Lecture Summary

Contents

Chapter 1: Introduction and Motivation

Chapter 2: Mathematical Reasoning and Proofs

- A **proposition** can be either true or false. If the proposition Is true, it is often called a theorem, a lemma, or a corollary
- A **negation** $\neg A$ is true iff A is false, $\{0,1\} \to \{0,1\}$; a **conjunction (AND)** $A \wedge B$ is true iff both A and B are true, $\{0,1\} \times \{0,1\} \to \{0,1\}$. A **disjunction (OR)** $A \vee B$ is true iff A or B (or both) are true, $\{0,1\} \times \{0,1\} \to \{0,1\}$
- A **formula** is a correctly formed expression involving propositional symbols and logical operator (of propositional logic)
- An **implication** is defined as follows: $A \to B :\Leftrightarrow \neg A \vee B$, i.e. it's only false if A is true and B is false; hence a **two-sided implication** is defined as follows: $A \leftrightarrow B :\Leftrightarrow (A \to B) \wedge (B \to A)$
- Two formulas F, G are (in propositional logic) **equivalent** if they correspond to the same function (table), $F \Leftrightarrow G$ or $F \equiv G$
- A **tautology** is a formula if it is true for all truth assignments of the involved symbols; A formula is called **satisfiable** if it is true for at least one truth assignment, **unsatisfiable** otherwise. F is a tautology iff $\neg F$ is unsatisfiable.
- $F \Rightarrow G :\Leftrightarrow F \to G$ is a tautology; this implication is transitive $F \Rightarrow G$ and $G \Rightarrow H$ then $F \Rightarrow H$; more generally: $F_1 \Rightarrow F_2, F_2 \Rightarrow F_3, \dots, F_{n-1} \Rightarrow F_n$ proves F_n
- Let U be a universe, then a ***k*-ary predicate *P*** is a function P on U with $U^k \to \{0,1\}$, assigning to each list $x_1, \dots x_k$ a value $P(x_1, \dots, x_k)$ which is either 0 (false) or 1 (true). E.g. $\text{less}(x,y) = \begin{cases} 1, & \text{if } x \le y \text{ and } x \ne y \\ 0, & \text{else} \end{cases}$, simpler: $x < y$, or $\text{rational}(c) :\Leftrightarrow \exists m,n (c = m/n \wedge \gcd(m,n) = 1)$
- $\forall, \exists$: $\forall x\, P(x)$ means $P(x)$ is true for all $x \in U$; $\exists x\, P(x)$ means $P(x)$ is true for some $x \in U$ i.e. there exists an $x \in U$ for which $P(x)$ is true
- **Proof patterns**: Modus Ponens (if F and $F \to G$ are tautologies, then G is also a tautology), direct proof of an implication (assume F, derive G from F), indirect proof of an implication (assume $\neg G$ and derive $\neg F$, i.e. prove $\neg G \to \neg F$), proof by contradiction (If $\neg F \to G$ and $\neg G$ are tautologies, then F is also a tautology), existence proof ($\exists x\, P(x)$), inexistence proof ($\neg\exists x\, P(x)$, $\neg\exists\, P(x) \Leftrightarrow \forall x\, \neg P(x)$), b< counterexample ($\neg\forall x\, P(x) \Leftrightarrow \exists x\, \neg P(x)$), induction (basis step: prove $P(0)$, induction step: prove $\forall n \left(P(n) \to P(n+1)\right)$

Rules

- $F \wedge G \Leftrightarrow G \wedge F,\ F \vee G \Leftrightarrow G \vee F$
- $F \wedge (G \wedge H) \Leftrightarrow (F \wedge G) \wedge H \Leftrightarrow F \wedge G \wedge H,\ F \vee (G \vee H) \Leftrightarrow (F \vee G) \vee H \Leftrightarrow F \vee G \vee H$
- $\neg\big(\neg(F)\big) \Leftrightarrow F$
- $\neg(F \vee G) \Leftrightarrow \neg F \wedge \neg G$
- $\neg(F \wedge G) \Leftrightarrow \neg F \vee \neg G$
- $\forall x\, P(x) \wedge \forall x\, Q(x) \Leftrightarrow \forall x \left(P(x) \wedge Q(x)\right),\ \exists\big(P(x) \wedge Q(x)\big) \Rightarrow \exists x\, P(x) \wedge \exists x\, Q(x)$
- $\neg\forall x\, P(x) \Leftrightarrow \exists x \neg P(x),\ \neg\exists x\, P(x) \Leftrightarrow \forall x \neg P(x)$
- $\exists y \forall x\, P(x,y) \Rightarrow \forall x \exists y\, P(x,y)$

Additional Wisdom[1]

- Never draw a conclusion from a the statement to be proven (e.g. $1 < 0$)
- To express even/odd, you can use $\exists k\ n = 2k\ (+1)$
- $\exists y\, \forall x\, P(x,y) \overset{\Rightarrow}{\underset{\Leftarrow}{\neq}} \forall x\, \exists y\, P(x,y)$
- Every square number can be expressed as the sum of two or more other square numbers.
- "iff" means $\Leftrightarrow$ and for a proof both directions need to be proven.

Chapter 3: Sets, Relations, and Functions

- $A = B :\Leftrightarrow \forall x (x \in A \leftrightarrow x \in B)$, the **cardinality** of a set is $|A|$. A set can have predicates $\{x \in A | P(x)\}$
- There is no order in a set, yet **ordered pairs** can exist: $(a,b) = (c,d) :\Leftrightarrow a = c \wedge b = d$

[1] Mostly conclusions from the exercises

- A set A is a **subset** of set B if: $A \subseteq B :\Leftrightarrow \forall x(x \in A \rightarrow x \in B)$; e.g. $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$; $A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$
- $\{\ \}$ or $\emptyset$ is the **empty set**, $\forall A(\emptyset \subseteq A)$; $|\{\emptyset\}| = 1, |\emptyset| = 1, \mathcal{P}(\emptyset) = \{\emptyset\}, |\mathcal{P}(\emptyset)| = 1$
- The **power set** of A is the set of all subsets of A, denoted $\mathcal{P}(A) \coloneqq \{S | S \subseteq A\}$ or 2^A, for $|A| = k, |\mathcal{P}(A)| = 2^k$
- The **union** is defined as $A \cup B \coloneqq \{x | x \in A \vee x \in B\}$, the **intersection** is $A \cap B \coloneqq \{x | x \in A \wedge x \in B\}$; $\cup\mathcal{A} \coloneqq \{x | \exists A \in \mathcal{A}: x \in A\}, \cap\mathcal{A} \coloneqq \{x | \forall A \in \mathcal{A}: x \in A\}$; the **complement** of a set is $\bar{A} \coloneqq \{x \in U | x \notin A\} = A^c$
- The **Cartesian product** of two sets is the set of all ordered pairs with the first component from the first set and the second component from the second set, denoted $A \times B = \{(a, b) | a \in A \wedge b \in B\}, |A \times B| = |A| \cdot |B|$
- **Russell's paradox** $R = \{A | A \notin A\}$
- A **(binary) relation** ρ from a set A to a set B is a subset of $A \times B$. If $A = B$, then ρ is called a relation **on** A; $(a, b) \in \rho$ or $a\ \rho\ b$, e.g. $=, \neq, <, >, \leq, \geq, |, \nmid, a \equiv_m b \Leftrightarrow a - b = km$ for some k; the **identity relation** is $\mathrm{id} = \{(a, a) | \in A\}$; relations can be represented as a matrix $M^{\rho}_{|A| \times |B|}$ or with a directed graph with $|A| + |B|$ vertices; the **inverse** of a relation $\hat{\rho}$ is defined as $a\ \rho\ b \Leftrightarrow b\ \hat{\rho}\ a$; the **composition** is denied as $a\ \rho \circ \sigma\ c \Leftrightarrow a\ \rho\sigma\ c :\Leftrightarrow \exists b \in B: (a\ \rho\ b \wedge b\ \sigma\ c)$, the n-fold of ρ is denoted ρ^n
- The following properties may exist on relations: **reflexive**: $a\ \rho\ a\ \forall a \in A$, i.e. $id \subseteq \rho$, **irreflexive** $a\ \not\rho\ a\ \forall a \in A$[2], **symmetric** $\rho = \hat{\rho}$ i.e. $a\ \rho\ b \Leftrightarrow b\ \rho\ a$, **antisymmetic** $\rho \cap \hat{\rho} \subseteq \mathrm{id}$ i.e. $a\ \rho\ b \wedge b\ \rho\ a \Rightarrow a = b$, **transitive** $a\ \rho\ b \wedge b\ \rho\ c \Rightarrow a\ \rho\ c$ (ρ is transitive iff $\rho^2 \subseteq \rho$).
- The **transitive closure** denoted ρ^* is $\rho^* = \bigcup_{n=1}^{\infty} \rho^n$
- An **equivalence relation** is reflexive, symmetric and transitive. For an equivalence relation θ on a set A, the set of elements of A that are equaivalent to $a \in A$ is called **equivalence class** of a and is defined as: $[a]_\theta \coloneqq \{b \in A | b\ \theta\ a\}$, e.g. of the relation $\equiv_3$: $[0] = \{\dots, -6, -3, 0, 3, 6, \dots\}, [1] = \{\dots, -5, -2, 1, 4, 7, \dots\}, [2] = \{\dots, -4, -1, 2, 5, \dots;$. The intersection of the equivalence relation is also an equivalence relation, e.g. $\equiv_3 \cap \equiv_5 = \equiv_{15}$
- A **partition** is a set of mutually disjoint subsets that cover the set i.e. $S_i \cap S_j = \emptyset$ for $i \neq j$, $\bigcup_{i \in I} S_i = A$; The set A/θ of equivalence classes of θ on A is a partition of A and denoted by $A/\theta \coloneqq \{[a]_\theta\ a \in A\}$ and is called the quotient set or $A \bmod \theta$; e.g. $\mathbb{Q} = \mathbb{Z} \times (\mathbb{Z} - \{0\})/\sim$ where $(a, b) \sim (c, d) :\Leftrightarrow ad = bc$
- A **partial order** on a set is a reflexive, antisymmetric and transitive relation. A set with a partial order is called **poset**, denoted as $(A; \preccurlyeq)$; if $a \preccurlyeq b$ or $b \preccurlyeq a$ the two elements are called **comparable** otherwise incomparable; if any two elements of a poset are comparable, then the poset is called **totally ordered** by $\preccurlyeq$; a poset is **well-ordered** if it is totally ordered and if ever non-empty subset of the poset has a least element
- The **Hasse diagram** of a (finite) poset is the directed graph whose vertices are labelled with the elements and where there is an edge from a to b iff b covers (i.e. $a \prec b$ and $\nexists c: a \prec c$ and $c \prec b$) a
- A totally ordered subset $C \subseteq A$ of a poset is called a **chain**; the subset $B \subseteq A$ of a poset is called an **antichain** if any two distinct elements in B are incomparable
- For given posets $(A, \preccurlyeq), (B, \sqsubseteq)$ the relation $\leq$ defined on $A \times B$ by $(a_1, b_1) \leq (a_2, b_2) :\Leftrightarrow a_1 \preccurlyeq a_2 \wedge b_1 \sqsubseteq b_2$ is a partial order relation.
- **Special elements in poset** $a \in S$ is aminimal (maximal) element of $S \subseteq A$ if there exsists no $b \in S$ with $b \prec a$ ($b \prec a$); $a \in S$ is the least (greatest) element of S if $a \preccurlyeq b$ ($a \succcurlyeq b$) for all $b \in S$; $a \in S$ is a lower (upper) bound iof S if $a \preccurlyeq b$ ($a \succcurlyeq b$) for all $b \in S$; $a \in S$ is the greatest lower bound (least upper bound) of S if a is the greatest (least) element of the set of all lower (upper) bounds of S
- If two elements a, b in a poset have a greates lower bound, then it is called the **meet** of a and b, $a \wedge b$. If the two elements have a least upper bound, it is called the **join**, $a \vee b$.; a poset in which very pair of elements has a meet and a joins is called a **lattice**.
- A **function** $f: A \rightarrow B$ is from a domain to a codomain is a relation on $A \times B$, i.e. $f \subseteq A \times B$ with the special properties: totally defined: $\forall a \in A\ \exists b \in B\ \ a\ f\ b$, well deinfed: $a\ f\ b \wedge a\ f\ b' \Rightarrow b = b'$; if the property of totally defined is dropped, it is called a **partial** function; the **image** of $S \subseteq A$ under f, denoted $f(S)$ is the set $\mathrm{Im}\ f = f(S) \coloneqq \{f(a) | a \in S\}$; the **inverse image e(preimage** of $T \subseteq B$, is $f^{-1} \coloneqq \{a \in A | f(a) \in T\}$; **properties**: injective: $a \neq b \Rightarrow f(a) \neq f(b)$ (no collisions), surjective (onto): $\forall b \in B, b = f(a)$ for some $a \in A$ i.e. $f(A) = B$ (every value in the codomain is taken on for some argument), bijctive if it is both injective and surjective; $(h \circ g) \circ f = h \circ (g \circ f)$

Rules

[2] $\not\rho$ actually means "not ρ", I just can't input here

- $\{a\} = \{b\} \Leftrightarrow a = b$
- **Theorem 3.3** Sets A, B, C: indmepotence $A \cap A = A = A \cup A$, commutativity $A \cup B = B \cup A, A \cap B = B \cap A$, associtaitivty $A \cap (B \cap C) = (A \cap B) \cap C, A \cup (B \cup C) = (A \cup B) \cup C$, absorption $A \cap (A \cup B) = A, A \cup (A \cap B) = A$, distibutitvity $A \cap (B \cup C) = (A \cap B) \cup (A \cap C), A \cup (B \cap C) = (A \cup B) \cap (B \cup C)$, complemntarity $A \cap \bar{A} = \emptyset, A \cup \bar{A} = U$, consistency $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$

Additional Wisdom

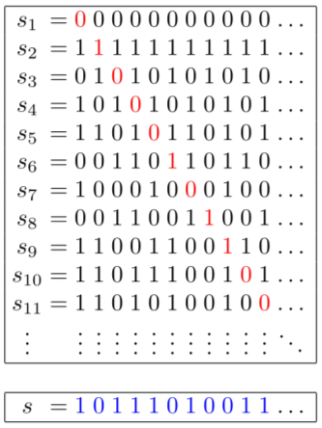
- $\emptyset \times A = \emptyset, |\emptyset \times A| = 0, \ \mathcal{P}(\emptyset) = \{\emptyset\}, |\mathcal{P}(\emptyset)| = 1$
- $A \subseteq B \Leftrightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$
- A set with n elements, hs (at most) $2^{n(n-1)}$ reflexive relations
- Composition of relations: http://math.stackexchange.com/questions/107988/relations-binary-composition, takeaway: to get ρ^2, square the adjacency matrix

Chapter 4: Combinatorics and Counting

- $\forall i, j, 1 \leq i < j \leq n: A_i \cap A_j = \emptyset \Rightarrow |A_1 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i|$ and $|A_1 \times \ldots \times A_n| = \prod_{i=1}^{n} |A_i|$; for non-disjoint sets: $|A \cup B| = |A| + |B| - |A \cap B|$ more generally: $|A_1 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i_1 < 1_2 \leq n} |A_{i_1} \cap A_{i_2}|$

	Ordered	**Unordered**
With repetition	n^k	$\binom{n+k-1}{k}$
Without repetition	$\frac{n!}{(n-k)!}$	$\binom{n}{k} \coloneqq \frac{n!}{k!\,(n-k)!}$

- **Double-counting principle** to count $S \subseteq A \times B$, $|S| = \sum_{a \in A} m_a = \sum_{b \in B} n_b$
- **Pigeon-Hole principle** If a set of n objects is partitioned into $k < n$ sets, then at least one of these sets contains at least $\left\lceil \frac{n}{k} \right\rceil$ objects
- $\binom{n}{k} = \binom{n}{n-k}; n > 0: \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$; **binomial theorem**: $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k, \sum_{k=0}^{n} \binom{n}{k} = 2^n, \sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0, \binom{m+n}{k} = \sum_{i=0}^{k} \binom{m}{i} \binom{n}{k-i}, \binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$
- Two sets have the same **cardinality**, denoted $A \sim B$, if a bijection $A \to B$ exists; the cardinality of B is at least the cardinality of A, dnoted $A \preccurlyeq B$, if $A \sim C$ for some subset $C \subseteq B$; B **dominates** A, dnoted $A \prec B$, if $A \preccurlyeq B$ and $A \not\sim B$; a set A is called **countable** if $A \preccurlyeq \mathbb{N}$ and **uncountable** otherwise; A set is countable iff it is finite or if $A \sim \mathbb{N}$; the set $\{0,1\}^* \coloneqq \{\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, \ldots\}$ of finite binary sequences is countable; the set $\mathbb{N} \times \mathbb{N} (= \mathbb{N}^2)$ of ordered pairs of natural numbers is countable, more generally for two countable sets their cartesian product is countable, i.e. $A \preccurlyeq \mathbb{N} \wedge B \preccurlyeq \mathbb{N} \Rightarrow A \times B \preccurlyeq \mathbb{N}$; $\mathbb{Q}$ is cuotanble; $\mathbb{R}$ is uncountable and such is the interval $[0,1)$; for countable sets A, A_1, A_2 the following hold: for any $n \in \mathbb{N}$, the set A^n of n-tuples over A is countable, the union $A_1 \cup A_2 \cup \ldots$ of a countable list of countable sets is countable, the set A^* of finite sequences over A is countable; $\{0,1\}^\infty$ is uncountable which can b proven using Cantor's diagonalization argument (*aside*)



- $\sim$ is an equivalence relation; $\preccurlyeq$ is transitive; $A \subseteq B \Rightarrow A \preccurlyeq B$; a subset of countbale set us also countable $A \subseteq B \wedge B \preccurlyeq \mathbb{N} \Rightarrow A \preccurlyeq \mathbb{N}$; $A \preccurlyeq B \wedge B \preccurlyeq A \Rightarrow A \sim B$; for two sets A, B exctly one of $A \prec B, A \sim B, B \prec A$ holds
- $A \not\preccurlyeq \mathbb{N} \wedge A \preccurlyeq B \Rightarrow B \not\preccurlyeq \mathbb{N}$,in particular, if a subset of B is uncountable, then so is B; if A is countable, B is countable, then $A - B$ is uncountable

Chapter 5: Graph Theory

- A **graph** $G = (V, E)$ consists of a finite set V of **vertices** and a set $E \subseteq \{\{u, v\} \subseteq V | u \neq v\}$ of **edges**. A simple graph doesn't contain any loops, a graph with multiple edge between two vertices is called a multigraph.
- The **neighborhood** of a vertex is the set $\Gamma(v) \coloneqq \{u \in V | \{u, v\} \in E\}$, the **degree** is the number of edge (or vertices) connected do a vertex, $\deg v \coloneqq |\Gamma(v)|$; a graph is called k-regular if $\deg v = k$ for all vertices; A **directed** graph consists of a finite set of vertices V and a set of (directed) edges $E \subseteq V \times V$; the **in-degree** is the number of edges

entering a vertex, $\deg^- v$, the **out-degree** the number of edges leaving a vertex, $\deg^+ v$; in a directed graph: $\sum_{(v \in V)} \deg^- v = \sum_{v \in V} \deg^+ v = |E|$

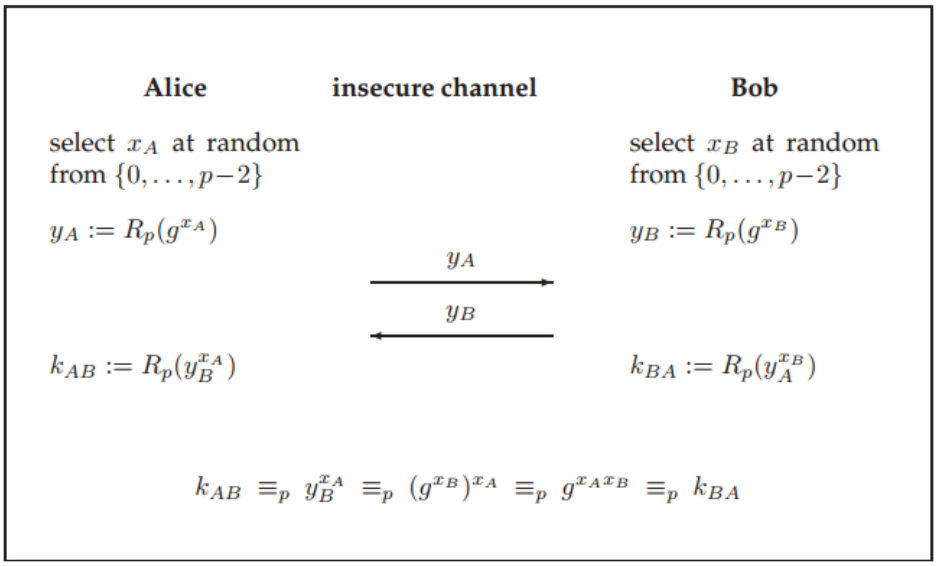
- A graph $G = (V, E)$ is a **subgraph** of a graph $H = (V', E')$, sometimes denoted $G \sqsubseteq H$ if $V \subseteq V'$ and $E \subseteq E'$; the **union** of two graphs is the graph $G \cup G \coloneqq (V \cup V', E \cup E')$; the **complement** is the graph $\bar{G} = (V, \bar{E})$
- A graph is **bipartite** if V can be split into two disjoint sets $V_1, V_2; V = V_1 \cup V_2$, such that no edge connects two vertices in the same subset $V_i (i = 1,2)$.
- The **adjacency matrix** $A_G = [a_{ij}]$ of an undirected (if the graph is directed, replace $\{v_i, v_j\}$ by (v_i, v_j)) graph is the binary $n \times n$ matrix where $a_{i,j} = \begin{cases} 1, & if\ \{v_i, v_j\} \in E \\ 0, & \text{otherwise} \end{cases}$
- Two graphs are **isomorphic**, $G \cong H$, if a bijection $\pi: V \to V'$ exists, such that renaming the vertices of G accorindg to π results in H, i.e. if $\{u, v\} \in E \Leftrightarrow \{\pi(u), \pi(v)\} \in E'$; A graph is **contained** in a graph, $G \preccurlyeq H$, if a subprah K of H exists which that is isomorphic to G: $G \preccurlyeq H: \Leftrightarrow \exists K (G \cong K \wedge K \sqsubseteq H)$
- A **complete** graph of n vertices, K_n, is a simple graph in which any pair of vertices is connected and is $(n-1)$-regular, $G \preccurlyeq K_n$; a $(\boldsymbol{m}, \boldsymbol{n})$**-mesh** is a graph $M_{m,n}$ on mn vertices with $V = \{(i,j) | 1 \leq i \leq m, 1 \leq j \leq n\}$ where $(i,j), (i',j')$ are connected iff $i = i'$ and $|j - j'| = 1$ or $j = j'$ and $|i - i'| = 1$; a **path** P_n consists of $n+1$ vertices connected like a chain, $V = \{v_0, \dots, v_n\}, E = \{\{v_0, v_1\}, \{v_2, v_3\}, \dots \{v_{n-1}, v_n\}\}$; a **cycle** $C_n, n \geq 3$ conists of n vertices connect cyclicaccly; a $\boldsymbol{d}$**-dimensional hypercube** Q_d is a graph on $V = \{0,1\}^d$ with $\{u, v\} \in E$ iff u, v differ in exactly one bit; a **complete bipartite graph** $K_{m,n}$ has $m + n$ verices, $K_{m,n} = (V, E), V = B \cup W, B \cap W = \emptyset, |B| = m, |W| = n, E = \{\{u, v\} | u \in V \wedge v \in W\}$
- A **walk** of length n from u to v is a sequence of vertices such that consecutive vertices are connected, if all the vertices are distinct, then a walk is called a **path** if all the edges (but not necessarily the vertices) in the walk are distinct, it is called a **tour**, when starting and endpoint are identical, then a path of length ≥ 3 is called a **cycle** and a tour is called a **circuit**; an undirected d graph is **connected** of any two vertices are connect by a path; the maximal connect subgraphs of a graphs are called the **components**
- A cycle in a graph that visits all vertices is called **Hamiltonian** and if such a cycle exists, the graph is called **Hamiltonian**; A graph for which $|V| \geq 3,\ \deg u + \deg v \geq |V|$, every non-adjacent pair of vertices is Hamiltonian, in particular of $\deg v \geq |V|/2$ for all $v \in V$ it is Hamiltonian; $Q_d, d \geq 2$ is Hamiltonian; a Hamiltonian cycle in a hypercube is called a **Gray code**
- A **tree** is an undirected connected graph with no cycles. A **forest** is an undirected graph with no cycles, i.e. the union of several disjoint vertex sets. A **leaf** is a vertex with degree 1; a tree with $n \geq 2$ vertices has at least 2 leaves; for a graph G with n vertices, the following statements are equivalent: G is a tree, G has $n-1$ edges and is acyclic, G has $n-1$ edge and is connected; a **spanning tree** of a connected graph G is a subgraph of G which is a tree and ontians all vertices of G;
- A **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 of a leaf from the root. The vertices on the path from the root to v are called ancestors of v. The ancestor which is a neighbor of v is called the parent, and v is called a child of the parent. A rooted tree is a d-ary tree if every vertex has at most d children.
- A graph is **planar** if it can be drawn in the plane with no edges crossing. By drawing the graph, the plane is divided into disjoint **regions** (one being infinite). The **degree** of a region is the number of edges one encounters in a walk around the region0s boundary (it the edge is a bridge, it is counted twice); **Euler's formula** a plane drawing of a connected graph divides the plane into $r \coloneqq |E| - |V| + 2$ regions; for any connected plane graph, the sum of the degrees of the regions is equal to $2|E|$; every connected planar graph with $|V| \geq 3$ satifies $|E| \leq 3|V| - 6$, of the graph is bipartite $|E| \leq 2|V| - 4$; K_n is planar iff $n \leq 4$; $K_{3,3}$ is not planar
- If any (or a sequence thereof) of deletion of edge, deletion of singleton vertices or neighboring vertices is performed on a graph G and the resulting graph H is non-planar, then G is non-planar.
- A **polyhedron** is a solid bounded by a finite number of (plane) polygon faces. The vertices and edges of these polygons 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 $m, n \geq 3$ each vertex meets exactly m faces (and hence m edges) and each face is a regular n-gon; There are exactly five regular polyhedral, $(m, n) = (3,3), (4,3), (3,5), (5,3)$

Chapter 6: Number Theory

- For integers a, b with $a \neq 0$ we say that a **divides** b, denoted $a \mid b$, if there exists an integer c such that $b = ac$. In this case, a is called a **divisor** or **factor** of b and b is called a **multiple** of a. The (unique) integer c is called the **quotient** when b is divided by a, and we write $c = \frac{b}{a}$ or $c = b/a$. We write $a \nmid b$ if a does not divide b.
- **Euclid** for all integers $a, d, d \neq 0$ unique integers q, r exists to satify: $a = dq + r,\ 0 \leq r < |d|$; the remainder r is often denoted $R_d(a)$ or $a \bmod d$: the set of possible nonnegative remainders: $S \coloneqq \{s | s \geq 0 \text{ and } a = dt + s \text{ for some } t \in \mathbb{Z}\}$
- For $a \neq 0, b \neq 0$, d is called a **greatest common divisor** of a, b if d divides both a, b and if every common divisor of a, b divides d, i.e. $d \mid a, d \mid b,$ and $c \mid a \wedge c \mid b \Rightarrow c \mid d$; the unique positive greatest common divisor is often denoted $\gcd a, b$, if $\gcd a, b = 1$, a, b are called **relatively prime**; for $a, b \in \mathbb{Z}$ the **ideal** generated by a, b, denoted (a, b) is the set $(a, b) \coloneqq \{ua + vb | u, v \in \mathbb{Z}\}$, $(a) \coloneqq \{ua | u \in \mathbb{Z}\}$ and $d \in \mathbb{Z}$ exists such that $(a, b) = (d)$, in that case d is the greatest common divisor; $u, v \in \mathbb{Z}$ exist such that $\gcd a, b = ua + vb$
- Aside: (extended) Euclid's gcd-algorithm

```
σ1 := a; σ2 := b;
u1 := 1; u2 := 0;
v1 := 0; v2 := 1;
while σ2 > 0 do begin
    q := σ1 div σ2;
    r := σ1 − qσ2;
    σ1 := σ2; σ2 := r;
    t := u2; u2 := u1 − qu2; u1 := t;
    t := v2; v2 := v1 − qv2; v1 := t;
end;
d := σ1; u = u1; v := v1;
```

- An integer $p > 1$ is **prime** if the only positive divisor are 1 and p, otherwise it is called **composite**; 1 is neither prime nor composite; if p is a prime which divides the product of $x_1 x_2 \ldots x_n$ of some integer $x_1, \ldots, x_n$ then p divdes one of them, $p \mid x_i$ for some $i \in \{1, \ldots, n\}$; every positive integer can be written uniquely as the product of primes.
- Unless n is square ($n = c^2$ for some $c \in \mathbb{Z}$), $\sqrt{n}$ is **irrational**
- The **least common multiple** l of a, b, denoted $l = \operatorname{lcm} a, b$, is the common multiple of a, b which dives eery common mutple of a, b, i.e. $a \mid l, b \mid l, l > 0$ and $a \mid l' \wedge b \mid l' \Rightarrow l \mid l'$
- $a = \prod_i p_i^{e_i}, b = \prod_i p_i^{f_i}$, $\gcd a, b = \prod_i p_i^{\min e_i, f_i}, \operatorname{lcm} a, b = \prod_i p_i^{\max e_i, f_i}, \gcd a, b \cdot \operatorname{lcm} a, b = ab$
- There are infinitely many primes while gaps between primes can be arbitrarily large; the **prime counting function** $\pi: \mathbb{R} \to \mathbb{N}$ is defined as follows: for any real $x, \pi(x)$ is the number of primes $\leq x$, $\lim_{x \to \infty} \frac{\pi(x) \ln x}{x} = 1$
- For $a, b, m \in \mathbb{Z}, m \geq 1$, a is **congruent** to b **modulo** m if m divides $a - b$. $a \equiv b \pmod m$ or $a \equiv_m b$, i.e. $a \equiv_m b \coloneqq \Leftrightarrow m \mid (a - b)$; $a = b \Rightarrow a \equiv_m b\ \forall m$; $m \geq 1, \equiv_m$ is an equivalence relation on $\mathbb{Z}$; if $a \equiv_m b,\ c \equiv_m d$ then $a + c \equiv_m b + d$ and $ac \equiv_m bd$
- There are m equivalence classes of the equivalence relation $\equiv_m$, namely $[0], [1], \ldots [m - 1]$. Each equivalence class $[a]$ has a natural representative $R_m(a) \in [a]$ in the set $\mathbb{Z}_m \coloneqq \{0, \ldots, m - 1\}$ of remainders modulo m; for any $a, b, m \in \mathbb{Z}, m \geq 1$: $a \equiv_m R_m(a), a \equiv_m b \Leftrightarrow R_m(a) = R_m(b)$ and $R_m(a + b) = R_m\big(R_m(a) + R_m(b)\big), R_m(ab) = R_m\big(R_m(a) \cdot R_m(b)\big)$
- $ax \equiv_m 1$ has a solution $x \in \mathbb{Z}_m$ iff $\gcd a, m = 1$ which is unique and is called the **multiplicative inverse** of a module m, $x \equiv_m a^{-1}$ or $x \equiv_m 1/a$
- **The Chinese Remainder Theorem**: Let $m_1, m_2, \ldots, m$ be pairwise relatively prime integers and let $M = \prod_{i=1}^{r} m_i$. For every list $a_1, \ldots, a_r$ with $0 \leq a_i < m_i$ for $1 \leq i \leq r$, the system of congruence equations
  $x \equiv_{m_1} a_1$
  $x \equiv_{m_2} a_2$
  $\ldots$
  $x \equiv_{m_r} a_r$
  for x has a unique solution x satisfying $0 \leq x < M$



– Figure 6.2: The Diffie-Hellman key agreement protocol.

Additional Wisdom

- Square numbers have an odd amount of divisors, since their square root doesn't get a partner.
- The set of prime numbers is uncountable and has some nice properties.

Chapter 7: Algebra

- An **operation** on a set S is a function $S^n \to S$ where $n \geq 0$ is called the **arity** of the operation; an **algebra** is a pair$\langle S;\Omega\rangle$ where S is a set (the **carrier** of the algebra) and $\Omega = (\omega_1, \dots, \omega_n)$ is a list of operations on S; e.g. $\langle \mathbb{Z};+,-,0,\cdot,1\rangle \leftrightarrow \langle \mathbb{Z};+,\cdot\rangle, \langle \mathbb{Z}_m;\oplus\rangle, \langle \mathbb{Z};\odot\rangle, \langle \mathcal{P}(A);\cup,\cap,\bar{}\,\rangle$
- $\langle S;*\rangle$ can have (1) neutral elements, (2) associativity, and (3) inverse elements (and any combination)
- A left (right) **neutral element** (or **identity element**) of an algebra $\langle S;*\rangle$ is an element $e \in S$ such that $e * a = a$)$a * e = a$) for all $a \in S$ If $e * a = a * e = a$ for all $a \in S$, then e is simply called neutral element; if the operation is called addition, e is usually denoted as 0 and 1 if it's called multiplication; if $\langle S;*\rangle$ has a left and a right neutral element, then they're equal. $\langle S;*\rangle$ can have at most one neutral element.
- A binary operation $*$ on a set is **associative** if $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$; a **semigroup** is an algebra where $\langle S;*\rangle$ where $*$ is associative; e.g. (shorthand) $\langle \begin{matrix}\mathbb{Z}\\ \mathbb{Q}\\ \mathbb{R}\end{matrix}; \overset{+}{\cdot}\rangle, \langle \mathbb{Z}_m; \begin{matrix}\oplus\\ \odot\end{matrix}\rangle$
- A **monoid** is an algebra $\langle M;*,e\rangle$ where $*$ is associative and e is the neutral element, e.g. (shorthand) $\langle \begin{matrix}\mathbb{Z}\\ \mathbb{Q}\\ \mathbb{R}\end{matrix}; \begin{matrix}+ & 0\\ \cdot & 1\end{matrix}\rangle, \langle \mathbb{Z}_m; \begin{matrix}\oplus & 0\\ \odot & 1\end{matrix}\rangle$
- A left (right) **inverse element** of an element a in an algebra $\langle S;*,e\rangle$ is an element $b \in S$ such that $b * a = e$ ($a * b = e$). If $b * a = a * b = e$, then b is simply called an inverse of a. If both inverses exist, they are equal and a has at most one inverse
- A **group** is an algebra $\langle G,*\rangle$ (more precisely $\langle G;*, \hat{}\,, e\rangle$) satisfying the following axioms: G1: $*$ is associative, G2: there exists a (neutral) element e such that $a * e = e * a = a$ for all $a \in G$, G3: every $a \in G$ has an inverse element $\hat{a}$, i.e. $a * \hat{a} = \hat{a} * a = e$; for multiplication the inverse is written as a^{-1} or $1/a$, for addition – a.
- A group (or monoid or semigroup) is called **commutative** or **abelian** if $a * b = b * a$ for all $a, b \in G$; For a group $\langle G;*, \hat{}\,, e\rangle$ the following hold for all $a, b, c \in G$: $\widehat{(\hat{a})} = a$, $\widehat{a * b} = \hat{b} * \hat{a}$, left cancellation $a * b$)$a * c \Rightarrow b = c$, right cancellcation $b * a = c * a \Rightarrow b = c$, the equation $a * x = b$ has a unique soltion x for any a, b and so does the equation $x * a = b$
- A homomorphism is a structure-preserving map from one algebraic system to another; for two compatible algebras $\langle S;\Omega\rangle$ and $\langle S';\Omega'\rangle$ a function $\psi: S \to S'$ is called a **homomorphism** from $\langle S;\Omega\rangle$ to $\langle S';\Omega'\rangle$ if for every $\omega \in \Omega$ (of arity n) and corresponding $\omega' \in \Omega'$ (also of arity n) $\psi\big(\omega(a_1, \dots, a_n)\big) = \omega'\big(\psi(a_1), \dots, \psi(a_n)\big)$ for every $a_1, \dots, a_n \in$

S; e.g. $\psi: a \mapsto R_m(a)$ from $\mathbb{Z}$ to $\mathbb{Z}_m$; a mapping ψ from a group $\langle G;*, \widehat{\ }, e\rangle$ to a group $\langle G',\star, \widehat{\ }, e'\rangle$ is, by definition, a homomorphism if: $\psi(e) = e'$ and $\psi(\hat{a}) = \widehat{\psi(a)}$ for all a and $\psi(a * b) = \psi(a) \star \psi(b)$ for all a, b

- A bijective homomorphism is called an **isomorphism** and the two algebras are called **isomorphic**, $\langle S; \Omega\rangle \cong \langle S'; \Omega'\rangle$ if such an isomorphism exists; Isomorphic structures are identical from an algebraic viewpoint, differing only in the naming of the elements. All structural properties, not referring to the naming of the elements, are identical. In other words, both structures contain the same mathematical truth; e.g. $\langle \mathbb{Z}_6;\oplus\rangle \times \langle \mathbb{Z}_{10};\oplus\rangle \cong \langle \mathbb{Z}_2;\oplus\rangle \times \langle \mathbb{Z}_{30};\oplus\rangle$
- The **direct product** of n groups is the algbra $\langle G_1 \times \ldots \times G_n;\star\rangle$ where the operation $\star$ is component wise: $(a_1, \ldots, a_n) \star (b_1, \ldots, b_n) = (a_1 *_1 b_1, \ldots, a_n *_n b_n)$; in this group the neutral element and the inversion operation are component-wise in the respective groups
- A subset H of a group $\langle G;* \widehat{\ }, e\rangle$ is called a **subgroup** of G, denoted $G \leq G$ if $\langle H;*, \widehat{\ }, e\rangle$ is a group, i.e. if H is closed with respect to all operations: $a * b \in H$ for all $a, b \in H$ and $e \in H$ and $\hat{a} \in H$ for all $a \in H$; the trivial subgroups are $\{e\}$ and G itself; subgroups of $\mathbb{Z}_{12}$: $\{0\}, \{0,6\}, \{0,4,8\}, \{0,3,6,9\}, \{0,2,4,6,8,10\}$
- The **order** of a, $\operatorname{ord} a$, is the least $m \geq 1$ such that $a^m = e$, if m doesn't exists, $\operatorname{ord} a = \infty$, $\operatorname{ord} e = 1$; if $\operatorname{ord} a = 2$ then $a^{-1} = a$ and a is a self-inverse; e.g. $\operatorname{ord} a = \infty \ \forall a \in \langle \mathbb{Z} - \{0\}; +\rangle$; for a finite group, $|G|$ is called the **order** of G; in a finite group, every element has a finite order
- The smallest subgroup of a group containing the element $a \in G$ is the **group generated by a**, denoted $\langle a\rangle$, defined as $\langle a\rangle := \{a^n \mid n \in \mathbb{Z}\}$, if the group is finite $\langle a\rangle := \{e, a, a^2, \ldots, a^{\operatorname{ord} a - 1}\}$. This generated group is called **cyclic** and g is called a **generator** of G ($G = \langle g\rangle$). If g is a generator, so is g^{-1}; e.g. $\langle \mathbb{Z}, +, -, 0\rangle$, $\langle \mathbb{Z}_n, \oplus\rangle$
- A cyclic group of order n is isomorphic to $\langle \mathbb{Z}_n, \oplus\rangle$ (and hence abelian)
- **Lagrange** G finite, $H \leq G$: the order of H divides the order of G, i.e. $|H|$ divides $|G|$
- For a finite group, the order of every element divides the group order, $\operatorname{ord} a$ divides $|G|$ for every $a \in G$; G finite, $a^{|G|} = e$ for every $a \in G$; every group of prime order is cyclic and in such a group every element except the neutral element is a generator
- $\mathbb{Z}_m^* := \{a \in \mathbb{Z}_m \mid \gcd a, m = 1\}$; $\varphi: \mathbb{Z}^+ \to \mathbb{Z}^+, \varphi(m) = |\mathbb{Z}_m^*|$; e.g. $\mathbb{Z}_{18}^* = \{1,5,7,11,13,17\}, \varphi(18) = 6$; p prime: $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$; if $m = \prod_{i=1}^{r} p_i^{e_i} = \prod_{\substack{p \mid m \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$, then $\varphi(m) = \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1}$; $\langle \mathbb{Z}_m^*; \odot, ^{-1}, 1\rangle$is a group
- For all $m \geq 2$ and all a with $\gcd a, m = 1$, $a^{\varphi(m)} \equiv_m 1$, in particular for every prime p and every a is not divisible by p, $a^{p-1} \equiv_p 1$
- Let G be some finite group, $e \in \mathbb{Z}$ a given exponent relatively prime to $|G|$. The (unique) e-th root of $y \in G$, namly $x \in G$ satisfying $x^3 = y$ can be computed according to $x = y^d$ where d is the multiplicative inverse of $e \bmod |G|$, i.e. $d \equiv_{|G|} e^{-1}$

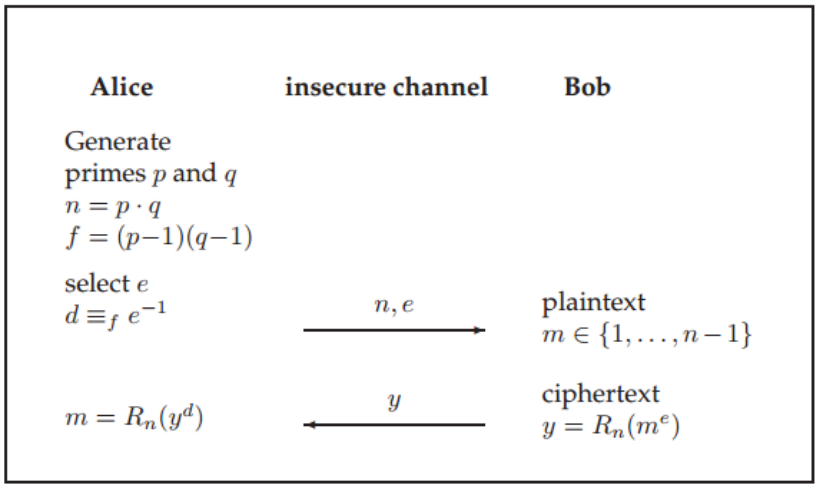


Figure 7.1: The RSA public-key cryptosystem. Alice's public key is the pair (n, e) and her secret key is d. The public key must be sent to Bob via an authenticated channel. Bob can encrypt a message, represented as a number in $\mathbb{Z}_n$, by raising it to the eth power modulo n. Alice decrypts a ciphertext by raising it to the dth power modulo n.

- A **ring** $\langle R; +, -, 0, \cdot, 1\rangle$ is an algebraic system for which $\langle R; 1, -, 0\rangle$ is an abelian group and $\langle R; \cdot, 1\rangle$ is a monoid and $a(b+c) = ab + ac$ and $(b+c)a = ba + ca$ for all $a, b, c \in R$ (left and right distributive laws). A ring is called **commutative** if multiplication is commutative ($ab = ba$); e.g. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \langle \mathbb{Z}_m; \oplus, \ominus, 0, \odot, 1\rangle$; for any ring $\langle R; +, -, 0, \cdot, 1\rangle$: $0a = a0 = 0$ for all $a \in R$, $(-a)b = -ab$, $(a)(-b) = ab$, if R is non-trivial (i.e. more than one element), then $1 \neq 0$; in any commutative ring: if $a \mid b$ and $b \mid c$, then $a \mid c$, if $a \mid b$ then $a \mid bc$, if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$
- An element $a \neq$ of a commutative ring R is called a **zerodivisor** if $ab = 0$ for some $b \neq 0$ in R
- An element u of a ring R is called a **unit** if u is invertible, i.e. if $uv = vu = 1$ for some $v \in R$ ($v = u^{-1}$). The sets of units of R is denoted by R^*; e.g. $\mathbb{Z}^* = \{-1, 1\}, \mathbb{R}^* = \mathbb{R} - \{0\}, \mathbb{Z}_m = \mathbb{Z}_m^*$, for $\mathbb{Z}_m$ every non-zero element is either a unit or a zerodivisor; for a ring R, R^* is a multiplicative group; An **integral domain** is a nontrivial commutative ring without zerodivisors: $ab = 0 \Rightarrow a = 0 \vee b = 0$; e.g. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
- A **polynomial** $a(x)$ over a ring R in the indeterminate x is a formal expression of the form $a(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{d} a_i x^i$ for some non-negative integer d. The degree $\deg a(x)$ is the greatest i for which $a_i \neq 0$. The spaical polynomial 0 is dened to have degree "minus infinity". Let $R[x]$ denote the set of polynomial in x over R and is a ring.
- $a(x) + b(x) = \sum_{i=0}^{\max d,d'} (a_i + b_i)x^i$ and $a(x)b(x) = \sum_{i=0}^{d+d'} \left(\sum_{(k=0)}^{i} a_k b_{i-k}\right) x^i = \sum_{i=0}^{d+d'} (\sum_{u+v=i} a_u b_v) x^i = a_d b'_d x^{d+d'} + \cdots + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + (a_0 b_1 + a_1 b_0)x + a_0 b_0$;
  e.g. $a(x) = 2x^2 + 3x + 1, b(x) = 5x + 6, a(x) + b(x) = 2x^2 + (3+5)x + (1+6) = 2x^2 + x, a(x)b(x) = (2 \cdot 5)x^3 + (3 \cdot 5 + 2 \cdot 6)x^2 + (1 \cdot 5 + 3 \cdot 6)x + 1 \cdot 6 = 3x^3 + 6x^2 + 2x + 6$
- If D is an integral domain, then so is $D[x]$ and the units are the constant polynomials which are units of D, i.e. $D[x]^* = D^*$
- A **field** is a nontrivial commutative ring F in which every nonzero element is a unit, i.e. $F^* = F - \{0\}$; e.g. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$; $\mathbb{Z}_p$ is only a field iff p is prime; a field is an integral domain; a finite integral domain is a field.
- $GF(p) = \mathbb{Z}_p$
- A polynomial is called **monic** if the leading coefficient is 1; a polynomial $a(x)$ with degree at least 1 is called **irreducible** if it is disable only by constant polynomials and by constant multiples of $a(x)$; for polynomials $a(x), b(x)$ in $F[x]$, a polynomial $d(x)$ is called a **greatest common divisor** of $a(x), b(x)$ if $d(x) \mid a(x), d(x) \mid b(x)$ and if every common divisor of $a(x), b(x)$ divides $d(x)$. Moreover, the monic polynomial $g(x)$ of largest degree such that $g(x) \mid a(x), g(x) \mid b(x)$ is called the greatest common divisor of $a(x), b(x)$, denoted $\gcd a(x), b(x)$
- F field. For any $a(x)$ and $b(x) \neq 0$ in $F[x]$ there exists unique $q(x), r(x)$ (quotient, remainder, resp.) such that $a(x) = b(x) \cdot q(x) + r(x)$ and $\deg r(x) < \deg b(x)$
- $a(x) \in R[x]$. An element $\alpha \in R$ for which $a(\alpha) = 0$ is called a **root** of $a(x)$; for a field $F, \alpha \in F$ is a root of $a(x)$ iff $x - \alpha$ divides $a(x)$; a polynomial of degree 2 or 3 over a field is irreducible iff it has no root; for a root α, the **multiplicity** is the highest power of $x - \alpha$ diving $a(x)$: for an integral domain D, a nonzero polynomial $a(x) \in D[x]$ of degree d has at most d roots, counting multiplicities.
- A polynomial $a(x) \in F[x]$ of degree d is uniquely determined by any $d+1$ values of $a(x)$, i.e. by $a(\alpha_1), \ldots, a(\alpha_{d+1})$ for any distinct $\alpha_1, \ldots, \alpha_{d+1} \in F$; $a(x) = \sum_{i=1}^{(d+1)} \beta_i u_i(x)$ with $\beta_i = a(\alpha_i)$ for $i = 1, \ldots, d+1$ and $u_{i(x)} = \frac{(x-\alpha_1)\ldots(x-\alpha_{i-1})(x-\alpha_{i+1})\ldots(x-\alpha_{d+1})}{(\alpha_i-\alpha_1)\ldots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\ldots(\alpha_i-\alpha_{d+1})}$
- $a(x) \equiv_{m(x)} b(x) :\Leftrightarrow m(x) \mid \big(a(x) - b(x)\big)$; congruence modulo $m(x)$ is an equivalence relation on $F[x]$ and eache quivalcne class has a unique representative of degree less than $\deg m(x)$
- Let $m(x)$ be a polynomial of degree d over F. Then $F[x]_{m(x)} \coloneqq \{a(x) \in F[x] | \deg a(x) < d\}$; F finite field, q elements, $m(x)$ degree d over F, then $\left|F[x]_{m(x)}\right| = q^d$; $F[x]_{m(x)}$ is a ring with respect to addition and multiplication modulo $m(x)$; the congruence equation $a(x)b(x) \equiv_{m(x)} 1$ has a solution $b(x) \in F[x]_{m(x)}$ iff $\gcd a(x), m(x)) = 1$. The solution is unique, i.e. $F[x]^*_{m(x)} = \left\{a(x) \in F[x]_{m(x)} \middle| \gcd a(x), m(x) = 1\right\}$; the ring $F[x]_{m(x)}$ is a field iff $m(x)$ is irreducible
- A **(t, n)-secret sharing scheme** for a finite domain $\mathcal{S}$ is a method for sharing a secret value $s \in \mathcal{S}$ among n parties $P_1, \ldots, P_n$ such that any t of the parties can reconstruct s but no $t-1$ (or fewer) parties have any information about s; Let $n < q$ and let each aprty P_i be (publicly) assigned a unique element α_i of $GF(q)$. If $a_1, \ldots, a_{t-1}$ are chosen

uniformly at random from $GF(q)$ and each party P_i gets the share $a(\alpha_i)$ where the polynomial $a(x) \in GF(x)$ is defined by $a(x) \coloneqq a_{t-1}x^{t-1} + \cdots + a_1x + s$ then this is a (t, n)-secret sharing scheme

- The **encoding function** E of en arror-correcting code for some alphabet $\mathcal{A}$ takes k information symbols $a_0, \dots, a\_(k-1) \in \mathcal{A}$ and encodes them into a list $[c_0, \dots, c_{n-1}]$ of $n > k$ symbols in $\mathcal{A}$ (the codeword): $E: \mathcal{A}^k \to \mathcal{A}^n$: $[a_0, \dots, a_{k-1}] \mapsto E(a_o, \dots, a_{k-1}) = [c_0, \dots, c_{n-1}]$; An $(\boldsymbol{n}, \boldsymbol{k})$**-error-correcting code** $\mathcal{C}$ over the alphabet $\mathcal{A}$ with $|\mathcal{A}| = q$ is a subset of carindaltiy q^k of $\mathcal{A}^n$; **The Hamming distance** between two code words is the number of positions at which the two code words differ; The **minimum distance** of an error-correcting code $\mathcal{C}$ is the minimum of the Hamming distance between any two code words; A code $\mathcal{C}$ with minimum distance d can correct t errors iff $d \geq 2t + 1$
- Let $\mathcal{A} = GF(q)$ and $\alpha_0, \dots, \alpha_{n-1}$ be arbitrary distinct elements of $GF(q)$. Consider the encoding function $E(a_o, \dots, a_{k-1}) = [a(\alpha_0), \dots, a(\alpha_{n-1})]$ where $a(x)$ is the polynomial $a(x) \coloneqq a_{k-1}x^{k-1} + \cdots + a_1x + a_0$. This code has minimum distance $n - k + 1$

Additional Wisdom

- Rings > integral domains > fields
- Apply the definitions.
- $GF(2) = \{0,1\}$, $GF(2)[x] = $ Polynome über $\{0,1\}$, $GF(2)[x]_{x^2+x+1} = \{0,1,x,x+1\}$, $GF(2)[x]_{x^2+x+1}[y] =$ Polynome von Grad d mit $GF(2)[x]_{x^2+x+1}$ als Werte zum Einsetzen in y

Chapter 8: Logic

- Every statement (formula) $s \in \mathcal{S}$ is either true or false. The function $\tau: \mathcal{S} \to \{0,1\}$ is called the **truth function** and assigns to every $s \in \mathcal{S}$ its truth value $\tau(s)$. A proof $p \in \mathcal{P}$ for a statement s is relative to a **verification function** $\phi: \mathcal{S} \times \mathcal{P} \to \{0,1\}$ where $\phi(s,p) = 1$ means that the proof is accepted. A **proof system** is a quadruple $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$. The proof system is **sound** if no false statement has a proof, i.e. for all s for which a p with $\phi(s,p) = 1$ exists, $\tau(s) = 1$. A proof system is **complete** if every true statement has a proof, i.e. if for all s with $\tau(s) = 1$ a p with $\phi(s,p) = 1$ exists.
- The **syntax** of a logic defines an alphabet (of allowed symbols) and specifies which strings (over the alphabet) are (syntactically) correct formulas; A formula generally contains certain variable parts which are not determined (by the formula) and can take on values in certain domains. A particular choice of these variable parts is called a **structure**; A structure is **suitable** for a formula F if all variable elements of F are defined (i.e., fixed), i.e., if it makes the formula true or false; The **semantics** of a logic is a function σ aissnign to each formula F and each structure $\mathcal{A}$ suitable for F a truth value $\sigma(F, \mathcal{A})$ in $\{0,1\}$; A (suitable) structure $\mathcal{A}$ for whioch a formula F is true is called a **model** for F and one writes $\mathcal{A} \vDash F$. More generally, for a set M of formulas, a (suitable) structure for which all formulas in M are rtue is caked a modek for M, denoted $\mathcal{A} \vDash M$. If $\mathcal{A}$ is not a model for M one writes $\mathcal{A} \nvDash M$.
- A formula F (or set M of frmulas) is callked **satisfiable** if there exists a model for F (M), and **unsatisfiable** otherwise. The symbol $\bot$ is used for an satisfiable formula; A formula is called a **tautology** or **valid** if it is true for every suitable structure. The symbol $\top$ is used for a tautology; A formula G is a **logical consequence** of a formula F (or a set M), dnoted $F \vDash G$, if every structure for both F (M) and G, whch is a model for F (M), is also a model for G; Two formulas F, G are **equivalent**, dented $F \equiv G$ ($F \Leftrightarrow G$), if every trucutre suitbale for both F, G yields the same truth value for F, G, i.e. if each is logical consequence of the other: $F \equiv G: \Leftrightarrow F \vDash G \text{ and } G \vDash F$.
- A theorem (to be proven) can be one of the following three types: a formula F, a steametn about a formula F, or a statement about the logic.
- A **derivation rule** is a rule for deriving a formula from a set of formulas (Called the precondition). We write $\{F_1, \dots, F_k\} \vdash_R G$ if G can be derived from the set $\{F_1, \dots, F_k\}$ by rule R; A logical **calculus** K is a fininte set of derivation rules: $K = \{R_1, \dots, R_m\}$; A **derivation** of a formula G from a set M of fmroumlas in a cluclus K is a finite sequence (of some length n) of applications of rules in K leading to G. More precisely, we have $M_0 \coloneqq M, M_i \coloneqq M_{i-1} \cup \{G_i\}$ for $1 \leq i \leq n$ where $N \vdash_{R_i} G_i$ for some $N \subseteq M_{i-1}$ and for some $R_i \in K$ and where $G_n = G$. We write $M \vdash_K G$ if there is a derivation of G from M in the calculus K.
- A derivation rule R is **correct** if for every set M of formulas and every formula F: $M \vdash_R F \Rightarrow M \vDash F$; A calculus K is **sound** or **correct** if for every set M of formulas and every formula F, if F can be derived from M then F is also a logical consequence of M: $M \vdash_K F \Rightarrow M \vDash F$, and K is **complete** if for every M and F, if F is a logical consequence of M, then F can also be derived from M: $M \vDash F \Rightarrow M \vdash_K F$; If $F \vdash_K G$ for a sound calculus, then $\vDash (F \to G)$

- An **atomic formula** is of the form $A_i, i \in \mathbb{N}$. A **formula** is defined inductively: an atomic formula is a formula, and if F, G are formulas, then also $\neg F, (F \wedge G), (F \vee G)$ are formulas; For a set M of atomic formulas, a **truth assignment** is a function $\mathcal{A}: M \to \{0,1\}$. Let $\widehat{M}$ be the set of formulas built from atomic formulas in M. We extend the domain of $\mathcal{A}$ to $\widehat{M}$ as follows: $\mathcal{A}\big((F \wedge G)\big) = 1$ iff $\mathcal{A}(F) = 1$ and $\mathcal{A}(G) = 1$, $\mathcal{A}\big((F \vee G)\big) = 1$ iff $\mathcal{A}(F) = 1$ or $\mathcal{A}(G) = 1$, $\mathcal{A}(\neg F) = 1$ iff $\mathcal{A}(F) = 0$
- A **literal** is an atomic formula or the negation of an atomic formula; A formula F is in **conjunctive normal form (CNF)** if it is a conjunction of disjunctions of literals, i.e., if it is of the form $F = \big(L_{11} \vee \dots \vee L_{1m_1}\big) \wedge \dots \wedge \big(L_{n1} \vee \dots \vee L_{nm_n}\big)$ for some literals L_{ij}; A formula F is in **disjunctive normal form (DNF)** if it is a disjunction of conjunctions of literals, i.e., if it is of the form $F = \big(L_{11} \wedge \dots \wedge L_{1m_1}\big) \vee \dots \vee \big(L_{n1} \wedge \dots \wedge L_{nm_n}\big)$ for some literals L_{ij}; Every formula is equivalent to a formula in CNF and also to a formula in DNF.
- Given such a formula F, one can use the truth table of F to derive an equivalent formula in DNF, as follows. For every row of the function table evaluating to 1 one takes the conjunction of the n literals defined as follows: If $A_i = 0$ in the row, one takes the literal A_i , otherwise the literal $\neg A_i$. This disjunction is a formula whose function table is 1 exactly for the row under consideration (and 0 for all other rows). Then one takes the disjunction of all these conjunctions. Given such a formula F, one can also use the truth table of F to derive an equivalent formula in CNF, as follows. For every row of the function table evaluating to 0 one takes the disjunction of the n literals defined as follows: If $A_i = 0$ in the row, one takes the literal $\neg A_i$, otherwise the literal A_i. This conjunction is a formula whose function table is 0 exactly for the row under consideration (and 1 for all other rows). Then one takes the conjunction of all these disjunctions.
- A **clause** is a set of literals; The set of clauses associated to a formula $F = \big(L_{11} \vee \dots \vee L_{1m_1}\big) \wedge \dots \wedge \big(L_{n1} \vee \dots \vee L_{nm_n}\big)$ in CNF, denoted $\mathcal{K}(F)$, is the set $\mathcal{K}(F) \coloneqq \Big\{\big\{L_{11}, \dots, L_{1m_1}\big\}, \dots, \big\{L_{n1}, \dots, L_{nm_n}\big\}\Big\}$. The set of clauses associated with a set $M = \{F_1, \dots, F_k\}$ of formulas is the union of their clause sets: $\mathcal{K}(M) \coloneqq \bigcup_{i=1}^{k} \mathcal{K}(F_i)$; A clause K is a **resolvent** of clauses K_1, K_2 if there is a literal L such that $L \in K_1, \neg L \in K_2$, and $K = (K_1 - \{L\}) \cup (K_2 - \{\neg L\})$; Given a set $\mathcal{K}$ of clauses, a resolution step takes two clauses $K_1 \in \mathcal{K}, K_2 \in \mathcal{K}$, computes a resolvent K and adds K to $\mathcal{K}$. This can be written as $\{K_1, K_2\} \vdash_{\mathrm{res}} K$. The resolution calculus, denoted Res, consist of a single rule $\mathrm{Res} = \{\mathrm{res}\}$; The resolution calculus is sound if $\mathcal{K} \vdash_{\mathrm{Res}} K$ then $\mathcal{K} \vDash K$; A set M of formulas is unsatbifiable iff $\mathcal{K}(M) \vdash_{\mathrm{Res}} \emptyset$.
- A **variable** is of the form $x_i, i \in \mathbb{N}$; a **function symbol** is of the form $f_i^{(k)}, i, k \in \mathbb{N}$, where k denotes the number of arguments of the function, for $k = 0$ this is called a **constant**; a **predicate symbol** is of the form $P_i^{(k)}$ (same as above); a **term** is denied inductively: a variable is a term, and if $t_1, \dots, t_k$ are termsn, then $f_i^{(k)}(t_1, \dots, t_k)$ is a term; a **formula** is defined inductively: if $t_1, \dots, t_k$ are termsn, then $P_i^{(k)}(t_1, \dots, t_k)$ is a formula, called an anotimic formula. If F, G are formulas, then also $\neg F, (F \wedge G), (F \vee G)$ are formulas. $\forall x_i\, F$, $\exists x_i\, F$ are formulas.
- Every occurrence of a variable in a formula is either bound or free. If a variable x occurs in a (sub-)formula of the form $\forall x\, G$ or $\exists x\, G$, then it is **bound**, otherwise it is **free**. A formula is **closed** if it contains no free variables.
- For a formula F, a variable x and a term t, $F[x/t]$ denotes the formulas obtained from F by substituoung every free occurrence of x by t.
- A **structure** is a tuple $\mathcal{A} = (U, \phi, \psi, \xi)$ where: U is a non-empty set, the **universe**; ϕ is a function assigning to each function symbol (in a certain subset of all function symbols) a function, where for a k-ary function symbol f, $\phi(f)$ is a function $U^k \to U$; ψ is a function assigning to each predicate symbol (in a certain subset of all predicate symbols) a function, where for a k-ary function symbol P, $\psi(P)$ is a function $U^k \to \{0,1\}$; ξ is a function assigning to each variable symbol (in a certain subset of all variable symbols) a value in U.
- For a structure $\mathcal{A} = (U, \phi, \psi, \xi)$ we define the value of terms and the truth value formulas under that structure. The value $\mathcal{A}(t)$ of a term t is defined recursively as follows: if t is a variable, then $\mathcal{A}(t) = \xi(t)$. If t is of the form $f(t_1, \dots, t_k)$ for terms $t_1, \dots, t_k$ and a k-ary function symbol f, then $\mathcal{A}(t) = \phi(f)\big(\mathcal{A}(t_1), \dots, \mathcal{A}(t_k)\big)$; The truth value of a formula F is defined recursively as follows: $\mathcal{A}\big((F \wedge G)\big) = 1$ iff $\mathcal{A}(F) = 1$ and $\mathcal{A}(G) = 1$. $\mathcal{A}\big((F \vee G)\big) = 1$ iff $\mathcal{A}(F) = 1$ or $\mathcal{A}(G) = 1$. $\mathcal{A}(\neg F) = 1$ iff $\mathcal{A}(F) = 0$. If F is of the form $F = P(t_1, \dots, t_k)$ for terms $t_1, \dots, t_k$ and a k-ary predicate symbol P, then $\mathcal{A}(F) = \psi(P)\big(\mathcal{A}(t_1), \dots, \mathcal{A}(t_k)\big)$. If F is of the form $\forall x\, G$ or

$\exists x\ G$, then let $\mathcal{A}_{[x\to u]}$ be the same strucurre as $\mathcal{A}$ expect that $\xi(x)$ is overwritten by u (i.e. $\xi(x) = u$): $\mathcal{A}(\forall x\ G) = \begin{cases} 1, & \text{if } \mathcal{A}_{[x\to u]}(G) = 1 \text{ for all } u \in U \\ 0, & \text{else} \end{cases}$, $\mathcal{A}(\exists x\ G) = \begin{cases} 1, & \text{if } \mathcal{A}_{[x\to u]}(G) = 1 \text{ for some } u \in U \\ 0, & \text{else} \end{cases}$

- If one replaces a subformula G of a formula F by an equivalent (to G) formula H, then the resulting formula is equivalent to F.
- For a formula F in which x occurs onl< free and in which y does not occur, $\forall x\ G \equiv \forall y\ G[x/y]$ and $\exists x\ G \equiv \exists y\ G[x/y]$; By appropriately renaming quantified variables one can transform any formula into an equivalent formula in which no variable appears both as a bound and a free variable and such that all variables appearing after the quantifiers are distinct. Such a formula is said to be in **rectified** form.
- A formula of the form $Q_1x_1Q_2x_2 \dots Q_nx_nG$ where Q_i are arbitrary quantifiers $(\forall, \exists)$ and G is a fomrula free of quantifiers, is said to be in **prenex form**.
- $\neg\exists x\forall y\ \big(P(y,x) \leftrightarrow \neg P(y,y)\big),\ \big[\equiv \forall x\exists y\ \big(P(y,x) \leftrightarrow P(y,y)\big)\big]$
- There exists no set that contains all sets S that do not contain themselves, i.e. $\{S | S \notin S\}$ is not a set; The set $\{0,1\}^\infty$ is not countable; There are function $\mathbb{N} \to \{0,1\}$ that are not computed by any program.

Rules

- $F \to G$ stands for $\neg F \vee G$; $F \leftrightarrow G$ stands for $(F \to G) \wedge (G \to F) \Leftrightarrow (F \wedge G) \vee (\neg F \wedge \neg G)$
- **Lemma 8.2** idempotence: $F \wedge F \equiv F$ and $F \vee F \equiv F$; commutativity : $F \wedge G \equiv G \wedge F$ and $F \vee G \equiv G \vee F$; associativity : $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$ and $(F \vee G) \vee H \equiv F \vee (G \vee H)$; absorption : $F \wedge (F \vee G) \equiv F$ and $F \vee (F \wedge G) \equiv F$; distributive law: $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$ and $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$; double negation: $\neg\neg F \equiv F$; de Morgan's rules: $\neg(F \wedge G) \equiv \neg F \vee \neg G$ and $\neg(F \vee G) \equiv \neg F \wedge \neg G$; tautology rules $F \vee \top \equiv \top$ and $F \wedge \top \equiv F$; unsatifiability rules: $F \vee \bot \equiv F$ and $F \wedge \bot \equiv \bot$; $F \vee \neg F \equiv \top$ and $F \wedge \neg F \equiv \bot$
- **Lemma 8.6** $\neg(\forall x\ F) \equiv \exists x\ \neg F$; $\neg(\exists x\ F) \equiv \forall x\ \neg F$; $(\forall x\ F) \wedge (\forall x\ G) \equiv \forall x(F \wedge G)$; $(\exists x\ F) \vee (\exists x\ G) \equiv \exists x\ (F \vee G)$; $\forall x\forall y\ F = \forall y\forall x\ F$; $\exists x\exists y\ F \equiv \exists y\exists x\ F$; $(\forall x\ F) \wedge H \equiv \forall x(F \wedge H)$; $(\forall x\ F) \vee H \equiv \forall x(F \vee H)$; $(\exists x\ F) \wedge H = \equiv \exists x(F \wedge H)$; $(\exists x\ F) \vee H \equiv \exists x\ (F \vee H)$

Additional Wisdom

- Be accurate and state your rules.