1. Mathematical Reasoning, Proofs and a First Approach to Logic

D. (Conjunction) $A \wedge B$ **D.** (Precedence) $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$
D. (Disjunction) $A \vee B$
D. (Implication) $A \rightarrow B :\Leftrightarrow \neg A \vee B$
D. (Constant Functions) $\top$ constant 1, $\bot$ constant 0
L. $\mathcal{F}$ is a tautology iff $\neg \mathcal{F}$ is unsatisfiable
T. (Transitivity / Composition of Implications)
$(\mathcal{F} \rightarrow \mathcal{G}) \wedge (\mathcal{G} \rightarrow \mathcal{H}) \Rightarrow (\mathcal{F} \rightarrow \mathcal{H})$
T. (De Morgan)
$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$, $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$

1.1 Proof Patterns and Techniques

D. (Direct Proof) of an implication $\mathcal{F} \rightarrow \mathcal{G}$
Assume $\mathcal{F}$, then derive $\mathcal{G}$
T. (Contraposition) $\mathcal{F} \rightarrow \mathcal{G} \Leftrightarrow \neg\mathcal{G} \rightarrow \neg\mathcal{F}$
D. (Indirect Proof) of an implication $\mathcal{F} \rightarrow \mathcal{G}$
Via contraposition: Assume $\neg\mathcal{G}$, derive $\neg\mathcal{F}$
D. (Modus Ponens) $\mathcal{F} \wedge (\mathcal{F} \rightarrow \mathcal{G}) \Rightarrow \mathcal{G}$
Prove $\mathcal{F}$, prove $\mathcal{F} \rightarrow \mathcal{G}$ to derive $\mathcal{G}$ via modus ponens
D. (Case Distinction) $\mathcal{F}_1 \vee \ldots \vee \mathcal{F}_n$
Complete List of Cases: $\mathcal{F}_1, \ldots, \mathcal{F}_n$ which have to be true
If $\forall i \in \{1, \ldots, n\} : \mathcal{F}_i \rightarrow \mathcal{G}$ then also $\mathcal{G}$ is true
D. (Proof by Contradiction) of a statement $\mathcal{F}$
Assume $\neg\mathcal{F}$, derive $\bot$
T. If $\neg\mathcal{F} \Rightarrow \bot$, then $\mathcal{F}$ is also a tautology
D. (Existence Proof) $\exists x\, P(x)$ Constructive, Non-Constructive
D. (Inexistence Proof) $\neg\exists x\, P(x)$
D. (Proof by Counterexample) $\neg\forall x\, P(x)$
D. (Proof by Induction) of $\forall n \in \mathbb{N}, n \geq k$: $P(n)$
1. Basis Step: Prove $P(k)$ (lowest)
2. Induction Hypotesis: Assume that there exists an $n \in \mathbb{N}$ for which $P(n)$ holds
3. Induction Step: Prove $\forall n \geq k$: $P(n) \rightarrow P(n+1)$
(by using the induction hypotesis)
$P(n+1) :\Leftrightarrow \ldots \overset{\text{I.V.}}{=} \ldots = P(n+1)$ □

2. Sets, Relations and Functions

2.1 Sets and Operations on Sets

A-set is defined by
- property $\{x \mid P(x)\}$, or
- listing $\{x_1, x_2, \ldots\}$

D. (Set Equality, Subset)
$A = B :\Leftrightarrow (A \subseteq B) \wedge (B \subseteq A) \Leftrightarrow \forall x (x \in A \leftrightarrow x \in B)$
D. (Proper Subset) $A \subset B :\Leftrightarrow A \subseteq B \wedge A \neq B$
D. (Cardinality) number of elements in A, denoted $|A|$
L. $|A|, |B| \in \mathbb{N}$: $|A| \neq |B| \Leftrightarrow A \neq B$
L. $|A|, |B| \in \mathbb{N}$: $|A \times B| = |A| \cdot |B|$
D. (Cartesian Prod.) $A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$
D. (Union) $A \cup B = \{x \mid x \in A \vee x \in B\}$
D. (Intersection) $A \cap B = \{x \mid x \in A \wedge x \in B\}$
D. (Complement) $\overline{A} = A^c := \{x \in \mathcal{U} \mid x \notin A\}$
D. (Difference) $B - A := \{x \in B \mid x \notin A\}$
D. (Empty Set) denoted $\emptyset$ or $\{\}$ property $\forall x (x \notin \emptyset)$
L. $\forall A : \emptyset \subseteq A$
L. The empty set is unique: $\emptyset' \subseteq \emptyset \wedge \emptyset \subseteq \emptyset' \Rightarrow \emptyset' = \emptyset$
D. (Power Set) $\mathcal{P}(A) = 2^A = \{S \mid S \subseteq A\}$
T. $|A| = k \in \mathbb{N} \Rightarrow |\mathcal{P}(A)| = 2^k$
T. (Algebra of Sets)
Idempotence: $A \cap A = A$, $A \cup A = A$
Commutativity of $\cap$ and $\cup$
Associativity of $\cap$ and $\cup$
Absorbtion: $A \cap (A \cup B) = A$, $A \cup (A \cap B) = A$
Distributivity: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Complementarity: $A \cap \overline{A} = \emptyset$, $A \cup \overline{A} = \mathcal{U}$
Consistency: $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$

2.2 Relations

D. (Relation) $\rho \subseteq A \times B$, $a \rho b :\Leftrightarrow (a,b) \in \rho \subseteq A \times B$
$a \not\rho b :\Leftrightarrow (a,b) \notin \rho \subseteq A \times B$
Empty Relation: $\emptyset$
Complete Relation: $A \times B$ 2^{n^2}
Relation on A: $\rho \subseteq A \times A$

D. (Identity Relation) $\mathrm{id} = \{(a,a) \mid a \in A\}$
D. (Inverse of a Relation) $a \rho b \Leftrightarrow b \hat{\rho} a$
Matrix: Transpose Graph: Reverse Edges
D. (Composition of Relations) $\rho \subseteq A \times B$ $\sigma \subseteq B \times C$
$a \rho\sigma b = a (\rho \circ \sigma) b :\Leftrightarrow \exists b \in B : a \rho b \wedge b \sigma c$
Matrix: Clamping Mult, Graph: $\rightarrow \bullet \rightarrow$ Composition of Walks
D. (n-fold Composition) $\rho \subseteq A^2$: ρ^n Edges for
Matrix: n-times clamp mult, Graph: Walks of lenght n
L. (Associativity of Rel Comp.) $\rho(\sigma\phi) = (\rho\sigma)\phi$
L. (Inverses of Composition) $\widehat{\rho\sigma} = \hat{\sigma}\hat{\rho}$ (Analog: Matrix Mu
D. (Properties of Relations) $\rho \subseteq A \times A$:
- reflexive if: $\forall a \in A\, (a \rho a)$ $2^{(n^2-n)}$
  - i.e., if $\mathrm{id} \subseteq \rho$
  - Matrix: All diagonal elements are 1.
  - Graph: All vertices have a loop
- irreflexive if: $\forall a \in A\, (a \not\rho a)$ $2^{(n^2-n)}$
  - i.e. if $\mathrm{id} \cap \rho = \emptyset$
  - Matrix: All diagonal elements are 0.
  - Graph: No loops
- symmetric if: $\forall a,b \in A (a \rho b \leftrightarrow b \rho a)$ $2^{\sum_{i=0}^{n} k} = 2^{\frac{n(n+1)}{2}} = 2^{(n$
  - Matrix: symmetric: $M_\rho = M_\rho^T$
  - Graph: not directed or c for every edge there is the inv
- antisymmetric if: $\forall a,b \in A (a \rho b \wedge b \rho a \rightarrow a = b)$
  - equivalently: $\forall a,b \in A (a \rho b \wedge a \neq b \rightarrow b \not\rho a)$
  - L. iff $\rho \cap \hat{\rho} \subseteq \mathrm{id}$ $2^n \cdot 3^{\binom{n}{2}}$
  - Matrix: Diagonal 1 or 0.
    Left and Right side of diag are opposites
  - Graph: No cycle of length 2
- transitive if: $\forall a,b,c (a \rho b \wedge b \rho c \rightarrow a \rho c)$
  - L. iff $\rho^2 \subseteq \rho$ no simple formula, check others first
  - Graph: Transitive Hull $\rho = \rho^*$

Other Numbers of Relations:
- symmetric and reflexive (or irreflexive): $2^{\binom{n}{2}}$
- symmetric and antisymmetric: 2^n (subset of id)
- antisymmetric and reflexive (or irreflexive): $3^{\binom{n}{2}}$
- symmetric and antisymmetric and reflexive (or irreflexive): 1

D. (Transitive Closure) $\rho^* := \bigcup_{n=1}^{\infty} \rho^n$
Matrix: $\bigvee_{n=1}^{\infty} M^n$ Graph: Transitive Hull (Matrix has clamped multiplication

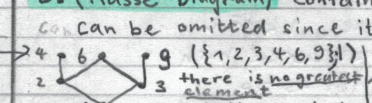
2.2 Equivalence Relations

in this subsection: θ = eq. rel

D. (Equivalence Relation) θ is reflexive, symmetric, transitive
D. (Equivalence Class) $[a]_\theta = \{b \in A \mid b \theta a\}$
complete relation: one equivalence class
id: all classes are singletons $\{a\}$ for $a \in A$
D. (Partition) of a set A in mutually disjoint subsets
$S_i \cap S_j = \emptyset$ for $i \neq j$ and $\bigcup_{i \in I} S_i = A$
D. (Set of Equivalence Classes)
quotient set of A by θ, A mod θ:
$A/\theta := \{[a]_\theta \mid a \in A\}$
L. The intersection of two equivalence rel. is an equivalence re
T. The set A/θ is a partition of A.

2.3 Partial Order Relations

B, A = poset
in this subsection $\preceq$ = part. orde
D. (Partial Order) $\preceq$ is reflexive, antisymm. and transitiv
D. (Partially Ordered Set, poset) $(A; \preceq)$
D. $a \prec b :\Leftrightarrow a \preceq b \wedge a \neq b$
D. (Comparability) To elements a,b of a poset are called comparable if $a \preceq b$ or $b \preceq a$ is true, otherwise incomparab
D. (Total Order) if any two elements of a poset A are comparal
D. (Well Ordered) Every non-empty subset of A has a least e
L. Every finite totally ordered poset is well ordered.
T. (Cartesian Product of Posets) $(A, \preceq)$ $(B, \sqsubseteq)$ Then $\leq$ is defined a
$(a_1, b_1) \leq (a_2, b_2) :\Leftrightarrow a_1 \prec a_2 \wedge b_1 \sqsubseteq b_2$
$\leq$ is a partial order
T. (Lexicographic Order) $\leq_{lex}$ for two posets $(A, \preceq)$ $(B, \sqsubseteq)$
$(a_1, b_1) \leq_{lex} (a_2, b_2) :\Leftrightarrow a_1 \prec a_2 \vee (a_1 = a_2 \wedge b_1 \sqsubseteq b_2)$
$\leq_{lex}$ is a partial order
T. If both $(A, \preceq)$ and $(B, \sqsubseteq)$ are totally ordered then so is $(A \times B, \preceq$
D. (Covering) b covers a iff $a \prec b \wedge (\nexists c : a \prec c \wedge c \prec b)$
D. (Hasse Diagram) contains only covering edges. Direction can be omitted since it's assumed that the edges point upwa



({1,2,3,4,6,9}|)
there is no greatest element
4,6,9 are maximal elements
2 is the least elem of {2,4,6}
1,2 are a lower bound for {2,4}

D. (Special Elements) $(A,\preceq)$ poset $S \subseteq A$

1. $a \in S$ is a minimal (maximal) element of S if there exists no $b \in S$ with $b \prec a$ ($b \succ a$)
2. $a \in S$ is the least (greatest) element of S if $a \preceq b$ ($a \succeq b$) for all $b \in S$.
3. $a \in A$ is a lower (upper) bound of S if $a \preceq b$ ($a \succeq b$) for all $b \in S$
4. $a \in A$ is the greatest lower bound (least upper bound) $\text{glb}(S)$ ($\text{lub}(S)$) of S if a is the greatest (least) element of the set of all lower (upper) bounds of S.

D. (Meet) if $\{a,b\} \subseteq A$ have a glb it's called the meet of a and b

D. (Join) if $\{a,b\} \subseteq A$ have a lub it's called the join of a and b

D. (Lattice) A poset $(A,\preceq)$ in which every pair of elements has a meet and a join is called a lattice.

2.4 Functions

D. (Function) from A to B, $f: A \to B$ (domain, codomain) is a relation with special properties

1. $\forall a \in A\ \exists b \in B: a f b$ (f is: totally defined)
2. $\forall a \in A\ \forall b,b' \in B: a f b \wedge a f b' \to b = b'$ (well-defined)

D. (Set of all Functions) $B^A = \{f \mid f: A \to B\}$ (i.e. as sets)

D. (Partial Function) only satisfies condition 2 of above

D. (Equality) Two functions are equal if they're equal as relations.

D. (Image of a Set) $S \subseteq A$ under f is $f(S) := \{f(a) \mid a \in S\} \subseteq B$

D. (Image) or range of f is $f(A) = \text{im}(f)$

D. (Preimage) of a set $T \subseteq B$ is $f^{-1}(T) = \{a \in A \mid f(a) \in T\} \subseteq A$

D. (Function Properties) $f: A \to B$ $|A| = m$ $|B| = n$

1. injective if $\forall a,b \in A: a \neq b \to f(a) \neq f(b)$ $n^{\underline{m}}$ $(m \leq n)$
2. surjective if $\forall b \in B\ \exists a \in A: f(a) = b$ $\sum_{k=1}^{n} (-1)^{n-k} \binom{n}{k} k^m$ $(m \geq n)$
3. bijective if f is both, injective and surjective $n!$ $(m = n)$

D. (Inverse Function) For a bijective function the inverse relation f^{-1} is also a function

D. (Composition) $f: A \to B$ $g: B \to C$ $(g \circ f)(a) = g(f(a))$

T. Function composition is associative $(h \circ g) \circ f = h \circ (g \circ f)$

3. Combinatorics and Counting

Enumeration: Listing the elements in a systematic manner
Counting: Computing the cardinality of the set

3.1 Basic Counting Principles

Addition Principle: The cardinality of the union of disjoint (finite) sets is equal to the sum of their cardinalities

Multiplication Principle: The cardinality of the cross product of finite sets is equal to the product of their cardinalities

Bijection Principle: If there is a bijection between two finite sets A and B then $|A| = |B|$.

Inclusion-Exclusion Principle: For any finite sets $A_1, \dots, A_n$:

$$|A_1 \cup \dots \cup A_n| = \sum_{k=1}^{n} |A_k| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \dots + (-1)^{n-1} |A_1 \cap \dots \cap A_n|$$

T. (Bonferroni Inequalities) Lets say we stop at the previous principle and get S so far. Then if the next sign would be a + then $S \leq |A_1 \cup \dots \cup A_n|$
- then $S \geq |A_1 \cup \dots \cup A_n|$

Double Counting Principle: Let say we want to count $|S|$, where $S \subseteq A \times B$. We may either count
- for every $a \in A$ the number m_a of $b \in B$ s.t. $(a,b) \in S \subseteq A \times B$
- or for every $b \in B$ the number m_b of $a \in A$ s.t. $(a,b) \in S \subseteq A \times B$

$$|S| = \sum_{a \in A} m_a = \sum_{b \in B} m_b$$

Matrix Analogy: Count by row or by column.

Pigeonhole Principle: If a set of n objects is partitioned into $k < n$ sets, then at least one of these sets contains $\lceil \frac{n}{k} \rceil$ objects.

D. (Factorial) $n! = n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 2 \cdot 1$

D. $n^{\underline{k}} = n \cdot (n-1) \cdot \dots \cdot (n-k+1) = \prod_{i=0}^{k-1} (n-i) = \frac{n!}{(n-k)!}$

D. (Binomial Coefficient) $\binom{n}{k} = \frac{n^{\underline{k}}}{k!} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!}$

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

For $k < 0$ or $k > n$ we define $\binom{n}{k} = 0$
The results can also be constructed with Pascal's Triangle starting with $\binom{0}{0}$ as tip.

Drawing k elements from a set of size n:

	Ordered		Unordered	
	Number	Examples	Number	Examples
with repetition	n^k	aa ab ac ba bb bc ca cb cc	$\binom{n+k-1}{k}$	aa ab ac bb bc cc
without repetition	$n^{\underline{k}}$	ab ac ba bc ca cb	$\binom{n}{k}$	ab ac bc

Example: $\{a,b,c\}$, $n=3$, $k=2$

3.2 Binomial Coefficients

L. (Symmetry of Pascal's Triangle) $\binom{n}{k} = \binom{n}{n-k}$

L. (Pascal's Identity) For $n > 0$ $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

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

C. $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

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

L. (Vandermonde's Identity) Let $k,m,n \geq 0$ $m+n > 0$ then $\binom{m+n}{k} = \sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i}$ in particular: $\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$

3.3 Countable and Uncountable Sets

D. (Cardinality, Countability)

(i) Two sets A and B have the same cardinality, denoted $A \sim B$, if there exists a bijection $A \to B$.
(ii) The cardinality of B is at least the cardinality of A, denoted $A \preceq B$, if $A \sim C$ for some $C \subseteq B$.
(iii) B dominates A, denoted $A \prec B$, if $A \preceq B$ and $A \not\sim B$.
(iv) A set A is called countable if $A \preceq \mathbb{N}$, and uncountable otherwise

L. (i) $\sim$ is an equivalence relation
(ii) $\preceq$ is transitive
(iii) $A \subseteq B \Rightarrow A \preceq B$
(iv) $A \subseteq B \wedge B \preceq \mathbb{N} \Rightarrow A \preceq \mathbb{N}$
(v) $A \preceq B \wedge B \preceq A \Rightarrow A \sim B$
(vi) For two sets A,B exactly one of $A \prec B$, $A \sim B$, $A \succ B$ holds

T. $|A|, |B| \in \mathbb{N}$: $(A \sim B \Leftrightarrow |A| = |B|)$

T. A set A is countable iff A is finite or $A \sim \mathbb{N}$
Hence $A \prec \mathbb{N} \Rightarrow A$ is finite.

T. The set $\{0,1\}^* := \{\varepsilon, 0, 1, 00, 01, 10, 11, \dots\}$ of finite binary sequences is countable

T. The set $\mathbb{N} \times \mathbb{N}$ $(= \mathbb{N}^2)$ is countable

C. $A \preceq \mathbb{N} \wedge B \preceq \mathbb{N} \Rightarrow A \times B \preceq \mathbb{N}$

C. $\mathbb{Q} \preceq \mathbb{N}$

T. Let A and A_i for $i \in \mathbb{N}$ be countable sets
(i) For any $n \in \mathbb{N}$, the set A^n of n-tuples is countable
(ii) The union $\bigcup_{i \in \mathbb{N}} A_i$ of a countable list $A_1, A_2, \dots$ of countable sets is countable
(iii) The set A^* of finite sequences over A is countable.

D. $\{0,1\}^\infty$ denotes the set of semi-infinite binary sequences
semi-infinite: bounded in one direction, unbounded in other

T. The set $\{0,1\}^\infty$ is uncountable.

L. $A \not\preceq \mathbb{N} \wedge A \preceq B \Rightarrow B \not\preceq \mathbb{N}$
In particular if a subset of B is uncountable, then so is B

L. $A \not\preceq \mathbb{N} \wedge B \preceq \mathbb{N} \Rightarrow A - B \not\preceq \mathbb{N}$

T. The set $\mathbb{R}$ of real numbers is uncountable

T. The interval $[0,1)$ of real numbers is uncountable

4. Graph Theory

D. ((Simple) Graph) $G = (V,E)$ $E = \{\{u,v\} \subseteq V \mid u \neq v\}$

D. (Neighborhood) of a vertex v $\Gamma(v) := \{u \in V \mid \{u,v\} \in E\}$

D. (Directed Graph) $G = (V,E)$ $E \subseteq V \times V$

D. (In-degree) $\deg^-(v)$ number of edges entering v

D. (Out-degree) $\deg^+(v)$ number of edges leaving v

D. (Complement) of a graph G is $\bar{G} = (V, \bar{E})$

D. (Adjacency Matrix) $A_G = (a_{ij})$ $a_{ij} = 1 :\Leftrightarrow \begin{cases} 1, & (a_i, a_j) \in E \\ 0, & (a_i, a_j) \notin E \end{cases}$

L. (Sum of Degrees)

$$\sum_{v \in V} \deg^-(v) = \sum_{v \in V} \deg^+(v) = |E| \qquad \sum_{v \in V} \deg(v) = 2|E|$$

For the next few definitions let $G=(V,E)$ and $H=(V',E')$

D. (Subgraph) $G \sqsubseteq H :\iff V \subseteq V' \wedge E \subseteq E'$

D. (Union) $G \cup H = (V \cup V', E \cup E')$

D. (Contained) $G \trianglelefteq H :\iff \exists K : (G \cong K \wedge K \sqsubseteq H)$

D. (Graph Isomorphism) $G \cong H$ if there exists a bijection $\pi : V \leftarrow V'$ s.t.: $\{u,v\} \in E \iff \{\pi(u), \pi(v)\} \in E'$

L. $\trianglelefteq$ is a partial order on graphs.

L. $\cong$ is an equivalence relation on graphs.

Isomorphism Checks: Vertices of highest degree, common paths, common shapes (triangles), isomorphisms to common known graphs

4.1 Some Special Graphs

D. (Complete Graph) of n vertices, denoted K_n (any pair of vertices is connected.)

D. (Empty Graph) complement of complete graph. (no edges)

D. (m,n-Mesh) $M_{m,n}$ on $m \cdot n$ vertices

$V = \{(i,j) \mid 1 \le i \le m \wedge 1 \le j \le n\}$

$E = \{\{(i,j),(i',j')\} \mid (i=i' \wedge |j-j'|=1) \vee (|i-i'|=1 \wedge j=j')\}$

D. (d-dimensional Hypercube) Q_d

$V = \{0,1\}^d$, $\{u,v\} \in E \iff u$ and v differ in only one bit.

D. (Bipartite Graph) If V can be split into two disjoint sets V_1, V_2 such that no edge connects two vertices in the same subset V_i $(i=1,2)$

D. (Complete Bipartite Graph) $K_{m,n}$ is a graph on $m+n$ vertices

$V = B \cup W$ and $B \cap W = \emptyset$ and $|B|=m$, $|W|=n$

$E = \{\{u,v\} \mid u \in B \wedge v \in W\}$

L. Here are some observations about the special graphs:

$P_3 \cong K_{2,1}$ $\quad C_4 \cong K_{2,2} \cong Q_2 \cong M_{2,2}$

$P_m \trianglelefteq C_n \iff m < n$ $\quad C_2^d \trianglelefteq Q_d$

4.2 Paths and Cycles

D. Walk [Weg]: any walk through a graph with repetition of vertices and edges allowed.

- Tour [Tour]: all edges are distinct
  - Circuit [Schleife]: start and endpoint are the same
- Path [Pfad]: all vertices are distinct
  - ($\Rightarrow$ edges are distinct $\Rightarrow$ every path is a tour)
  - A path P_n of length n consist of
    - $n+1$ vertices $V = \{v_0, \dots, v_n\}$
    - n edges $E = \{\{v_0,v_1\}, \dots, \{v_{n-1},v_n\}\}$
- Cycle [Kreis, Zyklus]: start and endpoint identical
  - ($\Rightarrow$ every cycle is a circuit)
  - A cycle C_n consists of
    - n vertices $V = \{v_1, \dots, v_n\}$
    - n edges $E = \{\{v_1,v_2\}, \dots \{v_n,v_1\}\}$
  - Hamiltonian Cycle: all vertices are visited

D. (Hamiltonian Graph) a (directed) graph with a hamilt. cycle

T. In a graph G there exists a walk of length ℓ from u to v iff $(A_G)^\ell$ is not zero at position (u,v). Actually this entry corresponds to the number of distinct walks of length ℓ from u to v.

D. (Connected Components) An undirected graph G is connected if any two vertices are connected by a path. The maximal connected subgraphs of G are called components.

T. The complete graph K_n is trivially hamiltonian. Hence adding enough edges will always turn a graph hamiltonian.

T. A graph $G=(V,E)$ for which

$|V| \ge 3$ and $\deg(u) + \deg(v) \ge |V|$

for every non-adjacent pair $(u,v) \notin E$ is hamiltonian.

In particular: $\forall v \in V : \deg(v) \ge \frac{|V|}{2} \Rightarrow G$ is hamiltonian

T. The hypercube Q_d is hamiltonian for $d \ge 2$.

D. (Gray Code) is a hamiltonian cycle in a hypercube

L. A bipartite graph can have a hamiltonian cycle only if the two sets have equal size.

L. From the previous lemma it follows that the mesh $M_{m,n}$ has no hamiltonian cycle if both m and n are odd.

4.3 Trees

D. (Tree) Undirected connected graph with no cycles.

D. (Forest) undirected graph with no cycles, ie., the union of several trees with disjoint vertex sets.

D. (Leaf) is a vertex with degree 1.

L. A tree with $n \ge 2$ vertices has at least 2 leaves.

T. (Tree Properties) For a graph G with n vertices TFAE:

(i) G is a tree.

(ii) G has $n-1$ edges and no cycles.

(iii) G has $n-1$ edges and is connected.

D. (Spanning Tree) of a connected graph G is a subgraph of G which is a tree and contains all vertices of G.

D. (Rooted Tree) is a tree with a distinguished vertex: the root. There is a unique path from the root to every vertex v. Its length is the distance of v from the root. The height or depth of the tree is the maximal distance from the root to a leaf.

Further terms: ancestor, parent, child.

D. (d-ary Tree) a rooted tree where every vertex has at most d children.

(Note: Any graph can be embedded in 3-dim. space without crossings)

4.4 Planar Graphs

D. (Planarity) A graph is planar if it can be drawn in the plane with no edges crossing.

D. (Regions, Degree) A drawing of a planar graph divides the plane into disjoint regions, one of which is infinite. The degree of a region is the number of edges one encounters in a walk around the region's boundary. An edge is counted twice if it's a bridge.

T. (Euler's formula) A plane drawing of a connected planar graph divides the plane into

$r := |E| - |V| + 2$ regions.

T. For any connected planar graph the sum of the degrees of the regions is equal to $2|E|$.

T. Every connected planar graph $G=(V,E)$ wit $|V| \ge 3$ satisfies

$|E| \le 3|V| - 6$.

If G is bipartite, then the following stronger ineq. holds

$|E| \le 2|V| - 4$.

C. K_n is planar $\iff n \le 4$.

C. $K_{3,3}$ is not planar. K_5 is not planar.

Planarity Preserving Operations:

1. Deletion of edges
2. Deletion of singleton vertices
3. Merging neighboring vertices (ie. delete edge between them, replacing the two main tail by a single vertex, edges)

L. If a sequence of these operations is performed on a graph G and the resulting graph H is not planar then so is G.

D. (Polyhedron) is a solid bounded by a finite number of (plane) polygon faces. The vertices and edges of these polygons are are the vertices and edges of the polyhedron. A polyhedron is convex if the straight line segment connecting any two points lies entirely within it. A polyhedron is regular if for some $m,n \ge 3$ each vertex meets exactly m faces (and hence m edges) and each face is a regular n-gon.

T. There are exactly five regular polyhedra:

	$\lvert V\rvert$	$\lvert F\rvert$ Faces	$\lvert E\rvert$	m=Faces met per Vertex	n=Edges of n-gons (Faces)
Tetraeder	4	4	6	3	3
Hexaeder	8	6	12	3	4
Oktaeder	6	8	12	4	3
Dodekaeder	20	12	30	3	5
Ikosaeder	12	20	30	5	3

5. Number Theory

Note that the integers $\mathbb{Z}$ are a ring. Many of these concepts can be defined for any ring.

5.1 Divisors and Division

D. (Divisibility) For $a,b \in \mathbb{Z}$ with $a \neq 0$ we define

$a \mid b :\iff \exists c \in \mathbb{Z} : ac = b$ (every non-zero a divides 0) (1 and -1 divide all $\mathbb{Z}$)

D. (Euclid, Quotient Remainder)

$\forall a,d \in \mathbb{Z}$ $(d \neq 0)$ $\exists! q,r \in \mathbb{Z} : a = dq + r \wedge 0 \le r < |d|$

D. (A greatest common divisor) $d \neq 0$; a,b not both 0 then

$d := \gcd(a,b) \overset{\neg(a=b=0)}{\iff} (d \mid a \wedge d \mid b) \wedge (\forall c \in \mathbb{Z} - \{0\} : c \mid a \wedge c \mid b \Rightarrow c \mid d)$

D. (The greatest common divisor) $d := |\gcd(a,b)|$

D. (Relatively Prime) are a and b $\iff \gcd(a,b) = 1$

D. (Ideal) generated by a (and b)

$(a,b) := \{ua + vb \mid u,v \in \mathbb{Z}\}$ $\quad (a) := \{ua \mid u \in \mathbb{Z}\}$

L. Every ideal can be generated by a single integer:

$\forall a,b \in \mathbb{Z}$ (not both 0) $\exists d \in \mathbb{Z} : (a,b) = (d)$ where $d := \gcd(a,b)$

C. $\forall a,b \in \mathbb{Z}$ (not both 0) $\exists u,v \in \mathbb{Z} : \gcd(a,b) = u \cdot a + v \cdot b$

Euclid's GCD Algorithm, efficiently computes $d=\gcd(a,b)$ as well as u and v s.t. $u\cdot a+v\cdot b=\gcd(a,b)$ $\quad a\geq b$

Application:

	q	s_1	s_2	u_1	u_2	v_1	v_2
after-init	$\lfloor \frac{a}{b} \rfloor$	a	b	1	0	0	1
after n-th loop	$\lfloor \frac{s_1}{s_2} \rfloor$	s_2	$s_1-qs_2=:Rs_2(s_1)$	u_2	u_1-qu_2	v_2	v_1-qv_2
termination if		s_2	$\boxed{\leq 0}$	u_2		v_2	

The result is: $d:=s_1$, $u=u_1$, $v=v_1$

Example: $\gcd(789,22)$

	q	s_1	s_2	u_1	u_2	v_1	v_2
after init	35	789	22	1	0	0	1
after 1st loop	1	22	19	0	1	1	-35
after 2nd loop	6	19	3	1	-1	-35	36
after 3rd loop	3	3	1	-1	7	36	-251
termination		1	$\boxed{0}$	7		-251	

Hence, $\gcd(789,22)=1$ and $7\cdot 789-251\cdot 22=1=\gcd(a,b)$
Thus the ideal $(782,22)=(1)$
Since 789 and 22 are coprime the equation $22x\equiv_{789}1$ has a unique solution $x=v_1=(-251)\equiv_{789}538$. (multiplicative inverses)

5.2 Factorisation into Primes

D. (Prime) A positive integer $p>1$ is called prime if the only positive divisors of p are p and 1.
D. (Composite) An integer greater than 1 that is not a prime.
L. If p is a prime which divides the product $x_1\cdot x_2\cdot\ldots\cdot x_n$ of some integers then p divides one of them, i.e., $\exists i\in\{1..n\}: p\mid x_i$
T. (Fundamental Theorem of Arithmetic) Every positive integer can be written uniquely as the product of primes.
T. $\sqrt{n}$ is irrational unless n is a square, i.e., $\exists c\in\mathbb{Z}: n=c^2$.
D. (Least Common Multiple) of two positive integers a and b is the common multiple ℓ of a and b which divides every common multiple ℓ' of a and b.
$\ell:=\operatorname{lcm}(a,b)$ $\quad a\mid\ell'\wedge b\mid\ell'\Rightarrow\ell\mid\ell'$

Building GCD and LCM of Prime Factorisation of a and b!

$a=\prod_i p_i^{e_i}$ $\quad b=\prod_i p_i^{f_i}$ It's easy to see that $\gcd(a,b)\cdot\operatorname{lcm}(a,b)=ab$

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

Addition and Multiplication Rules:

even + even = even	even · even = even
even + odd = odd	even · odd = odd
odd + odd = even	odd · odd = odd

5.3 Congruences and Modular Arithmetic

D. (Congruence) For $a,b,m\in\mathbb{Z}$ $m\geq 1$
$a\equiv b\pmod m :\Leftrightarrow a\equiv_m b :\Leftrightarrow m\mid(a-b)$
L. For any $m\in\mathbb{Z}$ $m\geq 1$, $\equiv_m$ is an equivalence rel. on $\mathbb{Z}$.
L. (Compatibility with arithmetic operations)
$(a\equiv_m b)\wedge(c\equiv_m d)\Rightarrow(a+c\equiv_m b+d\wedge ac\equiv_m bd)$
C. Let $f(x_1,\ldots,x_k)$ be a multi-variate polynomial in k variables with integer coefficients, and let $m\geq 1$. If $a_i\equiv_m b_i$ for $1\leq i\leq k$, then $f(a_1,\ldots,a_k)\equiv_m f(b_1,\ldots,b_k)$.
L. $a=b\Rightarrow a\equiv_m b$ $\quad a\not\equiv_m b\Rightarrow a\neq b$
L. For any $a,b,m\in\mathbb{Z}$ with $m\geq 1$ $\quad(a\equiv_m R_m(a))$
i) $R_m(a+b)=R_m(R_m(a)+R_m(b))$
ii) $R_m(a\cdot b)=R_m(R_m(a)\cdot R_m(b))$
L. $(\exists x\in\mathbb{Z}_m: ax\equiv_m 1)\Leftrightarrow\gcd(a,m)=1$ (has a solution)
T. (Chinese Remainder Theorem) Let $m_1,m_2,\ldots,m_r$ be pairwisely relatively prime. Let $M=\prod_{i=1}^r m_i$. For every list $a_1,\ldots,a_r$ with $0\leq a_i\leq m_i$ for $0\leq i\leq r$, the system of congruence equations has a unique solution x satisfying $0\leq x\leq M$.

$x\equiv_{m_1} a_1\Rightarrow M_1=M/m_1$ Solve $M_1N_1\equiv_{m_1}1\rightsquigarrow N_1$
$x\equiv_{m_2} a_2\Rightarrow M_2=M/m_2$ Solve $M_2N_2\equiv_{m_2}1\rightsquigarrow N_2$
$\vdots$ $\quad\vdots$
$x\equiv_{m_r} a_r\Rightarrow M_r=M/m_r$ Solve $M_rN_r\equiv_{m_r}1\rightsquigarrow N_r$

Then
$$x\equiv R_M\left(\sum_{i=1}^r a_iM_iN_i\right).$$

6. Logic

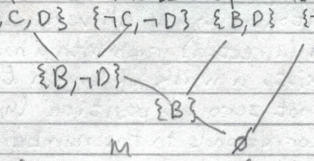
D. (Proof System) $\Pi=(\mathcal{F},\mathcal{P},\tau,\phi)$
$\mathcal{F}$: Set of mathematical statements
$\mathcal{P}$: Set of proofs.
$\mathcal{I}:\mathcal{F}\to\{0,1\}$ truth function, defines meaning of $s\in\mathcal{F}$
$\phi:\mathcal{F}\times\mathcal{P}\to\{0,1\}$ $\quad\phi(s,p)=1\Rightarrow p$ is a valid proof for s.
D. (Soundness) $\forall s\in\mathcal{F}\ \forall p\in\mathcal{P}:\ \phi(s,p)=1\Rightarrow\mathcal{I}(s)=1$
D. (Completeness) $\forall s\in\mathcal{F}(\ \mathcal{I}(s)=1\Rightarrow\exists p\in\mathcal{P}:\phi(s,p)=1)$
D. (Logical Consequence) G is a logical consequence of F iff every structure suitable both, which is a model for F is also a model for G. $F\models G$. (F could also be a set of formulas)
D. (Equivalence) $F\equiv G:\Leftrightarrow F\models G$ and $G\models F$

6.1 Logical Calculi

D. (Derivation Rule) $\{F_1,\ldots,F_k\}\vdash_R G$, if G can be derived from $F_1,\ldots,F_k$ by rule R.
D. (Calculus) $K=\{R_1,\ldots,R_m\}$ (set of derivation rules)
D. (Correctness) $M\vdash_R F\Rightarrow M\models F$ (Correctness of rules)
D. (Soundness) $M\vdash_K F\Rightarrow M\models F$ (Correctness of calculus)
D. (Completeness) $M\models F\Rightarrow M\vdash_K F$
One writes $\vdash_K F$ if F can be derived from the empty set of formulas.
L. If $F\vdash_K G$ for a sound calculus, then $\models(F\to G)$
E. (Calculus that is not sound) has a rule which is incorrect, like $\{A\vee B\}\vdash A\wedge B$.
E. (Calculus that is complete but not sound) $\varnothing\vdash_R F$, $K=\{R\}$
E. (Calculus that is sound but not complete) Has correct rules:
$\{A\wedge B\}\vdash_{R_1}A$ $\quad\{A,A\to B\}\vdash_{R_2}B$ (Therefore, not complete)
Does not allow to derive $A\wedge B\vdash B\wedge A$.
When applying a calculus, say which rule and which args you are applying and number the resulting formulas too.

6.2 Propositional Logic

E. Extend the propositional logic with: $\oplus$ exclusive or.
Syntax: For all formulas F and G, $(F\oplus G)$ is also a formula.
Semantics: $\mathcal{A}((F\oplus G))=1$ if and only if $\mathcal{A}(F)=1$ or $\mathcal{A}(G)=1$, but not both.
D. (CNF) $\bigwedge(\bigvee x_{ij})$ For every row = 0, or the inverse literals, and after.
D. (DNF) $\bigvee(\bigwedge x_{ij})$ For every row = 1, and literals, or after.
E. (Resolution Calculus) Show that
$G=(\neg B\wedge\neg C\wedge\neg D)\vee(\neg B\wedge\neg D)\vee(C\wedge D)\vee B$
is a tautology, is equivalent to showing that
$\neg G=(B\vee C\vee D)\wedge(B\vee D)\wedge(\neg C\vee\neg D)\wedge\neg B$
is unsatisfiable. The sets of clauses are:



T. A set of formulas is unsatisfiable if $K(M)\vdash_{Res}\varnothing$.
T. The resolution calculus is sound.

6.3 Predicate Logic

D. (Closed Formula) has no free variables. (in same formula)
D. (Rectified Formula) No variable appears free and bounded.
E. (Prenex Form)
$F=\neg\forall x\ \exists y\ P(x,y)\wedge\forall x\ Q(y,x)$ (z is a free variable)
$=\exists x\ \forall y\ \neg P(x,y)\wedge\forall a\ Q(z,a)$
$=\exists x\ \forall y\ \forall a\ \neg P(x,y)\wedge Q(z,a)$
L. $\neg\forall x\ F\equiv\exists x\neg F$ $\quad\neg\exists x\ F=\forall x\neg F$
$\forall xF\wedge\forall xG\equiv\forall x(F\wedge G)$ $\quad\vee$ analog
$\forall x\forall y\ F\equiv\forall y\forall x\ F$ $\quad\exists$ analog

T. (Barber's Paradox) The formula
$F:=\neg\exists x\ \forall y\,(P(y,x)\leftrightarrow\neg P(y,y))$
$=\forall x\ \exists y\,(P(y,x)\leftrightarrow P(y,y))$ (where $x=y$)
is a tautology
C. There exists no set that that contains all sets S that do not contain themselves.
T. The set $\{0,1\}^{\infty}$ is uncountable.
C. There are functions $\mathbb{N}\to\{0,1\}$ that are not computed by any program.

Multiplicative Inverses over Finite Fields

	GF(n)					
	2	3	5	7	11	13
1^{-1}	1	1	1	1	1	1
2^{-1}		2	3	4	6	7
3^{-1}			2	5	4	9
4^{-1}			4	2	3	10
5^{-1}				3	9	8
6^{-1}				6	2	11
7^{-1}					8	2
8^{-1}					7	5
9^{-1}					5	3
10^{-1}					10	4
11^{-1}						6
12^{-1}						12

Irred. Polynomials over GF(2)

1: x, $x+1$

2: x^2+x+1

3: x^3+x+1, x^3+x^2+1

4: x^4+x+1, $x^4+x^3+x^2+x+1$, x^4+x^3+1

5: x^5+x^2+1, $x^5+x^3+x^2+x+1$, x^5+x^3+1, $x^5+x^4+x^3+x+1$, $x^5+x^4+x^3+x^2+1$, $x^5+x^4+x^2+x+1$

over GF(3)

2: x^2+2x+2, x^2+1, x^2+x+2

3: x^3+2x+1, x^3+x^2+x+2, x^3+x^2+2, x^3+2x^2+x+1, x^3+x^2+2x+1, x^3+2x^2+2x+2, x^3+2x+2, x^3+2x^2+1

Multiplication in $GF(2)[x]_{x^2+x+1}$

·	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

L. (Interpolation Property) A polynomial $a(x) \in F[x]$ of degree at mostly d is uniquely determined by any $d+1$ values $a(\alpha_0), \dots, a(\alpha_{d+1}) \in F$ $a(\alpha_i) = \beta_i$ distinct

$$a(x) = \sum_{i=1}^{d+1} \beta_i u_i(x) \qquad u_i(x) = \frac{(x-\alpha_1)\cdots(x-\alpha_{i-1})(x-\alpha_{i+1})\cdots(x-\alpha_{d+1})}{(\alpha_i-\alpha_1)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_{d+1})}$$

Diffie-Hellman:

Agree publicly on (p, g) g = generator p = prime modulus (Key Exchange)

Alice: select x_A at random from $\{0, \dots, p-2\}$

Bob: select x_B at random from $\{0, \dots, p-2\}$

$$y_A = R_p(g^{x_A}) \xrightarrow{y_A} \qquad \xleftarrow{y_B} y_B = R_p(g^{x_B})$$

$$k_{AB} := R_p(y_B^{x_A}) \equiv_p y_B^{x_A} \equiv_p (g^{x_B})^{x_A} \equiv_p (g^{x_A})^{x_B} \equiv_p y_A^{x_B} \equiv_p R_p(y_A^{x_B}) =: k_{BA}$$

RSA: (Crypto System)

Public & Private Key Generation:

1.) Choose two very large primes p and q
2.) Create RSA modulus $N = p \cdot q$
3.) Determine $\varphi(N) = (p-1)\cdot(q-1)$
4.) Choose number e with $1 < e < \varphi(N)$ and $\gcd(e, \varphi(N)) = 1$ (a prime for e is just fine)
5.) Determine d from $e \cdot d \equiv_{\varphi(N)} 1$ with gcd-alg.

⇝ Private-Key: (d, N) of Alice. Public Key: (e, N) of Alice.

Message Exchange:

Now Bob sends to Alice a message $m \in \{1, \dots, n-1\}$

Ciphertext of message = $y = R_N(m^e)$

Decyphering by Alice $m = R_N(y^d)$

(t,n)-Secret-Sharing Scheme among n parties, where t can reconstruct, but $t-1$ can't.

Algebras

1) $\forall a,b,c \in S: a*(b*c) = (a*b)*c$ Associativity
2) $\exists e \in S: \forall a \in S: e*a = a*e = a$ Neutral Element
3) $\forall a \in S \; \exists \hat{a} \in S: a*\hat{a} = \hat{a}*a = e$ Inverses
4) $\forall a,b \in S: a*b = b*a$ Commutativity

(left and right always equal)

1) Magma
1)-2) Monoid
1)-3) Group, Subgroup
1)-4) Commutative/Abelian Group

Ring: $\langle R, +, -, 0\rangle$ add. Abelian Group (ext) $\langle R, \cdot, 1\rangle$ mul. Monoid

Commutative Ring: (ext) $\cdot$ is also commutative

Integral Domain: Non triv. comm. Ring w/o zerodivisors $ab = 0 \Rightarrow a = 0 \vee b = 0$

Field: (ext ⇄ iff finite)
$\langle F; +, -, 0\rangle$ Abelian Group
$\langle F - \{0\}; \cdot, ^{-1}, 1\rangle$ Abelian Group (every non-zero elem. is a unit) i.e. $F^* = F - \{0\}$

Group Theorems:

Left/Right Cancellation Laws:

i) $(\hat{a}) = a$ iii) $a*b = a*c \Rightarrow b = c$
ii) $\widehat{a*b} = \hat{b}*\hat{a}$ iv) $b*a = c*a \Rightarrow b = c$
v) Unique solutions x for $a*x = b$ and $x*a = b$

Subgroup $H \leq G$: $\forall a,b: a*b \in H \wedge e \in H \wedge \hat{a} \in H$

Homomorphism: $\psi: G \to H$ iff 3) $\psi(a \cdot b) = \psi(a) * \psi(b)$
1) $\psi(e_G) = e_H$ 2) $\psi(\hat{a}) = \psi(a)^{-1}$
Isomorphism: bijective Homomorphism

Direct Product of Groups: Operation is component-wise

Ring Theorems:

i) $a0 = 0a = 0$ ii) $(-a)b = -ab$ more than 1 element
iii) $(-a)(-b) = ab$ iv) if R is non-trivial: $1 \neq 0$

Ring Definitions:

$\deg(a(x)\cdot b(x)) \leq \deg(a(x)) + \deg(b(x))$
$\deg(a(x)+b(x)) \leq \max\{\deg a, \deg b\}$ T. $R[x]$ is a ring
Characteristic = $\mathrm{ord}(1)$ in add. group (= 0 if $\mathrm{ord}(1) = \infty$)
Unit: u iff u is invertible
R^* = set of units is a multiplicative Group
def. $\deg(\text{zero polynomial}) = -\infty$

Commutative Ring Definitions:

Divisor a of b: $a|b \Leftrightarrow \exists c: b = ac$
Zerodivisor $a \neq 0$ $b \neq 0$ and $ab = 0$
$\deg(a(x)\cdot b(x)) = \deg(a(x)) \cdot \deg(b(x))$

Theorems:

$a|b \wedge b|c \Rightarrow a|c$
$a|b \Rightarrow a|bc$ for all $c \in R$
$a|b \wedge a|c \Rightarrow a|(b+c)$

Integral Domain Theorems:

D is int. dom. $\Rightarrow D[x]$ is int dom. and $D[x]^* = D^*$ (const. polynomials)
If $a|b$ then $a = bc$ and c is unique $c = \frac{b}{a}$
Every non-zero polynomial of degree d has at most d roots
$b(x)|a(x) \Rightarrow v\cdot b(x)|a(x)$ for all $v \neq 0$ $a(x) = b(x)\cdot c(x) = (v\cdot b(x))(v^{-1}\cdot c(x))$

Field Theorems: (and Defs)

The monic polynomial of highest degree that divides $a(x)$ and $b(x)$ is called the greatest common divisor.
There exist unique $a(x) = b(x)\,q(x) + r(x)$ $\deg(r(x)) < \deg(b(x))$ $b(x) \neq 0$
α is a root iff $(x-\alpha) \mid p(x)$.
A polynomial of deg 2, or 3 is irred. if it has no root.
$\mathbb{Z}_p$ is a field if p is prime
The congruence $\equiv_{m(x)}$ is an equivalence relation and each class has a unique representative of degree less than $\deg(m(x))$
If F has q elements and $\deg(p(x)) = d$, then $|F[x]_{m(x)}| = q^d$
$F[x]_{m(x)}$ is a ring with respect to addition & mult modulo $m(x)$
$F[x]_{m(x)}$ is a field iff $m(x)$ is irreducible
The congruence equation $a(x)\,b(x) \equiv_{m(x)} 1$ has a unique solution iff $\gcd(a(x), m(x)) = 1$
$F^*_{[x]_{m(x)}} = \{a(x) \in F[x] \mid \gcd(m(x), a(x)) = 1\}$

Error-Correcting Codes:

$\mathcal{A}$ Alphabet $|\mathcal{A}| = q$
$E: \mathcal{A}^k \to \mathcal{A}^n$ $k < n$ encoding function (codomain or image of E)
(n,k)-error correcting code C is a subset of card. q^k of $\mathcal{A}^n$
Hamming distance: #positions at which to codewords differ
Minimum Distance = Min. Hamming Distance
$D: \mathcal{A}^n \to \mathcal{A}^k$ decoding function
T. A code C with minimum distance d can correct t errors iff $d \geq 2t+1$, s.t. $D(E(\text{codeword})) = \text{codeword}$
T. Let $\mathcal{A} = GF(q)$ and let $\alpha_0, \dots, \alpha_{n-1}$ be arbitrary distinct elements of $GF(q)$. Consider the encoding function $E(a_0 \dots a_{k-1}) = [a(\alpha_0), \dots, a(\alpha_{n-1})]$ where $a(x)$ is the

STRUCTURE OF GROUPS

Order of a group = $|G|$

order of $a \in G$: the least m s.t. $a^m = e$

Group G

subgroup Def: $a*b \in H \ \forall a,b \in H$; $e \in H$; $\hat{a} \in H \ \forall a \in H$

if $H \leq G$: $\Rightarrow |H| \mid |G|$

$\forall a \in G$: $a^{|G|} = e$

Anti-Inverse: $a^{-1} = a$, $\text{ord}(a) = 2$

G finite $\Rightarrow$ $\forall a \in G$: $\text{ord}(a)$ is finite and $\text{ord}(a) \mid |G|$

Def:
- $a^0 = e$
- $a^n = a \cdot a^{n-1}$ $n \geq 1$
- $a^n = (a^{-1})^n$ $n \leq -1$

$a^m \cdot a^n = a^{m+n}$

$(a^m)^n = a^{m \cdot n}$

if $g \in G$ has finite order: $\forall m \in \mathbb{Z}$: $a^m = a^{R_{\text{ord}(a)}(m)}$

the smallest subgroup containing $a \in G$ = Group generated by a: $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

Cyclic Group: with generator a

if $|G|$ is prime, then G is a cyclic group and every element except e is a generator.

Let $e \in \mathbb{Z}$, e relatively prime to $|G|$ (i.e. $\gcd(e, |G|) = 1$)
The (unique) e-th root of $y \in G$ namely $x^e = y$ can be computed according to $x = y^d$ where $d \equiv_{|G|} e^{-1}$ (multiplicative inverse of e mod $|G|$)

if it has finite order n

$\langle a \rangle \cong \langle \mathbb{Z}_n; \oplus \rangle$

$\Downarrow$ $\langle a \rangle$ is abelian

$\uparrow$ commutative

Thm: $\langle \mathbb{Z}_m^*; \odot, ^{-1}, 1 \rangle$ is a group

cyclic iff $m = 2$, $m = 4$, $m = p^e$ or $m = 2 \cdot p^e$ where p is an odd prime and $e \geq 1$

$\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid \gcd(a, m) = 1\}$

Euler Function: $\varphi(m) = |\mathbb{Z}_m^*|$

(Fermat, Euler): $\forall m \geq 2 \ \forall a \ \gcd(a, m) = 1 : a^{\varphi(m)} \equiv_m 1$

in particular, for every prime p and every a $p \nmid a$: $a^{p-1} \equiv_p 1$

if $m = \prod_{i=1}^{r} p_i^{e_i} \Rightarrow \varphi(m) = \prod_{i=1}^{r} (p_i - 1) \cdot p_i^{e_i - 1}$