Mega Summary HS24

Contents

Disclaimer

this summary was written purely for my own understanding, and does not claim that it is “correct” (as “compatible with the sources”) in any way | mistakes may have been made | notation may be wrong (on purpose) | use at your own caution

Scripts

DiskMath: https://crypto.ethz.ch/teaching/DM24/
LinAlg: https://ti.inf.ethz.ch/ew/courses/LA24/index.html
AandD: HS24 Moodle Course

Written by Emil S.

2 - Logic Intro

Propositional logic

statements: and, or, not, $\Rightarrow$ formulas/functions: A, $A \to B$, $\neg A$

$F \equiv G$ / $F \vdash G$: for all truth assignments with $F=1$, $G=1$ / they are equal

A, B, C = "propositional symbols"

equivalence rules: comm./ass., distr., absorption, demorgan, $\neg\neg A$, tautology, ...

tautology/valid: A true for all truth assignments

satisfiable/unsatisfiable: true for some/none truth assignments

L2.2 F tautology $\Leftrightarrow$ $\neg F$ unsatisfiable

L2.3 $F \to G$ tautology $\Leftrightarrow$ $F \vdash G$

function tables:

A	B	$A \to B$	$\neg A \vee B$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

$\to$: $A \to B \equiv \neg A \vee B$

Predicate logic

D2.10 k-ary predicate P on U is function $U^k \to \{0,1\}$

D2.11 $\forall x$ = "true for all x"
$\exists x$ = "true for some x"

interpreting a formula: defining all the free parts

Proof Patterns

composing implications: if $S \Rightarrow T$ and $T \Rightarrow Q$ then $S \Rightarrow Q$

L2.5 $(A \to B) \wedge (B \to C) \vdash (A \to C)$

Indirect proof: proof $S \Rightarrow T$: assume not T and prove not S

L2.6 $\neg A \to \neg B \equiv B \to A$

Modus Ponens: proof S: prove R, prove $R \Rightarrow S$

L2.7 $A \wedge (A \to B) \vdash B$

Case Distinction: proof S: find $R_1, R_2, \dots, R_n$; prove at least one R_i is true; prove $R_k \Rightarrow S$ for all k

L2.8 $(A_1 \vee A_2 \vee \dots \vee A_k) \wedge (A_1 \to B) \wedge \dots \wedge (A_k \to B) \vdash B$

Contradiction: proof S: assume S false $\to$ prove T $\to$ prove T false (contradiction)

L2.9 $(\neg A \to B) \wedge \neg B \vdash A$ and $(A \vee B) \wedge \neg B \vdash A$

Existence Proofs: proof $\exists x \in X$ s.t. $S_x = 1$: constructive = find specific x and prove S_x
non-constructive = not for specific x

Pigeonhole Principle: if set of n objects is partitioned into k sets then at least one set must contain $\lceil \frac{n}{k} \rceil$ elements

Counterexample: disprove $\forall x\, P(x)$ by showing some x s.t. $P(x) = 0$

Induction: Base Case $P(0)$ $\to$ Induction Hypothesis "for some k" $\to$ Induction Step $P(k) \Rightarrow P(k+1)$

3 - Sets

Sets

$E(x,y) \;/\; x \in y$ "x is in set y".

D3.2 $A = B \overset{\text{def}}{\iff} \forall x\,(x \in A \leftrightarrow x \in B)$ L3.1 $\{a\} = \{b\} \Rightarrow a = b$

$+\ \{a,b\} = \{b,a\}$ $+\ (a,b) \overset{\text{def}}{=} \{\{a\},\{a,b\}\}$ $+\ (a,b) = (c,d) \overset{\text{def}}{\iff} a = c \wedge b = d$

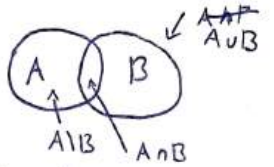
Subsets D3.3 $A \subseteq B \overset{\text{def}}{\iff} \forall x\,(x \in A \to x \in B)$ "A subset of B"

Equality L3.2 $A = B \iff (A \subseteq B) \wedge (B \subseteq A)$ L3.3 $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$

Union $A \cup B \overset{\text{def}}{=} \{x \mid x \in A \overset{\vee}{\wedge} x \in B\}$

Intersection $A \cap B \overset{\text{def}}{=} \{x \mid x \in A \wedge x \in B\}$

Difference $B \setminus A \overset{\text{def}}{=} \{x \mid x \in B \wedge x \notin A\}$



T3.4 $A \subseteq B \iff A \cap B = A \iff A \cup B = B$ "consistency"
+ Idempotence, ass., comm; distr., absorption

Empty set $\emptyset$ or $\{\}$ A is empty if $\forall x \neg(x \in A)$ L3.6 $\forall A\,(\emptyset \subseteq A)$
L3.5 there is only one empty set

Powerset $P(A) \overset{\text{def}}{=} \{S \mid S \subseteq A\}$ is a set of subsets of A

$|P(A)| = 2^{|A|}$ ∘ the empty set is element of every powerset, as is A itself

∘ $P(\emptyset) = \{\emptyset\}$, $P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$, $P(\{\emptyset,\{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset,\{\emptyset\}\}\}$, $\{1,2\} \in P(\mathbb{N})$

D3.8 **Product of Sets** $A \times B = \{(a,b) \mid a \in A \wedge B \in B\}$

Relations

D3.9 a relation p from A to B is a subset of $A \times B$; If $A = B$ then p is "on" A

D3.10 id_A "identity relation on A" $= \{(a,a) \mid a \in A\}$

D3.11 **Inverse** $\hat{p} \overset{\text{def}}{=} \{(b,a) \mid (a,b) \in p\}$ is a relation from B to A for $p : A \to B$

in matrix representation

	a	b	c
1	0	0	1
2	0	1	0
3	0	0	1

$= \{(1,c),(2,b),(3,c)\}$

Special Properties: A relation on A is called:

∘ $a\,p\,a = (a,a) \in p$

reflexive if $a\,p\,a$ for all $a \in A$, if $id_A \subseteq p$

irreflexive if $a \not p\, a$ for all $a \in A$, if $id_A \cap p = \emptyset$

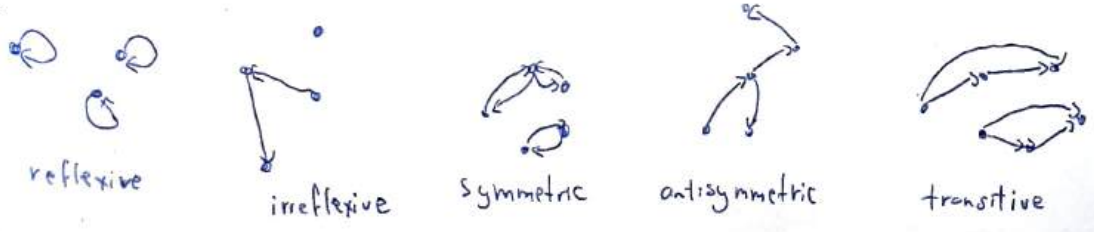
Symmetric if $a\,p\,b \iff b\,p\,a$, if $p = \hat{p}$

antisymmetric if $a\,p\,b \wedge b\,p\,a \Rightarrow a = b$, if $p \cap \hat{p} \subseteq id_A$

transitive if $a\,p\,b \wedge b\,p\,c \Rightarrow a\,p\,c$ (for all $a,b,c \in A$)

L3.9 p transitive $\iff p^2 \subseteq p$

WARNING: $\emptyset = p$ is not reflexive if $A \neq \emptyset$, but transitive, symmetric, antisymmetric since those only care about the tuples in p, but reflexivity needs to hold for all elements in A!
symmetric and antisymmetric are not opposites, not symmetric ⇎ antisymmetric



Composition $p \circ q \overset{\text{def}}{=} \{(a,c) \mid \exists b ((a,b) \in p \wedge (b,c) \in \sigma)\}$ for $p: A \to B$, $q: B \to C$

L3.7 $p \circ (q \circ \phi) = (p \circ q) \circ \phi$

D3.18 Transitive Closure $p^* = \bigcup_{n \in \mathbb{N} \setminus \{0\}} p^n$ (in graph representation, contains (a,b) if b is reachable from a)

Equivalence Relations

D3.19 An equivalence relation is reflexive, symmetric, transitive

D3.20 equivalence class of a $[a]_\theta \overset{\text{def}}{=} \{b \in A \mid b \,\theta\, a\}$ for θ is equiv. relation on A

L3.10 The intersection of two equiv.-rel. is a equiv.-rel

D3.21 Partition is a set of subsets of A $\{S_i \mid i \in I\}$ s.t. they cover A and are disjoint, so: $S_i \cap S_j = \emptyset$ $\forall i \neq j$ and $\bigcup_{i \in I} S_i = A$

D3.22 $A/\theta \overset{\text{def}}{=} \{[a]_\theta \mid a \in A\}$ is "quotient set of A by θ" with θ equiv.-rel. on A

T3.11 A/θ is a partition of A

Partial Order Relations

D3.23 A partial order relation is reflexive, transitive, antisymmetric

- A set with a p.o. relation on A is a "poset" and denoted $(A; \preceq)$ with $\preceq$ the relation

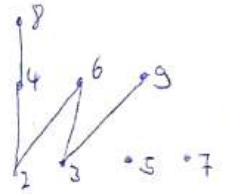
D3.24 If $a \preceq b$ or $b \preceq a$ then a, b are comparable, otherwise incomparable

D3.25 If all $a, b \in A$ are comparable, then A is totally ordered

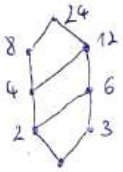
D3.26 In $(A; \preceq)$ b covers a if $a \prec b$ and $\nexists c$ with $a \prec c$ and $c \prec b$ ("between" a and b)

- $a \prec b \overset{\text{def}}{\Leftrightarrow} a \preceq b$ and $a \neq b$

D3.27 Hasse Diagram of A is a directed graph with edge (a,b) if b covers a (or without arrows but b drawn higher than a)



for "|"



D3.28 Direct Product of posets $(A; \preceq)$ and $(B; \sqsubseteq) = (A; \preceq) \times (B; \sqsubseteq)$ is the set $A \times B$ with the relation $\leq: (a_1, b_1) \leq (a_2, b_2) \overset{\text{def}}{\Leftrightarrow} a_1 \preceq a_2 \wedge b_1 \sqsubseteq b_2$

T3.12 $(A; \preceq) \times (B; \sqsubseteq)$ is a poset

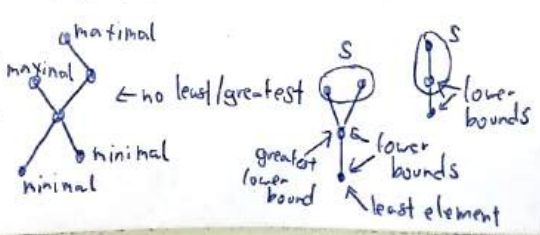
T3.13 The lexographical order $\leq_{lex}$ on $A \times B$ for $(A; \preceq)$ and $(B; \sqsubseteq)$ is:

$(a_1, b_1) \leq_{lex} (a_2, b_2) \overset{\text{def}}{\Leftrightarrow} a_1 \prec a_2 \vee (a_1 = a_2 \wedge b_1 \sqsubseteq b_2)$

D3.29 Special Poset Elements: for $(A; \preceq)$ and $S \subseteq A$ a is a

- a minimal (maximal) element of A if $\nexists b \in A$ with $b \prec a$ ($b \succ a$)
- the least (greatest) element of A if $a \preceq b$ ($a \succeq b$) for all $b \in A$
- a lower (upper) bound of S if $a \preceq b$ ($a \succeq b$) for all $b \in S$
- the greatest lower (least upper) bound of S if a is the greatest (least) element of all lower (upper) bounds of S

! there can be multiple minimal elements and bounds, but only one least/greatest of them and there might be none.



D3.30 A poset is "well-ordered" if it's totally ordered and every non-empty subset has a least element

D3.31 If in poset A: a,b have a least upper bound it is the **join** of a,b $a \vee b$
a,b have a greatest lower bound it is the **meet** of a,b $a \wedge b$

D3.32 **Lattice** is a poset where all a,b have meet and join

here a,b don't have a join since there is no least among the two upper bounds, so not a lattice!

Functions

D3.33 **Function** $f: A \to B$ from domain A to codomain B is a relation from A to B with:
- totally-defined: $\forall a \in A \; \exists b \in B \; a f b$
- well-defined: $\forall a \in A \; \forall b,b' \in B \; (a f b \wedge a f b' \to b = b')$

so it maps from A to B and we write $f: A \to B$, $a \mapsto b$

D3.34 The set of all functions from A to B is B^A.
And there are $|B|^{|A|}$ different such functions.

D3.35 A "partial function" $A \to B$ only fulfills well-defined property

D3.36 **Image of** $S \subseteq A$ $f(S) \stackrel{\text{def}}{=} \{f(a) \mid a \in S\}$

D3.37 **Image / Range of** f $\mathrm{Im}(f) = f(A) \subseteq B$

D3.38 **Preimage of** $T \subseteq B$ $f^{-1}(T) \stackrel{\text{def}}{=} \{a \in A \mid f(a) \in T\}$

D3.39 **Function Properties**: A function $f: A \to B$ is called
- **Injective** if for $a \neq a'$ we have $f(a) \neq f(a')$
- **Surjective** if $f(A) = B$ so if for all $b \in B$, $b = f(a)$ for some $a \in A$
- **bijective** if it is both of them

D3.40 For a bijective function the **Inverse** f^{-1} is the relation inverse **Inverse Function**

D3.41 **Composition** of $f: A \to B$ and $g: B \to C$ is $g \circ f$ or gf is $(g \circ f)(a) = g(f(a))$

! Composition of functions is different than for relations, for relations $p \circ q = \to p \to q \to$ but for functions $f \circ g = \to g \to f \to = f(g(a))$

L3.14 $h \circ (g \circ f) = (h \circ g) \circ f$ for functions

Countability

D3.42
a) A, B are ~~equi~~ **equinumerous**, $A \sim B$ if $\exists$ a bijection from $A \to B$
b) B **dominates** A, $A \preceq B$ if $A \sim C$ for some subset $C \subseteq B$ or there exists an injection from A into B
c) A is **countable** if $A \preceq \mathbb{N}$ and otherwise **uncountable**

L3.15
i) $\sim$ is equivalence relation
ii) $\preceq$ is transitive, so $A \preceq B \wedge B \preceq C \Rightarrow A \preceq C$
iii) $A \subseteq B \Rightarrow A \preceq B$

T3.16 $A \preceq B \wedge B \preceq A \Rightarrow A \sim B$

T3.17 A is countable $\iff$ A finite or $A \sim \mathbb{N}$

T3.18 $\{0,1\}^* \stackrel{\text{def}}{=} \{0, 1, e, 00, 01, \ldots\}$ of finite binary sequences is countable

o e = the empty sequence

T3.19 $\mathbb{N}^2$ is countable

C 3.20 If A, B countable then $A \times B$ countable

C 3.21 $\mathbb{Q}$ is countable

T3.22 Let A and A_i for $i \in \mathbb{N}$ be countable:

i) A^n is countable for any $n \in \mathbb{N}$

ii) $\bigcup_{i \in \mathbb{N}} A_i$, the union of $A_1, \ldots, A_2, \ldots$ of a countable list of countable sets is countable

iii) A^*, the set of finite sequences of elements of A is countable

D3.43 +T3.25 $\{0,1\}^\infty$ the set of infinite binary sequences, or the set of functions $f: \mathbb{N} \to \{0,1\}$ is uncountable. Per Cantors Diagonalisation Argument

+ $\mathbb{R}$ is uncountable

D 3.44 +C3.24 A function $\mathbb{N} \to \{0,1\}$ is computable if there is a program that returns for any input n $f(n)$. There are uncomputable functions.

4 - Number Theory

Division

D4.1 For integers a, b a **divides** b, or $a|b$, if $\exists c$ s.t. $ac = b$.
Then a is a **divisor** of b and b a **multiple** of a.
If $a \neq 0$ and c exists it is called **quotient** and $c = \frac{b}{a}$.
$a \nmid b$ = "a does not divide b".

T4.1 $\forall a, d \neq 0$ there exist unique q and r s.t. ← Euclids Theorem
$a = dq + r$ and $0 \leq r < |d|$

D4.2 For a, b not both 0, d is **a greatest common divisor** of a, b if it divides both and all other common divisors divide it. So if
$d|a \wedge d|b \wedge \forall c\,((c|a \wedge c|b) \rightarrow c|d)$

D4.3 $\gcd(a,b)$ is the unique positive greatest common divisor of a, b.
If $\gcd(a,b) = 1$ then a, b are **relatively prime**.

L4.2 $\gcd(m, n - qm) = \gcd(m, n)$
$\gcd(m, R_m(n)) = \gcd(m, n)$

○ The r from T4.1 is also called $R_d(a)$ or a mod d or the "rest" of a to d.

D4.4 The ideal (a,b) generated by a, b is $(a,b) \overset{\text{def}}{=} \{ua + vb \mid u, v \in \mathbb{Z}\}$
$(a) \overset{\text{def}}{=} \{ua \mid u \in \mathbb{Z}\}$

L4.3 For a, b $\exists d$ s.t. $(a,b) = (d)$

L4.4 If $(a,b) = (d)$ then d is a g.c.d. of a, b

C4.5 For $a, b \in \mathbb{Z}$ (not both 0) there exist $u, v \in \mathbb{Z}$ s.t. $\gcd(a,b) = ua + vb$

D4.5 Least common multiple $\operatorname{lcm}(a,b)$ is a common multiple that divides all other common multiples of a and b: $L = \operatorname{lcm}(a,b) \Leftrightarrow a|L \wedge b|L \wedge \forall m\,((a|m \wedge b|m) \rightarrow L|m)$

(Extended) Euclid Algorithm

Finding $\gcd(32, 88)$:

$\gcd(32, 88) = \gcd(32, 88 - 2 \cdot 32)$
$= \gcd(32, 24)$
$= \gcd(32 - 24, 24)$
$= \gcd(8, 24)$
$= \gcd(8, 24 - 3 \cdot 8)$
$= \gcd(8, 0)$
$= 8$

Finding $p \cdot 32 + q \cdot 88 = 8$:

	32	88	
32	1	0	
88	0	1	Since $24 = 88 - 2 \cdot 32$
24	-2	1	
8	3	-1	Since $8 = 32 - 1 \cdot 24$
0	-11	4	Since $0 = 24 - 3 \cdot 8$

So we always look at the decomposition into a, b of the numbers we are subtracting and calculate the new decomposition from that.

Primes

D4.6 $p>1 \in \mathbb{N}$ is called **prime** if the only positive divisors of p are p and 1.
$q>1$ not prime is called **composite**.

T4.6 Every positive integer has a unique **Prime Factorization**

L4.7 If p prime divides $x_1 \cdot x_2 \cdot \dots \cdot x_n$ then p divides at least one x_i for some i

⊕ If $a = \prod_i p_i^{e_i}$ and $b = \prod_i p_i^{f_i}$ then

+ $\gcd(a,b) = \prod_i p_i^{\min(e_i,f_i)}$ and + $\operatorname{lcm}(a,b) = \prod_i p_i^{\max(e_i,f_i)}$

+ $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab$

4.12 every composite integer n has a prime factor $\leq \sqrt{n}$

Modular Arithmetic

D4.8 for $a,b \in \mathbb{Z}$ and $m \geq 1 \in \mathbb{Z}$, a is **congruent to b modulo m** if m divides $a-b$.

$$a \equiv_m b \overset{\text{def}}{\iff} m \mid (a-b)$$

L4.13 for $m \geq 1$, $\equiv_m$ is equivalence relation

○ $a \not\equiv_m b \Rightarrow a \neq b$ and $a = b \Rightarrow a \equiv_m b$

L4.14 If $a \equiv_m b$ and $c \equiv_m d$, then $a+c \equiv_m b+d$ and $ac \equiv_m bd$

C4.15 For a polynomial $f(x_1, x_2, \dots x_n)$ if $a_i \equiv_m b_i$ for all $i \leq n$ then
$f(a_1, \dots, a_n) \equiv_m f(b_1, \dots, b_n)$

L4.16 for any $a,b,m \in \mathbb{Z}$ with $m \geq 1$: (i) $a \equiv_m R_m(a)$ (ii) $a \equiv_m b \iff R_m(a) = R_m(b)$

C4.17 $R_m(f(a_1, \dots, a_k)) = R_m(f(R_m(a_1), \dots, R_m(a_k)))$

L4.18 $ax \equiv_m 1$ has a (unique) solution if and only if $\gcd(a,m) = 1$ (in $x \in \mathbb{Z}_m$)

D4.19 The **multiplicative inverse of a mod m** is the unique solution to $ax \equiv_m 1$ if $\gcd(a,m) = 1$. It is also written $x \equiv_m a^{-1}$

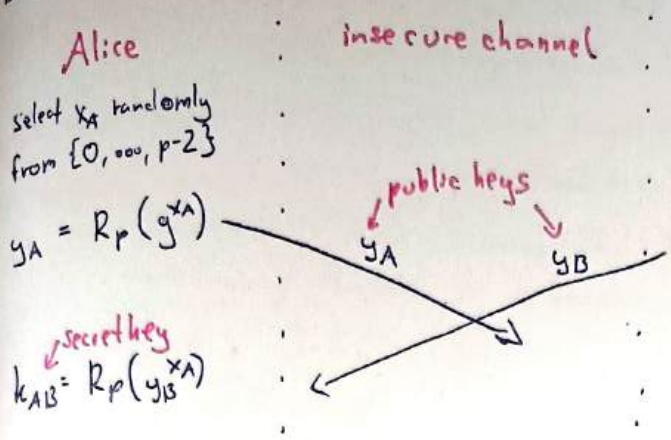
○ $\mathbb{Z}_m = \{0, \dots, m-1\}$ is the set of remainders mod m. $\equiv_m$ has the equivalence classes $[0], \dots, [m-1]$

T4.19 **Chinese Remainder Theorem**: Let $m_1, m_2, \dots, m_r$ be pairwise relatively prime. And $M = \prod_{i=1}^{r} m_i$. For every list $a_1, \dots, a_r$ with $0 \leq a_i < m_i$ for $1 \leq i \leq r$, the system

$$\begin{aligned} x &\equiv_m a_1 \\ x &\equiv_m a_2 \\ &\vdots \\ x &\equiv_m a_r \end{aligned}$$

has a unique solution x with $0 \leq x < M$

Diffie Hellman Key Agreement



$k_{AB} \equiv_p y_B^{x_A} \equiv_p (g^{x_B})^{x_A} \equiv_p g^{x_A x_B} \equiv_p k_{BA}$

g and a large prime p are publicly agreed upon before the process.

The security is based on the "discrete logarithm problem", the fact that $x \to R_p(g^x)$ is a one-way-function, from an x the output is easily computable, but not the other way around.

Algebra

Intro

D5.1 **Operation** on a set S is a (partial) function $S^n \to S$, with n being the "arity" of the operation.

D5.2 **Algebra** is a pair $\langle S; \Omega \rangle$ where S is a set ("carrier" of the algebra) and $\Omega = (\omega_1, \dots, \omega_n)$ is a list of operations on S.

Monoids and Groups

D5.3. **left/right neutral element** (or "identity element") of an algebra $\langle S; * \rangle$ is $e \in S$ s.t. $e*a = a$ / $a*e = a$ $\forall a \in S$. If $e*a = a*e = a$ $\forall a \in S$ then S is **neutral element**.

L5.1 $\langle S; * \rangle$ has at most one neutral element; If it has right and left neutral element, they are equal

D5.4 A binary operation $*: S^2 \to S$ is ~~associative~~ **associative** if $a*(b*c) = (a*b)*c$ $\forall a,b,c \in S$

D5.5 **Monoid** is an algebra $\langle M; *, e \rangle$ with * associative and e neutral element

D5.6 **left/right inverse element** of a in $\langle S; *, e \rangle$ is $b \in S$ s.t. $b*a = e$ / $a*b = e$.
If $b*a = a*b = e$ then b is **inverse** of a.

L5.2 In a monoid $\langle M; *, e \rangle$, if a has left and right inverses, they are equal. So a has at most one inverse.

D5.7 **Group** is an algebra that satisfies the group axioms for $\langle G; *, \hat{}, e \rangle$:

- G1 * is associative
- G2 e is a neutral element, so $a*e = e*a = a$ $\forall a \in G$
- G3 every $a \in G$ has an inverse $\hat{a}$ s.t. $a*\hat{a} = \hat{a}*a = e$

D5.8 **commutative/abelian Group** is a group if $\forall a,b \in G$ $a*b = b*a$

L5.3

a) $\widehat{(\hat{a})} = a$

b) $\widehat{a*b} = \hat{b}*\hat{a}$

c) left cancellation law $a*b = a*c \Rightarrow b = c$

d) right cancellation law. $b*a = c*a \Rightarrow b = c$

e) The equations $a*x = b$ and $x*a = b$ have unique solutions for all a, b.

Group Structure

D5.9 direct product of n groups $\langle G_1;*_1\rangle \dots \langle G_n;*_n\rangle$ is the algebra $\langle G_1\times\dots\times G_n;*\rangle$ where $*$ is defined component-wise: $(a_1,\dots,a_n)*(b_1,\dots,b_n)=(a_1*b_1,\dots,a_n*b_n)$

L5.4. $\langle G_1\times\dots\times G_n;*\rangle$ is a group where neutral element/inverse are component-wise in the groups

D5.10 group homomorphism for $\langle G;*,\hat{},e\rangle$ and $\langle H;\circ,\sim,e'\rangle$ a function $\Psi: G\to H$ is a group homomorphism if $\forall a,b:\ \Psi(a*b)=\Psi(a)\circ\Psi(b)$. If Ψ is bijective it is an **isomorphism**, G and H are **isomorphic** and we write $G\cong H$.

L5.5 a) $\Psi(e)=e'$ b) $\Psi(\hat{a})=\widetilde{\Psi(a)}$

D5.11 subgroup is a subset $H\subseteq G$ of a group $\langle G;*,\hat{},e\rangle$ if $\langle H;*,\hat{},e\rangle$ is a group, if it is closed under all operations: ① $a*b\in H\ \forall a,b\in H$ ② $e\in H$ ③ $\hat{a}\in H\ \forall a\in H$

power notation $a^0=e$, $a^n=a\cdot a^{n-1}$, $a^n=(a^{-1})^{|n|}$ if $n<0$

D5.12 order $\mathrm{ord}(a)$ of $a\in G$ is the least $m\geq 1$ such that $a^m=e$. (If no such m exists we say $\mathrm{ord}(a)=\infty$.)

L5.6 In finite group G every element has a finite order

D5.13 for finite group G, $|G|$ is called **order** of G

D5.14 for group G and $a\in G$ the group **generated by** a, $\langle a\rangle \overset{\text{def}}{=} \{a^n \mid n\in\mathbb{Z}\}$
→ for finite groups $\langle a\rangle \overset{\text{def}}{=} \{e,a,a^2,\dots,a^{\mathrm{ord}(a)-1}\}$

D5.15 $G=\langle g\rangle$ is called **cyclic** and g a **generator** of G

T5.7 A cyclic group of order n is isomorphic to $\langle\mathbb{Z}_n;\oplus\rangle$ (and hence abelian)

T5.9 Lagrange Theorem for G finite group and H subgroup of G, $|H|$ divides $|G|$

↳ **C5.9** for finite group G, $\mathrm{ord}(a)$ divides $|G|$ $\forall a\in G$

↳ **C5.10** for finite group G: $a^{|G|}=e$ for all $a\in G$

↳ **C5.11** Every group of **prime order** ($|G|=p$ for p prime) is cyclic, and there every element except e (neutral element) is a generator.

$\mathbb{Z}_n^*$ and Eulers Function

D5.16 $\mathbb{Z}_m^* \overset{\text{def}}{=} \{a\in\mathbb{Z}_m \mid \gcd(a,m)=1\}$

D5.17 Euler function $\varphi:\mathbb{Z}^+\to\mathbb{Z}^+$ is the cardinality of $\mathbb{Z}_m^*$: $\varphi(m)=|\mathbb{Z}_m^*|$

L5.12 If the prime factorization of m is $m=\prod_{i=1}^{r} p_i^{e_i}$, then $\varphi(m)=\prod_{i=1}^{r}(p_i-1)\,p_i^{e_i-1}$

T5.13 $\langle\mathbb{Z}_n^*;\odot,^{-1},1\rangle$ is a group

C5.14 Fermats Little Theorem for all $m\geq 2$ and a with $\gcd(a,m)=1$:

$$a^{\varphi(m)}\equiv_m 1$$ and so for every prime p and $p\nmid a$: $a^{p-1}\equiv_p 1$

T5.15 $\mathbb{Z}_n^*$ is cyclic $\iff$ $n=2$, $n=4$, $n=p^e$ or $n=2p^e$ where p odd prime and $e\geq 1$

RSA

T5.16 for G finite group and $e\in\mathbb{Z}$ s.t. $\gcd(e,|G|)=1$ the function $x\mapsto x^e$ is a bijection and the unique eth root of y is x s.t. $x^e=y$ is $x=y^d$, where d is s.t. $ed\equiv_{|G|}1$.

RSA

Alice	insecure channel	Bob
① generate primes p and q, $n=p\cdot q$, $f=(p-1)(q-1)$		
② select e, $d\equiv_f e^{-1}$	n,e →	③ plaintext $m\in\{1,\dots,n-1\}$, ciphertext $c=R_n(m^e)$
④ $m=R_n(c^d)$	← c	

Security is based on the fact that the order of $\mathbb{Z}_n^*$ is only computable if p and q are known. (And with it the inverse to e: d.)

Rings and Fields

D5.18 Ring $\langle R;+,-,0,\cdot,1\rangle$ is an algebra for which:
1) $\langle R;+,-,0\rangle$ is commutative group 2) $\langle R;\cdot,1\rangle$ is monoid
3) left+right distr. law holds, so: $a(b+c)=ab+ac$ and $(b+c)a=ba+ca$ $\forall a,b,c\in R$

A ring is **commutative** if multiplication is also commutative ($ab=ba$)

L5.17 for any ring $\langle R;+,-,0,\cdot,1\rangle$ and $a,b\in R$:
a) $0a=a0=0$ b) $(-a)b=-(ab)$ c) $(-a)(-b)=ab$ d) If R is nontrivial (has more than one element) then $1\neq 0$.

D5.19 characteristic is the order of 1 in the additive group. (If finite, otherwise 0 (not ∞ !))

D5.20 unit is an element u in a ring R that is invertible, so $uv=vu=1$ for some v in R (we write $v=u^{-1}$). The set of units of R is R^*.

L5.18 for a ring R, R^* is a group (multiplicative group of units of R)

D5.21 for $a,b\in R$ with R a commutative ring, a **divides** b if $\exists c\in R$ s.t. $ac=b$ (then $a|b$)
b "multiple of a", a "divisor of b"

L5.19 In a commutative ring:
1) "|" is transitive, so $a|b$ and $b|c \Rightarrow a|c$ 2) $a|b \Rightarrow a|bc$ $\forall c$ 3) $a|b$ and $a|c \Rightarrow a|(b+c)$

D5.22 greatest common divisor (in a ring) of a,b (not both 0) is d such that:
$d|a \wedge d|b \wedge \forall c((c|a \wedge c|b) \rightarrow c|d)$

D5.23 zerodivisor is an element $a\neq 0$ in a commutative ring if $ab=0$ for some $b\neq 0$.

D5.24 integral domain is a (nontrivial) commutative ring without zero divisors, so
$\forall a,b\,(ab=0 \rightarrow (a=0 \vee b=0))$

L5.20 in an integral domain, if $a|b$ then c with $ac=b$ is unique (and called quotient, $c=\frac{b}{a}$)

Polynomial Rings

D5.25 polynomial $a(x)$ over a commutative ring R in the indeterminate x is a formal expression:
$a(x)=\sum_{i=0}^{d} a_i x^i$ for $d\geq 0$ and $a_i\in R$. The **degree** $\deg(a)$ of a is the greatest i s.t. $a_i\neq 0$. The zero polynomial 0 has degree $-\infty$. $R[x]$ = "set of polynomials in x over R"
! $a(x)+b(x)$ and $a(x)\cdot b(x)$ are defined as usual

T5.21 For any commutative ring R, $R[x]$ is also a commutative ring

L5.22 For D integral domain:
1) $D[x]$ is integral domain 2) $\deg(a(x)\cdot b(x)) = \deg(a(x))+\deg(b(x))$
3) The units of $D[x]$ are the constant polynomials that are units of D: $D[x]^* = D^*$

Fields

D5.26 Field is a nontrivial commutative ring in which every (nonzero) element is a unit, so $F^* = F\setminus\{0\}$
o ring F field $\Leftrightarrow \langle F\setminus\{0\};\cdot,^{-1},1\rangle$ abelian group o $GF(m)$ = "field with m elements" ($=\approx \mathbb{Z}_m^*$)

T5.23 $\mathbb{Z}_p$ is a field $\Leftrightarrow p$ is prime

T5.24 A field is an integral domain

Polynomials over Fields

D5.27 a polynomial is called **monic** if the leading coefficient is 1

D5.28 **irreducible polynomial** $a(x) \in F[x]$ if it has degree 1 and is only divisible by constant polynomials and constant multiples of $a(x)$.

D5.29 the monic polynomial $g(x)$ of largest degree s.t. $g(x) | a(x)$ and $g(x) | b(x)$ is called the greatest common divisor of $a(x)$ and $b(x)$, $\gcd(a(x), b(x))$

T5.25 for F a field: For any $a(x)$ and $b(x) \neq 0$ in $F[x]$ there exists a unique $g(x)$ ("quotient") and $r(x)$ ("remainder") s.t.: $a(x) = b(x) \cdot g(x) + r(x)$ and $\deg(r(x)) < \deg(b(x))$

Polynomial Evaluation for a ring R and $a(x) \in R[x]$, $a(x)$ can be interpreted as a function $R \to R$ by defining the evaluation of $a(x)$ at $\alpha \in R$ in the usual way. then $a(x): R \to R$, $\alpha \mapsto a(\alpha)$

L5.28 Polynomial evaluation is compatible with the ring operations:
$\cdot c(x) = a(x) + b(x) \Rightarrow c(\alpha) = a(\alpha) + b(\alpha)\ \forall \alpha$; $\cdot c(x) = a(x) \cdot b(x) \Rightarrow c(\alpha) = a(\alpha) \cdot b(\alpha)\ \forall \alpha$

D5.33 **Root** of a polynomial $a(x) \in R[x]$ is an element $\alpha \in R$ s.t. $a(\alpha) = 0$

L5.29 For a field F: $\alpha \in F$ is a root of $a(x) \iff (x - \alpha)$ divides $a(x)$

C5.30 $a(x)$ over F of degree 2 or 3 is irreducible $\iff$ $a(x)$ has no roots

T5.31 a nonzero polynomial of over a field F of degree d has at most d roots

L5.32 A polynomial $a(x) \in F[x]$ of degree d is uniquely determined by ~~and~~ any $d+1$ values of $a(x)$, so by $a(\alpha_1) \dots a(\alpha_{d+2})$ for distinct $\alpha_1 \dots \alpha_{d+1}$. For $\beta_i = a(\alpha_i)$, $a(x)$ is given by Lagranges interpolation formula: $a(x) = \sum_{i=1}^{d+1} \beta_i v_i(x)$ with $v_i(x) = \frac{(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_{i-1})(x-\alpha_{i+1})\cdot\ldots\cdot(x-\alpha_{d+1})}{(\alpha_i-\alpha_1)\cdot\ldots\cdot(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdot\ldots\cdot(\alpha_i-\alpha_{d+1})}$

Finite Fields

Remainder + mod $R_{m(x)}(a(x)) =$ unique remainder when dividing $a(x)$ by $m(x)$, $a(x) \equiv_{m(x)} b(x) \overset{\text{def}}{\iff} m(x) | (a(x) - b(x))$

L5.33 congruence modulo $m(x)$ is an equivalence relation, each equivalence class has a unique representative with degree $< \deg(m(x))$

D5.34 $F[x]_{m(x)} \overset{\text{def}}{=} \{a(x) \in F[x] \mid \deg(a(x)) < d\}$ for $m(x)$ a polynomial of degree d over F

L5.34 If F has q elements then $|F[x]_{m(x)}| = q^d$

L5.35 $F[x]_{m(x)}$ is a ring with addition and multiplication modulo $m(x)$

L5.36 $a(x)b(x) \equiv_{m(x)} 1$ has a solution $b(x) \in F[x]_{m(x)} \iff \gcd(a(x), m(x)) = 1$, the solution is unique

T5.37 The ring $F[x]_{m(x)}$ is a field $\iff$ $m(x)$ is irreducible ($F[x]_{m(x)}$ would be called an "extension field" of F)

Error-Correcting Codes

D5.35 (n,k) **encoding function** E for an Alphabet $\mathcal{A}$ is injective function that maps a list $(a_0, \dots, a_{k-1}) \in \mathcal{A}^k$ of k symbols to a list $(c_0, \dots, c_{n-1}) \in \mathcal{A}^n$ of $n > k$ (encoded) symbols in $\mathcal{A}$, called **codeword**: $E: \mathcal{A}^k \to \mathcal{A}^n : (a_0, \dots, a_{k-1}) \mapsto E((a_0, \dots, a_{k-1})) = (c_0, \dots, c_{n-1})$

D5.36 (n,k) **error correcting code** over the alphabet $\mathcal{A}$ with $|\mathcal{A}| = q$ is a subset of $\mathcal{A}^n$ of cardinality q^k.

D5.37 Hamming Distance between two of equal length over a finite alphabet is the number of positions where the strings differ

D5.38 minimum distance of an error correcting code C, $d_{min}(C)$, is the minimum Hamming Distance between any two codewords

D5.39 decoding function D for an (n,k)-encoding function is a function $D: \mathcal{A}^n \to \mathcal{A}^k$

D5.40 A decoding function D is t-error correcting for encoding function E if for any $(a_0,\dots,a_{k-1})$ $D((r_0,\dots,r_{n-1})) = (a_0,\dots,a_{k-1})$ for any $(r_0,\dots,r_{n-1})$ with Hamming distance at most t from $E((a_0,\dots,a_{k-1}))$. A code C is t-error correcting if $\exists$ E and D with $C = Im(E)$ where D is t-error correcting.

T5.41 Code C with min. distance d is t-error correcting $\Leftrightarrow$ $d \geq 2t+1$

T5.42 for $A = GF(q)$ and $\alpha_0,\dots,\alpha_{n-1}$ arbitrary distinct elements of A. The encoding function $E((a_0,\dots,a_{k-1})) = ((a(\alpha_0)),\dots,a(\alpha_{n-1}))$, where $a(x)$ is the polynomial $a(x) = a_{k-1}x^{k-1} + \dots + a_1x + a_0$,

This code has minimum distance $n-k+1$.

Logic

Σ^* = set of finite bitstrings

Proof Systems

S set of syntactic representations of statements ($\subseteq \Sigma^*$)

P set of —"— of proof strings ($\subseteq \Sigma^*$)

$T(s)$ "truth function", assigns each $s \in S$ its truth value; defines "semantics" of objects in S

$\phi: S \times P \to \{0,1\}$ "verification function" that decides if a proof p is valid for a statement s, then $\phi(s,p) = 1$, otherwise $\phi(s,p) = 0$

D6.1 Proof System is a quadruple $\Pi = (S, P, \tau, \phi)$

D6.2 A proof system $\Pi = (S, P, \tau, \phi)$ is sound if no false statement has a proof, so if for all s for which p with $\phi(s,p) = 1$ exists it holds that $\tau(s) = 1$

D6.3 A proof system $\Pi = (S, P, \tau, \phi)$ is complete if every true statement has a proof, so if for all $s \in S$ with $\tau(s) = 1$, there exists $p \in P$ with $\phi(s,p) = 1$

→ We also require ϕ to be efficiently computable (so we cannot just say $\phi(s,p) = 1 \Leftrightarrow \tau(s) = 1$ since τ does not have to be efficiently computable)

General Elementary Logic Concepts

D6.4 The Syntax of a defines alphabet Λ of allowed symbols and specifies which strings in Λ^* are formulas (so syntactically correct)

→ some symbols are understood as variables

D6.5 The semantics of a logic defines a function free: assigns to each formula $F = (f_1,\dots,f_k) \in \Lambda^*$ a subset free$(F) \subseteq \{1,\dots,k\}$ of indices. If $i \in$ free(F) then f_i "occurs free" in F

D6.6 Interpretation consists of a set $\mathcal{Z} \subseteq \Lambda$ of symbols of Λ, a domain (set of possible values) for each symbol in $\mathcal{Z}$, and a function that assigns each symbol in $\mathcal{Z}$ a value in its domain.

D6.7 An interpretation is **suitable** for a formula F if it assigns a value to all symbols occuring free in F.

D6.8 Semantics also defines a function σ, which assigns to each formula F and each Interpretation $\mathcal{A}$ suitable for F a truth value $\sigma(F,\mathcal{A})$ in $\{0,1\}$. We also write $\mathcal{A}(F)$ and say "the truth value of F under interpretation $\mathcal{A}$"

D6.9 Model is a suitable interpretation for F, $\mathcal{A}$, for which $\mathcal{A}(F)=1$. ("model for F") We write $\mathcal{A} \models F$ or $\mathcal{A} \not\models F$ if its not a model.

For a set of formulas M for which all formulas in M are true under $\mathcal{A}$ we write $\mathcal{A} \models M$.

D6.10 A formula (or set of formulas) is **satisfiable** if $\exists$ a model for F. Otherwise "unsatisfiable" and we write $\bot$.

D6.11 A formula is **tautology** or **valid** if it is true for every suitable interpretation. We write "$\top$" for tautology.

D6.12 formula G is a **logical consequence** of a Formula F (or set M of formulas): $F \models G$, $M \models G$ if every interpretation suitable for both F and G, that is a model for F is also a model for G.

D6.13 formulas F and G are **equivalent**, $F \equiv G$ if every interpretation suitable for both yields the same truth value for F and G. $F \equiv G \overset{\text{def}}{\Leftrightarrow} F \models G$ and $G \models F$

- A set of formulas is like an AND-conjunction of the formulas; an interpretation is a model for a set if it is one for every formula in it

D6.14 If F is tautology, we also write $\models F$

D6.15 If F and G formulas then also $\neg F$, $(F \wedge G)$, $(F \vee G)$, $(F \to G) = (\neg F \vee G)$, $(F \leftrightarrow G) = (F \wedge G) \vee (\neg F \wedge \neg G)$

(conjunction, disjunction)

D6.16 Rules for $\vee, \wedge, \neg$

1) $\mathcal{A}((F \wedge G)) = 1 \Leftrightarrow \mathcal{A}(F)=1$ and $\mathcal{A}(G)=1$
2) $\mathcal{A}((F \vee G)) = 1 \Leftrightarrow \mathcal{A}(F)=1$ or $\mathcal{A}(G)=1$
3) $\mathcal{A}(\neg F) = 1 \Leftrightarrow \mathcal{A}(F)=0$

LG.1 • $F \wedge F \equiv F$, $F \vee F \equiv F$ idempotence • commutativity • associativity • $F \wedge (F \vee G) \equiv F$, $F \vee (F \wedge G) \equiv F$ absorption distr. law • double negation • $\neg(F \wedge G) \equiv \neg F \vee \neg G$, $\neg(F \vee G) = \neg F \wedge \neg G$ de morgan • tautology / unsatisfiability rule

LG.2 F tautology $\Leftrightarrow \neg F$ unsatisfiable

LG.3 These three statements are equivalent:

1) $\{F_1, F_2, \ldots, F_k\} \models G$ 2) $(F_1 \wedge F_2 \wedge \ldots \wedge F_k) \to G$ is tautology 3) $\{F_1, F_2, \ldots, F_k, \neg G\}$ unsatisfiable

Logical Calculi:

D6.17 derivation / inference rule is rule for deriving from a set of formulas (premises). We write $\{F_1, \ldots F_k\} \vdash_R G$ if G can be derived from the set by rule R. (Formally $\vdash_R$ is a relation.)

D6.18 Application of derivation rule R: for a set of formulas M: ① select subset N of M such that $N \vdash_R G$ for some G ② add G to the set M

D6.19 (logical) calculus K is a finite set of derivation rules; $K = \{R_1, \ldots, R_n\}$

D6.20 **derivation** of a formula G from a set M of formulas in a calculus K is a finite sequence of applications of rules in K leading to G.

- $M_0 = M$
- $M_i = M_{i-1} \cup \{G_i\}$ for $i \leq n$ where $N \vdash_{R_j} G_i$ for some $N \subseteq M_{i-1}$ and $R_j \in K$
- $G_n = G$

We write $M \vdash_K G$ if there is a derivation ~~from~~ of G from M in K.

D6.21 A derivation rule is **correct** if $M \vdash_R F$ implies $M \models F$ for any set of formulas F and formula F: $M \vdash_R F \Rightarrow M \models F$ if R correct

D6.22 A calculus K is **sound or correct** if for every set of formulas M and formula F, if F can be derived from M, then it is also a logical consequence of M: $M \vdash_K F \Rightarrow M \models F$.

K is **complete** if for all M, F, if F is logical consequence of M, then F can also be derived from M: $M \models F \Rightarrow M \vdash_K F$

Propositional Logic

D6.23 (Syntax) **atomic formula** is a symbol of the form A_i with $i \in \mathbb{N}$.

A **formula** is: 1) an atomic formula is a formula
2) If F, G formulas then also $\neg F, (F \wedge G), (F \vee G)$ are formulas

- In prop. logic the free symbols are the atomic formulas

D6.24 For a set of atomic formulas an interpretation $\mathcal{A}$, **truth assignment**, is a function $\mathcal{A}: \Sigma \to \{0,1\}$. It is suitable for a formula F if Σ contains all atomic formulas in F. **Semantics** (truth value) for atomic formulas are $\mathcal{A}(F) = \mathcal{A}(A_i)$ for $F = A_i$ and by def. 6.16: $\mathcal{A}((F \wedge G)) = 1 \Leftrightarrow \mathcal{A}(F) = 1$ and $\mathcal{A}(G) = 1$, $\mathcal{A}((F \vee G)) = 1 \Leftrightarrow$ -"- or -"-, $\mathcal{A}(\neg F) = 1 \Leftrightarrow \mathcal{A}(F) = 0$

D6.25 **literal** is an atomic formula or the negation of an atomic formula

D6.26 **Conjunctive Normal Form (CNF)** is a formula if it is the conjunction of disjunctions of literals: $F = (L_{11} \vee \dots \vee L_{1j}) \wedge (L_{21} \vee \dots \vee L_{2k}) \wedge \dots \wedge (L_{x1} \vee \dots \vee L_{xm})$

D6.27 **Disjunctive Normal Form (DNF)** is a formula if it is the disjunction of conjunctions of literals: $F = (L_{11} \wedge \dots \wedge L_{1j}) \vee \dots \vee (L_{x1} \wedge \dots \wedge L_{xm})$

T6.4 Every formula is equivalent to a formula in CNF and DNF

↳ Constructing DNF/CNF from truth table:

~~formula~~	A	B	C	formula
	0	0	0	0
	0	0	1	0
	0	1	0	1
	0	1	1	0
	1	0	0	1
	1	0	1	1
	1	1	0	1
	1	1	1	0

→ DNF = $(\neg A \wedge B \wedge \neg C) \vee (A \wedge \neg B \wedge \neg C) \vee (A \wedge B \wedge \neg C)$
= taking all rows for which formula is true and disjuncting them

→ CNF = $(A \vee B \vee C) \wedge (A \vee B \vee \neg C) \wedge (A \vee \neg B \vee \neg C) \wedge (\neg A \vee \neg B \vee \neg C)$
= taking all rows for which formula is false and negating them and then conjuncting them

Resolution Calculus

D6.28 A **clause** is a set of literals

D6.29 for a formula in CNF $F = (L_{11} \vee \dots \vee L_{1x}) \wedge \dots \wedge (L_{y1} \vee \dots \vee L_{yx})$ the set of clauses associated with it is $K(F) \stackrel{\text{def}}{=} \{\{L_{11}, \dots, L_{1x}\}, \dots, \{L_{y1}, \dots, L_{yx}\}\}$.

The set of clauses associated with ~~the~~ a set of formulas is the union of their clause sets: $K(M) \stackrel{\text{def}}{=} \bigcup_{i=1}^{k} K(F_i)$

→ The formula associated with a clause is true if some literal in the clause is true and a set of ~~formulas~~ clause is true if ~~the associated set~~ every clause in it is true. So a clause represents OR and a set represents AND between the clauses.

D6.30 A clause k is a **resolvent** of clauses k_1 and k_2 if there is a literal L such that $L \in k_1$, $\neg L \in k_2$ and $k = (k_1 \setminus \{L\}) \cup (k_2 \setminus \{\neg L\})$.

- Resolving k from k_1 and k_2 is a rule (the only one in the resolution calculus) and denoted by: $\{k_1, k_2\} \vdash_{res} k$

L6.5 The resolution calculus is sound, so $K \vdash_{res} k \implies K \models k$

T6.6 A set of formulas is unsatisfiable $\iff K(M) \vdash_{res} \emptyset$

Predicate (first order) Logic

D6.31 Syntax

- **variable symbol** is of the form x_i with $i \in \mathbb{N}$
- **function symbol** is of the form $f_i^{(k)}$ with $i, k \in \mathbb{N}$, k denotes number of arguments, if $k=0$ they are called constants
- **predicate symbol** is of the form $P_i^{(k)}$ with $i, k \in \mathbb{N}$, k again number of args.
- **term** is defined inductively: A variable is a term and if $t_1, \dots, t_k$ terms then $f_i^k(t_1, \dots, t_k)$ is a term
- **formula** is defined inductively: 1) for arg i,k if $t_1, \dots, t_k$ terms then $P_i^k(t_1, \dots, t_k)$ is an atomic formula
  2) If F, G formulas then $\neg F, (F \wedge G), (F \vee G)$ formulas
  3) If F formula then, for any i, $\forall x_i$ and $\exists x_i$ are formulas

We use f, g, h for functions; x, y, z for variables; a, b, c for constants

D6.32 Every occurence of a variable in a formula is either ~~bou~~ **bound** or **free**. If a variable x occurs in a subformula of $\forall x$ or $\exists x$ then it is bound, otherwise free. A formula is **closed** if it contains no free variables

D6.33 For formula F, variable x and term t $F[x/t]$ denotes the formula obtained from F by substituting every free ~~occurce~~ occurence of x by t.

D6.34 **interpretation structure** is a tuple $\mathcal{A} = (U, \phi, \psi, \xi)$ where

- U is non-empty universe
- ϕ is function assigning to each function symbol a function, where for f^k, $\phi(f)$ is a function $U^k \to U$
- ψ is function assigning to each predicate symbol a function, where for P^k, $\psi(P)$ is function $U^k \to \{0,1\}$
- ξ is function assigning to each variable symbol a value in U

→ we write $U^{\mathcal{A}}$, $f^{\mathcal{A}}$, $P^{\mathcal{A}}$ instead of $\phi(P)$, ...

D6.35 An interpretation structure is **suitable** for a formula F if it defines all function symbols, predicate symbols, and free variables of F.

DC.36 Semantics For $\mathcal{A}=(U,\phi,\psi,\xi)$ we define:

- The value $\mathcal{A}(t)$ of a term t recursively:
  - If t is variable then $\mathcal{A}(t)=\xi(t)$ (for eg $t=x$; then $\mathcal{A}(t)=\xi(x)$)
  - If t is $f(t_1,\dots,t_k)$ then $\mathcal{A}(t)=\phi(f)(\mathcal{A}(t_1),\dots,\mathcal{A}(t_k))$
  - We also allow a term to be a (fixed) element of U
- The truth value of a formula by def. 6.16 (for $\vee,\wedge,\neg$) and recursively:
  - If F is $F=P(t_1,\dots,t_k)$ then $\mathcal{A}(F)=\psi(P)(\mathcal{A}(t_1),\dots,\mathcal{A}(t_k))$
  - If F is $\forall x G$ or $\exists x G$ then let $\mathcal{A}_{[x\to u]}$ for u in U be the same structure as $\mathcal{A}$ except that $\xi(x)$ is overwritten by u: $(\xi(x)=u)$

$$\mathcal{A}(\forall x G)=\begin{cases}1 \text{ if } \mathcal{A}_{[x\to u]}(G)=1 \text{ for all } u \text{ in } U\\ 0 \text{ else}\end{cases}$$

$$\mathcal{A}(\exists x G)=\begin{cases}1 \text{ if } \mathcal{A}_{[x\to u]}(G)=1 \text{ for some } u \text{ in } U\\ 0 \text{ else}\end{cases}$$

↖ this defines the function σ btw.

! We can extend predicate logic to include "=", but "$\neq$" is never allowed! ! → write $\neg(a=b)$

LG.7 Some equivalence rules for formulas F,G,H in which x does not occur free in H

1) $\neg(\forall x F)\equiv\exists x\neg F$
2) $\neg(\exists x F)\equiv\forall x\neg F$
3) $(\forall x F)\wedge(\forall x G)\equiv\forall x(F\wedge G)$
4) $(\exists x F)\vee(\exists x G)\equiv\exists x(F\vee G)$
5) $\forall x\forall y F\equiv\forall y\forall x F$
6) $\exists x\exists y F\equiv\exists y\exists x F$
7) $(\forall x F)\wedge H\equiv\forall x(F\wedge H)$
8) $(\forall x F)\vee H\equiv\forall x(F\vee H)$
9) $(\exists x F)\wedge H\equiv\exists x(F\wedge H)$
10) $(\exists x F)\vee H\equiv\exists x(F\vee H)$

LG.8 If we replace a sub-formula G of a formula F by an equivalent (to G) formula H, then the resulting formula is equivalent to F.

LG.9 For a formula G in which y does not occur:

- $\forall x G\equiv\forall y G[x/y]$
- $\exists x G\equiv\exists y G[x/y]$

DC.37 rectified is a formula in which no variable occurs both as bound and free and in which all the variables appearing after a quantifier are distinct.

DC.38 prenex form is a formula of the form $Q_1x_1Q_2x_2\dots Q_nx_nG$ where Q_i is an arbitrary quantifier ($\exists$ or $\forall$) and G a formula free of quantifiers.

TG.10 Every formula has an equivalent one in prenex form. → We obtain it by first renaming the variables to avoid conflicts and then using the rules of LG.7 to put the quantifiers $\forall,\exists$ to the front

! $\neg\exists$ and $\neg\forall$ are not allowed in prenex form

LG.11 $\forall x F\models F[x/t]$ for any term t ! also for $t=f(t)$!

TG.12 $\neg\exists x\forall y(P(y,x)\leftrightarrow\neg P(y,y))$

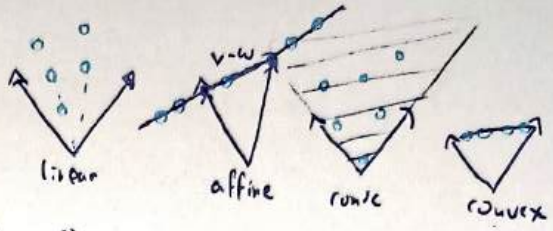
→ $\{S\mid S\notin S\}$ is not a set → $\{0,1\}^{\omega}$ uncountable → $\exists$ uncomputable functions $\mathbb{N}\to\{0,1\}$

Vectors

- $\begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} x+a \\ y+b \end{bmatrix}$, $\lambda \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \lambda x \\ \lambda y \end{bmatrix}$

D1.4 Linear combination of x, y is $\lambda x + \mu y$ with $\lambda, \mu \in \mathbb{R}$ (or $\lambda_1 x_1 + \lambda_2 x_2 + \dots + \lambda_n x_n$ for more vectors x_i)

D1.7 A linear combination is
a) affine if $\lambda_1 + \dots + \lambda_n = 1$
b) conic if $\lambda_j \geq 0$ for $j = 1, \dots, n$
c) convex if both affine and conic



Sequence $(v_j)_{j=1}^n \overset{\text{def}}{=} (v_1, v_2, \dots, v_n)$ $\quad (v_j)_{j=1}^0 = ()$

Sum $\sum_{i=1}^n v_i \overset{\text{def}}{=} v_1 + v_2 + \dots + v_n$ with $\sum_{i=1}^0 v_i = 0$

Vector $[i^2]_{i=1}^5 = \begin{bmatrix} 1 \\ 4 \\ 9 \\ 25 \\ 36 \end{bmatrix}$

D1.9 Scalar Product $v \cdot w = v_1 w_1 + v_2 w_2 + \dots + v_m w_m$ for $v, w \in \mathbb{R}^m$

D1.10 a) $v \cdot w = w \cdot v$ "symmetry"
b) $(\lambda v) \cdot w = \lambda (v \cdot w) = v \cdot \lambda \cdot w$ "taking out scalars"
c) distributivity holds
d) $v \cdot v \geq 0$ and $v \cdot v = 0 \Leftrightarrow v = 0$

D1.11 Euclidian norm $\|v\| \overset{\text{def}}{=} \sqrt{v \cdot v}$

- a unit vector is a vector with norm 1, so $\|v\| = 1$
- for $v \neq 0$ $\frac{v}{\|v\|}$ is a unit vector
- $\|v\|_1 \overset{\text{def}}{=} \sum_{i=1}^m |v_i|$ and $\|v\|_\infty \overset{\text{def}}{=} \max_{i=1}^m |v_i|$
- standard unit vectors in $\mathbb{R}^m$ are $e_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ $e_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ $\dots$ $e_m = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$

L1.12 Cauchy-Schwarz $|v \cdot w| \leq \|v\| \cdot \|w\|$

D1.14 Angles The angle between two vectors v, w is $\cos(\alpha) = \frac{v \cdot w}{\|v\| \cdot \|w\|} \in [-1; 1]$

D1.15 v, w are perpendicular/orthogonal if $v \cdot w = 0$ ($\cos(\alpha) = 0$ between v, w)

L1.16 Triangle Inequality $\|v + w\| \leq \|v\| + \|w\|$

D1.18 Vectors $v_1, \dots, v_n$ are linearly independent/dependent if none/at least one of them is a linear combination of the others. So if $\nexists k$ / $\exists k$ s.t.

$$v_k = \sum_{\substack{i=1 \\ i \neq k}}^n \lambda_i v_i \quad \text{for scalars } \lambda_i$$

- the zero-vector 0 is always linearly dependent (even if there are no other vectors) since the empty sum is 0 or all scalars can be 0.

- collinear = "vectors on same line"

D1.19 Alternative Definition for lin. dependence
a) at least one of the vectors is a lin. comb. of the other ones
b) There are scalars s.t. $\sum_{i=1}^n \lambda_i v_i = 0$ with at least one $\lambda_i \neq 0$
c) at least one of the vectors is a lin. comb of the previous ones

0_X is a nontrivial linear combination of $v_1 \dots v_n$ if $\exists \lambda_i$ $\sum_{i=1}^{n} \lambda_i v_n = 0_X$ with at least one $\lambda_i \neq 0$

L1.21 If $v_1 \dots v_n$ are linearly independent then the scalars λ_i s.t. $\sum_{i=1}^{n} \lambda_i v_i = x$ are unique for x.

D1.22 the Span of vectors $v_1 \dots v_n \in \mathbb{R}^m$ is the set of all their linear combinations:

$$\text{span}(v_1 \dots v_n) \stackrel{\text{def}}{=} \left\{ \sum_{j=1}^{n} \lambda_j v_j \;\middle|\; \lambda_j \in \mathbb{R} \text{ for } 1 \leq j \leq n \right\}$$

L1.23 If $v \in \mathbb{R}^m$ is a linear combination of $v_1, \dots, v_n$ then $\text{span}(v_1 \dots v_n) = \text{span}(v_1 \dots v_n, v)$

Matrices

Matrices

D2.1 Matrix: $m \times n$ matrix $= A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & & \\ \vdots & & \ddots & \\ a_{m1} & & & a_{mn} \end{bmatrix} = [a_{ij}]_{i=1}^{m}{}_{j=1}^{n} = \begin{bmatrix} - & v_1 & - \\ - & v_2 & - \\ & \vdots & \\ - & v_m & - \end{bmatrix} = \begin{bmatrix} | & | & & | \\ v_1 & v_2 & \cdots & v_n \\ | & | & & | \end{bmatrix}$

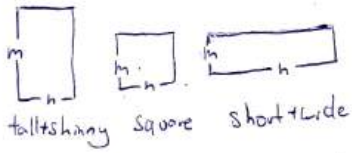
D2.2 for $A, B \in \mathbb{R}^{m \times n}$, $\lambda \in \mathbb{R}$

a) $A+B = [a_{ij}+b_{ij}]_{i=1}^{m}{}_{j=1}^{n}$

b) $\lambda A = [\lambda a_{ij}]_{i=1}^{m}{}_{j=1}^{n}$

c) $0 = [0]_{i=1}^{m}{}_{j=1}^{n}$ = "$m \times n$ zero matrix"

d) "A is square matrix" if $m = n$



D2.3 for a $m \times m$ square matrix A

i) $j < i$, $j = i$, $j > i$ then a_{ij} is below, on, above the diagonal

a) If $a_{ii} = 1$ for all i and $a_{ij} = 0$ for all $i \neq j$ then $A = I$ the identity matrix

$I = [\delta]_{i=1}^{n}{}_{j=1}^{n}$ with δ the Kronecher Delta $\stackrel{\text{def}}{=} \delta_{ij} = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$

b) If $a_{ij} = 0$ for all $i \neq j$ then A is diagonal matrix

c) If $a_{ij} = 0$ for all $j < i$ / $j > i$ then A is upper triangular / lower triangular

d) $a_{ij} = a_{ji}$ for all i, j then A is symmetric

- $I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \end{bmatrix}$ $\begin{bmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & d \end{bmatrix}$ diagonal $\begin{bmatrix} a & e & f & h \\ 0 & b & c & g \\ 0 & 0 & c & y \\ 0 & 0 & 0 & d \end{bmatrix}$ $\begin{bmatrix} a & 0 & 0 & 0 \\ e & b & 0 & 0 \\ f & g & c & 0 \\ h & y & z & d \end{bmatrix}$ upper / lower triangular $\begin{bmatrix} a & x & y \\ x & b & z \\ y & z & c \end{bmatrix}$ symmetric

- all other entries of an upper/lower triangular matrix could also be zero, so it could also be a diagonal matrix and a diagonal matrix can also be the null matrix.

D2.4 Vector multiplication

for $A = \begin{bmatrix} | & | & & | \\ v_1 & v_2 & \cdots & v_n \\ | & | & & | \end{bmatrix} \in \mathbb{R}^{m \times n}$, $x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in \mathbb{R}^n$: $\quad Ax = \sum_{j=1}^{n} x_j v_j \in \mathbb{R}^m$

D2.5 $Ax = \left[\sum_{j=1}^{n} a_{ij}x_j\right]_{i=1}^{m} \in \mathbb{R}^m$

C2.6 $Ix = x$

D2.7 for $A = \begin{bmatrix} -v_1- \\ -v_2- \\ \vdots \\ -v_n- \end{bmatrix} \in \mathbb{R}^{m\times n}$, $x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in \mathbb{R}^n$ then $Ax = \begin{bmatrix} v_1 \cdot x \\ v_2 \cdot x \\ \vdots \\ v_m \cdot x \end{bmatrix} \in \mathbb{R}^m$

$$\begin{bmatrix} A \end{bmatrix} \cdot \begin{bmatrix} x \end{bmatrix} = \begin{bmatrix} v_1 x \\ v_2 x \\ \vdots \\ v_m x \end{bmatrix} = \begin{bmatrix} a_{11}x_1 & a_{12}x_2 & \cdots & a_{1n}x_n \\ a_{21}x_1 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ a_{m1}x_1 & \cdots & & a_{mn}x_n \end{bmatrix} = x_1\begin{bmatrix} v_1 \end{bmatrix} + x_2\begin{bmatrix} v_2 \end{bmatrix} + \cdots + x_n\begin{bmatrix} v_n \end{bmatrix}$$

= a new vector in $\mathbb{R}^m$ whose entry i is obtained by multiplying row i of A with x.

Space / Rank

D2.8 Column Space $C(A)$ of A is the span of its columns: $C(A) \overset{\text{def}}{=} \{Ax \mid x \in \mathbb{R}^n\} \subseteq \mathbb{R}^m$

D2.9 for $A = [v_1 v_2 \cdots v_n]$ the columns who are a l.a.comb. of the others are dependent columns and if not independent. rank(A) = number of indep. columns

D2.11 Transpose A^T of A: $A^T \overset{\text{def}}{=} [a_{ji}]_{i=1}^{n}{}_{j=1}^{m}$ so A^T is a $n \times m$ matrix where entry $a^T_{ij} = a_{ji}$ of the original matrix A $m \times n$.

D2.12 $(A^T)^T = A$ o A ~~Square~~ Symmetric matrix $\iff A^T = A$

D2.13 Row Space $R(A)$ of the $m \times n$ matrix A is $R(A) \overset{\text{def}}{=} C(A^T)$

L2.14 If rank$(A) = 1$ then $\exists v, w \neq 0$ $v \in \mathbb{R}^m$ $w \in \mathbb{R}^n$ s.t. $A = [v_i w_j]_{i=1}^{m}{}_{j=1}^{n}$

Multiplication

D2.16 for $B = \left[\begin{smallmatrix} | & | & & | \\ x_1 & x_2 & \cdots & x_b \\ | & | & & | \end{smallmatrix}\right] \in \mathbb{R}^{n\times b}$ and $A \in \mathbb{R}^{a\times n}$ $AB = \left[\begin{smallmatrix} | & | & & | \\ Ax_1 & Ax_2 & \cdots & Ax_b \\ | & | & & | \end{smallmatrix}\right] \in \mathbb{R}^{a\times b}$

D2.17 $-\!\!\shortparallel\!\!-$ and $A = \begin{bmatrix} -v_1- \\ -v_2- \\ \vdots \\ -v_a- \end{bmatrix}$ $AB = \begin{bmatrix} v_1x_1 & v_1x_2 & v_1x_3 & \cdots & v_1x_b \\ v_2x_1 & v_2x_2 & \cdots & & v_2x_b \\ \vdots & & & & \\ v_ax_1 & v_ax_2 & \cdots & & v_ax_b \end{bmatrix} \in \mathbb{R}^{a\times b}$

→ So entry c_{ij} of $C = AB$ is the product of the ith row vector of A and the jth column vector of B

→ So to calculate the first row of AB we take v_1 and multiply it with all the x_b col.vectors of B after another, then repeat for the other rows.

! To multiply A and B, $A \doteq a \times n$ and $B \doteq n \times b$ and AB will be $a \times b$

L2.19 $(AB)^T = B^TA^T$ C2.20 $IA = A$, $AI = A$ if the dimensions work out

L2.21 rank$(A) = 1 \iff \exists v, w$ with $v \neq 0 \in \mathbb{R}^m$, $v \neq 0 \in \mathbb{R}^n$ s.t. $A = vw^T$

L2.22 Distributivity and Associativity hold with matrix multiplication

T2.23 CR-Decomposition For an $m \times n$ matrix A with rank$(A) = r$ there exist C, R s.t. $CR = A$ and C is the submatrix containing the indep. columns of A and $R \in \mathbb{R}^{r\times n}$ contains in columns i the factors for the linear combination of the vectors in C that give v_i of A.

Linear Transformations

D2.25 For A $m \times n$, $T_A: \mathbb{R}^n \to \mathbb{R}^m$ is the function $T_A(x) = Ax$

D2.26 a) $T_A(x+y) = T_A(x) + T_A(y)$ c) $T_A(\lambda x + \mu y) = \lambda T_A(x) + \mu T_A(y)$

b) $T_A(\lambda x) = \lambda T_A(x)$

D2.27 A function $T: \mathbb{R}^n \to \mathbb{R}^m$ is a **linear Transformation** if it holds that:
1) $T(x+y) = T(x) + T(y)$
2) $T(\lambda x) = \lambda T(x)$ for all $x, y \in \mathbb{R}^n$ and $\lambda \in \mathbb{R}$.

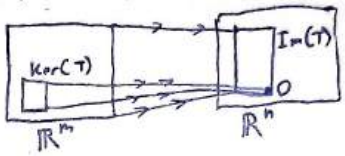
L2.28 For T a linear transformation: $T\left(\sum_{j=1}^{l} \lambda_j x_j\right) = \sum_{j=1}^{l} \lambda_j T(x_j)$

T2.29 For any linear transformation $T: \mathbb{R}^n \to \mathbb{R}^m$ $\exists A \in \mathbb{R}^{m \times n}$ s.t. $T = T_A$

L2.30 For $T_A: \mathbb{R}^n \to \mathbb{R}^a$, $T_B: \mathbb{R}^b \to \mathbb{R}^n$: $T_A(T_B(x)) = T_{AB}(x)$ for all $x \in \mathbb{R}^b$

D2.31 **Kernel and Image** for $T: \mathbb{R}^n \to \mathbb{R}^n$:
$\ker(T) \stackrel{def}{=} \{x \in \mathbb{R}^n \mid T(x) = 0\}$ "Kernel of T" and $\mathrm{Im}(T) = \{T(x) \mid x \in \mathbb{R}^n\}$ "Image of T"

! The kernel is a set on $\mathbb{R}^m$, The Image a set on $\mathbb{R}^n$.



O2.32 If $A \in \mathbb{R}^{m \times n}$ and $T = T_A$ then $\mathrm{Im}(T) = C(A)$

Linear Equations

D3.1 A System of linear equations in m equations and n variables:

$$\begin{matrix} a_{11}x_1 + \dots + a_{1n}x_n = b_1 \\ \vdots \qquad\qquad \vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n = b_m \end{matrix} \iff Ax = b \iff \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

O3.2. Columns of A lin.indep. $\iff Ax = b$ has unique solution

Gauss Elimination: Consider $Ab = [A|b] \in \mathbb{R}^{m \times n+1}$ and subtract rows from each other and swap them around until the A-part is upper triangular, then solve by back substitution.

L3.3 If $Ax = b$ is a $m \times n$-system and $M \in \mathbb{R}^{m \times m}$ the row operation matrix s.t. $MA = A'$, $Mb = b'$ is applying the operation to A and b, then $Ax = b$ and $A'x = b'$ have the same solutions.

C3.4. For $A' = MA$ with M a row-operation matrix, A has lin.indep. columns $\iff A'$ has lin.indep. columns.

Inverses

D3.7 **Inverse** of an $m \times m$ matrix M: M^{-1} s.t. $MM^{-1} = M^{-1}M = I$
If M^{-1} exists, M is called **invertible**

L3.8 The inverse is unique

L3.9 for A, B invertible AB also invertible and $(AB)^{-1} = B^{-1}A^{-1}$

L3.10 for A invertible, A^T also invertible and $(A^T)^{-1} = (A^{-1})^T$

T3.11 **Inverse Theorem** A invertible $\iff Ax = b$ unique solution $\forall b$ $\iff$ columns of A lin. independent

T3.13 **LU Decomposition** Let A be $m \times m$ where Gauss succeeds (without row exchanges) into an upper triangular matrix U. Then let c_{ij} for $i > j$ be the multiple of row j we subtract from row i. Then $A = LU$ with $L = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ c_{21} & 1 & & 0 \\ \vdots & & \ddots & \vdots \\ c_{m1} & \cdots & c_{m,m-1} & 1 \end{bmatrix}$. (Now we can solve ~~$LUb$~~ $LUx = b$ by first solving $Ly = b$ and then $Ux = y$.)

D3.14 **Permutation Matrix**
A permutation of $[n] = \{1 \dots n\}$ is a bijective function $\pi: [n] \to [n]$
The permutation matrix P of π is $P = [p_{ij}]_{i=1}^{n}{}_{j=1}^{n}$ with $p_{ij} = \begin{cases} 1 \text{ if } \pi(i) = j \\ 0 \text{ otherwise} \end{cases}$

L3.16 Inverse of P if P permutation matrix, $P^{-1} = P^T$

L3.17 for permutations π, π' with matrices P, P'; PP' is the matrix of $\pi' \circ \pi$

(To get $\pi(i)$ from P we need to calculate $e_i P$, not Pe_i.)
$\pi(i)$ means "at the ith place in the ordering will be element $\pi(i)$" and not "the place of element i"

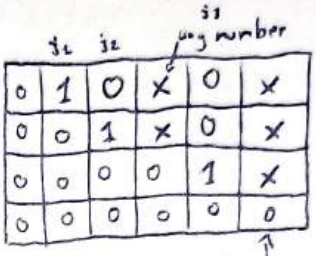
T3.18 LUP Decomposition If we need row exchanges for Gauss we can decompose A into $PA = LU$ where P is a permutation matrix. To do this we do gauss, but if we need to swap row i and j we keep track of that and exchange all the ~~pivots~~ c_s in L for row i and j (that we have used so far) and then in the end make P s.t. it represents the row swaps.

Gauss-Jordan

D3.19 (Reduced) Row Echelon Form An $m \times n$ matrix is in REF if: There exist $r \leq m$ column indices s.t. $1 \leq j_1 \leq \dots \leq j_r \leq n$ and

i) for $i = 1, 2, \dots, r$ we have $r_{ij_i} = 1$

ii) for all i, j we have $r_{ij} = 0$ if $i > r$ or $j < j_i$ or $j = j_k$ for some $k \neq i$

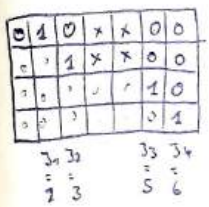


If $r = m$ then R is in reduced REF or RREF. We describe them by $REF(j_1 \dots j_r)$ or $RREF(j_1 \dots j_r)$.

→ So the columns in $j_1 \dots j_r$ are e_i for j_i and behind a column j_i all ~~and~~ columns have normal first i entries and then 0s. And everything before, above them is 0.

O3.20 A matrix in $REF(j_1 \dots j_r)$ has rank r.

→ We can easily solve $Ax = b$ with A in REF: $x_j = \begin{cases} b_i & \text{if } j = j_i \\ 0 & \text{else} \end{cases}$.



$\left[\begin{array}{c} x \end{array}\right] = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix}$ then $x = [0\ b_1\ b_2\ 0\ 0\ b_3\ b_4]$

If b has more non-zero entries than we have j_is, then there is no solution!

Elimination: We get A into REF by doing Gauss on it but dividing the rows by their pivots so we get a 1 there and then subtracting the row multiple also from the rows below it to get the 0s under the 1.

T3.21 For $A = m \times n$ matrix $\exists$ an invertible matrix M s.t. $R_0 = MA$ is in REF
M is the product of the matrices for all row (permutations) operations performed.

T3.22 For A $m \times n$ and M invertible and $R_0 = MA$ in $REF(j_1, \dots, j_r)$ then A has independent columns $j_1, \dots, j_r$.

T3.24 (Computing CR-Decomposition)
For A $m \times n$ and $R_0 = MA$ is in $REF(j_1, \dots, j_r)$: Then R results by transforming R_0 into RREF (by removing the 0-rows at the bottom) and C is the matrix with columns $j_1, \dots, j_r$ from A.
Now $CR = A$.

The fundamental Subspaces

Spaces

D4.1 Vector Space is a triple $(V; +, \cdot)$ where V is a set (of vectors) and:
$+: V \times V \to V$ a function "vector addition"
$\cdot: \mathbb{R} \times V \to V$ a function "vector multiplication" which satisfy the axioms:

commutativity $v+w = w+v$ — identity element: $1 \cdot v = v$
associativity $(u+v)+w = u+(v+w)$ — compatability $\cdot$ and $\cdot$ in $\mathbb{R}$ $(\lambda \cdot \mu) \cdot v = \lambda \cdot (\mu \cdot v)$
zero vector $\exists 0 \forall v \; v+0 = v$ — distributivity over $+$ $\lambda(v+w) = \lambda v + \lambda w$
negative vector $\forall v \exists -v \; (-v)+v = 0$ — distributivity over $+$ in $\mathbb{R}$ $(\lambda + \mu)v = \lambda v + \mu v$

D4.2 $(\mathbb{R}^n, +, \cdot)$ is a vector space

D4.3 Polynomial p is a sum of the form: $p = \sum_{i=0}^{m} p_i x^i$ for some $m \in \mathbb{N}$
→ The largest i s.t. $p_i \neq 0$ is the degree of p, the zero polynomial has degree -1

T4.4 $(\mathbb{R}[x], +, \cdot)$ is a vector space for $\mathbb{R}[x]$ = "set of polynomials with only variable x",
$p+q = \sum_{i=0}^{\max(n,m)} (p_i + q_i) x^i$, $\lambda p = \sum_{i=0}^{m} (\lambda p_i) x^i$

! For our definition, polynomials have to be finite!

T4.5 $(\mathbb{R}^{m \times n}, +, \cdot)$ is a vector space

F4.6 The zero vector in a vector space is unique

F4.7 $-v$ in a vector space exists and is unique

D4.8 Subspace of a vector space V is a nonempty subset $U \subseteq V$ if the axioms hold for all $v, w \in U$ and $\lambda \in \mathbb{R}$:
1) $v+w \in U$ 2) $\lambda v \in U$

L4.9 $0 \in U$ for all subspaces U
F4.10 $0v = 0$ in a vector space
L4.11 For A $m \times n$ matrix $C(A)$ is a subspace of $\mathbb{R}^m$
L4.12 For V vector space and U subspace, U is also a vector space

Bases

D4.13 Linear Combination of a set of vectors for $G \subseteq V$ (vector space) and $F \subseteq G$ a finite subset of G, $\sum_{v \in F} \lambda_v v$ is a linear combination of G. $(\lambda_v \in \mathbb{R})$

L4.14 Every linear combination of G is again in V
D4.15 Span (G) is the set of all linear combinations of G. G is Linearly independent if no vector $v \in G$ is a linear combination of $G \setminus \{v\}$

D4.16 Let V vector space. $B \subseteq V$ is a Basis of V if B is linear independent and $\text{Span}(B) = V$.
L4.17 For $A \in \mathbb{R}^{m \times n}$ the set of linear independent column vectors is a basis of $C(A)$.
D4.18 Every set $B = \{v_1, v_2, \dots, v_m\}$ of m linear indep. vectors is a basis of $\mathbb{R}^m$.
L4.19 Steinitz Exchange Lemma Let V vector space, $F \subseteq V$ a finite set of linearly independent vectors and $G \subseteq V$ a finite set with $\text{span}(G) = V$. Then it holds that:
i) $|F| \leq |G|$
ii) There exists subset $E \subseteq G$ with $|E| = |G| - |F|$ such that $\text{Span}(F \cup E) = V$

T4.20 For V vector space and $B, B' \subseteq V$ two bases of V. Then $|B| = |B'|$

D4.21 A vector space V is finitely generated if there exists a finite $G \subseteq V$ with $\text{span}(G) = V$

T4.22 For V vector space finitely generated and $G \subseteq V$ with $\text{span}(G) = V$, then V has a basis $B \subseteq G$

D4.23 Dimension For V finitely generated vector space, $\dim(V)$ is the size of any basis of V.

L4.24 For V vector space with $\dim(V) = d$:
a) A subset $F \subseteq V$ of d lin. indep. vectors is a basis of V
b) A subset $G \subseteq V$ of d vectors with $\text{span}(G) = V$ is a basis of V

Computing the four Subspaces

Column Space $C(A)$

T4.25 For A $m \times n$ matrix and R_0 in REF $(j_1, \dots, j_r)$ the result of Gauss Jordan on A, then A has independent columns $j_1, \dots, j_r$ and they form a basis of $C(A)$. So:
$\dim(C(A)) = r = \text{rank}(A)$

Row Space $R(A)$ $C(A^T)$

C4.26 for $A \in \mathbb{R}^{m \times n}$ $R(A)$ is a subspace of $\mathbb{R}^n$

L4.27 for $A \in \mathbb{R}^{m \times n}$ and $M \in \mathbb{R}^{m \times m}$ invertible, then $R(A) = R(MA)$ (and $C(B) = C(BN)$ for N invertible)

T4.28 for $A \in \mathbb{R}^{m \times n}$ and $R_0 = REF(j_1, \dots, j_r)$ the result of gauss-jordan on A, then the first r rows of R_0 are a basis of $R(A)$ and $\dim(R(A)) = r = \text{rank}(A)$

T4.29 $\text{rank}(A) = \text{rank}(A^T)$

C4.30 for $A = CR$ the columns of C are a basis for $C(A)$ and those of R for $R(A)$.

Nullspace $N(A)$

D4.31 for $A \in \mathbb{R}^{m \times n}$ the Nullspace of A is $N(A) \overset{\text{def}}{=} \{x \in \mathbb{R}^n \mid Ax = 0\} \subseteq \mathbb{R}^n$

L4.32 $N(A)$ is a subspace of $\mathbb{R}^n$

L4.33 Let $A \in \mathbb{R}^{m \times n}$ and $M \in \mathbb{R}^{m \times m}$ invertible, then $N(A) = N(MA)$

Computing the Nullspace with L4.34:

① Compute the RREF of A with Gauss Jordan

② Partition the equation $R_0 x = 0$ into ~~three~~ two matrices I and Q: $\begin{bmatrix} 1 & 2 & 0 & 3 \\ 0 & 0 & 1 & -2 \end{bmatrix} x = 0$

$$\Rightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_3 \end{bmatrix} + \begin{bmatrix} 2 & 3 \\ 0 & -2 \end{bmatrix} \begin{bmatrix} x_2 \\ x_4 \end{bmatrix} = 0$$

I $x(I)$ Q $x(Q)$

③ Calculate the i-th vector by setting $x(Q) = e_i$ and then solve the system for $x(I)$: e.g. for the first vector here:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_3 \end{bmatrix} + \begin{bmatrix} 2 & 3 \\ 0 & -2 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = 0 \Rightarrow \begin{bmatrix} x_1 \\ x_3 \end{bmatrix} + \begin{bmatrix} 2 \\ 0 \end{bmatrix} = 0 \Rightarrow v_1' = \begin{bmatrix} -2 \\ 0 \end{bmatrix} \Rightarrow \begin{matrix} x_1' = -2 \\ x_3' = 0 \end{matrix}$$

④ And then the i-th vector is: $\begin{bmatrix} -2 \\ 1 \\ 0 \\ 0 \end{bmatrix} \begin{matrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{matrix}$ here

T4.35 The vectors constructed ~~here~~ here form a basis of $N(A)$ and so $\dim(N(A)) = n - r = n - \text{rank}(A)$

Since we can calculate $n-r$ vectors by setting $x(Q)_i = 1$ for each entry (and the others to 0)

Left Nullspace $N(A^T)$

D4.36 Left Nullspace of $A \in \mathbb{R}^{m\times n}$ is the set of y s.t. $yA = 0^T$ or $A^T y = 0$:
$LN(A) \overset{def}{=} N(A^T) \subseteq \mathbb{R}^m$

L4.37 $LN(A)$ is subspace of $\mathbb{R}^m$

T4.38 for $A \in \mathbb{R}^{m\times n}$ and $R_0 = MA$ in REF, the last $m-r$ rows of M form a basis of $LN(A)$:
$\dim(LN(A)) = m-r = m - \text{rank}(A)$

Solution Space of $Ax=b$

D4.39 $Sol(A,b) \overset{def}{=} \{x \in \mathbb{R}^n \mid Ax = b\} \subseteq \mathbb{R}^n$ is the Solution Space of $Ax=b$

! If $b \neq 0$ then $Sol(A,b)$ is not a subspace of $\mathbb{R}^n$ since 0 is not in it!

T4.40 for $A \in \mathbb{R}^{m\times n}$, $b \in \mathbb{R}^m$ and s a solution to $Ax=b$, then: $Sol(A,b) = \{s + x \mid x \in N(A)\}$

L4.41 for $A \in \mathbb{R}^{m\times n}$ and $\text{rank}(A) = m$, $Ax=b$ has a solution for every $b \in \mathbb{R}^m$

- A system $Ax=b$ is called underdetermined if $n > m$ and overdetermined if $n < m$ for $A \in \mathbb{R}^{m\times n}$
- affine subspace is a shifted copy of a subspace

Orthogonality

Orthogonality

D5.1.1 Two vectors are orthogonal if $v^T w = 0$ (for v, w). Two subspaces are orthogonal if for all $v \in V, w \in V$, v and w are orthogonal.

L5.1.2 for $v_1, \dots, v_k$ basis of V and $w_1, \dots, w_\ell$ basis of W:
V, W orthogonal $\iff$ v_i and w_j orthogonal for all $i \in \{1..k\}, j \in \{1..\ell\}$

L5.1.3 for V, W orthogonal with bases $v_1, \dots, v_k$ for V and $w_1, \dots, w_\ell$ for W, then $\{v_1, \dots, v_k, w_1, \dots, w_\ell\}$ are linearly independent.

C5.1.4 if V, W orthogonal subspaces then $V \cap W = \{0\}$ and if $\dim(V) = k$ and $\dim(W) = \ell$, then $\dim(\{\lambda v + \mu w \mid \lambda, \mu \in \mathbb{R}, v \in V, w \in W\}) = k + \ell \leq n$

D5.1.5 The orthogonal complement of V (subspace $\mathbb{R}^n$) is $V^\perp = \{w \in \mathbb{R}^n \mid w^T v = 0 \ \forall v \in V\}$

T5.1.6 for a matrix $A \in \mathbb{R}^{m\times n}$: $N(A) = C(A^T)^\perp = R(A)^\perp$

T5.1.7 for V, W orthogonal subspaces of $\mathbb{R}^n$:
i) $W = V^\perp$ $\iff$ ii) $\dim(V) + \dim(W) = n$ $\iff$ Every $u \in \mathbb{R}^n$ can be uniquely written as $u = v + w$ with $v \in V, w \in W$

L5.1.8 $V = (V^\perp)^\perp$ for V subspace $\mathbb{R}^n$

C 5.1.9 for $A \in \mathbb{R}^{m\times n}$: $N(A) = C(A^T)^\perp$ and $C(A^T) = N(A)^\perp$

T 5.1.10 $\{x \in \mathbb{R}^n \mid Ax = b\} = x_1 + N(A)$ where $x_1 \in R(A)$ such that $Ax_1 = b$

L 5.1.11 for $A \in \mathbb{R}^{m\times n}$: $N(A) = N(A^TA)$ and $C(A^T) = C(A^TA)$

Projections

D 5.2.1 The projection of a vector b onto a subspace S (of $\mathbb{R}^m$) is the point on S that is closest to b. So $\text{proj}_S(b) = \underset{p\in S}{\text{argmin}} \|b-p\|$

NOTE: $\min_{p\in P} f(p)$ returns the minimum value of $f(p)$ while $\underset{p\in P}{\text{argmin}}\, f(p)$ returns the p for which $f(p)$ is minimal.

L 5.2.2 for $a \in \mathbb{R}^m \setminus \{0\}$, the projection of $b \in \mathbb{R}^m$ onto $S = \{\lambda a \mid \lambda \in \mathbb{R}\} = C(a)$ is given by: $\text{proj}_S(b) = \frac{aa^Tb}{a^Ta}$

L 5.2.3 The projection of a vector $b \in \mathbb{R}^m$ onto the subspace $S = C(A)$ can be written as: $\text{proj}_S(b) = A\hat{x}$, where $\hat{x}$ satisfies $A^TA\hat{x} = A^Tb$ ("normal equations")

L 5.2.4 A^TA is invertible $\Leftrightarrow$ A has linearly independent columns

C 5.2.5 If A has lin. indep. cols, then A^TA is square matrix, invertible and symmetric

T 5.2.6 for S subspace in $\mathbb{R}^m$ and A a matrix whose columns are basis of S, the projection of $b \in \mathbb{R}^m$ to S is given by: $\text{proj}_S(b) = Pb$, with $P = A(A^TA)^{-1}A^T$ (P: "projection matrix")

! We cannot simply expand $(A^TA)^{-1}$ since A^T, A are mostly not invertible !

- The projection matrix for $S^\perp$ is $I - P_S$

Least Squares

F 5.3.1 A minimizer of $\min_{\hat{x}\in\mathbb{R}^n} \|A\hat{x}-b\|^2$ is also a solution of $A^TA\hat{x} = A^Tb$, so when A has independent columns the unique minimizer is $\hat{x} = (A^TA)^{-1}A^Tb$

- for the problem of fitting data points $b_1, \dots, b_n$ to a line $\alpha x + \beta$ the solution is given by $\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = (A^TA)^{-1}A^Tb$ for $b = \begin{bmatrix}b_1\\ \vdots\\ b_n\end{bmatrix}$ and $A = \begin{bmatrix}t_1 & 1\\ \vdots & \vdots\\ t_n & 1\end{bmatrix}$, we want to minimize the error $\left\|b - A\begin{bmatrix}\beta\\ \alpha\end{bmatrix}\right\|^2$
  - ↳ the colums of A are most likely independent, except if all data points are from the same time

Orthonormal Bases and Gram Schmidt

D 5.4.1 Vectors $q_1, \dots, q_n$ are orthonormal if they are orthogonal and have norm 1. So for all $i,j \in \{1,\dots,n\}$: $q_i^Tq_j = \delta_{ij}$, where $\delta_{ij} = \begin{cases}0 \text{ if } i\neq j\\ 1 \text{ if } i=j\end{cases}$. If Q is the matrix with columns $q_1, \dots, q_n$ then: qs orthonormal $\Leftrightarrow$ $Q^TQ = I$! Q may not be square and so it is not said that $QQ^T = I$!

D 5.4.3 Orthogonal Matrix is a square matrix $Q \in \mathbb{R}^{n\times n}$ with $Q^TQ = I$. In this case $QQ^T = I$, $Q^{-1} = Q^T$ and the columns of Q form an orthonormal basis of $\mathbb{R}^n$.

P 5.4.6 If Q orthogonal then 1) $\|Qx\| = \|x\|$ 2) $(Qx)^T(Qy) = x^Ty$ $\forall x,y \in \mathbb{R}^n$

P5.4.7 for S subspace of $\mathbb{R}^m$ and $q_1, \dots, q_n$ orthonormal basis of S. And Q $n \times n$ matrix with qs as columns. Then projection matrix onto S is given by QQ^T and $\hat{x} = Q^T b$ for least squares.

A5.4.9 Gram-Schmidt Process transforms n lin.indep. vectors $a_1, \dots, a_n$ into an orthonormal basis for the span of $a_1, \dots, a_n$: $(q_1, \dots, q_n)$

- $q_1 = \frac{a_1}{\|a_1\|}$
- $q_k = a_k - \sum_{i=1}^{k-1} (a_k^T q_i) q_i$
- $q_k = \frac{q_k}{\|q_k\|}$

D5.4.11 QR-Decomposition
for A $m \times n$ matrix with lin.indep. columns, QR=A is given by Q ($m \times n$ matrix that contains the orthonormal vectors given by Gram-Schmidt on A) and $R = Q^T A$. (R is upper triangular)

F5.4.13
- Since $C(A) = C(Q)$, $\text{proj}_{C(A)}(b) = QQ^T b$
- Least squares solution to $Ax = b$ is $R\hat{x} = Q^T b$ ↙ easily solved by back-substitution since R is triangular

Pseudoinverse (Moore-Penrose Inverse)

! "full column rank" = $\text{rank}(A) = n$ for $A \in \mathbb{R}^{m \times n}$

D5.5.1 Pseudoinverse A^+ for matrices of full column rank. For $A \in \mathbb{R}^{m \times n}$ with $\text{rank}(A) = n$ we define $A^+ \in \mathbb{R}^{n \times m}$ as: $A^+ = (A^T A^{-1}) A^T$

P5.5.2 this pseudoinverse of A (for A full column rank) is a left inverse of A, so $A^+ A = I$

D5.5.3 Pseudoinverse A^+ for matrices of full row rank (! = "$\text{rank}(A) = m$ for $A \in \mathbb{R}^{m \times n}$). For $A \in \mathbb{R}^{m \times n}$ with $\text{rank}(A) = m$ we define $A^+ \in \mathbb{R}^{n \times m}$ as: $A^+ = A^T (AA^T)^{-1}$

L5.5.4 this pseudoinverse of A (for A full row rank) is a right inverse of A, so $AA^+ = I$

L5.5.5 For any matrix A and a vector $b \in C(A)$ the unique solution to $\min_{x \in \mathbb{R}^n} \|x\|^2$ s.t. $Ax = b$ is given by the vector $\hat{x} \in C(A^T)$ that satisfies $A\hat{x} = b$.

L5.5.6 for a full row rank matrix A, the unique solution is given by $\hat{x} = A^+ b$

D5.5.7 Pseudo inverse for all matrices for $A \in \mathbb{R}^{m \times n}$ with $\text{rank}(A) = r$ and CR decomposition $A = CR$ we define the pseudoinverse A^+ as $A^+ = R^+ C^+$. $C^+ = R^T (C^T A R^T)^{-1} C^T$

! note that C has full column and R full row rank

L5.5.8 Given $A \in \mathbb{R}^{m \times n}$ and $b \in \mathbb{R}^n$, the (unique) solution to $\min_{x \in \mathbb{R}^n} \|x\|^2$ s.t. $A^T A x = A^T b$ is given by $\hat{x} = A^+ b$.

P5.5.9 For $A \in \mathbb{R}^{m \times n}$ with $\text{rank}(A) = r$ and $S \in \mathbb{R}^{n \times r}$ and $T \in \mathbb{R}^{r \times n}$ s.t. $A = ST$, then: $A^+ = T^+ S^+$

T5.5.11 Let $A \in \mathbb{R}^{m \times n}$, then:
1) $AA^+A = A$ 2) $A^+AA^+ = A^+$ 3) A^+A / AA^+ is symmetric and projection matrix for projecting on $C(A^T)$ / $C(A)$
4) $(A^T)^+ = (A^+)^T$

P5.5.12 If for $A \in \mathbb{R}^{m \times n}$ $A: x \mapsto Ax$ is viewed as a function from $C(A^T)$ to $C(A)$ it is a bijection.

Farkas Lemma

→ see script :)

T5.6.1 Farkas Lemma Let $A \in \mathbb{Q}^{m \times n}$, $b \in \mathbb{Q}^m$. Either there exists a vector $x \in \mathbb{R}^n$ such that $Ax \leq b$ or there exists $y \in \mathbb{R}^m$ such that $y \geq 0$, $y^T A = 0$ and $y^T b < 0$.

The determinant

D6.0.4 Sign of permutation $\operatorname{sgn}(\sigma)$ for permutation $\sigma: \{1,\dots,n\} \to \{1,\dots,n\}$ of n elements, $\operatorname{sgn}(\sigma)$ is either 1 or -1. So if the number of elements that are "out of order" after the permutation is even, it is 1, otherwise -1.

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 \text{ if } |\{(i,j) \in \{1,\dots,n\} \times \{1,\dots,n\} \text{ such that } i<j \text{ and } \sigma(i) > \sigma(j)\}| \text{ is even} \\ 0 \text{ if } \text{-"-} \text{ is odd} \end{cases}$$

D6.0.6 Determinant $\det(A)$ for $A \in \mathbb{R}^{n\times n}$ (!square matrix only) is defined as:

$$\det(A) = \sum_{\sigma \in \Pi_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} A_{i,\sigma(i)}$$, where Π_n is the set of all permutations of n elements

P6.0.7 for a permutation matrix P corresponding to a permutation σ, $\det(P) = \operatorname{sgn}(\sigma)$ and sometimes we write $\operatorname{sgn}(P)$

P6.0.8 given a triangular matrix $T \in \mathbb{R}^{n\times n}$ we have: $\det(T) = \prod_{i=1}^{n} T_{ii}$ $\to \det(I) = 1$

T6.0.9 $\det(A^T) = \det(A)$ for $A \in \mathbb{R}^{n\times n}$

P6.0.10 If $Q \in \mathbb{R}^{n\times n}$ is orthogonal then $\det(Q) = 1$ or $\det(Q) = -1$

P6.0.11 $A \in \mathbb{R}^{n\times n}$ is invertible $\Leftrightarrow \det(A) \neq 0$

P6.0.12 for $A, B \in \mathbb{R}^{n\times n}$ we have $\det(AB) = \det(A)\det(B)$

P6.0.13 for $A \in \mathbb{R}^{n\times n}$ with $\det(A) \neq 0$ we have $\det(A^{-1}) = 1/\det(A)$

D6.0.15 for $A \in \mathbb{R}^{n\times n}$ and $\mathcal{A}_{ij} = (n-1)\times(n-1)$ matrix when removing row i and column j from A. Then the co-factors of A are $C_{ij} = (-1)^{i+j}\det(\mathcal{A}_{ij})$

P6.0.16 for $A \in \mathbb{R}^{n\times n}$ for any $1 \leq i \leq n$: $\det(A) = \sum_{j=1}^{n} A_{ij} C_{ij}$

P6.0.17 for $A \in \mathbb{R}^{n\times n}$ with $\det(A) \neq 0$ we have: $A^{-1} = \frac{1}{\det(A)} C^T$, where C is the $n\times n$ matrix with the co-factors of A as entries

P6.0.19 Cramers Rule

Let $A \in \mathbb{R}^{n\times n}$ s.t. $\det(A) \neq 0$ and $b \in \mathbb{R}^n$, then the solution $x \in \mathbb{R}^n$ of $Ax = b$ is given by $x_j = \frac{\det(B_j)}{\det(A)}$ where B_j is the matrix obtained by replacing the jth column of A with b.

- $\det(A) = \operatorname{sgn}(P) \cdot \det(U)$ for $PA = LU$ (LU-decomp. of A)

P6.0.21 If $A \in \mathbb{R}^{n\times n}$ and P permutation that swaps two elements (so PA swaps two rows of A) then $\det(PA) = -\det(A)$

P6.0.22 The determinant is linear in each row (and column). So for any $a_0, \dots, a_n \in \mathbb{R}^n$ and $d_0, d_1 \in \mathbb{R}$ we have:

$$\begin{vmatrix} - & d_0 a_0^T + d_1 a_1^T & - \\ - & a_2^T & - \\ & \vdots & \\ - & a_n^T & - \end{vmatrix} = d_0 \begin{vmatrix} - & a_0^T & - \\ - & a_2^T & - \\ & \vdots & \\ - & a_n^T & - \end{vmatrix} + d_1 \begin{vmatrix} - & a_1^T & - \\ - & a_2^T & - \\ & \vdots & \\ - & a_n^T & - \end{vmatrix}$$

and the same holds for the columns.

- $\det(A) = |A|$

Eigenvalues and -Vectors

Complex Numbers

Complex number $(a+ib)$ with $i^2 = -1$ / $\sqrt{-1} = i$

$(a+ib)+(x+iy) = (a+x)+i(b+y)$ $\quad (a+ib)(x+iy) = (ax-by)+i(ay+bx)$

$(a+ib)\cdot(a-ib) = a^2+b^2$ $\quad \frac{a+ib}{x+iy} = \frac{(a+ib)(x-iy)}{(x+iy)(x-iy)} = \left(\frac{ax+by}{x^2+y^2}\right)+i\left(\frac{bx-ay}{x^2+y^2}\right)$

- $\Re(a+ib) \overset{\text{def}}{=} a$ "real part"
- $\Im(a+ib) \overset{\text{def}}{=} b$ "imaginary part"
- $|z| \overset{\text{def}}{=} \sqrt{a^2+b^2}$ "modulus of $z = a+bi$"
- $\overline{a+bi} \overset{\text{def}}{=} a-bi$ "complex conjugate"

$|z|^2 = z\bar{z}$, $z_1 z_2 = \bar{z}_2 \bar{z}_1$, $\overline{z_1+z_2} = \bar{z}_1+\bar{z}_2$, $\frac{1}{z} = \frac{\bar{z}}{|z|^2}$

F7.0.1 Eulers Formula for $\theta \in \mathbb{R}$ we have

$$e^{i\theta} = \cos\theta + i\sin\theta \quad \to e^{i\pi} = -1$$

F7.0.2 A complex number can be written as $z = re^{i\theta}$ where r is the modulus of z and θ is an angle, also called "argument" of z.

T7.0.3 Fundamental Theorem of Algebra Any degree n ($n \geq 1$) polynomial (in $\mathbb{C}$) $P(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0$ (with $a_n \neq 0$) has a zero: $\lambda \in \mathbb{C}$ such that $P(\lambda) = 0$

C7.0.4 It actually has n zeros $\lambda_1, \dots, \lambda_n$ (possibly with repetitions) s.t. $P(z) = a_n(z-\lambda_1)\cdot\dots\cdot(z-\lambda_n)$

The number of times $\lambda \in \mathbb{C}$ appears in this expansion is called algebraic multiplicity of the zero

Complex-valued matrices and vectors exist. For $A \in \mathbb{C}^{m\times n}$ we have:

$\bar{A}$ is A, but we replace each entry with its complex conjugate

$A^* = \bar{A}^T$ "hermetian transpose"

$\|v\|^2 = v^*v = \bar{v}^T v = \sum_{i=1}^{n} \bar{v}_i v_i = \sum_{i=1}^{n} |v_i|^2$ dot-product $\langle v, w\rangle = w^* v$

Eigenvalues / Eigenvectors

D7.1.1 for $A \in \mathbb{R}^{n\times n}$, $\lambda \in \mathbb{C}$ is an eigenvalue of A and $v \in \mathbb{C}^n \setminus \{0\}$ is an eigenvector of A, associated with λ, if: $Av = \lambda v$

→ v and λ are "eigenvalue-eigenvector pair"

→ If $\lambda \in \mathbb{R}$ it is "real eigenvalue"

! $\varphi = \frac{1+\sqrt{5}}{2}$ "golden ratio"

P7.1.2 for $A \in \mathbb{R}^{n\times n}$:

λ eigenvalue of $A \iff \det(A-\lambda I) = 0$

v eigenvector (associated with λ) $\iff v \neq 0$ and $v \in N(A-\lambda I)$

P7.1.3 $\det(A-\lambda I)$ is a polynomial in λ of degree n. (The coefficient before λ^n is $(-1)^n$)

T7.1.4 Every matrix $A \in \mathbb{R}^{n\times n}$ has an (probably complex) eigenvalue

P7.1.6 If λ, v eigenvalue-vector-pair of A then λ^k, v are a pair for A^k (for $k \geq 1$)

P7.1.7 If A invertible and λ, v eigenvalue-vector-pairs of A, then $\frac{1}{\lambda}, v$ are such a pair for A^{-1}

P7.1.8 For $A \in \mathbb{R}^{n\times n}$ and $v_1, \dots, v_k \in \mathbb{R}^n$ eigenvectors to the eigenvalues $\lambda_1, \dots, \lambda_k \in \mathbb{R}$. If all λ's are distinct, then $v_1, \dots, v_k$ are linearly independent

T7.1.9 If $A \in \mathbb{R}^{n\times n}$ has n distinct real eigenvalues then there is a basis of $\mathbb{R}^n$ $v_1, \dots, v_n$ made up of eigenvectors of A.

Characteristic Polynomial of A: $(-1)^n \det(A-zI) = \det(zI-A) = (z-\lambda_1)(z-\lambda_2)\cdots(z-\lambda_n)$

P7.1.10 for $A \in \mathbb{R}^{n\times n}$ the eigenvalues of A are the same as those of A^T.

! ↳ But not the eigenvectors necessarily!

D7.1.11 trace of A $Tr(A) = \sum_{i=1}^{n} A_{ii}$ · $Tr(A) = \sum_{i=1}^{n} \lambda_i$ · $\det(A) = \prod_{i=1}^{n} \lambda_i$

T7.1.12 for $A \in \mathbb{R}^{n\times n}$ with eigenvalues $\lambda_1, \dots, \lambda_n$, then: (as they show up in the characteristic polynomial of A, may be repeated)

! algebraic multiplicity = number of times an eigenvalue shows up in the characteristic polynomial

These formulas are very useful for checking computations if one needs to calculate eigenvalues.

T7.1.14 for matrices $A, B, C \in \mathbb{R}^{n\times n}$:

1) $Tr(AB) = Tr(BA)$ 2) $Tr(ABC) = Tr(BCA) = Tr(\underbrace{CBA}_{C}\underbrace{B}_{B})$

CAUTION: The eigenvalues of $A+B$, AB cannot be computed from those of A, B and gauss-elimination does not preserve the eigenvalues!

P7.1.17 for $Q \in \mathbb{R}^{n\times n}$ an orthogonal matrix, if $\lambda \in \mathbb{C}$ eigenvalue of Q, then $|\lambda| = 1$

FF40 If $\lambda \in \mathbb{C}$ is eigenvalue of $A \in \mathbb{R}^{n\times n}$, so is $\bar{\lambda}$

T7.1.20 If we can build a basis of $\mathbb{R}^n$ out of the eigenvectors of $A \in \mathbb{R}^{n\times n}$, A has a complete set of real eigenvectors.

P7.1.21 for P proj projection matrix onto $U \subseteq \mathbb{R}^n$, P has two eigenvalues 1 and 0 and a complete set of real eigenvectors.

D7.1.22 geometric multiplicity of an eigenvalue λ of $A \in \mathbb{R}^{n\times n}$ is the dimension of $N(A - I\lambda)$

FF42 A matrix has a complete set of eigenvectors when the geometric/algebraic multiplicities are the same for all eigenvalues.

FF45 The eigenvalues of a $n\times n$ triangular matrix are those on the diagonal.

Change of Basis

If we have a vector written in the canonical basis $v = \sum_{i=1}^{n} v_i e_i$ then we can transform it into another basis $u_1, \dots, u_n$ by calculating: $v_u = U^{-1}v$ where U is the matrix with the u_is as columns and v_u is the vector s.t. $v = \sum_{i=1}^{n} v_{u_i} u_i$. Similarly we can obtain the representation of a vector u (in the basis $u_1, \dots, u_n$) in the canonical basis by calculating $u_c = U u$.

Now if we have a linear transformation as a $k\times h$ matrix A which takes in and outputs a vector in the canonical basis, we can also use it with other bases by firstly transforming to the canonical basis and then transforming back: $V^{-1}AU$ is the new matrix with U, V having the basis vectors of the other bases in them. Now if $A: \underbrace{\mathbb{R}^n}_{\text{in } e_i\text{-basis}} \to \underbrace{\mathbb{R}^m}_{\text{in } v\text{-basis}}$ then $V^{-1}AU: \underbrace{\mathbb{R}^n}_{\text{in } u\text{-basis}} \to \underbrace{\mathbb{R}^m}_{\text{in } v\text{-basis}}$

Diagonalizing a Matrix

T7.2.1 Let $A \in \mathbb{R}^{n\times n}$ be a matrix with a complete set of real eigenvectors and let $v_1, \dots, v_n \in \mathbb{R}^n$ be a basis formed with eigenvectors of A and let $\lambda_1, \dots, \lambda_n$ be the associated eigenvalues. Now let $V = [v_1, \dots, v_n] \in \mathbb{R}^{n\times n}$. Then $A = V\Lambda V^{-1}$, where Λ is a diagonal matrix with $\Lambda_{ii} = \lambda_i$.

D7.2.2 A matrix $A \in \mathbb{R}^{n\times n}$ is called diagonalizable if $\exists$ an invertible matrix V s.t. $\Lambda = V^{-1}AV$, where Λ is a diagonal matrix.

D7.2.3 Similar Matrices are $A, B \in \mathbb{R}^{n\times n}$ if $\exists$ an invertible matrix S s.t. $B = S^{-1}AS$

P7.2.4 Similar matrices have the same eigenvalues

Symmetric Matrices and Spectral Theorem

T7.3.1 Spectral Theorem Any symmetric matrix $A \in \mathbb{R}^{n\times n}$ has n real eigenvalues and an orthonormal basis made up of eigenvectors of A

C7.3.2 For any symmetric matrix $A \in \mathbb{R}^{n\times n}$ there exists an orthogonal matrix $V \in \mathbb{R}^{n\times n}$ (whose columns are eigenvectors of A) s.t. $A = V\Lambda V^T$ where Λ is diagonal with the eigenvalues of A on its diagonal. "Eigendecomposition"

C7.3.4 The rank of a real symmetric matrix A is the number of non-zero eigenvalues (counting repetitions)

P7.3.6 Let $A \in \mathbb{R}^{n\times n}$ and $v_1, \dots, v_n$ an orthonormal basis of eigenvectors of A and $\lambda_1, \dots, \lambda_n$ the associated eigenvalues. Then $A = \sum_{i=1}^{n} \lambda_i v_i v_i^T$

P7.3.7 Let $A \in \mathbb{R}^{n\times n}$ and symmetric and let $\lambda \in \mathbb{C}$ be an eigenvalue of A, then $\lambda \in \mathbb{R}$.

C7.3.8 Every symmetric matrix $\in \mathbb{R}^{n\times n}$ has a real eigenvalue λ.

P7.3.10 Rayleigh Quotient for a symmetric matrix $A \in \mathbb{R}^{n\times n}$ the Rayleigh Quotient, defined for $x \in \mathbb{R}^n \setminus \{0\}$ as $R(x) = \frac{x^TAx}{x^Tx}$ attains its maximum at $R(v_{max}) = \lambda_{max}$ and minimum at $R(v_{min}) = \lambda_{min}$. Where $\lambda_{max}, \lambda_{min}$ are the largest and smallest eigenvalues of A and v_{max}, v_{min} their eigenvectors.

D7.3.11 Positive Semidefinite (PSD) matrix is a symmetric matrix $A \in \mathbb{R}^{n\times n}$ whose eigenvalues are all ≥ 0. Positive definite (PD) is A if all eigenvalues are strictly > 0.

P7.3.12 A symmetric matrix $A \in \mathbb{R}^{n\times n}$ is positive semidefinite $\iff x^TAx \geq 0$ for all $x \in \mathbb{R}^n$.

" " is positive definite $\iff x^TAx > 0$ " " .

F7.3.13 If $A, B \in \mathbb{R}^{n\times n}$ are PSD (PD) then $A+B$ is PSD (PD)

D7.3.14 Gram Matrix Given n vectors $v_1, \dots, v_n$ in $\mathbb{R}^n$ we call their Gram Matrix the $n\times n$ matrix of inner products: $G_{ij} = v_i^Tv_j$. So if for $V \in \mathbb{R}^{n\times n}$ with columns $v_1, \dots, v_n$ then $G = V^TV$ is the Gram Matrix of V.

- We also sometimes call AA^T the Gram Matrix of A. $AA^T = \sum_{i=1}^{n} a_i a_i^T$

P7.3.16 For $A \in \mathbb{R}^{m\times n}$, the non-zero eigenvalues of $A^TA \in \mathbb{R}^{n\times n}$ are the same as those for $AA^T \in \mathbb{R}^{m\times m}$. Both are symmetric and PSD.

P7.3.17 Cholesky Decomposition Every symmetric PSD matrix M is a gram matrix of an upper triangular matrix C. $M = C^TC$ is the Cholesky Decomposition.

↳ To get it we take $M = V\Lambda V^T = V\Lambda^{1/2}\Lambda^{1/2}V^T = (V\Lambda^{1/2})(V\Lambda^{1/2})^T$

Then we take the QR decomposition s.t. $(V\Lambda^{1/2})^T = QR$

Now: $M = (V\Lambda^{1/2})(V\Lambda^{1/2})^T = (QR)^T(QR) = R^TQ^TQR = R^TR$

Now: $C = R$ results in the decomposition

The Singular Value Decomposition

D8.1.1 SVD - Singular Value Decomposition Let $A \in \mathbb{R}^{m \times n}$. There exist orthogonal matrices $U \in \mathbb{R}^{m \times m}$ and $V \in \mathbb{R}^{n \times n}$ such that $A = U \Sigma V^T$, where $\Sigma \in \mathbb{R}^{m \times n}$ is diagonal in the sense that $\Sigma_{ij} = 0$ when $i \neq j$, and its diagonal elements are non-negative and in descending order. And $U^T U = I$, $V^T V = I$.

The columns of U are called left singular vectors of A and are orthonormal.

The columns of V are called right singular vectors of A and are orthonormal.

The diagonal elements of Σ, $\sigma_i = \Sigma_{ii}$ are called singular values of A and are ordered as $\sigma_1 \geq \dots \geq \sigma_{\min(m,n)}$.

R8.1.2 If A has rank r we can write the SVD in a more compact form: $A = U_r \Sigma_r V_r$ where U_r ~~and V~~ $\in \mathbb{R}^{n \times r}$ and $V_r \in \mathbb{R}^{n \times r}$ contain only the first r left/right singular vectors and $\Sigma_r \in \mathbb{R}^{r \times r}$ is a diagonal matrix with the first r singular values. (Sometimes we omit the subscript "r" and instead specify the dimensions of the matrices)

R8.1.3 Let $A \in \mathbb{R}^{n \times n}$ and $A = U \Sigma V^T$ be its SVD, then:

$AA^T = U(\Sigma \Sigma^T) U^T$

and so the left singular vectors of A (columns of U) are the eigenvectors of AA^T and the singular values of A are the square-root of the eigenvalues of AA^T. (note that $\Sigma \Sigma^T$ is $m \times m$ diagonal). If $m > n$, A has n singular values and AA^T has m eigenvalues (which is larger than n), but the "missing" ones are 0.

And:

$A^T A = V(\Sigma^T \Sigma) V^T$

and so the right singular vectors of A (colums of V) are the eigenvectors of $A^T A$ and the singular values of A are the square-root of the eigenvalues of $A^T A$ (note that $\Sigma^T \Sigma$ is $n \times n$ diagonal). If $n > m$, than the "missing" ones are again zero.

→ So: left singular vectors = eigenvectors of AA^T; right singular vectors = eigenvectors of $A^T A$;
singular values = square roots of eigenvalues of $AA^T / A^T A$

P8.1.4 Let $A \in \mathbb{R}^{m \times n}$ be a matrix with rank r. Let $\sigma_1, \dots, \sigma_r$ be the non-zero singular values of A, $u_1, \dots, u_r$ the corresponding left singular vectors and $v_1, \dots, v_r$ the corresponding right singular vectors. Then $A = \sum_{k=1}^{r} \sigma_k u_k v_k^T$

T8.1.5 Holy Grail

Every matrix $A \in \mathbb{R}^{m \times n}$ has a SVD decomposition.

→ every linear transformation is diagonal when viewed in the bases of the singular vectors.

Vector and Matrix Norms

$$\|x\|_p = \left(\sum_{i=1}^{n} |x_i|^p\right)^{1/p}$$

- $\|x\|_1$ = "manhattan distance"
- $\|x\|_2$ = $\|x\|$ in this lecture

D8.2.1 $\|A\|_F$ Frobenius Norm $\quad \|A\|_F = \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} A_{ij}^2}$

$\|A\|_{op}$ Operator/Spectral Norm $\quad \|A\|_{op} = \max_{x \in \mathbb{R}^n \text{ s.t. } \|x\|=1} \|Ax\|$

$A \in \mathbb{R}^{n \times m}$ ist invertierbar :

$\Leftrightarrow \forall b \in \mathbb{R}^m$, $Ax = b$ unique solution
$\Leftrightarrow$ cols. of A lin. indep.
$\Leftrightarrow$ gauss succeeds on A $\forall b$
$\Leftrightarrow Ax = 0$ only has solution $x = 0$
$\Leftrightarrow N(A) = \{0\}$
$\Leftrightarrow C(A) = R(A) = \mathbb{R}^m$

$\Leftrightarrow \operatorname{rank}(A) = m$
$\Leftrightarrow \det(A) \neq 0$
$\Leftrightarrow \lambda_i \neq 0$ for $1, \dots, m$ =:
$\Leftrightarrow A^T$ invertible
$\Leftrightarrow A^{-1}$ exists
$\Leftarrow!$ A positive definit
$\Leftrightarrow$ Singular values all > 0

Basics

Big O,Ω,Θ

O: $O(f) = \{g: N \to \mathbb{R}^+ \mid \exists C>0 \ \forall n \in N: \ g(n) \leq C \cdot f(n)\}$

Ω: $\Omega(f) = \{g: N \to \mathbb{R}^+ \mid f \in O(g)\}$

Θ: $\Theta(f) = \{g: N \to \mathbb{R}^+ \mid g \in O(f) \text{ and } f \in O(g)\}$ for $f: N \to \mathbb{R}^+$

- we write "$g \in O(f)$, $g \gtrsim \Omega(f)$, $g \simeq \Theta(f)$" instead of "$\in$"
- $g \gtrsim \Omega(f) \iff f \in O(g)$

Limits
- $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0 \iff f \in O(g)$, but $f \notin \Theta(g)$
- $\lim_{n\to\infty} \frac{f(n)}{g(n)} = c \iff f = \Theta(g)$
- $\lim_{n\to\infty} \frac{f(n)}{g(n)} = \infty \iff f \gtrsim \Omega(g)$, but $f \notin \Theta(g)$

Master Theorem for $T(n) \leq a \cdot T(n/2) + C \cdot n^b$ for $a, C > 0$, $b \geq 0$, $T: \mathbb{N} \to \mathbb{R}^+$

Then for $n = 2^k$ (or any n if T increasing):
- If $b > \log_2 a$ then $T(n) \in O(n^b)$
- If $b = \log_2 a$ then $T(n) \in O(n^{\log_2 a} \cdot \log n)$
- If $b < \log_2 a$ then $T(n) \in O(n^{\log_2 a})$

⊕ If we have $\gtrsim |=$ instead of $\leq$ the cases hold with $\gtrsim \Omega \mid = \Theta$ instead

Calculating Limits

Sum $\sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$

Fibonacci: $Fib(n) \gtrsim \frac{1}{3} \cdot 1{,}5^n$ (and $\leq 1{,}7^n$ ca.)

$\log(n!)$ $\log(n!) = \Theta(n \cdot \log n)$

$\log n \in O(\sqrt{n}) \leq n \leq n^{x \cdot (y+1)} \leq x^n$

Sum2 $\sum_{i=1}^{n} f(i) \gtrsim \sum_{i=\lceil \frac{n}{2} \rceil}^{n} f(i)$ and $\leq n \cdot f(n)$

$n!$ $n! \gtrsim 1 \cdot 2 \cdot \ldots \cdot n \gtrsim \lceil n/10 \rceil \cdot \ldots \cdot n \gtrsim \lceil n/10 \rceil^{0{,}9n} \gtrsim (n/10)^{0{,}9n}$

$\lim_{n\to\infty} n! \approx \left(\frac{n}{e}\right)^n$

- $(\sqrt{a} + \sqrt{b})(\sqrt{a} - \sqrt{b}) = a - b$
- Raise to $e^{\ln}$: $\frac{a}{b} = \frac{e^{\ln a}}{e^{\ln b}} = e^{\ln a - \ln b}$
- $\ln(a \cdot b) = \ln(a) + \ln(b)$
- $\ln(a^b) = b \cdot \ln(a)$

! $f \in O(g)$ and $h \gtrsim \Omega(1) \not\Rightarrow f \in O(g(h))$

Counter: $f = n$, $g = n^2$, $h = \sqrt{n}$ and $g \circ h = n$

Induction to prove S for all $\mathbb{N}$

① Base Case prove S(0) (or S(start))

② Induction Hypothesis "we assume S holds for some k (= start)"

③ Induction step prove that "S holds for k" $\Rightarrow$ "S holds for k+1" by using the IH for k.

Karatsubas Schnellere schr. multiplikation durch "divide and conquer"

Lower-Bound-Analysis

- "muss alle Elemente einmal ansehen also $\geq n$"

Decision Tree

alle möglichen Ausgaben müssen vorkommen, also n Knoten, also Höhe von Baum $\log n$, also $\geq \log n$

Searching

Linear Search für unsortiere Arrays

Binary Search für sortierte Arrays $O(\log n)$

Sorting

Bubble Sort gehe n-mal durch und tausche x mit x+1 if $x > x+1$ | $O(n^2)$ worst case, best case can be $O(n)$ but we don't check and break if array sorted in the algo from lecture

Selection Sort gehe n-mal durch, suche kleinstes element und lege es an den Anfang | $O(n^2)$ Vergl. $O(n)$ Kopieren. again best case does not change

Insertion Sort mache n-mal: die ersten i Zahlen sind sortiert, füge die i+1te Zahl ein (mit binary search) | $O(n \log n)$ Vergl. $O(n^2)$ Vertauschungen

Wenn array sortiert best case ist schneller! $O(n \log n)$ unsere Implementation $O(n)$ linear backwards search Impl.

Merge Sort teile array in 2 Hälften, mergesort auf beide Hälften, dann merge beide wieder zsm., base case: length = 1 | $O(n \log n)$

Quick Sort Lege Pivot fest, teile array in 2 Teile: $\geq$ pivot und $<$ pivot, Sortiere die Teile rekursiv | $O(n^2)$ wenn pivot letztes Element (worst case wenn schon sortiert) $O(n \log n)$ wenn pivot zufällig

Heapsort makeheap(array)

Invarianten = Condition, die nach jeder loop-iteration hält, correctness proof wenn Invariante hält und das Endergebnis impliziert.

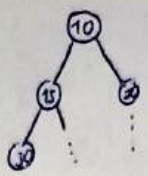
Sorting lower Bound $= \Omega(n \log n)$

decision tree

alle n! Sortierungen müssen vorkommen $\rightsquigarrow n \log n = \log(n!)$

Data Structures

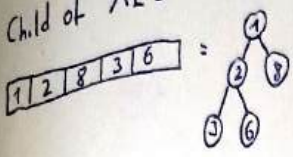
Heap keeps track of max or min



insert: insert at bottom and then "bubble up" if upper element is lower until you reach a larger one (for min-heap "greater until you reach smaller one")
in $O(\log n)$

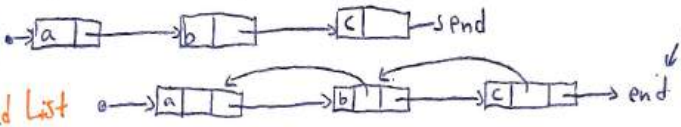
get top: in $O(1)$
remove top: in $O(\log n)$, repair heap by putting last element on top and then bubbling it down

Binary Tree as Array:
Child of A[k] in A[2k], A[2k+1]



Lists

- Array if length fixed, random access in $O(1)$
- Linked List



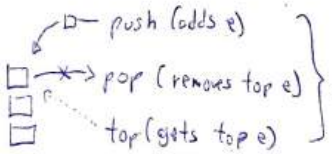
we also safe a pointer to end for fast insertion

- Doubly Linked List

	INSERT	GET	DELETE	INSERT AFTER
arr	$O(1)$	$O(1)$	$O(n)$	$O(n)$
Linked L	$O(n)$	$O(n)$	$O(n)$	$O(1)$
doubly linked L	$O(1)$	$O(n)$	$O(1)$	$O(1)$

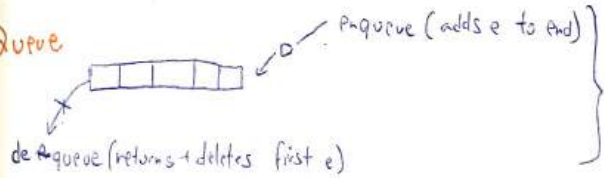
If we know memory location of element

Stack



all in $O(1)$ ← Implement with linked list

Queue

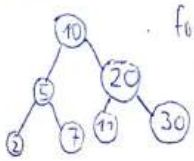


all in $O(1)$ ← Implement with doubly linked list

Priority Queue = (min/max) Heap insert() and getMax() in $\log n$

Dictionary has (key/value) pairs, each key unique
→ Implement as binary search tree or Hash Map

Binary Search Tree



for each node left child is ~~greater~~ smaller and right child is greater.

AVL Trees

Makes searching in binary trees $O(\log n)$ by balancing them. Keeps track for each node of height(left subtree) and height(right subtree) and if they differ by more than one restores it by rotation.

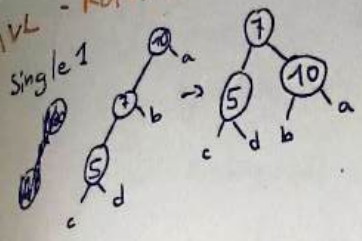
AVL-Condition

"for node n $|size(subtree_{left}(n)) - size(subtree_{right}(n))| \leq 1$"

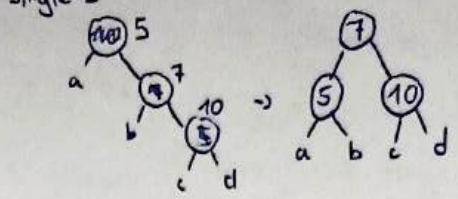
- An AVL Tree must also always be a binary-search tree

AVL - Rotation

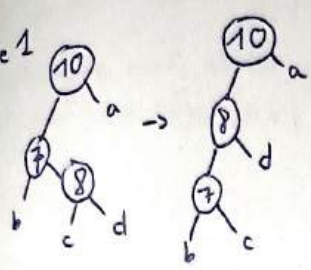
Single 1



Single 2

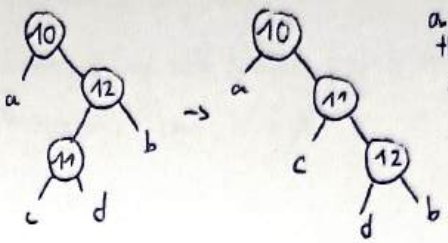


double 1



and then Single 1

double 2



and then Single 2

Dynamic Programming

Memoization speichere berats berechnete Rekursionen und frage sie ab, anstatt nochmal ausrechnen

Dynamic Programming Idee: berechne Werte von einem Teilproblem aus Werten von "kleineren" Teilproblemen

- DP-Tabelle: enthält Problem(a,b,c) an Index $dp_{a,b,c}$
- Rekursion: berechne Index (a,b,c) aus vorherigen Indizes
- Backtracking: Extrahiere Lösung aus fertiger Tabelle

Algorithms (see script)

- Fibonacci
- max subarray sum
- Jump Game
- Longest common Subsequense
- Edit Distance
- subset sum
- Knapsack
- Longest ascending subsequence

Graphs

UNDIRECTED GRAPH $G=(V,E)$, V "vertex set"/"Knotenmenge", E "edge set"/"Kantenmenge"

$e \in E = \{u,v\}$ "edge from u to v"/"Kante von...", u+v "endpoints"/"Endpunkte"

→ u,v "adjacent"/"benachbart" → e "incident"/"anliegend" to u,v

deg(v) "degree of v" = number of vertices adjacent to v deg(v)=0 "v isolated"

$(v_0, v_1, \dots, v_k)$ "walk"/"Weg" : if $\{v_a, v_{a+1}\} \in E \ \forall a \leq k-1$; k = "length"; v_0, v_k = "end points"

cycle/Zyklus walk with $k \geq 2$ and $v_0 = v_k$ (closed walk)

path/Pfad walk with $v_i \neq v_j \ \forall i \neq j$

cycle/Kreis closed walk with $k \geq 3$ and all vs different except v_0, v_k

eulerian walk walk that contains every edge $\in E$ exactly once

closed eulerian walk closed walk that contains every edge $\in E$ exactly once

Hamilton Path path that contains every vertex

Hamiltonian cycle cycle that contains every vertex

u reaches w if ∃ walk with endpoints u, w

connected component is an equivalence class of the relation "u reaches v"

A graph is connected if it has exactly one connected component

acyclic if a graph has no cycles

Tree is a connected, acyclic graph ↗ a leaf is a vertex in a tree with degree 1

Forest is an acyclic graph (every connected component is a tree)

! If not otherwise said, all the graphs we look at are undirected, no self loops $\{v,v\}$ are allowed and each edge $\{u,v\}$ appears only once in the graph. ! and $V \neq \emptyset$

DIRECTED GRAPH $G=(V,E)$ with $V \neq \emptyset$

edge $(u,v) \in E$ is ordered pair "edge from u to v" (again $u \neq v$)

↳ u direct predecessor of v, "starting vertex of e"
v direct successor of u, "end vertex of e"

! other vocabulary same as for undirected graphs but with "directed"-.

in-degree $deg_{in}(v)$ number of edges with v as end vertex

out-degree $deg_{out}(v)$ —"— starting vertex

Source/Quelle: vertex with $deg_{in}(v) = 0$

Sink/Senke: vertex with $deg_{out}(v) = 0$

DAG directed acyclic graph

! Again no (v,v) and multigraphs (graphs with same edge more than once), but (u,v) and $(v,u) \in E$ is allowed.

Graph Algorithms

Eulerian walk exists (in connected, undirected graph) $\iff$ number of uneven degrees ≤ 2

Handshake Lemma $\sum_{v \in V} deg(v) = 2 \cdot |E|$

walk is cycle $\iff$ end/start vertex incident to even number of vertices in walk

$\exists$ closed eulerian walk $\iff$ graph is a single connected component and all degrees even

↓

Algorithm to find them: find cycles until all edges are used up and then unite them to a big one

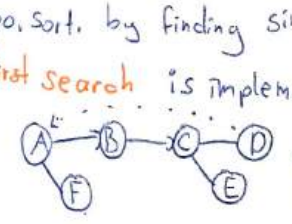
Topologische Sortierung (for directed graphs) is an ordering of the vertices such that you can remove the vertices in this order if (a,b) (↑ edge) means you need to remove a before b.

- $\exists$ closed walk $\iff$ $\exists$ topological sorting
- find a topo. sort. by finding sinks with DFS (can be removed)

DFS-depth first search is implemented with stack/recursively:

1. push start on stack
while stack not empty:
2. v ← stack.get
3. push all successors of v that are not visited on stack
4. mark v visited

DFS-Tree:



- back-edge: edge from v to already visited vertex (higher in tree, but same branch)
- cross-edge: edge to visited vertex lower in tree (other branch)
- forward-edge: normal edge

$\exists$ back-edge $\iff$ $\exists$ (directed) closed walk

distance $dist(u,v)$ is shortest length of walk from u to v

BFS uses a queue to first process all neighbours of current edge and then move to next level

enter[v] is the BFS step we added v to queue (1 for start) leave[v] BFS step we removed v from queue and processed it (2 for start)

Dijkstras Algo: finds shortest path in G with positive edge weights in $O((n+m)\cdot\log n)$

Bellman Ford —"— with all edge weights in $O(n\cdot m)$

Detecting negative cycles use Bellman Ford iteration an additional time → if some value decreases, neg. cycle exists

MST

MST minimum spanning tree is a subgraph H of a graph G that has a minimal sum of edge weights and is a tree and includes all vertices in G.

Boruvkas Algo. look at all ZHKs, add the minimum edges going from those ZHKs, connect to new ZHKs and repeat. ! ZHK = "Zusammenhangskomponente" = "connected component"

Prims Algo. look at one ZHK, repeatedly add the minimum edge bordering that ZHK until graph is connected; use a min-heap to do that ("min-heap" = "priority-queue"); Runtime: $O((|V|+|E|)\cdot\log|V|)$ same as Boruvska

! The minimum edge bordering a ZHK is always in the MST.

Kruskals Algo. Firstly sort all the edges for minimal weight; use union-find-structure to keep track of ZHKs; then add the minimal edges repeatedly ↓ until all are in one ZHK, Runtime: $O(\underbrace{|E|\cdot\log|E|}_{\text{sort}} + \underbrace{|V|\cdot\log|V|}_{\text{union-find}})$

Amortised Runtime Analysis is the runtime average taken over multiple iterations

pseudo-polynomial polynomial runtime in size of number but not in (bit) size of input

Union-Find-Structure keeps track of unions of elements that belong together; each union has a representant (initially the element itself for each element); each element stores the rep. of its union and a linked list of the members of it. Union(u,w) = search the smaller list of u or w → for each element in list change the representant to the one of other element and add it to their list.

⇒ Amortised runtime $O(\log n)$ per Union().

All pairs shortest paths find all shortest paths from/to all vertices

- If all weights = 1: n-times BFS
- If all weights ≥ 0: n-times Dijkstras, else:
- n-times Bellman Ford

Floyd-Warshall-Algo. DP with d^i_{uv} = "length of shortest path u to v which is only allowed to use in-between vertices ~~exist~~ $\{1,\dots,i\}$"; Runtime $O(n^3)$; If there exists a negative cycle it will output <0 for some entry

Johnsons-Algo. makes all edge weights ≥0 and then uses n-times Dijkstras on it; Runtime: $O(n\cdot(m+n)\log n)$

↑ with genious idea

Matrizen und Graphen

Number of different paths v→w If we have a $n \times n$ matrix A and A_{ij}: "number of different paths from i to j" then A^k will give us the number of different paths of length k for A_{ij}.

Strassens Algo. similar idea to KaratSubas Algo. but for matrices. makes A^2 in $O(n^{2.8})$ ca., "normally" would be $O(n^3)$

Median

We can find the median of an array of numbers in $O(n)$. → see script

Algorithm Cheat Sheet

name	for	needs	runtime	desc.
binarySearch	Searching	sorted Arr.	$O(\log n)$	watch out for edges in modified versions
mergeSort	Sorting	Array	$O(n \log n)$	
QuickSort	Sorting	Array	$O(n \log n)$	if random Pivot
InsertionSort	Sorting	Array	$O(n^2)$	optimal $O(n)$ if spec. implementation and already sorted
SelectionSort	Sorting	Array	$O(n^2)$	
BubbleSort	Sorting	Array	$O(n^2)$	
HeapSort	Sorting	+ Heap	$O(n \log n)$	
BFS	traversal	queue	$O(\lvert V\rvert + \lvert E\rvert)$	finds shortest paths for unweighted graph
DFS	traversal	(stack)	$O(\lvert V\rvert + \lvert E\rvert)$	can find toposort, cycles, sinks
Dijkstra	single shortest paths	edges ≥ 0, heap	$O((\lvert E\rvert + \lvert V\rvert)\log\lvert V\rvert)$	
Bellman-Ford	single shortest paths	Array	$O(\lvert E\rvert \cdot \lvert V\rvert)$	+1 iteration to find negative cycles
Prim	MSTs	Heap	$O((\lvert V\rvert + \lvert E\rvert)\cdot \log\lvert V\rvert)$	heap the vertices adjacent to ZHK
Boruvka	MSTs		$O((\lvert V\rvert + \lvert E\rvert)\cdot \log\lvert V\rvert)$	
Kruskals	MSTs	Union Find	$O(\lvert E\rvert \log\lvert E\rvert + \lvert V\rvert \log\lvert V\rvert)$	sort all edges first, then union find for vertices.
Floyd-Warshall	all pairs shortest paths		$O(\lvert V\rvert^3)$	DP
Johnson	all pairs shortest paths		$O(\lvert V\rvert^2 \log\lvert V\rvert + \lvert V\rvert\lvert E\rvert)$	① new node z ② 0-edges from z to all nodes ③ $h(i)$: distance from z to i (Bellman Ford) ④ $w'(v,w) = w(v,w) + h(v) - h(w)$ ⑤ n-times dijkstras on $w'(v,w)$-graph ⑥ extract solution with $-h(v) + h(w)$