Proof Patterns

formula with fixed interpretation is a statement
statement is either true or false

composition of implication:
$S \Rightarrow T$ and $T \Rightarrow U$ then $S \Rightarrow U$

Direct proof:
Assume S true, show $S \Rightarrow T$

Indirect proof:
Assume T false, show $\neg T \Rightarrow \neg S$

Proof by contradiction:
Prove S false, show $\neg T \Rightarrow S$

} to prove T

Pigeonhole principle:
n objects partitioned in $k \leq n$ sets, then at least one set contains $\lceil \frac{n}{k} \rceil$ objects.

Proof by induction:
Prove $P(0)$, prove $P(n) \Rightarrow P(n+1)$ for any n

Also: existence p., $\neg$p. by counter-example, case dist.

Proof systems

$T = (S, P, \tau, \emptyset)$: Set S of statements, set P of proofs, truth function $\tau: S \to \{0,1\}$, verification function $\emptyset: S \times P \to \{0,1\}$

T sound:
if $\emptyset(S,p)=1$ then $\tau(S)=1$

T complete:
if $\tau(S)=1$ then $\exists p$ s.t. $\emptyset(S,p)=1$

$\forall s$

Logic

Suitable interpretation:
assigns a value to (at least) each free symbol

Model:
S. int. for which a formula is true $A \models F$

F satisfiable: there exists a model for F

F unsatisfiable: otherwise $\perp$.

F tautology: true for any S. int $T / \models F$

$F \models G$: every model for F is model for G

$F \equiv G$: every s. int. has same truth value for F and G

The following statements are equivalent:
- $\{F_1, F_2, \dots F_K\} \models G$
- $(F_1 \wedge F_2 \wedge \dots F_K) \to G$ tautology
- $\{F_1, F_2, \dots F_K, \neg G\}$ unsatisfiable

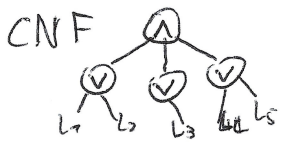
Propositional logic

Syntax: $F, \neg F, F \vee G, F \wedge G$ are formulas

Semantics: atomic formulas are free
$A(\neg F) = 1$ iff $A(F) = 0$
$A(F \vee G) = 1$ iff $A(F) = 1$ OR $A(G) = 1$
$A(F \wedge G) = 1$ iff $A(F) = 1$ AND $A(G) = 1$

Literal: $A, \neg A$ ...

CNF



ex. When is F false?

DNF

When is F true

function table!

Def: $F \to G \equiv \neg F \vee G$
$F \leftrightarrow G \equiv (F \wedge G) \vee (\neg F \wedge \neg G)$

For any formulas: idempotence, commutativity, associativity, absorption $F \wedge (F \vee G) \equiv F \equiv F \vee (F \wedge G)$, distributivity, double negation, de Morgan's rules,

Predicate Logic (extension of p.l.)

J.F.

Syntax: variables, function, predicates, terms (f(x))
- a predicate with terms as argument is formula
- $\forall x F, \exists x F$ are formulas

Semantics:
- variables bound to $\forall, \exists$ are not free.
- predicates and functions are free
- s. int. gives universe (non-empty set) and def. free v
- $A(\forall x F) = 1$ iff $A_{[x \to v]}(F) = 1$ for all $v \in U^A$
- $A(\exists x F) = 1$ iff $A_{[x \to v]}(F) = 1$ for some $v \in U^A$

Substitution:
$\forall x G \equiv \forall_y G[x/y]$ and $\exists x G \equiv \exists_y G[x/y]$ y not free in G

Universal instantiation:
$\forall x F \models F[x/t]$ for any term t

Prenex normal form:
$Q_1 x_1 Q_2 x_2 \dots Q_n x_n G$ where Q_i quantifiers
G formula w/out q.

ex. identify free variables → sub. bound variables with same name → take quantifiers out of brackets.
$\forall x (P(x,y)) \wedge Q(x) \equiv \forall s (P(s,y)) \wedge Q(x) \equiv \forall s (P(s,y) \wedge Q(x)$

Equivalences:
- $\neg(\forall x F) \equiv \exists x \neg F$
- $\neg(\exists x F) \equiv \forall x \neg F$
- $\forall x F \wedge \forall x G \equiv \forall x (F \wedge G)$
- $\exists x F \wedge \exists x G \equiv \exists x (F \wedge G)$
- $Q_1 Q_2 x F \equiv Q_2 Q_1 x F$

x not free in H:
- $(Q_1 x F) \wedge H \equiv Q_1 x (F \wedge H)$
- $(Q_1 x F) \vee H \equiv Q_1 x (F \vee H$

Logical calculi (set of rules to manipulate formulas)

Derivation rule: $\{F_1, \dots F_K\} \vdash_R G$ (precondition → $\{F_1,\dots F_K\}$, formula → G)

Applying R to set of formulas M:
- chose formulas $N \subseteq M$ such that $N \vdash_R G$
- add G to M $(M \to M \cup \{G\})$

Calculus $K = \{R_1, \dots R_n\}$ set of rules

If applying rules in K to M results in formula G:
$M \vdash_K G$

Sound: $\forall M \forall F \quad M \vdash_K F \Rightarrow M \models F$

Complete: $\forall M \forall F \quad M \models F \Rightarrow M \vdash_K F$

Resolution calculus for p.l. $Res = \{res\}$ (sound)

CNF: $(L_1 \vee L_2) \wedge (L_3 \vee L_4) \to K(F) = \{\{L_1, L_2\}, \{L_3, L_4\}\}$
(L_i: literal; $(L_3 \vee L_4)$: clause; $K(F)$: set of clauses)

Res:
$\{K_1, K_2\} \vdash_{res} K_1 \setminus \{L\} \cup K_2 \setminus \{\neg L\}$

Ex: $K(M) \vdash_{res} \emptyset \Leftrightarrow M$ unsatisfiable

$M \cup \{\neg F\}$ unsatisfiable $\Leftrightarrow M \models F$

$\neg F$ unsatisfiable $\Leftrightarrow F$ tautology

Sets

Equality:
$A = B \Leftrightarrow \forall x (x \in A \leftrightarrow x \in B)$
↳ $\{a\} = \{b\} \Leftrightarrow a = b$
↳ $|A| \neq |B| \Rightarrow A \neq B$

Subset
$A \subseteq B \Leftrightarrow \forall x (x \in A \to x \in B)$
↳ $A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$

Empty set:
- $\forall x (x \notin \emptyset)$
- there is only one
- subset of every set (also itself)
- NOT element of itself

Power set:
$P(A) = \{S \mid S \subseteq A\}$ all subsets of A
↳ $|A| = K \to |P(A)| = 2^K$

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

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

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

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

For any sets:
Idempotence, commutativity, associativity, absorption $A \cap (A \cup B) = A = A \cup (A \cap B)$, consistency $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$, distributivity

Cartesian product:
$A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$
↳ ordered pair: $(a,b) = (b,c) \Leftrightarrow a = c \wedge b = d$

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

$\emptyset \times A = \emptyset$

Relations

ρ relation from A to B: $\rho \subseteq (A \times B)$
↳ $(a,b) \in \rho$: $a \rho b$ otherwise: $a \not\rho b$
a relation is a subset

Inverse:
$\hat{\rho}$ from B to A: $\{(b,a) \mid (a,b) \in \rho\}$

Composition: (associative)
$\rho \subseteq (A \times B)$, $\sigma \subseteq (B \times A)$
$\Rightarrow \rho \circ \sigma = \{(a,c) \mid \exists b ((a,b) \in \rho \wedge (b,c) \in \sigma)\}$
↳ σ^n: n-fold composition of σ
↳ $\widehat{\rho \circ \sigma} = \hat{\sigma} \circ \hat{\rho}$

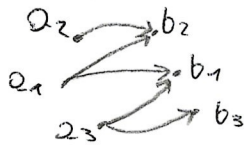
Identity on A:
$id = \{(a,a) \mid a \in A\}$

representations

Matrix

	b_1	b_2	b_3
a_1	1	1	0
a_2	0	1	0
a_3	1	0	1

Graph



A relation on A is:
- reflexive: if $a \rho a$ $\forall a \in A$ $(id \subseteq \rho)$
- irreflexive if $a \not\rho a$ $\forall a \in A$
- symmetric if $a \rho b \Rightarrow b \rho a$ $\forall a,b \in A$ $(\rho = \hat{\rho})$
- antisymmetric: if $(a \rho b \wedge b \rho a) \Rightarrow a = b$ $(\rho \cap \hat{\rho} \subseteq id)$
- transitive if $(a \rho b \wedge b \rho c) \Rightarrow a \rho c$ $(\rho^2 \subseteq \rho)$

Transitive closure on A:
$\rho^* = \bigcup_{n \in \mathbb{N} \setminus \{0\}} \rho^n$ (transitive)
if ρ transitive then $\rho^* = \rho$
$a \rho^* b \Leftrightarrow$ you can reach b from a by applying ρ

Equivalence relation θ reflexive, symmetric, transitive

Bsp: $id, =, \equiv_m (on\ \mathbb{Z})$,

$\theta_1 \cap \theta_2$ is an equivalence relation

Equivalence class:

$[a]_\theta = \{b \in A \mid b \theta a\}$

Bsp: $[1]_{\equiv_3} \{\dots, -5, -2, 1, 4, 7, \dots\}$

set of eq. classe:

$A/\theta = \{[a]_\theta \mid a \in A\}$ (partition of A)

Order relation $\preceq$ reflexive, antisymmetric, transitive

Bsp: $\leq (\mathbb{Q}, \mathbb{Z}, \mathbb{R}), \mid (\mathbb{N}\setminus\{0\}), \subseteq (P(A))$

relation $\prec$: $a \prec b \Leftrightarrow a \preceq b \wedge a \neq b$

poset $(A, \preceq)$ $\preceq$ p.o. rel. on A

- $a, b \in A$ comparable if $a \preceq b$ or $b \preceq a$
- if all elements of A are comparable, then A is totally ordered by $\preceq$.
- b covers a if $a \prec b$ and $\neg\exists c$ with $a \prec c \prec b$

Hasse: edge from a to b if b covers a

combination of posets:

$(A, \preceq) \times (B, \sqsubseteq) = (A \times B, \leq)$ also poset

with $(a_1, b_1) \leq (a_2, b_2) \Leftrightarrow (a_1 \preceq a_2) \wedge (b_1 \sqsubseteq b_2)$

lexicographic order:

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

$\hookrightarrow (A \times B) \leq_{lex})$ is poset

$S \subseteq A$ $a \in A$ minimal element if $\neg\exists b$ with $b \prec a$ [maximal]

$a \in A$ least element if $a \preceq b$ $\forall b \in A$ [greatest]

$a \in A$ lower bound of S if $a \preceq b$ $\forall b \in S$ [upper]

$a \in A$ greatest lower bound of S if greatest element of set of all lower bounds [least upper bound]

poset well ordered:

totally ordered and every subset has least el.

Meet:

greatest lower bound of a and b

Join:

least upper bound of a and b $\{a,b\} \subseteq A$

Lattice:

poset in which every pair has meet and join

Functions

relation $f: A \to B$ for which

- $\forall a \in A\ \exists b \in B$ afb
- $\forall a \in A\ \forall b, b' \in B\ ((afb \wedge afb') \to b = b')$

injective:

$a \neq b \Rightarrow f(a) \neq f(b)$ $\forall a, b \in A$

surjective:

$f(A) = B$ or $\forall b \in B\ \exists a \in A (f(a) = b)$

B^A set of functions $A \to B$

Countability of sets

$A \sim B$ (equinumerous):

exists bijection $A \to B$

$A \preceq B$ (B dominates A):

injection $A \to B$ or $A \sim C$ for $C \subseteq B$

- transitive: $A \preceq B \wedge B \preceq C \to A \preceq C$
- $A \subseteq B \Rightarrow A \preceq B$

A is countable if:

- is finite or
- $A \sim \mathbb{N}$ (bijection $\mathbb{N} \to A$, $A \to \mathbb{N}$)

Countable sets: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \{0,1\}^*, A \times B, A^n, A \cup B$ for countable A, B, $A^* = \{a_1 a_2 \dots a_n\}$, $A[x]$

Uncountable sets: $\mathbb{R}, \mathbb{R}\setminus\mathbb{N}, P(\mathbb{N}), \{0,1\}^\infty$

Number Theory

J.F.

$a|b \Leftrightarrow b = ak$ $\quad -a|0$, $\pm 1|a$ for any $a \neq 0$

Euclidean division:

$a = dq + r$ $\quad (d \neq 0, 0 \leq r < |d|)$

$\hookrightarrow Rd(a) := r$

$R_m(f(a_1, \dots a_k)) = R_m(f(R_m(a_1), \dots R_m(a_k)))$

ex. $gdc(a,m) = 1$, $R_m(a^{\varphi(m)}) = 1$

$\Rightarrow R_m(a^q) = R_m(a^{R_{\varphi(m)}(q)})$

Bsp: $R_{26}(7^{100}) = R_{26}((7^2)^{50}) = R_{26}(R_{26}(49)^{50}) = R_{26}(1^{50}) = 1$

Greatest common divisor:

- $gdc(m, n - qm) = gdc(m, n)$ $\forall q \in \mathbb{Z}$
- $gdc(m, R_m(n)) = gdc(m, R_m(n)) = gdc(m, n)$
- $gdc(a,b) = ua + vb$ $u, v \in \mathbb{Z}$, a, b not both 0

Extended GDC algorithm: $(b \geq a)$

(1) $b - q_1 \cdot a = r_1$ (eudid. div.)

(2) $a - q_2 \cdot r_1 = r_2$

$\vdots$

(...) $r_n - q \cdot r_{n+1} = 0 \to gdc(a,b) = r_{n+1}$

Then in the second to last eq. sub the remainder from the eq. above until $a \cdot v + b \cdot u$

Least common multiple:

$gdc(a,b) \cdot lcm(a,b) = a \cdot b$

Ideals:

$(a) = \{ua \mid u \in \mathbb{Z}\}$

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

$\forall a, b \in \mathbb{Z}\ \exists d \in \mathbb{Z}$ $(a,b) = d \to d$ is a greatest common divisor of a and b

Modular congruence

$a \equiv_m b \Leftrightarrow m|(a-b)$ $\quad m \geq 1$

$a \equiv_m b \wedge c \equiv_m d \Rightarrow \begin{cases} a+b \equiv_m c+d \\ ab \equiv_m cd \end{cases}$

Set $\mathbb{Z}_m = \{0, 1, \dots m-1\}$ $\quad |\mathbb{Z}_m| = m = |\mathbb{Z}/\equiv_m|$

$ax \equiv_m 1$ has unique sol. $x \in \mathbb{Z}_m$ iff $gdc(a,m) = 1$

multiplicative inverse, use GDC algo

$x + km$ is also sol.

Chinese remainder theorem

Let $m_1, \dots m_r$ relatively prime, $M = \prod_{i=1}^{r} m_i$
and $0 \le a_i < m_i$. $M_i := M/m_i$.

$$\begin{cases} x \equiv_{m_1} a_1 \\ \vdots \\ x \equiv_{m_r} a_r \end{cases}$$ has a unique solution $0 \le x < M$ ($x+kM$ also sol.)

For every M_i there is N_i such that $M_i N_i \equiv_{m_i} 1$

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

Diffie-Hellman

A	insecure channel	B
choose $x_A \in \{0..p-2\}$	large prime p, integer g	choose $x_B \in \{0..p-2\}$
$y_A = R_p(g^{x_A})$	y_A → , ← y_B	$y_B = R_p(g^{x_B})$
$K_{AB} = R_p(y_B^{x_A})$		$K_{BA} = R_p(y_A^{x_B})$

same secret key

↳ group $\langle \mathbb{Z}_p^*, \odot \rangle$

works for any cyclic group in which computing x from g^x is infeasable

Algebra $\langle S, * \rangle$ — Groups

Neutral element: $e \in S$ $e * a = a * e = a$ $\forall a \in S$ (unique)

Associativity: $a * (b * c) = (a * b) * c$ $\forall a,b,c \in S$

NOT associative: exponentiation

Monoid: $\langle S, *, e \rangle$ - $*$ associative
- e neutral element

Inverse:
$b \in S$ $b * a = a * b = e$ (unique)

Group $\langle G, *, \hat{}, e \rangle$ with
- G1 $*$ associative
- G2 e neutral element
- G3 every a has an inverse $\hat{a}$

BSP $\langle \mathbb{Z}, +, -, 0 \rangle$ $\langle \mathbb{Q}, +, -, 0 \rangle$ $\langle \mathbb{Q} \setminus \{0\}, \cdot, ^{-1}, 1 \rangle$
$\langle \mathbb{R}, +, -, 0 \rangle$ $\langle \mathbb{R} \setminus \{0\}, \cdot, ^{-1}, 1 \rangle$ $\langle \mathbb{Z}_m, \oplus, \ominus, 0 \rangle$
$\langle \mathbb{Z}_m^*, \odot, ^{-1}, 1 \rangle$ $\langle A^{n \times n}, \cdot, ^{-1}, I_n \rangle$ not commutative

For any group:
- $\widehat{(\hat{a})} = a$ — $\widehat{a * b} = \hat{b} * \hat{a}$
- $a * b = a * c \Rightarrow b = c$
- $b * a = c * a \Rightarrow b = c$
- $a * x = b$ has unique sol.

Direct product: $\langle G_1, *_1 \rangle \times \langle G_2, *_2 \rangle$
$\langle G_1 \times G_2, \star \rangle$ is a group where
- $(a_1, a_2) \star (b_1, b_2) = (a_1 *_1 b_1, a_2 *_2 b_2)$
- (e_1, e_2) is neutral element
- $\widehat{(a_1, a_2)} = (\hat{a}_1, \hat{a}_2)$

Group homomorphism

groups $\langle G, *, \hat{}, e \rangle$ $\langle H, \star, \tilde{}, e' \rangle$

$\varphi: G \to H$ is group homomorphism iff
$\varphi(a * b) = \varphi(a) \star \varphi(b)$. $\forall a,b \in G$

It follows:
- $\varphi(e) = e'$ — $\varphi(a^n) = \varphi(a)^n$ $\forall a \in G$
- $\varphi(\hat{a}) = \widetilde{\varphi(a)}$ $\forall a \in G$

If φ bijective then isomorphism, $G \simeq H$ (isomorphic)

BSP projection xy-plane $\langle \mathbb{R}^3, \text{vec.add.} \rangle \to \langle \mathbb{R}^2, \text{vec.add.} \rangle$

determinant: $\langle A^{n \times n}, \text{matrix} \cdot \rangle \to \langle \mathbb{R}, \cdot \rangle$

log: $\langle \mathbb{R}^{>0}, \cdot \rangle \to \langle \mathbb{R}, + \rangle$ isomorphism ($\log(a \cdot b) = \log(a) + \log$

$\varphi: \mathbb{Z}_6 \times \mathbb{Z}_{10} \to \mathbb{Z}_2 \times \mathbb{Z}_{30}$ $(a,b) \mapsto (a', b')$ $a' = R_2(a)$, $b' = R_3(a)$, $b' = R_{10}(b)$
isomorphism

Subgroups

$H \subseteq G$, $\langle H, *, \hat{}, e \rangle$ is subgroup of $\langle G, *, \hat{}, e \rangle$ if:
- H1 $a * b \in H$ $\forall a,b \in H$
- H2 $e \in H$
- H3 $\hat{a} \in H$ $\forall a \in H$

Then
$|H| \mid |G|$

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

Order of elements

$\text{ord}(a)$: least $m \ge 1$ such that $a^m = e$

If G finite:
- every element has finite order
- $\text{ord}(a) \mid |G|$ $\forall a \in G$
- $a^{|G|} = e$

Cyclic groups

$\in G$ finite order. Group generated by a:

$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is called cyclic

$-\langle a \rangle \subseteq G$ smallest subgroup containing a

Also:

- $|\langle g \rangle| = \text{ord}(g) \Leftrightarrow g$ is generator
- any group of prime order is cyclic every element except e is generator.
- g generator, then g^{-1} generator
- isomorphic to $\langle \mathbb{Z}_n, \oplus \rangle$ (commutative)

gen: every a with $gdc(a,n)=1$

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

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

$-m = \prod p_i^{e_i}$ (prime fact.) $\Rightarrow \varphi(m) = \prod (p_i - 1) p_i^{e_i - 1}$

$n \geq 2$:

$-a^{\varphi(n)} \equiv_n 1 \Leftrightarrow a \cdot a^{\varphi(n)-1} \equiv_n 1$

prime p, $p \nmid a$:

$-a^{p-1} \equiv_p 1$

$\mathbb{Z}_m^*$ cyclic iff $m = 2, 4, p^e, 2p^e$ (p odd prime, $e \geq 1$)

RSA

$\cdot$ finite group, $e \in \mathbb{Z}$ with $gdc(e, |G|) = 1$, Then

$x^e = y \Leftrightarrow x = y^d$ where $ed \equiv_{|G|} 1$

A	insecure channel	B
choose primes p, q $n = pq$ $\varphi(n) = (p-1)(q-1)$ choose e $gdc(e, \varphi(n)) = 1$	n, e →	message $m \in \mathbb{Z}_n^*$ encrypted message $y = R_n(m^e)$
$d \equiv_{\varphi(n)} e^{-1}$ $m = R_n(y^d)$	← y	

Group $\mathbb{Z}_n^*$

Rings

$\langle R, +, -, 0, \cdot, 1 \rangle$ for which:

R1 $\langle R, +, -, 0 \rangle$ is commutative group

R2 $\langle R, \cdot, 1 \rangle$ is monoid

R3 left and right distributive

Bsp $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \langle \mathbb{Z}_m, \oplus, \odot, 0 \rangle$ (commutative)

For any ring:

- $0a = a0 = 0$

  proof: $0 = -(a0) + a(0) = -(a0) + a(0+0)$
  $= 0 + a0 = a0$

- $(-a)b = -(ab)$ inverse

  proof: $(-a)b + ab = (-a+a)b = 0$

- $(-a)(-b) = ab$ inverse

  proof: $(-a)(-b) + (-(ab)) = (-a)(-b+b) = 0$

- if R non trivial, $1 \neq 0$

  proof assume $1 = 0$, show $|R| = 1$

Divisors: (in comm. rings)

- if $a|b$ and $b|c$ then $a|c$
- if $a|b$ then $a|bc$ $\forall c$
- if $a|b$ and $a|c$ then $a|(b+c)$

Characteristic:

order of 1 in additive group (=0 if inf.)

Units:

$\exists u^{-1} \in R$ $uu^{-1} = u^{-1}u = 1$

R^* (set of units) is mult. group

Zerodivisors:

$a \neq 0$ $\exists b \neq 0$ $ab = 0$

Integral domain:

non-trivial ring without zerodivisors

↳ $a|b$ $\exists$ unique c with $b = ac$

(R is commutative)

Bsp $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ p is prime

NOT $\mathbb{Z}_m$, if $gdc(a,m) \neq 1 \Rightarrow a$ zerodivisor

Polynomial rings

J.F

$R[x]$ set of polynomials over R. Is a ring.

D integral domain, so is $D[x]$, and $D[x]^* = D^*$

Fields

Non-trivial commutative ring in which every non-zero elem is a unit, so $F^* = F \setminus \{0\}$

$\Leftrightarrow \langle F \setminus \{0\}, \cdot, ^{-1}, 1 \rangle$ is commutative group

- a field is an integral domain
- a finite integral domain is a field

Bsp $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ NOT $\mathbb{Z}$, $R[x]$ for any R

$GF(m)$ $(= \mathbb{Z}_m)$ is a field iff m is prime

Polynomial fields

$b(x) | a(x) \Leftrightarrow v \cdot b(x) | a(x)$ for any $v \in F$ $v \neq 0$

Monic polynomial:

First coefficient is 1

Irreducible:

only divisible by constanst or multiple of itself

Ex. Irreducible polynomials (monic, from deg 2)

GF(2)	GF(3)		GF(4)			GF(5)	GF(7)	
111	101	1211	112	1021	1213	102	101	131
1011	112	1222	113	1031	1222	103	102	135
1101	122		121	1101	1232	111	104	136
10011	1021		122	1112	1233	112	113	141
11001	1022		131	1113	1301	123	114	145
11111	1102		133	1123	1312	124	116	146
	1112		1002	1132	1322	133	122	152
	1121		1003	1201	1323	136	123	153
	1201		1011		1333	141	125	155
						142	136	163
							166	166

Ex. Prove polynomial is irreducible

- first check for roots
- deg 1 → irreducible
- deg 2 → irreducible = no roots; red. = 2 factors of deg 1
- deg 3 → irreducible = no roots; red. = at least 1 factor of deg 1
- deg 4 → irreducible; → factor of deg 1; → irred. factor of deg 2
- deg d check monic polyn. of deg up to $d/2$

Eudidean division

$a(x) = d(x) \cdot q(x) + r(x)$ $(d(x) \neq 0, \deg(r(x)) < \deg(d(x)))$

Polynomials as functions

Any $a(x) \in R[x]$ is a function $a: R \to R$ $\alpha \mapsto a(\alpha)$

Root:

α for which $a(\alpha) = 0$

↳ in $F[x]$ α root $\Leftrightarrow (x-\alpha) \mid a(x)$

↳ $a(x) \in F[x]$ non-zero, $\deg(a(x)) = d$, then

a has at most d roots, and is uniquely determined by $d+1$ values of distinct α_i.

The ring $F[x]_{m(x)}$

Congruence modulo $m(x)$

$a(x) \equiv_{m(x)} b(x) \Leftrightarrow m(x) \mid (a(x) - b(x))$

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

- is a field iff m is irreducible
- $|F[x]_{m(x)}| = |F|^{\deg(m)}$

$a(x)b(x) \equiv_{m(x)} 1$ has a unique solution iff $\gcd(a(x), m(x)) = 1$.

It follows:

$$F[x]^*_{m(x)} = \{a(x) \in F[x] \mid \gcd(a(x), m(x)) = 1\}$$

Error-correcting codes

(n,k)-encoding function E for the alphabet $\{0,1\}$

$E: \{0,1\}^k \to \{0,1\}^n : (a_0, \dots a_{k-1}) \mapsto (c_0, \dots c_{n-1})$

- $n > k$
- is injective

The set of codewords $C = \mathrm{Im}(E)$ is called an error-correcting code ~~with cardinality~~

An (n,k)-error-correcting code has cardinality 2^k.

Hamming distance: (btw. two string of equal length)

number of positions at which they differ

Minimum distance of e.c.c. C:

$d_{min}(C)$ min. of Hamming distance btw. any two codewords

Decoding function $D: \{0,1\}^n \to \{0,1\}^k$ is

t-error correcting for E if any $(a_0, \dots a_{k-1})$

$D((r_0, \dots r_{n-1})) = (a_0, \dots a_{k-1})$

for any $(r_0, \dots r_{n-1})$ with Hamming distance at most t from $E((a_0, \dots a_{k-1})) = (c_0, \dots c_{k-1})$

C is t-error correcting if there exists E and D with $C = \mathrm{Im}(E)$ where D is t-error correcting

C with minimum distance d is t-error correcting $\Leftrightarrow d \geq 2t+1$

If alphabet $GF(q)$, $E((a_0, \dots a_{k-1})) = (a(\alpha_0), \dots a(\alpha_{n-1}))$

where: - $\alpha_0, \dots \alpha_{n-1} \in GF(q)$

- $a(x) = a_{k-1}x^{k-1} + \dots a_1 x + a_0$

The minimum distance is $n-k+1$

Barbatrucchi

Let $\gcd(m,n) = 1$

Algebra

Cyclic group with q elements:

$\to \mathbb{Z}_q$, $\mathbb{Z}_n \times \mathbb{Z}_m$ $(q = mn)$

Non cyclic:

$\to \mathbb{Z}_r^*$ $(\varphi(n) = q$, $\mathbb{Z}_a \times \mathbb{Z}_b$ $\begin{cases} ab = q \\ \gcd(a,b) \neq \end{cases}$

$\mathbb{Z}_a \times \mathbb{Z}_b$ not cyclic if $\gcd(a,b) \neq 1$!

Group isomorphic to:

$\mathbb{Z}_{mn} \to \mathbb{Z}_n \times \mathbb{Z}_m$

$G \to G \times \{e\}$

Find zerodivisors of $\mathbb{Z}_m / F[x]_m$

→ divisors of m and their multiples

= all a with $\gcd(a,m) \neq 1$

Units of a Field and a generator

$\to F^* = F \setminus \{0\} \to$ any el. except 1

How many units in Ring R:

$\to |R| -$ # zerodiv. $- 1$

Find inverse in a field:

→ a tentativi?

$\to (m+1) : a = a^{-1}$?

Number theory

$x \equiv_{mn} a \Leftrightarrow \begin{cases} x \equiv_m a \\ x \equiv_n a \end{cases}$

Compute $R_{mn}(\text{expr.})$

$\to \begin{cases} R_{mn}(\text{expr}) \equiv_m R_m(\text{expr}) \\ R_{mn}(\text{expr}) \equiv_n R_n(\text{expr}) \end{cases} \to$ CRT.

$R_m(n^x) = R_m(n R_{\varphi(m)}(x))$

$(\text{even})^x = \text{even}$, $(\text{odd})^x = \text{odd}$

In a ring every element is either: 0, a zerodivisor or a unit