Set theory

Definitions:

Collection of objects from same Universe U. Define a set:

① $\{x \in A \mid P(x)\}$ ② $\{a, b, c\}$

reference to el. in U

D. "=": $A = B \overset{\text{def}}{\iff} \forall x (x \in A \leftrightarrow x \in B)$

L: $\{a\} = \{b\} \Rightarrow a = b$

Ordered pair: (a, b)

D. "=": $(a, b) = (c, d) \iff a = c \wedge b = d$

D. subset: $A \subseteq B \iff \forall x (x \in A \to x \in B)$

$(\forall A \; A \subseteq A)$

Trans.: $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$

D. $\emptyset$: $\forall x \; x \notin \emptyset$ (unique)

L.: $\forall A \; (\emptyset \subseteq A)$ *

Power set: $P(A) = \{S \mid S \subseteq A\}$, $|P(A)| = 2^{|A|}$

(set of all subsets of A) every element can either be or not in the subset

$\forall A \; \emptyset \in P(A) \wedge A \in P(A)$

examples:

$P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}, \{1, 3, 7\} \in P(\mathbb{N})$

$P(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$

$|\ldots| = 8$

Union: $A \cup B = \{x \mid x \in A \vee x \in B\}$

$\bigcup \mathcal{A} = \{x \mid x \in A \text{ for some } A \in \mathcal{A}\}$

Intersection: $A \cap B = \{x \mid x \in A \wedge x \in B\}$

$\bigcap \mathcal{A} = \{x \mid x \in A \text{ for all } A \in \mathcal{A}\}$

} comm., assoc., distr.

where $\mathcal{A} = \{A_i \mid i \in I\}$

example: $\mathcal{A} = \{A_1, A_2, A_3\}$, $I = \{1, 2, 3\}$

Complement: $\overline{A} = \{x \in U \mid x \notin A\}$

Difference: $B \setminus A = \{x \in B \mid x \notin A\}$

Cart. Prod.: $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$

for finite sets: $|A \times B| = |A| \times |B|$

example: $\{1, 3\} \times \{2, 4\} = \{(1, 2), (1, 4), (3, 2), (3, 4)\}$

Recipes:

- prove $A = B$:
  show $A \subseteq B$ and $B \subseteq A$
- prove $A \subseteq B$
  take arbitrary $x \in A \Rightarrow$ show $x \in B$

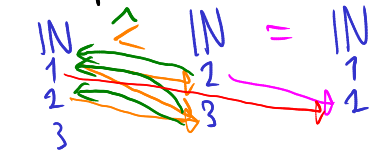
Relations:

D. relation p: $p \subseteq A \times B$, $a \; p \; b \overset{\text{def}}{\iff} (a, b) \in p$

$p \subseteq A \times A \triangleq$ relation on A

number of relations from A to B: $|P(A \times B)| = 2^{|A||B|}$

example:



Identity: $id = \{(a, a) \mid a \in A\}$

Matrix representation:

$(M^p)_{i,j} \iff i \; p \; j$ a, b, c, d, e, f, g

$$M^p = \begin{matrix} a \\ b \\ c \end{matrix} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

$p = \{(a, d), (a, e), (b, e), (b, f), (c, a)\}$

$M^{\hat{p}} = (M^p)^T$

Inverse: $\hat{p} = \{(b, a) \mid (a, b) \in p\}$, $a \; p \; b \iff b \; \hat{p} \; a$

Composition: $p \circ \sigma = \{(a, c) \mid \exists b ((a, b) \in p \wedge (b, c) \in \sigma)\}$

(associative) $= p\sigma$, $p \circ p = p^2$

all walks of length 2

L. $\widehat{p\sigma} = \hat{\sigma}\hat{p}$

Properties: relation on A

reflexive: $\forall a \; (a \; p \; a)$, $id \subseteq p$

example: id, "=", "|", "$\leq$" $p \subseteq p^2$

irreflexive: $\forall a (a \not p \; a)$

symmetric: $\forall a \forall b \; a (p \; b \iff b \; p \; a)$, $p = \hat{p}$

example: $\equiv_m$

antisymmetric: $\forall a \forall b ((a \; p \; b \wedge b \; p \; a) \to a = b)$

example: $\leq$, $|$

transitive: $\forall a \forall b \forall c ((a \; p \; b \wedge b \; p \; c) \to a \; p \; c)$

example: $\subseteq$, $\leq$, $<$, $\equiv_m$

L. p trans. $\iff p^2 \subseteq p$

Transitive closure: $p^* = \bigcup_{n \in \mathbb{N} \setminus \{0\}} p^n$

example: $a \; p^* \; b \iff$ there is a walk from a to b in G

Equivalence relation: $a \Theta b \Rightarrow a$ and b "equivalent"

1) reflexive 2) symmetric 3) transitive

example: "$\equiv$"

equivalence class: $[a]_\Theta = \{b \in A \mid a \Theta b\}$

example:
- connected component in a graph
- all points on the line through 0 with slope 1
- $[3]_{\equiv_2} = \{\ldots -1, 3, 5, 7, \ldots\}$

L. p and σ equiv. relations $\Rightarrow p \cap \sigma$ e.r.

Set of eq. classes: $A \setminus \Theta = \{[a]_\Theta \mid a \in A\}$ partition of A

rational numbers:

$(a, b) \sim (c, d) \iff ad = bc$

$\mathbb{Q} = \mathbb{Z} \times \mathbb{Z} \setminus \{0\} / \sim$

Partial order $\leq$

1) reflexive 2) antisymm. 3) trans.

$\leq$ on $A \Rightarrow (A; \leq)$ poset (p.o.s.)

example: directed graph, $\leq$, $(\mathcal{P}(A); \subseteq)$

↳ $a < b \Leftrightarrow a \leq b \wedge a \neq b$ (analogous to $<$)

Comparable: *

a and b comp. $\Leftrightarrow a \leq b \vee b \leq a$

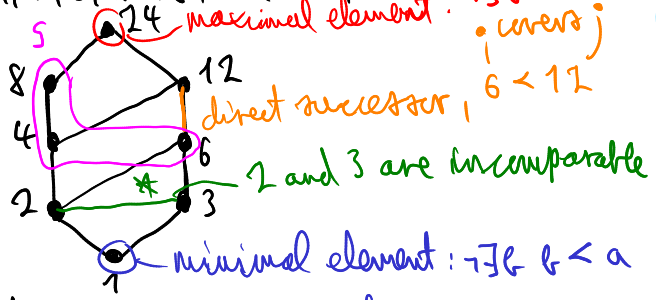
totally ordered:

example: $(\mathbb{Z}, \leq)$

$(A; \leq)$ t.o. $\Leftrightarrow \forall a \forall b$ a and b comparable

Hasse diagram:

$(\{1, 2, 3, 4, 6, 8, 12, 24\}; |)$



the least element: $\forall b\ a \leq b$

the greatest element: $\forall b\ b \leq a$

$S \subseteq A$. greatest lower bound: $\text{glb}(S) = 2$ — greatest in $\{l \in A \mid \forall s \in S\ l \leq s\}$

least upper bound: $\text{lub}(S) = 24$ — least in $\{u \in A \mid \forall s \in S\ s \leq u\}$

meet: $\text{glb}(\{a, b\})$ **join:** $\text{lub}(\{a, b\})$

well ordered:

totally ordered + $\forall S \in \mathcal{P}(S) \setminus \{\emptyset\}$ $\exists$ least el.

lattice:

$\forall a \forall b$ $\exists$ meet $\wedge$ $\exists$ join e.g.: $(\mathbb{N}; \leq)$,

$(A; \leq) \times (B; \sqsubseteq) \to (A \times B; \leq)$: $(a_1, a_2) \leq (b_1, b_2) \Leftrightarrow a_1 \overset{\wedge}{\leq} b_1 \wedge a_2 \sqsubseteq b_2$

Lexicogr. order: $(a_1, b_1) \leq_{lex} (b_1, b_2) \Leftrightarrow (a_1 < a_2) \vee (a_1 = a_2 \wedge b_1 \sqsubseteq b_2)$

poset! e.g. order words alph.

Functions:

1) $\forall a \in A\ \exists b\ a f b$ (fct. def.)

all f: $A \to B = B^A$ 2) $\forall a \in A\ \forall b, b' \in B\ (a f b \wedge a f b' \to b = b')$ (unique mapping to codomain)

composition: $(g \circ f)(a) = g(f(a))$ reverse order!

Countability: $f(A) = \{f(x) \mid x \in A\}$ $A \subseteq X$

equinumerous: $A \sim B \Leftrightarrow \exists$ bijection $A \to B$

dominate: $A \preceq B \Leftrightarrow \exists$ injection $A \to B$

$\Leftrightarrow \exists C \subseteq B$ $A \sim C$

Countable:

A countable $\Leftrightarrow A \preceq \mathbb{N}$

e.g. $\mathbb{N}, \mathbb{Q}, \{0,1\}^*$ $\Leftrightarrow A$ finite $\vee$ $A \sim \mathbb{N}$

L. trans: $A \preceq B \wedge B \preceq C \Rightarrow A \preceq C$

L.: $A \subseteq B \Rightarrow A \preceq B$

Cor.: $A \preceq \mathbb{N} \wedge B \preceq \mathbb{N} \Rightarrow A \times B \preceq \mathbb{N}$ ($\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$)

L. $\bigcup_{i \in \mathbb{N}} A_i$ is countable, A^n is count. $(a_1, \dots, a_n)$

L. $\{0,1\}^\infty$ is uncountable (diagonalization)

$\Rightarrow \mathbb{R}$ is uncountable

$\{0,1\}^\infty \hat{=} f: \mathbb{N} \to \{0,1\}$, e.g. prime(n), 00110101...

Computable: $f: \mathbb{N} \to \{0,1\}$ comp.

$\Leftrightarrow \exists$ program $\in \{0,1\}^*$ $\forall n$ $p(n) = f(n)$

Cor. $\exists f: \mathbb{N} \to \{0,1\}$ f is uncomputable

Recipes:

show equ. rel. (poset):

1) refl.: let $a \in A \Rightarrow a \Theta a$

2) symm.: let $a, b \in A$ assume $a \Theta b \Rightarrow b \Theta a$

antisymm.: let $a, b \in A$, $a \leq b \wedge b \leq a \Rightarrow a = b$

3) trans: let $a, b, c \in A$, ass. $a \Theta b \wedge b \Theta c \Rightarrow a \Theta c$

show injection $f: A \to B$

- let $a \neq a' \in A \to$ show $f(a) \neq f(a')$

show surjective: let $b \in B \to \exists a \in A$ $f(a) = b$

show A count.:

- injection $A \to \mathbb{N}/\{0,1\}^*$
- A_i count. $\Rightarrow \bigcup_{i=1}^{\infty} A_i$ count.

$A_1 \times A_2 \times \dots \times A_n$ count.

injection into $\mathbb{N}$

- $A_1, A_2, \dots, A_n$ countable, $f_1, f_2, \dots, f_n$ corresponding inj.

$\Rightarrow (a_1, a_2, \dots, a_n) \mapsto p_1^{f_1(a_1)} \cdot p_2^{f_2(a_2)} \cdots p_n^{f_n(a_n)}$ (injective due to uniqueness of prime factorization)

- geometric argument
- define easier set $B \subseteq A$ — show $\{0,1\}^\infty \to B$

show A uncountable:

- define injection $\{0,1\}^\infty / \mathbb{R} \to A$ injective
- cantor's diagonal argument: assume $\exists$ injection $A^\infty \to \mathbb{N}$

$\Rightarrow b_1 = a_{11}, a_{12}, \dots$ let $b_i^* = \overline{a_{ii}}$ not

$b_2 = a_{21}, a_{122}, \dots$ $\Rightarrow b_i^* \in A^\infty$ but b_i complete

$\Rightarrow \lightning \exists$ inj.

Number theory

$\forall a \neq 0\ a \mid 0$

Def. "|": $a \mid b \Leftrightarrow \exists c\ ac = b$

T. remainders: $\forall a\ a = dq + r$ $(d \neq 0)$

q, r unique, $0 \leq r < |d|$, $r = R_d(a)$

gcd:

$\gcd(a,b) = d \Leftrightarrow d \mid a \wedge d \mid b \wedge \forall c ((c \mid a \wedge c \mid b) \to c \mid d)$

$\gcd(a,b) = 1 \Rightarrow a$ and b relatively prime (no common prime factor)

T. euclid: $\gcd(m,n) = \gcd(m, R_m(n))$

ideal: $(a,b) = \{ua + vb \mid u, v \in \mathbb{Z}\}$ $\forall x, y \in (a,b) \Rightarrow x - y \in (a,b)$

Bsp.: $(10,16) = \{16, 10, \dots, 6, 4, 2, 0, -2, \dots\}$

L. ideal: 1) $\exists d$ $(a,b) = (d)$

2) $d = \gcd(a,b) = ua + vb$ $(u, v \in \mathbb{Z})$

T.: prime factorization is unique $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$

$a = \prod_i p_i^{e_i}$, $b = \prod_i p_i^{f_i}$ $\gcd(a,b) \cdot \text{lcm}(a,b) = a \cdot b$

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

Modulo: $a \equiv_m b \Leftrightarrow m \mid (a-b) \Leftrightarrow mk = a-b$

- $a \equiv_m b \wedge c \equiv_m d \Rightarrow a \square c \equiv_m b \square d \quad \square = +$ or $\cdot$
- $R_m(a) = \min\{a\}_{\equiv_m} \in \mathbb{Z}_m = \{0, \dots, m-1\}$
- $a \equiv_m R_m(a)$
- $a \equiv_m b \Leftrightarrow R_m(a) = R_m(b)$
- $R_m(a+b) = R_m(R_m(a) + R_m(b))$
  $R_m(a \cdot b) = R_m(R_m(a) \cdot R_m(b))$
  $R_m(a^b) = R_m(R_m(a)^b)$ (*)
- $R_9(247) = R_9(100 \cdot 2 + 10 \cdot 4 + 7) = R_9(2+4+7)$
  $R_{11}(247) = R_{11}(\dots) = R_{11}(1 \cdot 2 + (-1) \cdot 4 + 1 \cdot 7)$
- $\exists x \in \mathbb{Z}_m \; ax \equiv_m 1 \Leftrightarrow \gcd(a,m) = 1$ (multiplicat. inverse)
  unique with $\gcd(n,m) = 1$
- $a \equiv_{nm} b \Leftrightarrow a \equiv_n b \wedge a \equiv_m b$

Chinese remainder theorem: (CRT)

$m_1, \dots, m_r$ relatively prime, $M = \prod_{i=1}^{r} m_i$

$a_1, \dots, a_r$ s.t. $a_i \in \mathbb{Z}_{m_i}$ $(0 \le a_i < m_i)$

$$\left.\begin{aligned} x &\equiv_{m_1} a_1 \\ x &\equiv_{m_2} a_2 \\ &\vdots \\ x &\equiv_{m_r} a_r \end{aligned}\right\} \text{unique solution } x \in \mathbb{Z}_M$$

find x_i: $M_i = M_{m_i}$

find N_i s.t. $M_i N_i \equiv_{m_i} 1$

$\Rightarrow x = R_M\left(\sum_{i=1}^{r} a_i M_i N_i\right)$

e.g.: $R_{600}(7^{100}) = x = ?$

$M = 600 = 24 \cdot 25$

$R_{24}(7^{100}) = R_{24}((7^2)^{50}) = 1 \Rightarrow x \equiv_{24} 1$

$R_{25}(7^{100}) = R_{25}((-1)^{50}) = 1 \Rightarrow x \equiv_{25} 1$

$\Rightarrow x = 1 = R_{600}(7^{100})$

Diffie-Hellman:

only works if solving $y = g^x$ for x is intractable

$\langle g \rangle = \mathbb{Z}_p^*$ (generator)

$x_A, x_B \in \{0, 1, \dots, p-2\}$ — public / secret

Alice: $y_A = R_p(g^{x_A}) = g^{x_A}$ (in $\mathbb{Z}_p^*$)

Bob: $y_B = R_p(g^{x_B})$

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

Recipes:

Extended euclidean algorithm: $ax \equiv_m 1$

x s.t. $142 \cdot x \equiv_{553} 1$?

1) $\gcd(553, 142) = \gcd(142, R_{142}(553))$

$553 = 3 \cdot 142 + 127$

$\Rightarrow \gcd(142, 127)$

$142 = 1 \cdot 127 + 15$

$\Rightarrow \gcd(127, 15)$

$127 = 8 \cdot 15 + 7$

$\Rightarrow \gcd(15, 7) = 1$ $(15 = 2 \cdot 7 + 1)$

2) find u, v such that $553u + 142v = 1 \Rightarrow x = v$

$1 = 15 - 2 \cdot 7$

$= 15 - 2 \cdot (127 - 8 \cdot 15) = -2 \cdot 127 + 17 \cdot 15$

$= -2 \cdot 127 + 17 \cdot (142 - 127) = 17 \cdot 142 - 19 \cdot 127$

$= 17 \cdot 142 - 19(553 - 3 \cdot 142) = -19 \cdot 553 + 74 \cdot 142$

$\Rightarrow 74 \cdot 142 \equiv_{553} 1$

Show irrationality:

- $\log_{35} 7$: assume $\log_{35} 7 \in \mathbb{Q}$
  $\Rightarrow \log_{35} 7 = \frac{a}{b} \Rightarrow 7 = 5^{\frac{a}{b}} \Rightarrow 7^b = 5^a$ ↯ (unique prime fact.)

Show $p(x) \neq p(y)$

- check $p(x) \equiv_m p(y)$ for $m \in \{2, 3, 4, \dots\}$
  $p(x) \not\equiv_m p(y) \Rightarrow p(x) \neq p(y)$

Algebra:

Def.: $\langle S; \Omega \rangle$, S set, $\Omega = (\omega_1, \dots, \omega_n)$ = operations/constants

$\omega_i : S^n \to S$ / $e : S^0 \to S$

Algebras:

Neutral el.: $e \in S$

left neutral: $\forall a \in S \; e * a = a$

right " : " $a * e = a$

e.g. 0 with "+" or 1 with "·"

L. e is left n. and e' is right n. $\Rightarrow e = e'$, e unique

Associative: $\forall a, b, c \in S \; (a * b) * c = a * (b * c) \Rightarrow a^n$ is unique

Monoid: $\langle M; *, e \rangle$

1) $\exists e$ e is neutral el. 2) $*$ associative

Inverse: $a \in S$

left inverse: $b * a = e$

right " : $a * b = e$

L. $*$ associative $\Rightarrow b$ unique $\Rightarrow b = \hat{a}$ $(\hat{\cdot} : S \to S)$

e.g.: $-x$ in $\mathbb{Z}$

Group: $\langle G; *, \hat{\cdot}, e \rangle$

G1: $*$ associative

G2: e neutral el.: $a * e = e * a = a$

G3: $\forall a \in G \; \exists \hat{a} \in G \; a * \hat{a} = \hat{a} * a = e$

e.g.: $\langle \mathbb{Z}/\mathbb{R}/\mathbb{Q}; +, -, 0 \rangle$, $\langle \mathbb{Z}_m; \oplus, \ominus, 0 \rangle$

$\langle S_n; \circ, ^{-1}, id \rangle$ S^n = alle $f : \{1, \dots, n\} \to \{1, \dots, n\}$ (perm.)

trivial group: $\mathbb{Z}_1$, $\mathbb{Z}_2$

commutative: $\forall a, b \in G \; a * b = b * a$

L. properties:

- $\hat{\hat{a}} = a$
- $\widehat{a * b} = \hat{b} * \hat{a}$
- $a * b = a * c \Rightarrow b = c$
- $b * a = c * a \Rightarrow b = c$
- $a * x = b$, $x * a = b$ $\Rightarrow$ unique solution $x = \hat{a} * b$

Direct product: $\langle G_1 \times \dots \times G_n; * \rangle$ = (group)

$(a_1, \dots, a_n) \times (b_1, \dots, b_n) = (a_1 *_1 b_1, \dots, a_n *_n b_n)$

Group homomorphism: $\langle G; *, \hat{\cdot}, e \rangle, \langle H; \times, \tilde{\cdot}, e' \rangle$

$\psi : G \to H$ is a g.h. $\Leftrightarrow \forall a, b \; \psi(a * b) = \psi(a) \times \psi(b)$

ψ surjective $\to \psi$ is an isomorphism, $G \simeq H$

L. $\psi(e) = \psi(e')$

$\psi(\hat{a}) = \widetilde{\psi(a)}$

$\psi(a^n) = \psi(a)^n$

- non-inj.: $\psi : \mathbb{Z}_2 \to \mathbb{Z}_4$, $\psi(0) = 0$, $\psi(1) = 0$

e.g. $\ln(a \cdot b) = \ln(a) + \ln(b)$

- $\langle \mathbb{Z}_6; \oplus \rangle \times \langle \mathbb{Z}_{10}; \oplus \rangle \simeq \langle \mathbb{Z}_2; \oplus \rangle \times \langle \mathbb{Z}_{30}; \oplus \rangle$ with $\psi((a,b)) = (R_2(a), x)$, $x \equiv_3 a$, $x \equiv_{10} b$
- $\langle \mathbb{Z}_n; \oplus \rangle \simeq \langle \mathbb{Z}_p; \oplus \rangle \times \langle \mathbb{Z}_q; \oplus \rangle$ where $\gcd(p,q) = 1, n = p \cdot q$

Subgroups and order

Subgroup: $\langle H; *, \hat{\cdot}, e \rangle$, with $H \subseteq$ is a subgroup

$\Leftrightarrow \forall a, b$: 1) $a * b \in H$, 2) $e \in H$, 3) $\hat{a} \in H$ — all operations stay in H

trivial subgroups: $\{e\}$, G

e.g.: $G = \mathbb{Z}_{12}$, $\{0\}$, $\{0, 6\}$, $\{0, 4, 8\}$

Powers: $a^n = \underbrace{a * a * \ldots * a}_{n}$ $n \in \mathbb{Z}$

$a^0 = e$

$n<0$: $a^n = (a^{-1})^{|n|} = (a^{|n|})^{-1}$

$\Rightarrow a^m * a^n = a^{m+n}$

$\Rightarrow (a^m)^n = a^{mn}$

order:

$\text{ord}(a) = m \hat{=}$ minimum m s.t. $a^m = e$

G finite $\Rightarrow \text{ord}(a) < \infty$, $a^{\text{ord}(a)} = e$

e.g.: $\text{ord}(a) \geq 1 \Rightarrow a * a = e \Rightarrow a$ is "self-inverse"

$\text{ord}(a) < \infty \Rightarrow a^m = a^{R_{\text{ord}(a)}(m)}$

generater:

$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ $n<0$ possible

1) $\langle a \rangle$ is the smallest subgroup with a

$= \{e, a, a^2, \ldots, a^{\text{ord}(a)-1}\}$ $(a^{\text{ord}(a)-1} = e * a^{-1} = a^{-1})$

$|\langle a \rangle| = \text{ord}(a)$

2) $\langle g \rangle = G \Rightarrow G$ is cyclic, g is a generator of G, $\text{ord}(g) = |G|$

e.g.: $\langle 1 \rangle = \mathbb{Z}_n \Rightarrow 1$ always a generater

* $\gcd(g, n) = 1 \Leftrightarrow \langle g \rangle = \mathbb{Z}_n$

* Proof: $\gcd(g, n) = 1$

$\Leftrightarrow ug + v \cdot n = 1$

$\Leftrightarrow ug \equiv_n 1$

$\Leftrightarrow g \odot_n u = 1$

$\Leftrightarrow g^u = 1 \Leftrightarrow \langle g \rangle = \mathbb{Z}_n$

3) $\mathbb{Z}_p^*$ always cyclic ($\Rightarrow$ Diffie Hellman uses $\mathbb{Z}_p^*$)

• g generator $\Rightarrow \text{ord}(g^m) = \frac{n}{\gcd(m,n)}$

$\left(n \mid mk \Rightarrow \frac{n}{\gcd(m,n)} \mid \frac{m}{\gcd(m,n)} \cdot k \text{ as } np = k \cdot m\right)$

• $g^{km} = e \Rightarrow R_n(k \cdot m) = 0 \Rightarrow n \mid k \cdot m$

T. g cyclic $\Rightarrow \langle G; * \rangle \simeq \langle \mathbb{Z}_n; \oplus \rangle$

bijective group hom.: $\psi: \mathbb{Z}_n \to G$

$\psi(i) = g^i$

• $\mathbb{Z}_m \times \mathbb{Z}_n$ cyclic $\Leftrightarrow \gcd(m,n) = 1$

Lagrange: H subgroup of G

$\Rightarrow |H| \mid |G|$

1) $\forall a \in G$ $\text{ord}(a) \mid |G|$

2) $a^{|G|} = a^{k \cdot \text{ord}(a)} = e$

3) $|G|$ is prime $\Rightarrow \forall a \neq e$ a generater

Modulo group multiplication:

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

$\langle \mathbb{Z}_m^*; \odot, 1 \rangle$ is a group. Proof

$\exists x \; a \cdot x \equiv_m 1 \Leftrightarrow \gcd(a, m) = 1 \Rightarrow$ all elements have an inverse

$\gcd(a, m) = 1 \wedge \gcd(b, m) = 1$

$\Rightarrow \gcd(ab, m) = 1 = \gcd(R_m(ab), m) \Rightarrow a \odot b \in \mathbb{Z}_m^*$

Euler function:

$\varphi(m) = |\mathbb{Z}_m^*| \hat{=}$ # numbers relatively prime to m between 1 and m

e.g.: $\mathbb{Z}_{18}^* = \{1, 5, 7, 11, 13, 17\}$ prime

$\varphi(18) = 6$

• p prime $\Rightarrow \mathbb{Z}_p^* = \{1, \ldots, p-1\}$, $\varphi(p) = p-1$

L. $\varphi(m)$ $m = \prod_{i=1}^{r} p_i^{e_i}$

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

Proof sketch: $1, \varphi(p^e) = p^e - p = p^{e-1}(p-1)$ (skip every p-th prime)

Cor. $\gcd(a, m) = 1$:

$a^{\varphi(m)} \equiv_m 1$

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

$a^{\varphi(m)} \equiv_m R_m(a)^{\varphi(m)}$

$\equiv_m R_m(a)^{|G|} \equiv_m 1$ ($R_m(a) \in \mathbb{Z}_m^*$)

p prime

$a^{\varphi(p)} \equiv_p a^{p-1} \equiv_p a^{|G|} \equiv_p 1$

2. CRT:

$(a_1, \ldots, a_r), a_i \in \mathbb{Z}_{p_i^{e_i}}^*$

$\Rightarrow \gcd(x, m) = \gcd(x, p_i^{e_i})$

$= \gcd(R_{p_i^{e_i}}(x), p_i^{e_i})$

$= \gcd(a_i, p_i^{e_i}) = 1$

$\Rightarrow x \in \mathbb{Z}_m^*$

$\Rightarrow R_m(1^y) = R_m(2^{R_{\varphi(m)}(y)})$ ($\gcd(m, 1) = 1$)

RSA: generate primes p, q. $n = p \cdot q$

select $e \in \mathbb{N}$, $\gcd(e, \varphi(n)) = 1$

find d s.t. $de \equiv_{\varphi(n)} 1$

public: (n, e), **private:** d

sender: message $m \in \{1, \ldots, n-1\}$

$\downarrow c = R_n(m^e)$ cypher

receiver: $m = R_n(c^d)$

Proof sketch:

$m^{ed} \equiv_n m^{k \cdot \varphi(n) + 1} \equiv_n \left(m^{\varphi(n)}\right)^k \cdot m$

$\equiv_n m$

case $\gcd(m, n) = 1 \Rightarrow$ euler

case $\gcd(m, n) = p$:

$\left(m^{\varphi(n)}\right)^k \cdot m \equiv_p m \equiv_p 0$

$\left(m^{\varphi(q)}\right)^k \cdot m \equiv_q m \equiv_q R_q(m)$ ($\gcd(m, q) = 1$ euler)

CRT $\Rightarrow m$ unique solution $\in \mathbb{Z}_{p \cdot q}$

Ring: $\langle R; +, -, 0, \cdot, 1 \rangle$

1) $\langle R; +, -, 0 \rangle$ is a comm. group

2) $\langle R; \cdot, 1 \rangle$ is a monoid

3) $a(b+c) = (ab) + (ac)$,

$(b+c)a = (ba) + (ca)$ (distr. laws)

Commutative $\overset{\text{def}}{\Leftrightarrow}$ "$\cdot$" commutative

e.g.: $\mathbb{Z}, \mathbb{R}, \langle \mathbb{Z}_m; \oplus, \ominus, 0, \odot, 1 \rangle$ (4)

trivial ring: $R=\{0\}$ $(0=1)$

L. properties:
- $0a=a0=0$
- $(-a)b=-(ab)$
- $(-a)(-b)=(ab)$
- $|R|>1 \Rightarrow 0\neq 1$
- $\forall a\ 1\mid a,\ -1\mid a,\ a\mid 0$

comm. ring:
- $a\mid b \Rightarrow \forall c\ a\mid bc$
- $a\mid b \wedge a\mid c \Rightarrow a\mid(b+c)$

unit: (comm. ring) has inverse w.r.t. "$\cdot$"
$u\in R$ s.t. $\exists v\ uv=vu=1$, $v=u^{-1}$

R^* = set of all units $\quad \mathbb{Z}[i]=\{1,-i,i,-1\}$

e.g. $\mathbb{Z}_m^*$, $\mathbb{Z}^*=\{1,-1\}$, $\mathbb{R}^*=\mathbb{R}\setminus\{0\}$

L. $\langle R^*;1,^{-1},\cdot\rangle$ is a group.

zerodivisor: $a\neq 0$ is a zerodivisor $\{0\}$
$\Leftrightarrow \exists b\neq 0\ ab=0$ find z.d. of $\mathbb{Z}_n$: $\mathbb{Z}$
$\forall a\ \gcd(a,n)\neq 1 \to \mathbb{Z}=\mathbb{Z}_n\setminus(\mathbb{Z}_n^*\cup\{0\})$

integral domain: $|\mathbb{Z}|=\varphi(n)=n-1$
comm. ring with no zerodivisors: $\forall a,b\in R\ ab=0 \to (a=0 \vee b=0)$
e.g.: $\mathbb{N}$, $\mathbb{Z}$, ... $\quad \mathbb{Z}_m\times\mathbb{Z}_n$ or
$\mathbb{Z}_6$ is not an integral domain: $2\cdot 3=0$

Polynomials: $R[x]\hat{=}(R)^*$

$a(x)=a_d x^d+\dots+a_0 \hat{=}(a_0,a_1,\dots,a_d)$

$d=\deg(a(x))$, $\deg(a(x)b(x))\le \deg(a(x))+\deg(b(x))$

$a(x)b(x)=\sum_{i=0}^{d+d'}\left(\sum_{u+v=i} a_u\cdot b_v\right)x^i$

$a(x)+b(x)=\sum_{i=0}^{\max(d,d')}(a_i+b_i)x^i$

inverse of $p(x)$ in $R[x]^*_{m(x)}$: a) find $a(x)$ s.t. $p(x)\cdot a(x)=b$
b) extended euclidean algorithm: $\gcd(m(x),p(x))=\dots$

Properties:
- $R[x]$ is a ring
- D is int. d. $\Rightarrow D[x]$ is int. d.
- D " $\Rightarrow D[x]^*=D^*$

Field: nontrivial commutative ring, $F^*=F\setminus\{0\}$

e.g. $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}_p \Rightarrow$ F is an int. d.

GF(p) $\hat{=}$ field with p elements $\quad GF(p)=\mathbb{Z}_p$

monic polynomial: 1 in front / $a_d=1$

reason: $a(x)=b(x)\cdot c(x) \Rightarrow \forall v\ v\,b(x)\,(v^{-1}\,c(x))=a(x)$

irreducible: $a(x)$ irr. $\Leftrightarrow$ only divisors are c or $c\cdot a(x)$

gcd$(a(x),b(x))$ → largest degree, monic

remainders: $a(x)=b(x)\cdot q(x)+r(x)$
$\deg(r(x))<\deg(b(x))$, $\equiv_{m(x)}$, $R_{m(x)}(a(x))$

root: $a\in R[x]$, α root $\Leftrightarrow a(\alpha)=0$

L. α root $\Leftrightarrow (x-\alpha)\mid a(x)$

multiplicity: highest b s.t. $(x-\alpha)^b \mid a(x)$

T. $a(x)$ has at most d roots, with mult.

finite fields: → ring

$F[x]_{m(x)}=\{a(x)\in F(x)\mid \deg(a(x))<d\}$

$|F[x]_{m(x)}|=|F|^d$ (all poss. options for coeff.)

$a(x)b(x)\equiv_{m(x)}1 \Leftrightarrow \gcd(a(x),b(x))=1$

T. $F[x]_{m(x)}$ is a field $\Leftrightarrow m(x)$ is irreducible
$\Rightarrow$ field with $|F|^d$ elements

Polynomial interpolation: $a(x)\in F[x]$ at most
$a(x)$ is uniquely determined by $d+1$ values:
$a(\alpha_1), a(\alpha_2), \dots, a(\alpha_{d+1})$ with $\alpha_1,\dots,\alpha_{d+1}$ distinct
$\quad\|\quad\|\quad\|$
$\beta_1\quad\beta_2\quad\beta_{d+1}$

$$a(x)=\sum_{i=0}^{d+1}\beta_i u_i(x) \qquad u_i(\alpha_k)=\begin{cases}0 & k\neq i\\ 1 & k=i\end{cases}$$

$$u_i(x)=\frac{(x-\alpha_1)\cdots(x-\alpha_{i-1})(x-\alpha_{i+1})\cdots(x-\alpha_{d+1})}{(\alpha_i-\alpha_1)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_{d+1})}$$

inverses

Proof sketch uniqueness:
$a(x)'$ also agrees at $d+1$ values
$\Rightarrow a(x)-a'(x)$ has $d+1$ roots ↯ (T.)

Error-correcting codes: alphabet A

encoding: $E: A^k \to A^n$, $n>k$, "extra data"
$E((a_0,\dots,a_{k-1}))=(c_0,\dots,c_n)$
$C=\mathrm{im}(E)\hat{=}$"error-correcting code", $|C|=|A|^k$

min. (hamming) dist d_{min}: min. # differences between any $c_1,c_2\in C$ $\hat{=}$ corrects t errors in data

decoding: $D: A^n \to A^k$, t-error-correcting
$\Leftrightarrow D((r_0,\dots,r_{n-1}))=(a_0,\dots,a_{k-1})$ original
for any r with $hd(r,E(a))\le t$

T. D/C is t-error-correcting $\Leftrightarrow d_{min}\ge 2t+1$
$\hat{=}$ any c_1,c_2 differ in at least $2t+1$ pos.

T. polynomials: $A=GF(q)$, $a(x)=a_{k-1}x^{k-1}+\dots+a_1x+a_0$
$E((a_0,\dots,a_{k-1}))=(a(\alpha_0),\dots,a(\alpha_{n-1}))\to d_{min}=n-k+1$

Recipe: find generators of a cyclic group
1) order divides group order → write out divisors
$d_1, d_2, \dots, d_r \mid |G|$
2) for all $a\neq e$ calculate $a^{d_1}, a^{d_2}, \dots, a^{d_r}$
→ $\forall x\ a^{d_x}\neq e \Rightarrow a$ is a generator

check if polynomial is irreducible
- $d=1$: always irr.
- $d\in\{2,3\}$: irr. $\Leftrightarrow$ no root
- $d\ge 4$: irr. $\Leftrightarrow$ no root + no irr. factor of deg $\le d/2$

Logic: **Proof system:** syntax with symbols $\in \Sigma$

$\Pi = (S, P, \tau, \phi)$ — S: set of all statem., P: set of all proofs

truth function $\tau: S \to \{0,1\}$, $\tau = 1 \Leftrightarrow s$ is true

→ difficult to compute

verification function: → efficient to compute

$\phi: S \times P \to \{0,1\}$ $\phi = 1 \Leftrightarrow p$ is a valid proof

sound: $s \in S, \exists p \in P\ \phi(s,p) = 1 \Rightarrow \tau(s) = 1$

"no false statement has a proof"

complete: $\tau(s) = 1 \Rightarrow \exists p \in P\ \phi(s,p) = 1$

"all true statements have a proof"

trivial example: $S = P = \{0\}$

$\tau(0) = 0$, $\phi(0,0) = 1 \Rightarrow$ unsound

logical calculi: **interpretation A:** assigns values to symbols in a formula

predicate logic: truth assignment of atomic form.

prop. logic: $A = (U, \phi, \psi, \varepsilon)$ — free symbols

ϕ: defines/assigns functions

ψ: assigns function to predicates

ε: assigns value $\in U$ to all free variables

suitable: assigns values to all free symb.

model: $A \models F$ or $A \models M$ ($M = \{F_1, F_2, \dots, F_n\}$)

$\Leftrightarrow A(F) = 1$ or $A(M) = 1$ ($A(F_i) = 1$ for all i)

A must be suitable

satisfiable: $\Leftrightarrow$ F has a model / $A \models F$ for some A

tautology: $A \models F$ for any suitable A, $\models F$

L. F tautology $\Leftrightarrow \neg F$ unsatisfiable

logical consequence: F, G formulae

$F \models G \Leftrightarrow$ every A suitable for both F and G, $A(F) = 1 \Rightarrow A(G) = 1$

equivalence:

$F \equiv G \Leftrightarrow F \models G$ and $G \models F$

L: equivalent:

1. $\{F_1, \dots, F_k\} \models G$ — show with truth table
2. $(F_1 \wedge F_2 \wedge \dots F_k \wedge \to G) \equiv T$ (tautology)
3. $\{F_1, F_2, \dots, F_k, \neg G\}$ unsatisfiable

Def. $\wedge, \vee, \neg$: prop./pred. logic

$\wedge$: $A(F \wedge G) = 1 \Leftrightarrow A(F) = 1$ and $A(G) = 1$

$\vee$: $A(F \vee G) = 1 \Leftrightarrow A(F) = 1$ or $A(G) = 1$

$\neg$: $A(\neg F) = 1 \Leftrightarrow A(F) = 0$

Def. $\forall, \exists$: pred. logic $A_{[x \to u]}$ → set $\varepsilon(x)$ to $u \in U$

$A(\forall x\, G) = 1 \Leftrightarrow A_{[x \to u]}(G) = 1$ for all $u \in U$

$A(\exists x\, G) = 1 \Leftrightarrow A_{[x \to u]}(G) = 1$ for some $u \in U$

Normal form $L = F$ or $\neg F$ literal

CNF and DNF: CNF $\hat{=}$ "conjunction of disj."

$F = (L_{x_1} \vee \dots \vee L_{x_x}) \wedge \dots \wedge (L_{y_1} \vee \dots \vee L_{y_y})$

DNF $\hat{=}$ "disjunction of conjunctions"

$F = (L_{x_1} \wedge \dots \wedge L_{x_x}) \vee \dots \vee (L_{y_1} \wedge \dots \wedge L_{y_y})$

Prenex form: $Q_1 x_1 Q_2 x_2 \dots Q_n x_n\ G$

Derivation: **derivation rule:** $\{F_1, \dots, F_k\} \vdash_R G$

derivation: start with M. Take $N \subseteq M$. use $N \vdash_R G$

$M = M \cup \{G\}$ **calculus K:** set of deriv. rules: $\{R_1, \dots R_m\}$

can derive G from M with finite number of derivations $\Rightarrow M \vdash_K G$

complete: $M \models G \Rightarrow M \vdash_K G$

sound: $M \vdash_K G \Rightarrow M \models G$

Resolution calculus: take formula F in CNF

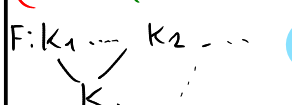
F: 

$K(F)$ = set of all clauses → $\emptyset \Rightarrow$ taut.

clauses → $\emptyset \Rightarrow$ unsatis.

$L \in K_1, \neg L \in K_2$:

$\{K_1, K_2\} \vdash_{Res} K = K_1 \setminus \{L\} \cup K_2 \setminus \{\neg L\}$

F: 

L. resolution calc. is sound

Show $M \models F \to G = M \cup \{\neg F\}$

$K(M) \vdash_{Res} \emptyset \Leftrightarrow F$ unsat. → show G unsat. ($K(G) \vdash_{Res} \emptyset$)

Recipes: show F taut. → show $\neg F$ unsat.

find CNF/DNF: a) use equivalences

b) draw truth table — disjunction: $A_i = 0 \to$ take A_i; $A_i = 1 \to$ take $\neg A_i$

CNF: for each row = 0: ⇒ formula is exactly 0 for these rows

DNF: for each row = 1: conjunction: $A_i = 0 \to$ take $\neg A_i$, $A_i = 1 \to$ take A_i

⇒ formula exactly 1 for these rows. 1) find free variables

Prenex form: 2) rectify by renaming variables

3) apply equivalences

Equivalences:

L 6.1: $\square = \wedge$ or $\vee$

$A \square A \equiv A$, $A \square A \equiv A$

$A \square B \equiv B \square A$, $A \square B \equiv B \square A$ (comm.)

$(A \square B) \square C \equiv A \square (B \square C)$ (assoc.)

$A \wedge (A \vee B) \equiv A \equiv A \vee (A \wedge B)$ *

$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$ * (1. distr)

$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$ * (1. distr)

$\neg\neg A \equiv A$

$\neg(A \wedge B) \equiv \neg A \vee \neg B$ * (de Morgan)

$\neg(A \vee B) \equiv \neg A \wedge \neg B$

$F \vee T \equiv T$ and $F \wedge T \equiv F$

$F \vee \bot \equiv F$ and $F \wedge \bot \equiv \bot$

$F \vee \neg F \equiv T$ and $F \wedge \neg F \equiv \bot$ *

Show calculus is sound: show for all R_i: $F \vdash_{R_i} G \Rightarrow F \models G$

Trans.: $A \to B \wedge B \to C \models A \to C$

L. 6.8: (Prop. logic) $Q = \forall$ or $\exists$

$\neg(\forall x\, F) \equiv \exists x\, \neg F$

$\neg(\exists x\, F) \equiv \forall x\, \neg F$

$(\forall x\, F) \wedge (\forall x\, G) \equiv \forall x\, (F \wedge G)$

$(\exists x\, F) \vee (\exists x\, G) \equiv \exists x\, (F \vee G)$

$Q x\, Q y\, F \equiv Q y\, Q x\, F$

$(Q x\, F) \square H \equiv Q x\, (F \square H)$

x not free in H!