicht abnehmend)

A function $f: \mathbb{N} \rightarrow \mathbb{R}^+$ is *eventually non-decreasing* exactly if

$$\exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad f(n) \leq f(n+1).$$

Definition 135 (b-smooth, Dt.: b-glatt)

A function $f: \mathbb{N} \rightarrow \mathbb{R}^+$ is *b-smooth* for some integer $b \geq 2$ exactly if f is eventually non-decreasing and if

$$\exists c \in \mathbb{R}^+ \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad f(b \cdot n) \leq c \cdot f(n).$$

Definition 136 (smooth, Dt.: glatt)

A function $f: \mathbb{N} \rightarrow \mathbb{R}^+$ is *smooth* if it is *b-smooth* for all integers $b \geq 2$.

Lemma 137

If $f: \mathbb{N} \rightarrow \mathbb{R}^+$ is *b-smooth* for some integer $b \geq 2$ then it is smooth.

Theorem 138 (Smoothness Rule)

Let $f, g: \mathbb{N} \rightarrow \mathbb{R}^+$, and consider an integer $b \geq 2$. If

- 1 f is a smooth function,
- 2 $g \in O(f \mid \text{“is power of } b\text{”})$, and if
- 3 g is an eventually non-decreasing function,

then $g \in O(f)$.

- Similarly for $\Omega(f)$ and $\Theta(f)$.
- Again, it is trivial to extend the definitions and lemmas such that \mathbb{N}_0 rather than \mathbb{N} is taken as the base set. Similarly, we can replace \mathbb{R}^+ by \mathbb{R}_0^+ provided that all functions are eventually non-zero.
- The same comments apply to the subsequent slides.

Smoothness Rule: Sample Application

- For $a, b \in \mathbb{R}_0^+$ we define $g: \mathbb{N} \rightarrow \mathbb{R}_0^+$ as

$$g(n) := \begin{cases} a & \text{if } n = 1, \\ 4g(\lceil \frac{n}{2} \rceil) + b \cdot n & \text{otherwise.} \end{cases}$$

- Note that $\lceil \frac{n}{2} \rceil = 2^{k-1}$ if $n = 2^k$.
- We would like to show that $g \in \Theta(n^2)$:
It suffices to

- prove that f , with $f(n) := n^2$, is smooth,
- prove that $g \in \Theta(f \mid \text{"is power of 2"})$,
- prove that g is eventually non-decreasing.

- Standard application in computer science: Solving the recurrence relation

$$T(n) = T\left(\lceil \frac{n}{2} \rceil\right) + T\left(\lfloor \frac{n}{2} \rfloor\right) + b \cdot n,$$

e.g., as derived when analyzing the complexity of merge sort.



Definition 139 (Recurrence relation, Dt.: Rekurrenzgleichung)

A *recurrence relation* is an equation that relates elements of a sequence t . It is of order k , for some $k \in \mathbb{N}$, if t_n can be expressed in terms of n and $t_{n-1}, t_{n-2}, \dots, t_{n-k}$, i.e., if t_n is of the form $t_n = f(t_{n-1}, t_{n-2}, \dots, t_{n-k}, n)$ for $f: \mathbb{R}^k \times \mathbb{N} \rightarrow \mathbb{R}$.

- Sample recurrence for $n \in \mathbb{N}_0$:

$$t_n := \begin{cases} 1 & \text{if } n = 0, \\ 2 \cdot t_{n-1} & \text{if } n > 0. \end{cases}$$

- Easy to see: $t_n = 2^n$ for all $n \in \mathbb{N}_0$.

Note

- We will freely mix the notations t_k and $t(k)$ for denoting the k -th element of a sequence $(t_n)_{n \in \mathbb{N}}$.

Recurrence Relations: The Tower-of-Hanoi Recurrence

- According to legend, life on Earth will end once the Brahmin priests managed to move the last disk in their 64-disk Tower-of-Hanoi problem . . .
- Also according to legend, the priests apply a recursive algorithm, thereby moving
 - (1) the top $n - 1$ disks from pole I to the auxiliary pole III,
 - (2) the largest (bottom-most) disk from pole I to pole II,
 - (3) the top $n - 1$ disks from pole III to pole II.
- If $T(n)$ denotes the number of moves for the n -disk ToH problem, they need two times $T(n - 1)$ moves for the recursive Steps (1) and (3), and one move for getting the largest disk from pole I to II in Step (2).
- Of course, $T(1) = 1$.
- Hence, we get the recurrence relation

$$T(n) = 2T(n - 1) + 1 \quad \text{with} \quad T(1) := 1$$

for the number T of moves for solving the Tower-of-Hanoi problem recursively.

- A solution of this recurrence relation tells us when life on Earth might end . . .
- So, is it already time for an apocalyptic mood?
- We start with classifying recurrence relations.



Definition 140 (Homogeneous recurrence, Dt.: homogene Rekurrenz)

A recurrence relation of order k is *homogeneous* if it is satisfied by the zero sequence.

- E.g., $t_n := 3n^2 \cdot t_{n-1} \cdot t_{n-2}$.

Definition 141 (Linear homogeneous recurrence)

A homogeneous recurrence relation of order k is *linear* if $t_n = \sum_{i=1}^k a_i(n) \cdot t_{n-i}$, where $a_i: \mathbb{N} \rightarrow \mathbb{R}$ for $i = 1, 2, \dots, k$.

- E.g., $t_n := n^2 \cdot t_{n-1} + 3t_{n-2}$.

Definition 142 (Linear homogeneous recurrence with constant coefficients)

A linear homogeneous recurrence relation of order k has *constant coefficients* if $t_n = \sum_{i=1}^k a_i \cdot t_{n-i}$, where $a_1, a_2, \dots, a_k \in \mathbb{R}$.

- E.g., $t_n := 2 \cdot t_{n-1} + 3t_{n-2}$.

Caveat

Even seemingly simple recurrence relations need not be easy to understand and solve.

- For instance, it is not known whether the so-called Collatz $3n + 1$ recursion [Lothar Collatz 1937] will result in $T(n) = 1$ for all $n \in \mathbb{N}$:

$$T(n) := \begin{cases} 1 & \text{if } n = 1, \\ T(\frac{3n+1}{2}) & \text{if } n > 1 \wedge n \not\equiv_2 0, \\ T(\frac{n}{2}) & \text{if } n > 1 \wedge n \equiv_2 0. \end{cases}$$

- E.g., for $n := 6$ one gets the equalities

$$T(6) = T(3) = T(5) = T(8) = T(4) = T(2) = T(1)$$

and, thus, $T(6) = 1$.

- Experiments have confirmed the Collatz conjecture up to roughly $5 \cdot 10^{18} \dots$

Heuristics for Solving Recurrences

- Constructive Induction:
 - First "guess" a solution.
 - Use "constructive" induction to verify that the solution guessed is correct.
- Cascading:
 - Restate the recurrence relation for $t_n, t_{n-1}, t_{n-2}, \dots$
 - Manipulate and rearrange the individual equations such that summing over all equations yields a closed-form expression for t_n .
- Iteration:
 - Expand the recurrence relation.
 - Derive a closed-form solution.

Note

- All heuristics require induction to prove that the result obtained is indeed correct!

Heuristics for Solving Recurrences: Constructive Induction

- Solve the recurrence relation $t_n = t_{n-1} + n$, with $t_0 := 0$.
- *Guess*: $t_n \in O(n^2)$.
- Our guess can be verified by showing $t_n \leq a \cdot n^2$ for suitable $a \in \mathbb{R}$.
- We get:

$$t_{n+1} = t_n + (n+1) \leq a \cdot n^2 + (n+1) \stackrel{a=2}{=} 2n^2 + (n+1) \leq 2(n+1)^2.$$

- Now use standard induction to show that $t_n \leq 2n^2$ is indeed correct for all $n \in \mathbb{N}_0$.

Heuristics for Solving Recurrences: Cascading

- Solve the recurrence relation $t_n = t_{n-1} + n$, with $t_0 := 0$.
- Restating the recurrence yields the following set of equations:

$$t_n = t_{n-1} + n$$

$$t_{n-1} = t_{n-2} + n - 1$$

$$t_{n-2} = t_{n-3} + n - 2$$

$$t_{n-3} = t_{n-4} + n - 3$$

$$\vdots$$

$$t_3 = t_2 + 3$$

$$t_2 = t_1 + 2$$

$$t_1 = t_0 + 1$$

$$t_n = t_0 + 1 + 2 + \cdots + (n-2) + (n-1) + n$$

- This indicates that

$$t_n = \sum_{i=0}^n i = \frac{n(n+1)}{2} \in \Theta(n^2),$$

which is proved by induction.



Heuristics for Solving Recurrences: Iteration

- Solve the recurrence relation $t_n = t_{n-1} + n$, with $t_0 := 0$.
- Iterating the recurrence yields

$$\begin{aligned}t_n &= t_{n-1} + n \\&= (t_{n-2} + (n-1)) + n \\&= (t_{n-3} + (n-2)) + (n-1) + n \\&= (t_{n-4} + (n-3)) + (n-2) + (n-1) + n \\&\vdots \\&= t_0 + 1 + 2 + \cdots + (n-1) + n \\&= 0 + 1 + 2 + \cdots + (n-1) + n.\end{aligned}$$

- Again, this indicates that

$$t_n = \sum_{i=0}^n i = \frac{n(n+1)}{2} \in \Theta(n^2),$$

which is proved by induction.



Real-World Problem: When Will Life on Earth End?

- We have the Tower-of-Hanoi recurrence relation

$$T(n) = 2T(n-1) + 1 \quad \text{with} \quad T(1) := 1.$$

- Iteration yields the following identities:

$$\begin{aligned} T(n) &= 2T(n-1) + 1 = 2^1 T(n-1) + 2^0 \\ &= 2(2^1 T(n-2) + 2^0) + 2^0 = 2^2 T(n-2) + 2^1 + 2^0 \\ &= 2^2(2^1 T(n-3) + 2^0) + 2^1 + 2^0 = 2^3 T(n-3) + 2^2 + 2^1 + 2^0 \\ &\vdots \\ &= 2^{n-1} T(n - (n-1)) + 2^{n-2} + \dots + 2^2 + 2^1 + 2^0 \\ &= 2^{n-1} + 2^{n-2} + \dots + 2^2 + 2^1 + 2^0 \\ &= 2^n - 1 \end{aligned}$$

- Hence, if the priests manage to move one disk per second then we would have to expect the end of Earth $2^{64} - 1$ seconds after they started, i.e., roughly within $5 \cdot 10^{11}$ years ...



Solving Linear Homogeneous Recurrence Relations With Constant Coefficients

Lemma 143

Consider the recurrence relation $a_0 t_n + a_1 t_{n-1} + \cdots + a_k t_{n-k} = 0$, with $a_i \in \mathbb{R}$. If (f_n) and (g_n) satisfy the recurrence relation then $(\alpha f_n + \beta g_n)$ satisfies the recurrence relation for all $\alpha, \beta \in \mathbb{R}$.

Proof: Suppose that

$$\sum_{i=0}^k a_i f_{n-i} = 0 \quad \text{and} \quad \sum_{i=0}^k a_i g_{n-i} = 0$$

for all $n \geq k$. Then:

$$\sum_{i=0}^k a_i (\alpha f_{n-i} + \beta g_{n-i}) = \alpha \sum_{i=0}^k a_i f_{n-i} + \beta \sum_{i=0}^k a_i g_{n-i} = 0.$$



Solving Linear Homogeneous Recurrence Relations With Constant Coefficients

- So, consider $a_0 t_n + a_1 t_{n-1} + \dots + a_k t_{n-k} = 0$
- Guess $t_n = x^n$ for some unknown $x \in \mathbb{R}$.
 - Then $a_0 x^n + a_1 x^{n-1} + \dots + a_k x^{n-k} = 0$.
 - Further $x^{n-k}(a_0 x^k + a_1 x^{k-1} + \dots + a_k) = 0$.
 - If we ignore the trivial solution $x = 0$ then we get

$$a_0 x^k + a_1 x^{k-1} + \dots + a_k = 0$$

as the so-called *characteristic equation* of the recurrence relation

$$a_0 t_n + a_1 t_{n-1} + \dots + a_k t_{n-k} = 0.$$

- Hence, any root r of this equation serves as a partial solution of the recurrence relation, with $t_n := r^n$.

Solving Linear Homogeneous Recurrence Relations With Constant Coefficients

- Suppose that the characteristic equation has k distinct roots r_1, \dots, r_k such that all roots are real numbers. I.e., the characteristic equation is given as

$$\prod_{i=1}^k (x - r_i) = 0.$$

- Then, the general solution of the recurrence relation is of the form

$$t_n = \sum_{i=1}^k c_i r_i^n,$$

for some constants $c_1, c_2, \dots, c_k \in \mathbb{R}$.

- The constants c_i are determined based on the initial condition(s).

Solving Linear Homogeneous Recurrence Relations With Constant Coefficients: Fibonacci Sequence

- Consider the *Fibonacci* sequence (over \mathbb{N}_0)

$$F_n := \begin{cases} 0 & \text{if } n = 0, \\ 1 & \text{if } n = 1, \\ F_{n-1} + F_{n-2} & \text{if } n \geq 2. \end{cases}$$

- We get

$$x^2 - x - 1 = 0$$

as the characteristic equation, and, therefore

$$x_1 = \frac{1 + \sqrt{5}}{2} \quad \text{and} \quad x_2 = \frac{1 - \sqrt{5}}{2}.$$

- Note: x_1 is known as the *golden ratio*, $\phi = 1.618 \dots$

Solving Linear Homogeneous Recurrence Relations With Constant Coefficients: Fibonacci Sequence

- This yields

$$F_n = c_1 \cdot \left(\frac{1 + \sqrt{5}}{2} \right)^n + c_2 \cdot \left(\frac{1 - \sqrt{5}}{2} \right)^n.$$

- The constants c_1, c_2 are determined by resorting to the initial conditions.

$$n = 0 : \quad F_0 = 0 = c_1 + c_2$$

$$n = 1 : \quad F_1 = 1 = c_1 \cdot \frac{1 + \sqrt{5}}{2} + c_2 \cdot \frac{1 - \sqrt{5}}{2}$$

- By solving this linear system we obtain $c_1 = -c_2 = \frac{1}{\sqrt{5}}$.
- Hence,

$$F_n = \frac{1}{\sqrt{5}} \cdot \left(\frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \cdot \left(\frac{1 - \sqrt{5}}{2} \right)^n.$$

Solving Linear Homogeneous Recurrence Relations With Constant Coefficients

- *Multiple roots*: Suppose that the characteristic equation has k distinct roots r_1, \dots, r_k of multiplicities m_1, \dots, m_k such that all roots are real numbers. I.e., the characteristic equation is given as

$$\prod_{i=1}^k (x - r_i)^{m_i} = 0.$$

- Then we have

$$t_n = \sum_{i=1}^k \sum_{j=0}^{m_i-1} c_{ij} n^j r_i^n,$$

for constants $c_{ij} \in \mathbb{R}$.

- E.g., for $(x - 2)^2(x - 1) = 0$ we get $t_n = c_{10}1^n + c_{20}2^n + c_{21}n2^n$.

Solving Linear Inhomogeneous Recurrence Relations With Constant Coefficients

- Assume we have an inhomogeneous recurrence relation of the following form:

$$a_0 \cdot t_n + a_1 \cdot t_{n-1} + \cdots + a_k \cdot t_{n-k} = b_1^n \cdot p_1(n) + b_2^n \cdot p_2(n) + \cdots + b_m^n \cdot p_m(n).$$

where b_i are constants and p_i are polynomials in n of degree $d_i \in \mathbb{N}$.

- Then the characteristic polynomial is:

$$(a_0 \cdot x^k + a_1 \cdot x^{k-1} + \cdots + a_k) \cdot \prod_{i=1}^m (x - b_i)^{d_i+1} = 0.$$

- Now proceed as in the homogeneous case.

Solving Linear Inhomogeneous Recurrence Relations With Constant Coefficients

Theorem 144

Consider the linear inhomogeneous recurrence relation

$$a_0 \cdot t_n + a_1 \cdot t_{n-1} + \cdots + a_k \cdot t_{n-k} = \sum_{i=1}^m b_i^n \cdot p_i(n),$$

where b_i are constants and p_i are polynomials in n of degree $d_i \in \mathbb{N}_0$, for $m \in \mathbb{N}_0$, and suppose that its characteristic equation

$$(a_0 \cdot x^k + a_1 \cdot x^{k-1} + \cdots + a_k) \cdot \prod_{i=1}^m (x - b_i)^{d_i+1} = 0$$

has s distinct roots r_1, \dots, r_s of multiplicities m_1, \dots, m_s such that all roots are real numbers. Then the general solution of the recurrence relation is given by

$$t_n = \sum_{i=1}^s \sum_{j=0}^{m_i-1} c_{i,j} n^j r_i^n = \sum_{i=1}^s (c_{i,0} r_i^n + c_{i,1} n r_i^n + c_{i,2} n^2 r_i^n + \cdots + c_{i,m_i-1} n^{m_i-1} r_i^n),$$

for constants $c_{ij} \in \mathbb{R}$.

Solving Linear Inhomogeneous Recurrence Relations With Constant Coefficients: Sample Solution

- Consider

$$t_n := \begin{cases} 0 & \text{if } n = 0, \\ 2t_{n-1} + n + 2^n & \text{otherwise.} \end{cases}$$

- The standard form of this recurrence is

$$t_n - 2t_{n-1} = n + 2^n = 1^n \cdot n^1 + 2^n \cdot n^0,$$

and we get

$$(x - 2) \cdot (x - 1)^2 \cdot (x - 2)^1 = (x - 1)^2 \cdot (x - 2)^2$$

as the characteristic equation.

- This yields

$$\begin{aligned} t_n &= c_{10} \cdot 1^n + c_{11} \cdot n \cdot 1^n + c_{20} \cdot 2^n + c_{21} \cdot n \cdot 2^n \\ &= c_{10} + c_{11} \cdot n + c_{20} \cdot 2^n + c_{21} \cdot n \cdot 2^n. \end{aligned}$$

Solving Linear Inhomogeneous Recurrence Relations With Constant Coefficients: Sample Solution

- This yields

$$\begin{aligned}t_n &= c_{10} \cdot 1^n + c_{11} \cdot n \cdot 1^n + c_{20} \cdot 2^n + c_{21} \cdot n \cdot 2^n \\&= c_{10} + c_{11} \cdot n + c_{20} \cdot 2^n + c_{21} \cdot n \cdot 2^n.\end{aligned}$$

- The constants $c_{10}, c_{11}, c_{20}, c_{21}$ are determined by resorting to the initial conditions.

$$\begin{aligned}n = 0 : \quad 0 &= c_{10} + c_{11} \cdot 0 + c_{20} \cdot 2^0 + c_{21} \cdot 0 \cdot 2^0 \\&= c_{10} + c_{20}\end{aligned}$$

$$n = 1 : \quad 3 = c_{10} + c_{11} + 2 \cdot c_{20} + 2 \cdot c_{21}$$

$$\vdots$$

Theorem 145 (Master theorem, Dt.: Hauptsatz der Laufzeitfunktionen)

Consider constants $c \in \mathbb{R}^+$, $k, n_0 \in \mathbb{N}$ and $a, b \in \mathbb{N}$ with $b \geq 2$, and let $T: \mathbb{N} \rightarrow \mathbb{R}_0^+$ be an eventually non-decreasing function such that

$$T(n) = a \cdot T\left(\frac{n}{b}\right) + c \cdot n^k$$

for all $n \in \mathbb{N}$ with $n \geq n_0$, where we interpret $\frac{n}{b}$ as either $\lceil \frac{n}{b} \rceil$ or $\lfloor \frac{n}{b} \rfloor$. Then we have

$$T \in \begin{cases} \Theta(n^k) & \text{if } a < b^k, \\ \Theta(n^k \log n) & \text{if } a = b^k, \\ \Theta(n^{\log_b a}) & \text{if } a > b^k. \end{cases}$$

- E.g., we get $T \in \Theta(n \log n)$ for T defined as follows:

$$T(n) = T\left(\left\lceil \frac{n}{2} \right\rceil\right) + T\left(\left\lfloor \frac{n}{2} \right\rfloor\right) + c \cdot n.$$

Theorem 146

Consider constants $k, n_0 \in \mathbb{N}$ and $a, b \in \mathbb{N}$ with $b \geq 2$, and a function $f: \mathbb{N} \rightarrow \mathbb{R}_0^+$ with $f \in \Theta(n^k)$. Let $T: \mathbb{N} \rightarrow \mathbb{R}_0^+$ be an eventually non-decreasing function such that

$$T(n) = a \cdot T\left(\frac{n}{b}\right) + f(n)$$

for all $n \in \mathbb{N}$ with $n \geq n_0$, where we interpret $\frac{n}{b}$ as either $\lceil \frac{n}{b} \rceil$ or $\lfloor \frac{n}{b} \rfloor$.

Then we have

$$T \in \begin{cases} \Theta(n^k) & \text{if } a < b^k, \\ \Theta(n^k \log n) & \text{if } a = b^k, \\ \Theta(n^{\log_b a}) & \text{if } a > b^k. \end{cases}$$

Master Theorem (Refined Asymptotic Version)

Theorem 147

Consider constants $n_0 \in \mathbb{N}$ and $a, b \in \mathbb{N}$ with $b \geq 2$, and a function $f: \mathbb{N} \rightarrow \mathbb{R}_0^+$. Let $T: \mathbb{N} \rightarrow \mathbb{R}_0^+$ be an eventually non-decreasing function such that

$$T(n) = a \cdot T\left(\frac{n}{b}\right) + f(n)$$

for all $n \in \mathbb{N}$ with $n \geq n_0$, where we interpret $\frac{n}{b}$ as either $\lceil \frac{n}{b} \rceil$ or $\lfloor \frac{n}{b} \rfloor$. Then we have

$$T \in \begin{cases} \Theta(f) & \text{if } \begin{cases} f \in \Omega\left(n^{(\log_b a) + \varepsilon}\right) \text{ for some } \varepsilon \in \mathbb{R}^+, \\ \text{and if the following regularity condition holds} \\ \text{for some } 0 < s < 1 \text{ and all sufficiently large } n: \\ a \cdot f\left(\frac{n}{b}\right) \leq s \cdot f(n), \end{cases} \\ \Theta\left(n^{\log_b a} \log n\right) & \text{if } f \in \Theta\left(n^{\log_b a}\right), \\ \Theta\left(n^{\log_b a}\right) & \text{if } f \in O\left(n^{(\log_b a) - \varepsilon}\right) \text{ for some } \varepsilon \in \mathbb{R}^+. \end{cases}$$

- This is a simplified version of the Akra-Bazzi Theorem [Akra&Bazzi 1998].



Real-World Application: Analysis of Fast Integer Multiplication

- The standard multiplication of two integers a, b represented as binary numbers with $2n$ bits each requires $\Theta(n^2)$ many additions and shifts of bits.
- Can we do any better and achieve $o(n^2)$ time? Yes!
- [Anatoliĭ Karatsuba 1960–1963:] Let

$$(a_{2n-1} a_{2n-2} \cdots a_1 a_0)_2 \quad \text{and} \quad (b_{2n-1} b_{2n-2} \cdots b_1 b_0)_2$$

be the $2n$ -bit binary representations of a and b . Hence, $a = \sum_{i=0}^{2n-1} a_i 2^i$ and $b = \sum_{i=0}^{2n-1} b_i 2^i$.

- We have

$$a \sim 2^n A_1 + A_0 \quad \text{and} \quad b \sim 2^n B_1 + B_0$$

with

$$A_1 := (a_{2n-1} a_{2n-2} \cdots a_{n+1})_2, \quad A_0 := (a_{n-1} a_{n-2} \cdots a_1 a_0)_2,$$

$$B_1 := (b_{2n-1} b_{2n-2} \cdots b_{n+1})_2, \quad B_0 := (b_{n-1} b_{n-2} \cdots b_1 b_0)_2.$$

- We get

$$a \cdot b \sim 2^{2n} A_1 \cdot B_1 + 2^n (A_1 \cdot B_0 + A_0 \cdot B_1) + A_0 \cdot B_0.$$



Real-World Application: Analysis of Fast Integer Multiplication

- We get

$$a \cdot b \sim 2^{2n} A_1 \cdot B_1 + 2^n (A_1 \cdot B_0 + A_0 \cdot B_1) + A_0 \cdot B_0,$$

which can be rewritten as

$$a \cdot b \sim (2^{2n} + 2^n) A_1 \cdot B_1 + 2^n (A_1 - A_0) \cdot (B_0 - B_1) + (2^n + 1) A_0 \cdot B_0.$$

- Thus, the multiplication of two $2n$ -bit binary numbers can be carried out recursively by computing
 - 1 three multiplications of n -bit binary numbers, plus
 - 2 a constant number of additions and shifts on n -bit binary numbers.
- Hence, if $T(n)$ denotes the total number of bit operations used by this recursive algorithm for n -bit binary numbers, then

$$T(n) = 3T\left(\frac{n}{2}\right) + f(n) \quad \text{with } f \in \Theta(n).$$

- The asymptotic version of the Master Theorem 146 allows us to conclude that

$$T \in \Theta(n^{\log_2 3}), \quad \text{i.e., that } T \in \Theta(n^{1.58496\dots}) \text{ and, thus, } T \in o(n^2).$$

- Even faster methods for integer multiplication exist, based on Fast Fourier Transform: [Schönhage&Strassen 1971], [Fürer 2007].



Graph Theory

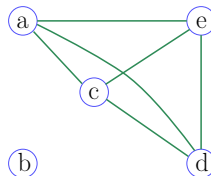
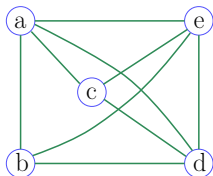
- What is a (Directed) Graph?
- Paths
- Trees
- Special Graphs
- Graph Coloring

Basic Definitions: Undirected Graph

Definition 148 (Graph, Dt.: (schlichter endlicher ungerichteter) Graph)

A (simple finite undirected) graph $\mathcal{G} = (V, E)$ with n vertices (aka *nodes*) and m edges consists of a vertex set $V = \{v_1, v_2, \dots, v_n\}$ and an edge set $E = \{e_1, e_2, \dots, e_m\}$, where $V \cap E = \emptyset$ and each edge is an *unordered* pair of distinct vertices:

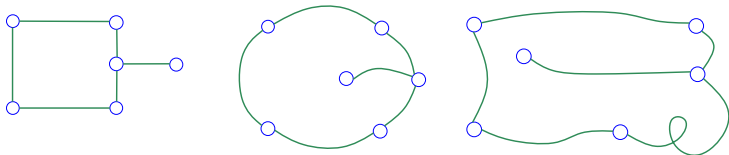
$$e \in E \Rightarrow e = \{u, v\} \text{ with } u, v \in V, \text{ where } u \neq v.$$



- It is common to mix the terms “*node*” (Dt.: Knoten) and “*vertex*” (Dt.: Ecke) freely.
- An edge $\{u, v\}$ is often denoted by uv .
- If we allow edges of the form uu then we get a *loop* (Dt.: Schlinge, Schleife) and the graph is no longer simple (Dt.: schlicht, einfach).
- If we allow multiple edges between two vertices then we get a *multigraph*.

Basic Definitions: Graphical Representation

- Graphical representation of a graph:
 - Denote the vertices by markers of the same form (circles, dots, squares, ...).
 - For every pair of vertex markers, draw a curve between them if the graph contains an edge between the corresponding vertices.
- The edges drawn may be curved and may intersect.
- However, it is poor practice to let an edge pass or touch any other vertex in addition to its two defining vertices.
- Use arrows to denote directed edges.

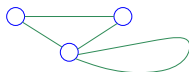


Basic Definitions: Graphical Representation

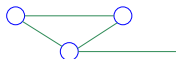
- Which of the following drawings show simple graphs?



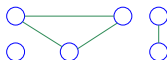
multigraph



not a simple graph (loop)



not a graph



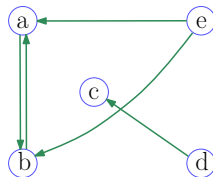
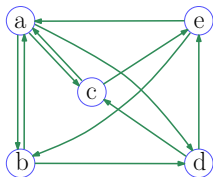
this is a graph!

Basic Definitions: Directed Graph

Definition 149 (Directed graph, Dt.: gerichteter Graph)

A (finite simple) directed graph, or digraph, $\mathcal{G} = (V, E)$ with n vertices (aka nodes) and m edges consists of a vertex set $V = \{v_1, v_2, \dots, v_n\}$ and an edge set $E = \{e_1, e_2, \dots, e_m\}$, where $V \cap E = \emptyset$ and each edge is an *ordered* pair of distinct vertices:

$$e \in E \Rightarrow e = (u, v) \text{ with } u, v \in V, \text{ where } u \neq v.$$



- For a digraph, uv indicates the edge (u, v) , i.e., an edge where u is the *tail* and v is the *head*.
- We will always denote a directed graph explicitly; that is, the term “graph” without the additional qualifier “directed” shall mean “undirected graph”.

Basic Definitions: How to Deal with $V = \emptyset$

- There is no consensus on whether or not to allow $V = \emptyset$ in the definition of a graph. (Of course, if $V = \emptyset$ then $E = \emptyset$.)
- And, indeed, there are pros and cons of allowing $V = \emptyset$.
- Furthermore, if $V = \emptyset$ is allowed, then there is little consensus on how to call such a graph:
 - Common terms are *order-zero graph*, K_0 , and *null graph*.
 - Some authors also use the term *empty graph* to indicate $V = \emptyset$ while other authors prefer to reserve this term for a graph with $E = \emptyset$ but $V \neq \emptyset$.

Convention

We will always assume that every (directed) graph has at least one node.

No common terminology

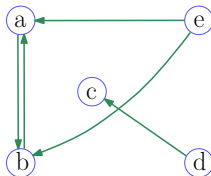
The terminology in graph theory lacks a rigorous standardization, both in the German and in the English literature.

- In several cases the meanings of different terms coincide for simple undirected graphs, which seems to serve as a justification for authors to freely mix and match terms.
- Thus, always make sure to check how some author defines standard terms of graph theory . . .

- There is an elementary one-to-one mapping from relations to digraphs!
- E.g., the relation R on the set $\{a, b, c, d, e\}$, with

$$R := \{(a, b), (b, a), (d, c), (e, a), (e, b)\}$$

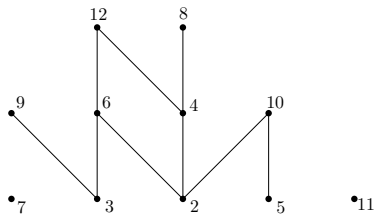
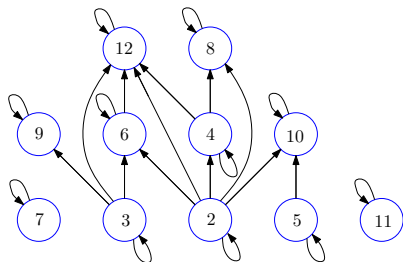
corresponds to the following directed graph:



- Hence, statements about relations can be translated to statements about digraphs, and vice versa.
- Note, though, that the digraph corresponding to a relation
 - need not be simple but might contain loops,
 - need not have a finite vertex set.

Directed Graphs and Relations: Hasse Diagram

- Consider the set (S, R) , where $S := \{n \in \mathbb{N} : 1 < n \leq 12\}$ and R denotes the partial order of divisibility on S . (That is, for $a, b \in S$, we have $a R b$ iff $a \mid b$.)



Hasse diagram

- Redraw the digraph such that all oriented (non-loop) edges point upwards.
- Now remove all loops (that result from the reflexivity of the partial order).
- Next, remove all edges implied by transitivity.
- Finally, shrink all node markers to dots.

Definition 150 (Hasse diagram)

The graph obtained after carrying out Steps (1)–(4) is the *Hasse diagram* of the poset.

Real-World Application: Precedence Graph

- Typically, some but likely not all statements of a computer program could be executed in parallel. Care has to be taken not to execute a statement that depends on results of statements that were not yet executed.
- A *precedence graph* is a directed graph that models dependencies. E.g., the dependence of statements of a computer program on other statements:
 - Each statement is represented by a vertex.
 - There is an edge from vertex u to vertex v if the statement that corresponds to v has to be executed after the statement of u .
- Precedence graphs are used in all sorts of scheduling tasks: E.g., job scheduling, concurrency control and instruction scheduling, resolving linker dependencies, data serialization, automated parallelization of sequential code.

(1) $a := 1$

(2) $b := 2$

(3) $c := 3$

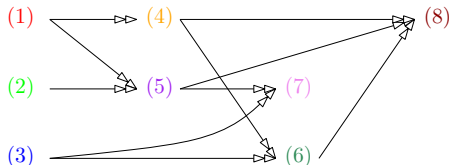
(4) $d := a + 2$

(5) $e := 2a + b$

(6) $f := d + c$

(7) $g := c + e$

(8) $h := d + e + f$



Basic Definitions: Adjacency and Degree

Definition 151 (Adjacent, Dt.: benachbart)

Two vertices $u, v \in V$ of a graph $\mathcal{G} = (V, E)$ are *adjacent* if $uv \in E$; the edge uv is *incident* to the vertices u and v .

Definition 152 (Degree, Dt.: Grad)

The *degree* (aka *valence*) of a vertex u of a graph $\mathcal{G} = (V, E)$ is the number of edges incident in u . It is denoted by $\deg(u)$.

For directed graphs, it is common to distinguish between the *in-degree*, $\deg^-(u)$, i.e., the number of edges vu for $v \in V$, and the *out-degree*, $\deg^+(u)$, i.e., the number of edges uv for $v \in V$.

The *degree of a graph* is the maximum of the degrees of its vertices.

Definition 153 (Subgraph, Dt.: Teilgraph)

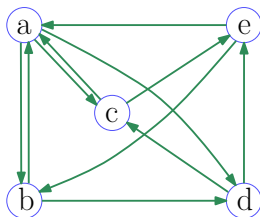
A graph $\mathcal{G}' = (V', E')$ is a *subgraph* of a (directed) graph $\mathcal{G} = (V, E)$ if $V' \subseteq V$ and $E' \subseteq E$ such that all edges of E' are formed by vertices of V' .

Basic Definitions: Adjacency Matrix

Definition 154 (Adjacency matrix, Dt.: Adjazenzmatrix)

The *adjacency matrix* of a (directed) graph $\mathcal{G} = (V, E)$ is an $n \times n$ matrix \mathbf{M} , where $n := |V|$ and

$$m_{ij} = \begin{cases} 1 & \text{if } v_i v_j \in E, \\ 0 & \text{otherwise.} \end{cases}$$



	a	b	c	d	e
a	0	1	1	1	0
b	1	0	0	1	0
c	1	0	0	0	1
d	0	0	1	0	1
e	1	1	0	0	0

- The adjacency matrix \mathbf{M} is symmetric for undirected graphs, and all diagonal elements are zero for simple graphs.
- Note: Storing \mathbf{M} (as an $n \times n$ array) requires $\Theta(n^2)$ memory!

Lemma 155 (Euler's Handshaking Lemma, Dt.: Handschlag-Lemma)

The sum over all degrees of vertices of a graph $\mathcal{G} = (V, E)$ equals twice the number of its edges, i.e., $\sum_{\nu \in V} \deg(\nu) = 2|E|$.

Corollary 156

In every graph the number of vertices of odd degree is even.

- Simple application of Euler's Handshaking Lemma:
 - Suppose that a party is attended by 15 guests. Is it possible that every guest at the party knows all others except for precisely one guest?
 - No: Consider a graph with 15 nodes (guests) where two nodes are linked by an edge if the corresponding guests do not know each other. Hence, we would get 15 nodes of degree one, in contradiction to Cor. 156.

Definition 157 (Walk, Dt.: Wanderung, Kantenfolge)

A *walk* of length k , with $k \in \mathbb{N}_0$, on $\mathcal{G} = (V, E)$ is an alternating sequence

$$v_0 e_1 v_1 e_2 v_2 \dots e_k v_k$$

of $k + 1$ vertices $v_0, v_1, \dots, v_k \in V$ and k edges $e_1, \dots, e_k \in E$ such that

$$\forall (1 \leq i \leq k) \quad e_i = v_{i-1} v_i.$$

- Often, a walk of length k is written simply as

$$v_0 v_1 v_2 \dots v_k.$$

Conventionally, v_0 is called the *start vertex* (or *initial vertex*) of the walk, and v_k is called its *end vertex* (or *terminal vertex*). Note that $v_{i-1} \neq v_i$ for $i \in \{1, 2, \dots, k\}$.

Definition 158 (Closed walk, Dt.: geschlossene Wanderung)

A walk is called *closed* if the start vertex and the end vertex are identical. A closed walk of length k is called *trivial* if $k \leq 2$.

Paths, Trails, Tours and Cycles

Definition 159 (Trail, Dt.: Weg)

A *trail* in a graph \mathcal{G} is a walk in which all edges are distinct.

Definition 160 (Path, Dt.: Pfad)

A *path* in a graph \mathcal{G} is a walk in which all vertices are distinct.

Definition 161 (Tour, Dt.: Tour)

A *tour* in a graph \mathcal{G} is a closed trail.

Definition 162 (Cycle, Dt.: Zyklus, Kreis)

A *cycle* in a graph \mathcal{G} is a non-trivial closed walk in which all but the start and the end vertices are distinct.

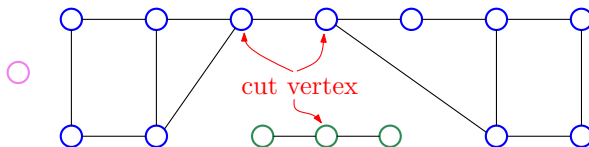
- Note: Distinct vertices implies distinct edges; i.e., every path is a trail and every cycle is a tour.
- Note that some authors prefer to use the terms “path”, “simple path”, “cycle” and “simple cycle” instead of “trail”, “path”, “tour” and “cycle” . . .



Connectedness

Definition 163 (Connected component, Dt.: Zusammenhangskomponente)

A *connected component* of a graph $\mathcal{G} = (V, E)$ is a maximal subgraph $\mathcal{G}' = (V', E')$ of \mathcal{G} such that for every unordered pair $\{u, v\}$, with $u, v \in V'$ and $u \neq v$, there exists a path between u and v within \mathcal{G}' .



Definition 164 (Cut vertex, Dt.: Artikulationspunkt, Schnittknoten)

A *cut vertex* of a graph $\mathcal{G} = (V, E)$ is a vertex $v \in V$ such that the removal of v and of all edges incident to v would increase the number of connected components.

Definition 165 (Connected, Dt.: zusammenhängend)

A graph $\mathcal{G} = (V, E)$ is *connected* if it contains only one connected component, i.e., if for every unordered pair $\{u, v\}$, with $u, v \in V$ and $u \neq v$, there exists a path between u and v .

Definition 166 (Weakly connected, Dt.: schwach zusammenhängend)

A directed graph is *weakly connected* if replacing all its directed edges by undirected edges results in a connected (undirected) graph.

Definition 167 (Strong component, Dt.: starke Zusammenhangskomponente)

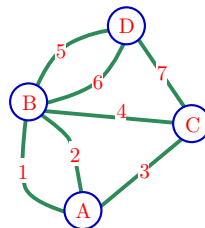
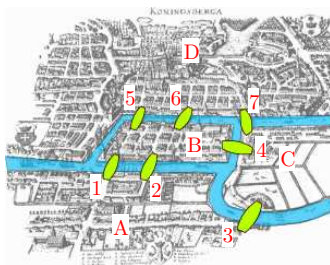
A *strong component* (aka *strongly connected component*) of a directed graph $\mathcal{G} = (V, E)$ is a maximal subgraph $\mathcal{G}' = (V', E')$ of \mathcal{G} such that for every ordered pair (u, v) , with $u, v \in V'$ and $u \neq v$, there exists a path from u to v within \mathcal{G}' .

Definition 168 (Strongly connected, Dt.: stark zusammenhängend)

A directed graph $\mathcal{G} = (V, E)$ is *strongly connected* if it consists of only one strongly connected component, i.e., if for every ordered pair (u, v) , with $u, v \in V$ and $u \neq v$, there exists a path from u to v .

Seven Bridges of Königsberg

- Early 18th century: Does there exist a trail (or even a tour) through the city of Königsberg that crosses every of its seven bridges exactly once? (Of course, every bridge had to be crossed fully, and no other means to get across the river Pregel were allowed.)



[Image credit for background image: [Wikipedia.](#)]

- In 1736, Leonhard Euler (1707–1783) treated this problem as a graph problem and proved, using a parity argument, that such a trail or tour does not exist.
- His solution is generally regarded as the first theorem of graph theory.



Euler Tour and Hamilton Cycle

Definition 169 (Euler trail, Dt.: Eulerscher Weg)

An *Euler trail* is a trail that contains all edges of a graph exactly once.

Definition 170 (Euler tour, Dt.: Eulersche Tour)

An *Euler tour* is a tour that contains all edges of a graph exactly once. A graph is an *Eulerian graph* if it has an Euler tour.

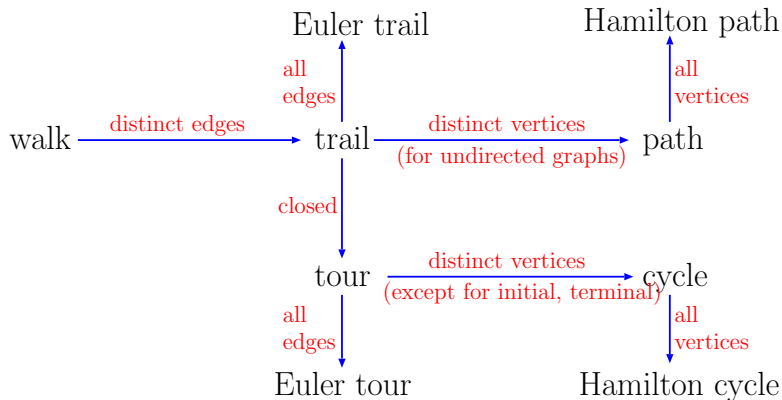
Definition 171 (Hamilton path, Dt.: Hamiltonscher Pfad)

A *Hamilton path* is a path that passes through all vertices of a graph exactly once.

Definition 172 (Hamilton cycle, Dt.: Hamiltonscher Kreis)

A *Hamilton cycle* is a cycle that passes through all vertices of a graph exactly once.

Euler Tour and Hamilton Cycle



Theorem 173

Suppose that every node of a graph \mathcal{G} has degree at least one. Then \mathcal{G} has an Euler tour if and only if \mathcal{G} is connected and every vertex of \mathcal{G} has even degree.

Theorem 174

Suppose that every node of a graph \mathcal{G} has degree at least one. Then \mathcal{G} has an Euler trail (but no Euler tour) if and only if \mathcal{G} is connected and exactly two vertices of \mathcal{G} have odd degrees.

Corollary 175

An Euler tour or trail in a graph $\mathcal{G} = (V, E)$ can be determined in $O(|E|)$ time, if it exists. Otherwise, again in $O(|E|)$ time, we can determine that neither an Euler tour nor an Euler trail exists in \mathcal{G} .

Constructive Proof of Theorem 173

Proof of Theorem 173: Let $\mathcal{G} = (V, E)$ be a graph such that every node of a graph \mathcal{G} has degree at least one.

Suppose that \mathcal{G} has an Euler tour T . It is obvious that \mathcal{G} is connected. Every occurrence of a vertex $v \in V$ in T is preceded and followed by an edge. Thus, each time T passes through v , two of the edges incident to v are consumed. Since T does neither start nor end in v , it is necessary that $\deg(v)$ is even.

Now suppose that every vertex of \mathcal{G} has even degree, and, of course, that \mathcal{G} is connected. We give a constructive proof that \mathcal{G} admits an Euler tour. Pick any vertex v to start with and trace out a trail T . Every edge that is being traversed is marked. As above, we observe that passing through a vertex that is neither the start nor the end vertex of T consumes two edges.

We realize that, eventually, T will get us back to v . (We cannot be stuck in some other vertex w since w has even degree.) If at the time when we are back at v every vertex of T has no unmarked incident edge then we are done. Otherwise, we start a new trail T' at a vertex w of T which has an unmarked incident edge and follow it until we get back to w .

This process continues until no unmarked edges remain. At the end the trails are spliced together appropriately.



Theorem 176

It is \mathcal{NP} -complete to determine whether a Hamilton cycle or Hamilton path exists in a general graph.

- Informally, Theorem 176 says that no (deterministic sequential) algorithm is known which determines the existence of a Hamilton cycle or path in an n -vertex graph in a time that is a polynomial function of n .
- Even worse, an efficient (polynomial-time) algorithm will never be found unless $\mathcal{P} = \mathcal{NP}$ holds, which seems rather unlikely.

Theorem 177 (Dirac, 1952)

If the degree of every vertex of an n -vertex graph \mathcal{G} , with $n \geq 3$, is at least $\lceil \frac{n}{2} \rceil$ then \mathcal{G} has a Hamilton cycle.

Theorem 178 (Ore, 1960)

If the sum of the degrees of every pair of non-adjacent vertices of an n -vertex graph \mathcal{G} , with $n \geq 3$, is at least n then \mathcal{G} has a Hamilton cycle.

Definition 179 (Acyclic, Dt.: zyklensfrei)

A graph is called *acyclic* if it contains no cycles.

Definition 180 (Tree, Dt.: Baum)

A *tree* is an undirected graph that is acyclic and connected.

- For trees most authors prefer to speak about *nodes* rather than vertices.
- Unless explicitly stated otherwise, we will only deal with trees that have at least one node.

Definition 181 (Rooted tree, Dt.: Baum mit Wurzel, Wurzelbaum)

A *rooted tree* is a directed graph with a node u such that

- 1 the graph contains u as node ("*root*"),
- 2 paths from u to all other nodes of the graph exist,
- 3 the in-degree of u is zero,
- 4 the in-degree of every other node of the graph is one.

Definition 182 (Child and parent, Dt.: Kind und Eltern)

For a rooted tree $\mathcal{T} = (V, E)$ and nodes $u, v \in V$, the node v is a *child* of the node u , and u is the *parent* of v , if the edge uv belongs to E . *Siblings* are nodes which share the same parent.

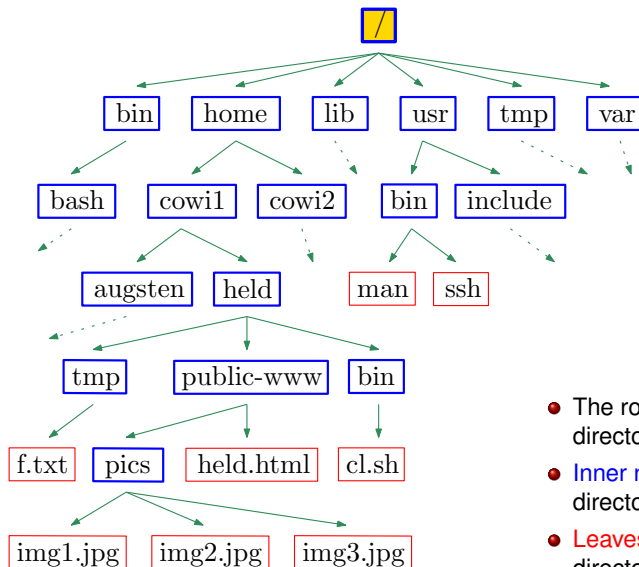
Definition 183 (Descendant and ancestor, Dt.: Nachfahre und Vorfahre)

In a rooted tree $\mathcal{T} = (V, E)$, with $u, v \in V$, a node v is a *descendant* of a node u , and u is an *ancestor* of v , if $u \neq v$ and if the path from the root to v contains u .

Definition 184 (Leaf, Dt.: Blatt)

A *leaf* of a rooted tree is a node without children. For a tree (that is not rooted) a leaf is a node with degree 1. All non-leaf nodes of a (rooted) tree are called *inner nodes*.

Real-World Application: File System as a Rooted Tree



- The root of the tree is the root directory /.
- **Inner nodes** are (non-empty) directories.
- **Leaves** are files (or empty directories).

Definition 185 (Subtree, Dt.: Teilbaum)

A tree $\mathcal{T}' = (V', E')$ is a (*proper*) *subtree* of a tree $\mathcal{T} = (V, E)$ rooted at the node u if

- 1 \mathcal{T}' is a subgraph of \mathcal{T} ,
- 2 \mathcal{T}' is rooted at a node v , where v is a child of u , and
- 3 \mathcal{T}' contains all descendants of v within \mathcal{T} , together with the appropriate edges of E .

Warning

Some authors do not require the node v to be a child of u but allow v to be any descendant of u .

Definition 186 (Forest, Dt.: Wald)

A *forest* is a graph all of whose connected components are trees.

Trees: Elementary Properties

Theorem 187

Every ordered pair of nodes in a tree is connected by exactly one path.

Theorem 188

In a rooted tree there exists exactly one path from the root to any node.

Lemma 189

Removing an edge from a (rooted) tree results in a graph with two connected components, each of which is a (rooted) tree.

Trees: Elementary Properties

Theorem 190

For every tree $\mathcal{T} = (V, E)$ we get $|E| = |V| - 1$.

Proof of Theorem 190 for rooted trees: We note that the subtree relation on rooted trees is well-founded and, thus, we can employ the principle of well-founded induction. Obviously, the claim holds for the minimal elements relative to this relation, i.e., for trees that contain no proper subtrees and, thus, have only a root and no edges. Now suppose that the equality claimed holds for all k subtrees $(V_1, E_1), \dots, (V_k, E_k)$ of a rooted tree $\mathcal{T} = (V, E)$. (We do not need to assume explicitly that it holds also for all subtrees of subtrees of \mathcal{T} .) We get

$$\begin{aligned}|E| &= k + \sum_{i=1}^k |E_i| = k + \sum_{i=1}^k (|V_i| - 1) = \sum_{i=1}^k |V_i| \\ &= |V| - 1,\end{aligned}$$

thus establishing the claim also for $\mathcal{T} = (V, E)$. □

Corollary 191

If $|V| > 1$ holds for a (rooted) tree $\mathcal{T} = (V, E)$, then \mathcal{T} has at least one leaf.

Definition 192 (Depth, Dt.: Tiefe)

The *depth* of the root u of a rooted tree $\mathcal{T} = (V, E)$ is 0, and the depth of a node $v \neq u$ of \mathcal{T} is k if the depth of the parent of v is $k - 1$, for all $v \in V$.

Warning

Some authors prefer to regard the root as a node at depth 1. Hence, make sure to check how the depth is defined in a textbook prior to using the results stated!

Definition 193 (Level, Dt.: Niveau)

A *level* of a rooted tree \mathcal{T} comprises all nodes of \mathcal{T} which have the same depth.

Definition 194 (Height, Dt.: Höhe)

The *height* of a rooted tree \mathcal{T} is the maximum depth of nodes of \mathcal{T} .

Definition 195 (Ordered tree, Dt.: geordneter Baum)

An *ordered tree* is a rooted tree \mathcal{T} such that the children of every node u of \mathcal{T} are arranged in some specific order, e.g., by means of a numbering scheme.

Definition 196 (Binary tree, Dt.: Binärbaum)

A *binary tree* is an ordered tree \mathcal{T} consisting of a root node u and at most two proper subtrees, which are called *left subtree*, L , and *right subtree*, R . If L (R , resp.) is a proper subtree then it is in turn a binary tree rooted in the left (right, resp.) child of u .

Definition 197 (Binary search tree, Dt.: binärer Suchbaum)

A *binary search tree* is a binary tree \mathcal{T} which has distinct values associated with its nodes such that (relative to some total order)

- if it has a proper left subtree L then
 - 1 all values of nodes in L are less than the root value,
 - 2 L is a binary search tree itself,
- if it has a proper right subtree R then
 - 3 all values of nodes in R are greater than the root value,
 - 4 R is a binary search tree itself.

Definition 198 (k-balanced tree, Dt.: k-balanzierter Baum)

A rooted binary tree is *height-balanced* with balance factor k if it either has no proper subtrees or if

- ➊ it has two proper subtrees and the heights of both subtrees differ by not more than k , or if
- ➋ it has one proper subtree of height at most $k - 1$,
and if
- ➌ all proper subtrees are height-balanced with balance factor k .

- E.g., for $k = 1$: AVL tree.
- Trees with balance factor 1 are simply called *balanced* or *self-balancing*.

Definition 199 (Perfectly balanced binary tree, Dt.: perfekt balanz. Binärbaum)

A binary tree \mathcal{T} is *perfectly balanced* if leaf nodes occur at most in the levels h and $h - 1$, where h is the height of \mathcal{T} .

- E.g., a heap is a perfectly balanced binary tree.

Height-Related Properties of Binary Trees

Lemma 200

For $i \in \mathbb{N}_0$, level i of a binary tree contains at most 2^i nodes.

Proof by induction: The claim holds for $i = 0$. If we have at most 2^k nodes on level k then we have at most $2 \cdot 2^k = 2^{k+1}$ nodes on level $k + 1$. \square

Lemma 201

Let h be the height and n be the number of nodes of a binary tree. Then $h \geq \lceil \log_2(n + 1) \rceil - 1$.

Proof: Lemma 200 implies that a binary tree with height h contains at most

$$\sum_{i=0}^h 2^i = 2^{h+1} - 1$$

nodes. Hence, $n \leq 2^{h+1} - 1$ and, thus, $h \geq \lceil \log_2(n + 1) \rceil - 1$. \square

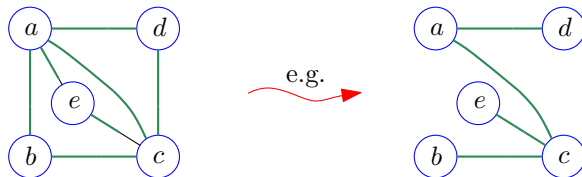
Theorem 202

If \mathcal{T} is a balanced binary tree with n nodes and height h then $h \in \Theta(\log n)$. \square

Definition 203 (Spanning tree, Dt.: spannender Baum)

A *spanning tree* of a connected graph \mathcal{G} is a subgraph of \mathcal{G} that

- 1 is a tree,
- 2 includes all vertices of \mathcal{G} .



Theorem 204

Every connected graph \mathcal{G} contains a spanning tree.

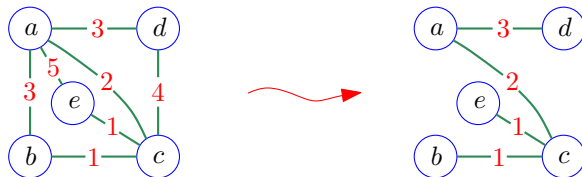
Spanning Trees

Definition 205 (Weighted graph, Dt.: gewichteter Graph)

An (*edge-*)*weighted graph* is a graph in which every edge is assigned a (non-negative) real number, the so-called *weight* or *cost*.

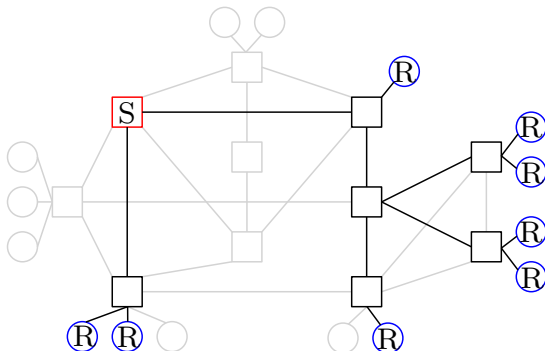
Definition 206 (Minimum spanning tree, Dt.: minimal spannender Baum)

A *minimum spanning tree* (MST) of a weighted connected graph \mathcal{G} is a spanning tree \mathcal{T} of \mathcal{G} such that the sum of the weights of the edges of \mathcal{T} is minimum over all spanning trees of \mathcal{G} .



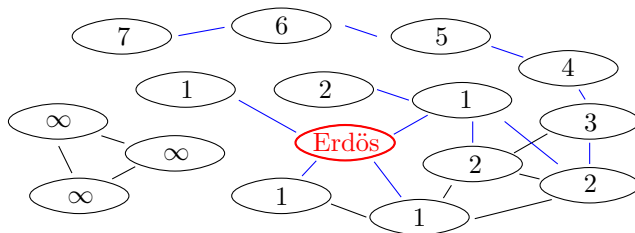
Real-World Application: IP Multicast Distribution Tree

- IP Multicasting is a one-to-many communication within an IP-based network: One source sends data to several receivers.
- Multicasting is based on a receiver-driven generation of a multicast distribution tree, thus reducing the amount of data that has to be distributed concurrently.
- Roughly, a multicast distribution tree is a spanning tree of all multicast receivers (or receiver groups), the source and intermediate routers.



Real-World Application: Collaboration Graph and the Erdős Number

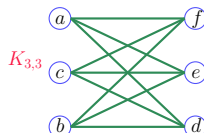
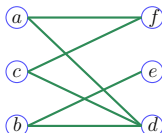
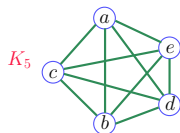
- A *collaboration graph* for a set of n scientists is a graph with n vertices such that two vertices are connected by an edge if the corresponding scientists have at least one joint publication.
- The *Erdős number* of a scientist is the “collaborative distance” of a scientist to the extremely prolific Hungarian mathematician Paul Erdős (1913–1996, more than 500 co-authors and more than 1 500 publications): Erdős has 0, and a scientist has Erdős number $k + 1$ if k is the lowest Erdős number of his/her co-authors.
- One’s Erdős number can be obtained by computing minimum-weight paths on a collaboration graph: Single-source shortest path or minimum-spanning tree (for appropriate weights).



Complete and Bipartite Graphs

Definition 207 (Complete graph, Dt.: vollständiger Graph)

A *complete graph* on n vertices, commonly denoted by K_n , is an undirected graph with n vertices in which every pair of vertices is adjacent.



Definition 208 (Bipartite graph, Dt.: bipartiter Graph)

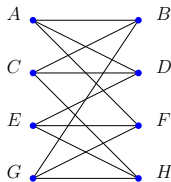
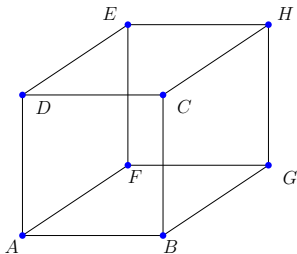
An undirected graph $\mathcal{G} = (V, E)$ is a *bipartite graph* if V can be partitioned into two (non-empty) subsets V_1, V_2 such that $E \subseteq \{ \{v_1, v_2\} : v_1 \in V_1, v_2 \in V_2 \}$.

Definition 209 (Complete bipartite graph, Dt.: vollständig-bipartiter Graph)

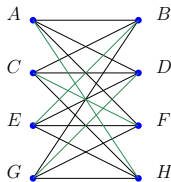
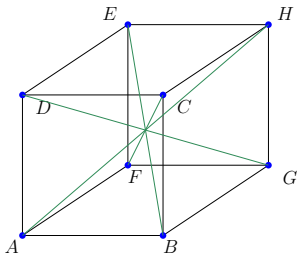
An undirected graph $\mathcal{G} = (V, E)$ is a *complete bipartite graph* if V can be partitioned into two (non-empty) subsets V_1, V_2 such that $E = \{ \{v_1, v_2\} : v_1 \in V_1, v_2 \in V_2 \}$. If $n := |V_1|$ and $m := |V_2|$ then \mathcal{G} is denoted by $K_{n,m}$.

Complete and Bipartite Graphs

- The edges and corners of a cube can be interpreted as a bipartite graph.



- If we add all **diagonals** that cross the cube then we get $K_{4,4}$.



Lemma 210

Let $\mathcal{G} = (V, E)$ be a bipartite graph and let V_1, V_2 be the partition of V according to Def. 208. Then

$$\sum_{v_1 \in V_1} \deg(v_1) = \sum_{v_2 \in V_2} \deg(v_2) = |E|.$$

Proof:

- As each edge has one vertex from V_1 , we can write

$$\sum_{v_1 \in V_1} \deg(v_1) = |E|.$$

- Similarly,

$$\sum_{v_2 \in V_2} \deg(v_2) = |E|.$$

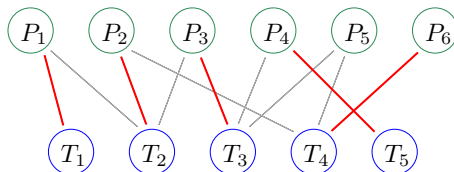


Real-World Application: Task Assignment and Matchings

- Suppose that we are given a set of tasks and a set of processors. We know which processor can carry out which tasks.
- These relations can be represented as a bipartite graph.
- How can we get the maximum number of tasks processed concurrently?

Definition 211 (Matching, Dt.: Paarung)

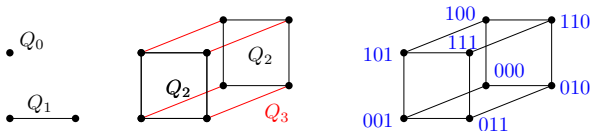
- A *matching* in a simple graph $\mathcal{G} = (V, E)$ is a subset E' of E such that no two edges of E' are incident upon the same vertex of V .
- A *maximal matching* is a matching that does not allow to add an additional edge.
- A *maximum matching* is a matching with the largest-possible number of edges.
- A *perfect matching* is a matching that leaves no vertex unmatched.



Definition 212 (Hypercube)

For $n \in \mathbb{N}_0$, the hypercube Q_n is defined recursively as follows:

- 1 Q_0 is a single vertex;
- 2 Q_{n+1} is obtained by taking two disjoint copies of Q_n and linking each vertex in one copy of Q_n to the corresponding vertex in the other copy of Q_n .



- We could also obtain Q_n by labeling 2^n vertices with distinct n -bit binary strings, and by connecting those vertices by edges whose strings differ in exactly one bit.

Lemma 213

Q_n is a regular bipartite graph of degree n with 2^n vertices and $n \cdot 2^{n-1}$ edges.

Real-World Application: Hamilton Cycles in Q_n Yield Gray Codes

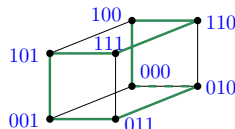
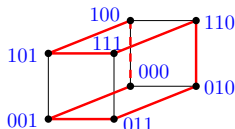
Definition 214 (Gray code)

A (cyclic) Gray code of an ordered sequence of 2^n entities, for $n \in \mathbb{N}$, is a sequence of n -bit binary strings such that the encodings of two neighboring entities have Hamming distance one, i.e., differ by exactly one bit.

- Gray codes are widely used in position encoders and for error detection and correction in digital communication.

Lemma 215

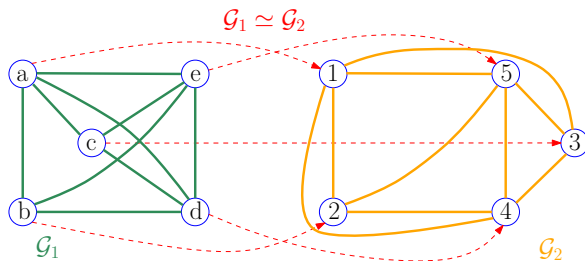
For $n \in \mathbb{N}$ with $n \geq 2$, the number of different n -bit Gray codes equals the number of different Hamilton cycles in Q_n .



Isomorphic Graphs

Definition 216 (Isomorphic, Dt.: isomorph)

Two (directed) graphs $\mathcal{G}_1 = (V_1, E_1)$ and $\mathcal{G}_2 = (V_2, E_2)$ are *isomorphic*, denoted by $\mathcal{G}_1 \simeq \mathcal{G}_2$, if there exists a one-to-one mapping f between V_1 and V_2 that preserves adjacency; i.e., $uv \in E_1 \Leftrightarrow f(u)f(v) \in E_2$ for all $u, v \in V_1$. Such a suitable function f is called *graph isomorphism*.

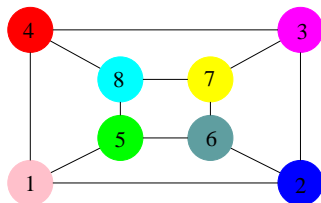
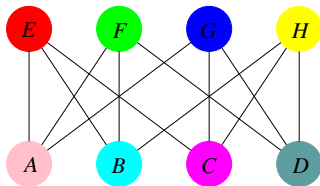


Lemma 217

The relation \simeq is an equivalence relation on graphs.

Isomorphic Graphs

- Don't be fooled by drawings! Two graphs may be isomorphic even if their drawings look strikingly different.

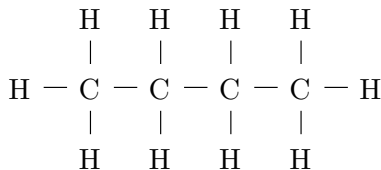


- Necessary (but not sufficient) conditions for two graphs to be isomorphic: same numbers of vertices and edges, same degrees.
- The complexity of the graph isomorphism problem for general n -vertex graphs is unknown. No polynomial-time algorithm is known, but the problem is also not known to be \mathcal{NP} -complete. In December 2015, László Babai announced a deterministic algorithm that runs in time $2^{O(\log^c n)}$ for some positive constant c , i.e., in quasi-polynomial time.
- Practically efficient algorithms for graph canonical labeling are known, though

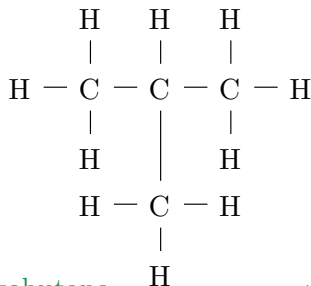


Real-World Application: Non-Isomorphic Trees Represent Molecules

- Molecules can be represented as graphs, where atoms are represented by vertices and bonds are represented by edges [Arthur Cayley 1857].
- Saturated hydrocarbons, C_nH_{2n+2} , are given by trees where each carbon atom is represented by a degree-four vertex and each hydrogen atom is a leaf.
- How many different isomers can exist for $n := 4$?
- We have exactly two non-isomorphic trees of this type and, thus, two different isomers of C_4H_{10} , namely butane and isobutane.



Butane



Isobutane

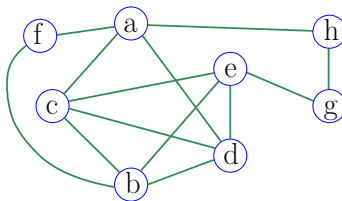
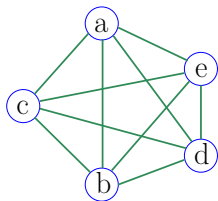


Subdivision of a Graph

Definition 218 (Subdivision, Dt.: Unterteilung)

An edge subdivision of the edge $uv \in E$ by means of the vertex $w \notin V$ transforms the graph $\mathcal{G} = (V, E)$ into the graph $\mathcal{G}' = (V', E')$, where $V' = V \cup \{w\}$ and $E' = (E \setminus \{uv\}) \cup \{uw, vw\}$.

A graph $\mathcal{G}' = (V', E')$ is a *subdivision graph* of $\mathcal{G} = (V, E)$ if \mathcal{G}' is obtained from $\mathcal{G} = (V, E)$ via a finite series of edge subdivisions.



Planar Graphs

Definition 219 (Planar graph, Dt.: planarer oder plättbarer Graph)

A *planar graph* is a graph which can be drawn in the plane without edge crossings. Such a drawing is called a (*planar*) *embedding* (Dt.: planare Einbettung).

Definition 220 (Planar subdivision, Dt.: planare Unterteilung)

A *face* of an embedding of a planar graph is a maximal connected region of the plane that is disjoint from all edges.

An embedding of a planar graph induces a *planar subdivision*, i.e., it subdivides the plane into several connected faces. (One of those faces, the so-called *outer face*, may be unbounded.)

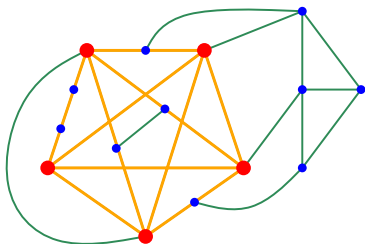
Theorem 221 (Kuratowski (1930))

A graph is planar if and only if it does not contain a subgraph that is isomorphic to a subdivision graph of K_5 or $K_{3,3}$.

Corollary 222

If a graph contains K_5 or $K_{3,3}$ as a subgraph then it is not planar.

- The following graph contains a subdivision graph of K_5 as a subgraph. Hence, it is not planar.



Theorem 223 (Wagner (1936), Fáry (1948), Stein (1951))

Any planar graph can be drawn in the plane without edge crossings such that all its edges are straight-line segments.

- Such a straight-line embedding of a planar graph is called *planar straight-line graph* (PSLG).

Theorem 224 (Euler, Dt.: Eulerscher Polyedersatz)

Consider an embedding of a connected planar graph \mathcal{G} . We denote

- the number of its vertices by v ,
- the number of its edges by e ,
- the number of its faces by f .

Then

$$v - e + f = 2.$$

Proof: Suppose that \mathcal{G} is connected but no tree. Therefore \mathcal{G} contains a cycle, and we may remove an edge from \mathcal{G} without destroying its connectivity. The removal of one edge of a cycle decreases both e and f by one, implying that the value of $v - e + f$ does not change. By using induction we can prove that a series of such edge removals (for breaking up cycles) does not change the value of $v - e + f$, while allowing us to transform \mathcal{G} into a tree.

If, however, \mathcal{G} is a tree then Thm. 190 tells us that $1 = v - e$. Since $f = 1$, we get $2 = v - e + f$, thus establishing the claim. □

- Euler's Formula generalizes to $v - e + f = 1 + c$ for a planar graph with c connected components.



Corollary 225

Let v, e, f for a connected planar graph \mathcal{G} as defined in Theorem 224. If $v \geq 3$ then

$$e \leq 3v - 6 \quad \text{and} \quad f \leq 2v - 4 \quad \text{and} \quad f \leq \frac{2}{3}e.$$

If every vertex of \mathcal{G} has a degree of three or greater then we get

$$v \leq \frac{2}{3}e \quad \text{and} \quad e \leq 3f - 6 \quad \text{and} \quad v \leq 2f - 4.$$

Furthermore, every planar graph contains one node with degree at most five.

Proof: We prove that $3f \leq 2e$, which is obvious for $f = 1$. We call an edge a “side” of a face if the edge is in the boundary of the face. Let k denote the total number of sides.

If $f > 1$ then each face is bounded by at least three sides, so $k \geq 3f$.

But each edge has at most two different sides, so $k \leq 2e$.

We conclude $3f \leq 2e$. □



Euler's Formula for Planar Graphs

Corollary 226

K_5 is not planar.

Proof: We get $v = 5$ and $e = \binom{5}{2} = 10$. So, $e \leq 3v - 6$ (Cor. 225) does not hold. \square

Definition 227 (Triangle-free, Dt.: dreiecksfrei)


A *triangle-free graph* is a graph which does not contain a cycle of length three, i.e., in which no three vertices form a triangle of edges.

Corollary 228

A triangle-free planar graph has one node of degree at most three and $e \leq 2v - 4$ holds (if $v \geq 2$).

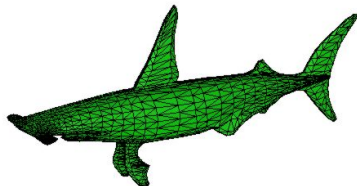
Corollary 229

$K_{3,3}$ is not planar.

Proof: $K_{3,3}$ is triangle-free and has six vertices and nine edges. If it were planar then, by Cor. 228, it could have at most $2 \cdot 6 - 4 = 8$ edges. Thus, $K_{3,3}$ is non-planar. 

Real-World Application: Number of Edges of a Polyhedron

- Suppose that a polyhedral model has n vertices. How many edges and faces can it have at most? What is the storage complexity relative to n ?



Theorem 230

The vertices and edges of a simple (bounded) polyhedron form a planar graph.

- Hence, Cor. 225 implies that an n -vertex polyhedron has $O(n)$ many edges and faces: We have at most $3n - 6$ edges and $2n - 4$ faces.

Graph Coloring

Definition 231 (Coloring, Dt.: Färbung)

An assignment of colors to all vertices of a graph \mathcal{G} is called a *(vertex) coloring* if adjacent vertices are assigned different colors.

Definition 232 (k -colorable, Dt.: k -färbbar)

A graph \mathcal{G} is *k -colorable* if \mathcal{G} admits a coloring that uses k colors.

Definition 233 (Chromatic number, Dt.: chromatische Zahl)

The *chromatic number* of a graph \mathcal{G} , written as $\chi(\mathcal{G})$, is the least number of colors required to color \mathcal{G} .

- $\chi(K_n) = n$.
- Determining $\chi(\mathcal{G})$ is \mathcal{NP} -hard even if \mathcal{G} is a planar 4-regular graph. Thus, it is rather unlikely that a polynomial-time algorithm will ever be found for determining $\chi(\mathcal{G})$. However, fairly efficient heuristics exist.

Lemma 234

A graph is 2-colorable if and only if it is bipartite.

Graph Coloring

- It is straightforward that every planar graph can be colored by six colors and that every triangle-free planar graph can be colored by four colors.
- Still easy to see: Every planar graph can be colored by five colors.

Theorem 235 (Four Color Theorem, Haken and Appel (1976))

Every planar graph can be colored using no more than four colors.

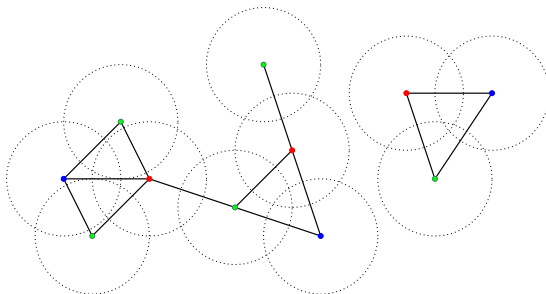
- Wolfgang Haken and Kenneth Appel used a super-computer at the University of Illinois to check 1 936 “reducible” configurations. The proof is not accepted by all mathematicians as it has two parts, one of which can only be solved using computers. (And the second part that is solveable by hand is also very tedious.)
- In 1996, Robertson et alii reduced the number of computer-checked cases to 633.
- In 2005, Benjamin Werner and Georges Gonthier used a general-purpose proof assistant (“Coq”) to prove the theorem.

Corollary 236

If every entity of a topographic map is a connected area then four colors suffice to color the map such that no two entities that share a common border (other than a common point) are colored with the same color.

Real-World Application: Channel Assignment

- We can solve the channel assignment problem by considering its so-called unit-disk graph, where
 - the vertices are given by the broadcast stations,
 - two vertices are connected by an edge if their service areas overlap.
- Obviously, the chromatic number of that graph equals the minimum number of frequencies needed.



Real-World Application: Index Registers

- Optimizing compilers try to store frequently used variables of the body of a loop in index registers of the CPU (rather than in regular memory).
 - How many index registers are needed for a given loop?
 - We set up a graph whose vertices are given by the variables, and where two vertices are connected by an edge if the corresponding variables ought to be kept in registers at the same time.
 - Then the chromatic number of that graph gives the minimum number of registers needed.
-
- Other applications of graph coloring:
 - Scheduling consumer-producer interactions to allow concurrency.
 - Sudoku puzzles.

7 Cryptography

- Introduction
- Symmetric-Key Cryptography
- Public-Key Cryptography

Introduction — What is Cryptography?

- Cryptography is the science of sending and receiving messages in secret code.
- A *sender* (“Alice”) sends an encoded message to a *receiver* (“Bob”).
- The goal is to keep the transmission of the message secure (from others to read it) and to ensure successful communication of the information.
- Cryptography has been used for at least two thousand years, see Caesar’s cipher.
- Likely, the most famous historical example of cryptography is the Enigma machine; its security breach ultimately helped significantly with the defeat of the submarine force of the German Third Reich.
- Two main schemes are in use nowadays:

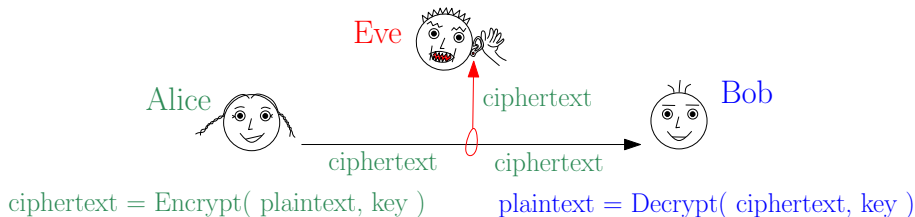
Symmetric-Key Cryptography (SKC): the same secret key is used for both encryption and decryption; aka secret-key cryptography.

Public-Key Cryptography (PKC): different keys are used for encryption and decryption, with some keys being known publicly; aka asymmetric-key cryptography.



- *Plaintext* — original message.
- *Ciphertext* — encoded/encrypted message.
- *Encryption* — generating ciphertext from plaintext.
- *Decryption / Deciphering* — generating plaintext from ciphertext.
- *Cryptanalysis* — trying to break the encryption by applying various methods.
- *Adversary, Spy* — the message thief.
- *Eavesdropper* — a secret listener who listens to private conversations.
- *Authentication* — the process of proving one's identity.
- *Privacy* — ensuring that the message is read only by the intended receiver.
(GnuPG: “Privacy is not a crime!”)

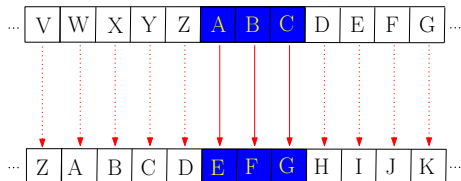
Eavesdropper Attacks



- Eve might attempt to
 - break the encryption,
 - replay the encrypted message (e.g., login) without breaking the encryption,
 - modify the message,
 - block the message,
 - fabricate a new message.

Classical Cryptography: Caesar's Cipher

- According to Suetonius, Caesar (100AD–44AD) used an encryption scheme (for communication with his generals) that shifted the alphabet of the plaintext by some fixed value.



- Suppose that the (Roman) letters are mapped to the numbers $0, 1, \dots, 25$.
- Then Caesar's encryption and decryption with shift n can be computed as follows:

$$\text{ciphertext} := \text{Encrypt}_n(\text{plaintext}) = (\text{plaintext} + n) \bmod 26$$

$$\text{plaintext} := \text{Decrypt}_n(\text{ciphertext}) = (\text{ciphertext} - n) \bmod 26$$

- With $n := 4$:

Plaintext: alea iacta est

Ciphertext: epie megxe iwx



Classical Cryptography: Caesar's Cipher

- Likely, Caesar's cipher was reasonably secure at the time when it was used.
- It is broken easily by means of frequency analysis and brute-force attacks — it offers no security by today's standards!
- Nevertheless, Caesar's cipher with $n := 13$, aka ROT13, has been (mis-)used for serious applications even rather recently.
- However, it is used within more complex systems, e.g., the Vigenère cipher.
- On a Unix machine, the `tr` utility can be used for carrying out Caesar's cipher.
E.g.,

```
echo "alea iacta est" | tr 'A-Za-z' 'E-ZA-De-za-d'
```


yields

```
epie megxe iwx.
```

Symmetric-Key Cryptography

- A single secret key is used for both encryption and decryption (aka “*secret-key algorithms*”).



- Simple example: Suppose that Alice wants to encrypt a bit string A . Then Alice and Bob could choose a secret key B and apply a bit-wise XOR (exclusive OR, \oplus) — an output bit is 1 if exactly one of the two input bits is 1 — in order to transmit $A \oplus B$. Then Bob would compute $(A \oplus B) \oplus B$ and, thus, retrieve A .

A	B	$A \oplus B$	$(A \oplus B) \oplus B$
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1

- Of course, the key must be known to both Alice and Bob, and, in fact, it must not be known to anybody else.

The Key Distribution Problem

- Of course, the key must be known to both Alice and Bob, and, in fact, it must not be known to anybody else.
- That is, Alice and Bob need to share the secret key in order to be able to encrypt and decrypt their messages!
- What is a secure mechanism for them to exchange a key??
 - Meet in person at a secret place and share the key?!
 - Share in parts?!
- The key distribution problem is a major roadblock on the road to secure communication among folks who do not meet regularly.
- A second big disadvantage is the need for multiple keys in order to encrypt messages intended for different receivers.

Public-Key Cryptography

- A pair of keys is used to encrypt and decrypt the messages, with one key being public.



- PKC make use of so-called *one-way functions* which are “easy” to compute for every input but extremely “hard” to invert for an output given. For example, consider
 - multiplication versus factorization (“factorization problem”):
 - If $f(a, b) := a \cdot b$, then
 $f(a, b) = 533$ for $a = 13, b = 41$;
 - While you can calculate $f(13, 41)$ in your head, it is less trivial to obtain a, b such that $f(a, b) = 533$;
 - exponentiation versus logarithms (“discrete log problem”):
 - If $f(a, b) := a^b$, then
 $f(a, b) = 243$ for $a = 3, b = 5$;
 - Again, finding a and b such that $\log_a 243 = b$ is considerably more difficult.
- Whitfield Diffie and his advisor Martin Hellman were the first to *publish* a PKC scheme in 1976. (They are the recipients of the 2015 ACM Turing Award.)

Real-World Application: Diffie-Hellman Symmetric Key Exchange

- Alice and Bob share two public numbers: a (large) prime number $p \in \mathbb{P}$ and a so-called generator $g \in \{2, 3, \dots, p-1\}$ such that for every $n \in \{1, 2, \dots, p-1\}$ there exists a $k \in \mathbb{N}$ with $n = g^k \bmod p$. (Then g is a “primitive root” modulo p).

	Alice	Bob
(1)	selects s with $1 < s < p-1$	selects t with $1 < t < p-1$
(2)	sends $S := g^s \bmod p$ to Bob	sends $T := g^t \bmod p$ to Alice
(3)	calculates $T^s \bmod p$	calculates $S^t \bmod p$

- We have

$$T^s \equiv_p (g^t)^s = g^{ts} = (g^s)^t \equiv_p S^t.$$

Hence, $k := T^s \bmod p = S^t \bmod p$ can be used as a common key by Alice and Bob.

- In general, the public information is p, g, S and T , while s and t are secret.
- To find s , Eve could attempt to solve the discrete log problem $g^s = S \bmod p$. Same for t . At present, nobody knows how to solve this problem efficiently. It is not even known how to compute $g^{st} \bmod p$ efficiently if $g^s \bmod p$ and $g^t \bmod p$ are known.



Real-World Application: Diffie-Hellman Key Exchange Sample

Alice	Bob
(1) selects s with $1 < s < p - 1$	selects t with $1 < t < p - 1$
(2) sends $S := g^s \bmod p$ to Bob	sends $T := g^t \bmod p$ to Alice
(3) calculates $T^s \bmod p$	calculates $S^t \bmod p$

- Alice and Bob make $p := 13$ and $g := 2$ public.
- Alice chooses the private value $s := 5$, while Bob chooses $t := 6$.
- We get $S := g^s \bmod p = 2^5 \bmod 13 = 32 \bmod 13 = 6$, and $T := g^t \bmod p = 2^6 \bmod 13 = 12$, which can be exchanged publicly, i.e., via an insecure communication channel.
- Finally, $T^s \bmod p = 12^5 \bmod 13 = (12140 \cdot 13 + 12) \bmod 13 = 12$, and $S^t \bmod p = 6^6 \bmod 13 = (3588 \cdot 13 + 12) \bmod 13 = 12$.
- Hence, Alice and Bob have managed to exchange 12 as a master key for their future communication.
- Of course, in practice considerably larger values are chosen for p !
- The Diffie-Hellman key exchange is vulnerable to man-in-the-middle attacks!



Lemma 237

Let $a, b \in \mathbb{N}$ such that $\gcd(a, b) = 1$. Then there exists $x \in \mathbb{Z}$ such that $ax \equiv_b 1$.

Proof: Since $\gcd(a, b) = 1$, Cor. 60 tells us that there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Hence, $ax = 1 - by \equiv_b 1$. □

Definition 238 (Euler's Totient Function, Dt.: Eulersche φ -Funktion)

Euler's totient function $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ is defined as

$$\varphi(n) := |U_n|, \quad \text{with } U_n := \{1 \leq k \leq n : \gcd(k, n) = 1\}.$$

The set U_n is called the *group of units* of n .

- Thus, $\varphi(n)$ gives the number of integers among $1, 2, \dots, n$ which are coprime to n .
- We have $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, and $\varphi(p) = p - 1$ for every $p \in \mathbb{P}$.

Lemma 239

Let $p, q \in \mathbb{P}$. If $p \neq q$ then $\varphi(pq) = (p-1)(q-1)$.

Proof: There are q multiples of p and p multiples of q within $\{1, 2, \dots, pq\}$, and the only common multiple of both p and q is pq . Hence, by the Inclusion-Exclusion Principle (Thm. 95), $\varphi(pq) = pq - p - q + 1$. □

Lemma 240 (Fermat/Euler)

Let $n \in \mathbb{N}$ and $m \in U_n$. Then $m^{\varphi(n)} \equiv_n 1$.

Corollary 241

Let $n \in \mathbb{N}$ and $m \in U_n$. If $n = pq$, with $p, q \in \mathbb{P}$ and $p \neq q$, then $m^{(p-1)(q-1)} \equiv_n 1$.

Real-World Application: RSA Cryptosystem

- The RSA system [Rivest, Shamir, Adleman 1977] makes use of Lemma 240 and of the fact that state-of-the-art factorization methods take far too long for products of numbers with several hundred digits each.
- The basic idea is very simple:
 - Select two distinct prime numbers p and q (each of which, in practice, has at least 150 digits) and compute $n = p \cdot q$.
 - Lemma 239 tells us that $\varphi(n) = (p - 1) \cdot (q - 1)$.
 - Select an integer $e \in \mathbb{N} \setminus \{1\}$ such that $\gcd(e, \varphi(n)) = 1$.
 - The numbers n and e are published (Bob's *public key*).
 - Compute a number d which is the inverse of e in $\mathbb{Z}_{\varphi(n)}$, i.e., such that $d \cdot e \equiv_{\varphi(n)} 1$. (Such a number exists due to Lem. 237.)
 - The number d is called Bob's *private key* and is kept secret.

Real-World Application: RSA Cryptosystem

- Hence, we have $n = p \cdot q$ and, thus, $\varphi(n) = (p - 1) \cdot (q - 1)$. Furthermore, $\gcd(e, \varphi(n)) = 1$ and $d \cdot e \equiv_{\varphi(n)} 1$.
- *Encoding the ciphertext:*
 - Alice encodes a message $x \in \mathbb{N}$, with $x < n$ to keep it in \mathbb{Z}_n and with $\gcd(x, n) = 1$, by using Bob's public key e and n :
 $y := x^e \bmod n$ with $0 < y < n$.
- *Decoding the ciphertext:*
 - Bob computes $z = y^d \bmod n$ with $0 < z < n$.
- Why does $z = x \bmod n$ hold?
 - The condition $d \cdot e \equiv_{\varphi(n)} 1$ ensures that there exists $k \in \mathbb{Z}$ such that

$$d \cdot e = k \cdot \varphi(n) + 1.$$

- It follows that

$$z \equiv_n y^d \equiv_n x^{de} = x^{k\varphi(n)+1} = (x^{\varphi(n)})^k x \stackrel{\text{L. 240}}{\equiv_n} (1)^k x = x.$$



Real-World Application: RSA Cryptosystem Sample

- Suppose that $p = 5$ and $q = 11$. Hence $n = 55$ and $\varphi(n) = 40$. Suppose further that three users chose the following keys:

	e	d
Alice	23	7
Bob	37	13
Caesar	9	9

- We have $23 \cdot 7 \equiv_{40} 1$ and $37 \cdot 13 \equiv_{40} 1$ and $9 \cdot 9 \equiv_{40} 1$.
- Let $x := 2$ (and use Mathematica to do the arithmetic).

Alice: $2^{23} = 8388608 = 152520 \cdot 55 + 8 \equiv_{55} 8 =: y$

$$8^7 = 2097152 = 38130 \cdot 55 + 2 \equiv_{55} 2 =: z$$

Bob: $2^{37} = 137438953472 = 2498890063 \cdot 55 + 7 \equiv_{55} 7 =: y$

$$7^{13} = 96889010407 = 1761618371 \cdot 55 + 2 \equiv_{55} 2 =: z$$

Caesar: $2^9 = 512 = 9 \cdot 55 + 17 \equiv_{55} 17 =: y$

$$17^9 = 118587876497 = 2156143209 \cdot 55 + 2 \equiv_{55} 2 =: z$$



Real-World Application: RSA Cryptosystem Analysis

- Note that there are $\varphi(n)$ many messages that can be sent for n given.
- Since $\frac{\varphi(n)}{n} = (1 - \frac{1}{p})(1 - \frac{1}{q})$ is close to 1 for large p, q , the probability of selecting a message that is not coprime to n is rather small.
- An eavesdropper who only knows n , e , and y cannot do much with this information. In particular, no efficient algorithm is known to factor p, q as a simple means to obtain $\varphi(n)$.
- Although n is publicly known, it is important to keep $\varphi(n)$ and, thus, also p, q secret!
- It is also important to ensure that $x^e > n$, i.e., that y is obtained by exponentiation and then by a reduction modulo n .
 - If $x^e < n$ then one could simply recover x by taking the e -th root of y . (After all, e is known publicly!)
 - Hence, it is wise to select e such that $2^e > n$.

The End!

I hope that you enjoyed this course, and I wish you all the best for your future studies.

