Proof Patterns

Direct proof of $S \Rightarrow T$: Assume S and then prove T
Indirect proof of $S \Rightarrow T$: Assume $\neg T$ and prove S
Modus Ponens prove R, prove $R \Rightarrow S$ to prove S
Case Dist. find $R_1 \dots R_n$, prove that at least one is true, prove $R_i \Rightarrow S$ for all R_i (to prove S)
Contradiction prove $\neg S \Rightarrow T$ and $\neg T$ (to prove S)
Existence show S_x for one $X \in \mathbb{X}$
Pigeonhole If n obj. partitioned into k sets then one of them has $\lceil \frac{n}{k} \rceil$ elements
Counterexample exhibit x s.t. $\neg S_x$
Induction prove $S(0)$ and $S(i) \Rightarrow S(i+1)$
Base case → Hypothesis → Induction Step

Sets

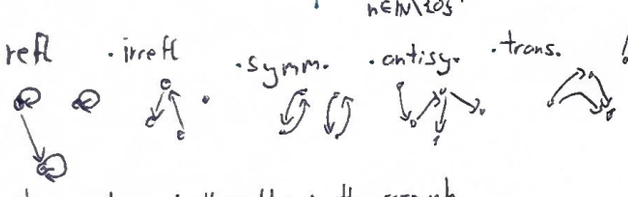
Russel Paradox $R = \{A \mid A \notin A\}$
$|A|$ = n.o. elems in A
$A = B \iff \forall x (x \in A \leftrightarrow x \in B)$
L3.1 $\{a\} = \{b\} \rightarrow a = b$
$A \subseteq B \iff \forall x (x \in A \rightarrow x \in B)$
L3.2 $A = B \iff (A \subseteq B) \wedge (B \subseteq A)$
L3.3 $A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$
$A \cup B = \{x \mid x \in A \vee x \in B\}$
$A \cap B = \{x \mid x \in A \wedge x \in B\}$
$B \setminus A = \{x \in B \mid x \notin A\}$
T3.4 idempotence, comm., ass., $A \cap (A \cup B) = A$, distr., $A \subseteq B \leftrightarrow A \cap B = A \leftrightarrow A \cup B = B$
$\emptyset = \forall x (\neg x \in \emptyset)$ is unique and subset of all sets
$P(A) = \{S \mid S \subseteq A\}$
$A \times B = \{(a,b) \mid a \in A, b \in B\}$
$(a,b) = (c,d) \leftrightarrow a = c \wedge b = d$

Relations

D3.9 p from A to B subset of $A \times B$
$(a,b) \in p = a\, p\, b$ (and $\notin = \not p$)
$id_A = \{(a,a) \mid a \in A\}$
$\{(a,b),(c,a)\}$ · $\begin{array}{c|ccc} & a & b & c \\ \hline a & 0 & 1 & 0 \\ b & 0 & 0 & 0 \\ c & 1 & 0 & 0 \end{array}$ = $a \to b$, $c \to a$
$\hat{p} = \{(b,a) \mid (a,b) \in p\}$ = "inverse"
$p \circ q = \{(a,c) \mid \exists b ((a,b) \in p \wedge (b,c) \in q)\}$ = "composition"
for $p: A \to B$, $q: B \to C$ and $p \circ q: A \to C$

$p^h = p \circ p \circ \dots \circ p$ (h-times)
L3.7 $p \circ (\sigma \circ \phi) = (p \circ \sigma) \circ \phi$
$\widehat{pq} = \hat{q}\hat{p}$ $\quad (pq = p \circ q)$

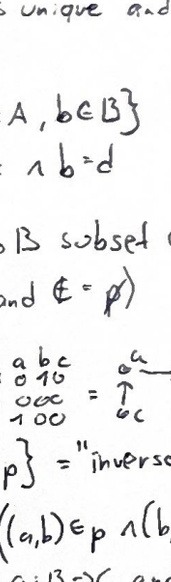
reflexive is p on A if $a\, p\, a$ for all $a \in A$, or if $id \subseteq p$
irreflexive = $a \not p a$ for all $a \in A$, or $id \cap p = \emptyset$
symmetric = $a\, p\, b \leftrightarrow b\, p\, a$, or $p = \hat{p}$
antisymmetric = $a\, p\, b \wedge b\, p\, a \rightarrow a = b$, or $p \cap \hat{p} \subseteq id$
transitive = $a\, p\, b \wedge b\, p\, c \rightarrow a\, p\, c$, or p transitive $\leftrightarrow p^2 \subseteq p$
trans. closure $p^* = \bigcup_{n \in \mathbb{N} \setminus \{0\}} p^n$



equivalence relation = reflexive, symmetric and transitive
$[a]_\theta = \{b \in A \mid b\, \theta\, a\}$ = "equivalence class of a on θ"
L3.10 if p, σ equiv. relations then $p \cap \sigma$ is equiv relation
partition of $A = \{S_i \mid i \in I\}$ s.t. $S_i \cap S_j = \emptyset$ and $\bigcup_{i \in I} S_i = A$
~~$A \setminus \theta$~~ $A/\theta = \{[a]_\theta \mid a \in A\}$ = "quotient set"
T3.11 A/θ is a partition of A

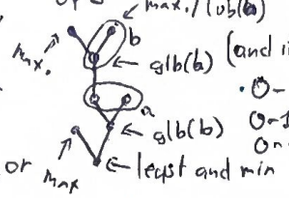
Partial Order Relations

partial order relation = reflexive, antisymmetric and transitive
$(A; \leq)$ = "poset" if $\leq$ p.o. relation
a, b comparable if $a \leq b$ or $b \leq a$, otherwise incomparable
totally ordered if all $a, b \in (A; \leq)$ are comparable
b covers a if $a < b$ and no c s.t. $a < c$ and $c < b$
$a \lessdot b = a \leq b \wedge a \neq b$
Hasse Diagram has edge (a,b) if b covers a (b above a)



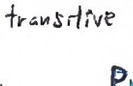
$(A; \leq_A) \times (B; \leq_B)$ = set $A \times B$ with relation
$(a_1, b_1) \leq (a_2, b_2) \leftrightarrow a_1 <_A a_2 \wedge b_1 \leq_B b_2$
T3.12 such a srt is partially ordered
$\leq_{lex}$ for $(A; \leq) \times (B; \leq)$ is
$(a_1, b_1) \leq_{lex} (a_2, b_2) \leftrightarrow a_1 < a_2 \vee (a_1 = a_2 \wedge b_1 \leq b_2)$

for $(A; \leq)$ poset and $S \subseteq A$:
minimal (maximal) element a if $\nexists b$ with $b < a$ ($b > a$)
least (greatest) element a if $\forall b\ a \leq b$ ($a \geq b$)
lower (upper) bound of S if $a \leq b$ ($a \geq b$) $\forall b \in S$
→ greatest lower bound / least upper bound is the greatest / least element of all lower / upper bounds of S



·0-multiple minimals, 0 or 1 least, 0 or 1 glb/lub

well-ordered if totally ordered and every non-empty subset has a least element.
·subset of poset is a poset
meet of a,b is the greatest lower bound of $\{a,b\}$
join of a,b is the least upper bound of $\{a,b\}$
·$a \wedge b$ = meet, $a \vee b$ = join
lattice is poset in which all pairs of elements have a meet and join



a, b have no join since there is no least among x, y?

Functions

function $f: A \to B$ is relation $A \times B$ with
1) totally def. $\forall a \in A\ \exists b \in B\ a\, f\, b$
2) well def. $\forall a \in A\ \forall b, b' \in B\ (a\, f\, b \wedge a\, f\, b' \rightarrow b = b')$
B^A = set of all functions $A \to B$
partial function is only well defined
image $f(S) = \{f(a) \mid a \in S\}$
image $f(A) = Im(f)$ for $f: A \to B$
Preimage $f^{-1}(T) = \{a \in A \mid f(a) \in T\}$
D3.39 $f: A \to B$ is called
·injective if $a \neq a' \rightarrow f(a) \neq f(a')$
·surjective if $f(A) = B$ or $\forall b \in B\ \exists a$ s.t. $f(a) = b$
·bijective if its both
$g \circ f = gf = g(f(x))$ for $f: A \to B$, $g: B \to C$
·reverse of relation composition
L3.14 $g \circ (f \circ h) = (g \circ f) \circ h$

Countability

$A \sim B$ if bijection $A \to B$ exists = "equinumerous"
$A \lesssim B$ if $A \sim C$ for $C \subseteq B$ or if exists injection $A \to B$ = "B dominates A"
A countable if $A \lesssim \mathbb{N}$, uncountable otherwise
$\sim$ is equivalence relation
$\lesssim$ is transitive
·$A \subseteq B \rightarrow A \lesssim B$
T3.16 $A \lesssim B \wedge B \lesssim A \rightarrow A \sim B$
A countable $\leftrightarrow$ A finite or $A \sim \mathbb{N}$
$\{0,1\}^*$ = set of finite binary sequences is countable
$\mathbb{Q}$ is countable $\mathbb{R}$ is uncountable
·for A_i countable and $i \in \mathbb{N}$:
- A^n countable
- $\bigcup_{i \in \mathbb{N}} A_i$ countable
- A^* countable = "finite sequences over A"

$A \times B$ countable for A, B countable
$\{0,1\}^\infty = \{f: \mathbb{N} \to \{0,1\}\}$ is uncountable = "infinite binary sequences"
Cantor Dia. Argument flip bit i of sequ. i

Number Theory

$a \mid b \iff \exists c$ s.t. $ac = b$ (otherwise $a \nmid b$)
Euclid $\forall a\ \forall d \neq 0\ \exists$ unique q, r:
$a = dq + r$ and $0 \leq r < |d|$
$gcd(a,b)$ is positive d:
$d \mid a \wedge d \mid b \wedge \forall c ((c \mid a \wedge c \mid b) \rightarrow c \mid d)$
a, b relatively prime $\iff gcd(a,b) = 1$
L4.2 $gcd(m, n - qm) = gcd(m, n)$
$(a,b) = \{au + bv \mid u, v \in \mathbb{Z}\}$ = "ideal generated by a, b"
$(a) = \{ua \mid u \in \mathbb{Z}\}$
L4.3 $\forall a, b\ \exists c$ s.t. $(a,b) = (c)$
L4.4 $(a,b) = (d) \rightarrow d = gcd(a,b)$ for not both $a, b \neq 0$
C4.5 $\forall a, b\ \exists u, v$ s.t. $gcd(a,b) = ua + vb$
$lcm(a,b)$ is d s.t.
$a \mid d \wedge b \mid d \wedge \forall m ((a \mid m \wedge b \mid m) \rightarrow d \mid m)$

(Extended) Euclid

Computes $\gcd(a,b) = ua + vb$:

	72	14	
72	1	0	
14	0	1	} 1·72 − 5·14
2	1	−5	} 1·14 − 7·2
0	−7	36	= 1·14 − 7(72 − 5·14)

→ $\gcd(72,14) = 2 = 1\cdot 72 - 5\cdot 14$

Diffie-Hellman

choose prime p and basis g, then

Alice: select x_A from $\{0 \dots p-2\}$; $y_A = R_p(g^{x_A})$

Bob: select x_B from $\{0 \dots p-2\}$; $y_B = R_p(g^{x_B})$

$y_A \rightarrow$, $\leftarrow y_B$

$k_{AB} = R_p(y_B^{x_A})$, $k_{BA} = R_p(y_A^{x_B})$

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

Security based on the fact that x_A is not possible to compute from y_A.

Primes

prime = $p > 1$ with only divisors 1 and p, otherwise "composite"

T4.6 Every pos. integer has unique prime factorization

L4.7 If p prime divides $a \cdot b \cdot c \dots$ then it divides at least one of $a, b, c \dots$

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

for $a = \prod_i p_i^{e_i}$, $b = \prod_i p_i^{f_i}$ · $\gcd(a,b)\cdot\operatorname{lcm}(a,b) = ab$

Modulo

$a \equiv_n b \leftrightarrow n \mid (a-b)$ $R_n(a)$ = "remainder of a by n"

$\equiv_n$ is equivalence relation on $\mathbb{Z}$ for $n \geq 1$

L4.14 $a \equiv_n b$ and $c \equiv_n d \rightarrow a+c \equiv_n b+d$, $ac \equiv_n bd$

C4.15 $a_i \equiv_n b_i \rightarrow f(a_1,\dots a_n) \equiv_n f(b_1 \dots b_n)$

L4.16 · $a \equiv_n R_n(a)$ · $a \equiv_n b \leftrightarrow R_n(a) = R_n(b)$

C4.17 $R_n(f(a_1 \dots a_n)) = R_n(f(R_n(a_1) \dots R_n(a_n)))$

$ax \equiv_n 1$ has (unique) solution $\leftrightarrow \gcd(a,n) = 1$

→ called "multiplicative inverse"

Chinese Remainder Theorem

for $m_1, \dots, m_r$ relatively prime, $M = \prod_{i=1}^r m_i$. For every list $a_1 \dots a_r$ with $a_i < m_i$ the system:

$x \equiv_{m_1} a_1$

$x \equiv_{m_2} a_2$

$\vdots$

$x \equiv_{m_r} a_r$ has a unique solution satisfying $0 \leq x < M$.

Finding solution

let $M_i = M/m_i$ and N_i s.t. $M_i N_i \equiv_{m_i} 1$

then $x = R_m\left(\sum_{i=1}^r a_i M_i N_i\right)$ is the solution.

direct product

$\langle G_1 \times \dots \times G_n, * \rangle$ of n groups $\langle G_i, *_i \rangle$ where $*$ is def.:

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

L5.4 this is a group where neutral/inverse elements are component-wise

homomorphism is a function $\psi: G \rightarrow H$ with $\psi(a * b) = \psi(a) \diamond \psi(b)$ $\forall a,b$ (where $*$ is op. on G and $\diamond$ on H)

isomorphism is bijective homomorphism

$G \cong H$ if G isomorphic to H

L5.5 for ψ homomorphism $\langle G; *, \hat{}, e\rangle \rightarrow \langle H; \diamond, \tilde{}, e'\rangle$:

· $\psi(e) = e'$ · $\psi(\hat{a}) = \widetilde{\psi(a)}$

Algebra

operation is function $S^n \rightarrow S$ with "arity" n

algebra is pair $\langle S; \Omega\rangle$ with S "carrier" set and Ω list of operations on S

Groups and Monoids

left/right neutral element is $e \in S$ with $e * a = a$ / $a * e = a$ $\forall a \in S$. If $e*a = a*e = a$ then "neutral element"

L5.1 neutral element is unique

associative $a \times (b \times c) = (a \times b) \times c$

monoid is $\langle M; *, e\rangle$ with $*$ associative and e neutral element

left/right inverse of a is b s.t. $b * a = e$ / $a * b = e$. If both hold then "inverse".

L5.2 inverse is unique

GROUP is algebra $\langle G; *, \hat{}, e\rangle$ with:

G1 $*$ associative

G2 e neutral element

G3 every $a \in G$ has an inverse $\hat{a}$

commutative/abelian group if $a * b = b * a$ $\forall a,b$

L5.3 · $\hat{(\hat{a})} = a$ · $\widehat{a*b} = \hat{b} * \hat{a}$

· l/r cancellation law:
$a*b = a*c \rightarrow b = c$
$b*a = c*a \rightarrow b = c$

· $a * x = b$ has unique solution for any a,b (and so does $x * a = b$)

Subgroup of group G is $H \subseteq G$ if:

1 $a * b \in H$ for all $a,b \in H$ ("closed")

2 $e \in H$ 3 $\hat{a} \in H$ for all $a \in H$

powers $a^0 = e$, $a^n = a \cdot a^{n-1}$, $a^{-n} = (a^{-1})^{|n|}$

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

Order $\operatorname{ord}(a)$ of $a \in G$ is the least m s.t. $a^m = e$, if it does not exist $\operatorname{ord}(a) = \infty$

L5.6 In finite group, all elements have finite order

$|G|$ = "order of G" = n.o. elements in G

cyclic group $G = \langle a\rangle$ is the group generated by $a = \{a^n \mid n \in \mathbb{Z}\}$ (a: "generator")

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

Lagrange for H subgroup of G, $|H| \mid |G|$ "order of H divides order of G"

C5.9 for finite group G, $\operatorname{ord}(a) \mid |G|$ $\forall a \in G$

C5.10 for finite group G, $a^{|G|} = e$ $\forall a \in G$

C5.11 every group of prime order is cyclic with any element except e as a generator

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

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

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

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

Fermat for all $m \geq 2$ and a s.t. $\gcd(a,m) = 1$:

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

T5.15 $\mathbb{Z}_m^*$ cyclic $\leftrightarrow m = 2, m = 4, m = p^e, m = 2p^e$ where p odd prime and $e \geq 1$

RSA

T5.16 for G finite group and $\gcd(|G|, e) = 1$, the function $x \mapsto x^e$ is a bijection and the unique e-th root of $y \in G$ satisfying $x^e = y$ is

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

RSA

Alice

generate primes p and q

$n = p \cdot q$, $f = (p-1)(q-1)$

select e

$d \equiv_f e^{-1}$

$n, e \rightarrow$

$\leftarrow c$

$m = R_n(c^d)$

Bob

plaintext $m \in \{1 \dots n-1\}$

ciphertext $c = R_n(m^e)$

- $|\mathbb{Z}_n^*| = \varphi(n) = (p-1)(q-1)$
- $m \mapsto e = R_n(m^e)$
- $c \mapsto m = R_n(c^d)$
- compute d with $ed \equiv_{(p-1)(q-1)} 1$
- security is based on the fact that $|\mathbb{Z}_n^*| = f$ can only be computed when p, q are known (and with it d)

Rings and Fields

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

1 $\langle R; +, -, 0\rangle$ is abelian group

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

3 left/right distributive law holds
$(a+b)c = ac + bc$, $c(a+b) = ca + ab$

commutative Ring if $ab = ba$ $\forall a,b$

L5.17 for any ring:

- $0a = a0 = 0$
- $-(-a)b = -(ab)$
- $-(-a)(-b) = ab$
- $1 \neq 0$ if R is non-trivial ($|R| \geq 2$)

characteristic of a Ring is the order of 1 in the additive group. If it is infinite, then characteristic = 0, not ∞.

Unit is $u \in R$ if u is invertible, if $\exists a: au = 1$

R^* = the set of units of R

L5.18 R^* is a (multiplicative) group

$a|b$ = "a divides b" if $\exists c$ s.t. $ac = b$

L5.19 In a commutative ring:
- $a|b \wedge a|c \rightarrow a|bc \ \forall c$
- $a|b \rightarrow a|bc \ \forall c$
- $a|b \wedge a|c \Rightarrow a|(b+c)$

greatest common divisor applies as with numbers to all ring elements in the same way

Zerodivisor = element $a \neq 0$ of commutative ring s.t. $ab = 0$ for some b

integral domain = nontrivial, commutative ring without zerodivisors. So $\forall a,b\,(ab=0 \rightarrow a=0 \vee b=0)$

L5.20 in integral domain, if $a|b$ then c with $ac=b$ is unique

polynomial $a(x)$ is $\sum_{i=0}^{d} a_i x^i$ over a commutative Ring. **deg**(a) = "degree of a" is the greatest i for which $a_i \neq 0$. (0 has degree $-\infty$)

$R[x]$ set of polynomials (in x) over R

→ sum/products of polynomials work as usual

T5.21 for R comm. ring, $R[x]$ also comm. ring

L5.22 for D integral domain:
- $D[x]$ integral domain
- $\deg(a(x)\cdot b(x)) = \deg(a) + \deg(b)$
- $D[x]^* = D^*$ (constant polynomials)

Fields

field is nontrivial commutative ring s.t. every nonzero element is a unit, so $F^* = F \setminus \{0\}$ $\leftrightarrow (F\setminus\{0\}; \cdot, ^{-1}, 1)$ is a belian group

T5.23 $\mathbb{Z}_p$ field $\leftrightarrow$ p prime

T5.24 A field is an integral domain

Polynomials over Fields

monic is $a(x) \in F[x]$ if the leading coefficient is 1

irreducible is $a(x) \in F[x]$ if it is only divisible by constants and constant multiples of $a(x)$.

gcd$(a(x), b(x))$ = $g(x)$ of largest degree such that $g(x)|a(x)$ and $g(x)|b(x)$

T5.25 for any $a(x), b(x) \in F[x]$ there are unique $g(x), r(x)$ s.t.
$a(x) = b(x)\cdot g(x) + r(x)$ and $\deg(r(x)) < \deg(b(x))$

Evaluation of $a(x)$ at α is defined as usual as $a(\alpha)$

L5.28
- $e(x) = a(x) + b(x) \rightarrow e(\alpha) = a(\alpha) + b(\alpha)$
- $c(x) = a(x)b(x) \rightarrow c(\alpha) = a(\alpha)\cdot b(\alpha)$

root for $a(x) \in R[x]$ is $\alpha \in R$ with $a(\alpha) = 0$

L5.29 α root of $a(x) \leftrightarrow (x-\alpha) \mid a(x)$ for $(x-\alpha)|a(x))$

C5.30 $a(x) \in F[x]$ of degree 2,3 is irreducible only if it has no root.

T5.31 $a(x) \in F[x]$ with $\deg(a(x)) = d$ has at most d roots

interpolation a polynomial $a(x) \in F[x]$ is uniquely determined by $d+1$ values of $a(x)$, so $a(\alpha_1) \dots a(\alpha_{d+1})$ for distinct α. ($d = \deg(a)$)
→ for $\beta_i = a(\alpha_i)$ we have $a(x) = \sum_{i=1}^{d+1} \beta_i u_i(x)$

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

L5.33 $\equiv_{m(x)}$ is an equivalence relation on $F[x]$ and each equiv.-class has representative $r(x)$ with $\deg(r(x)) < \deg(m(x))$

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

L5.34 for F with q elements and $m(x)$ of degree d: $|F[x]_{m(x)}| = q^d$

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

L5.36 $a(x)b(y) \equiv_{m(x)} 1$ has a solution $b(x) \in F[x]_{m(x)}$ if and only if $\gcd(m(x), a(x)) = 1$

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

T5.37 $F[x]_{m(x)}$ is field $\leftrightarrow$ $m(x)$ irreducible

$GF(p)$ = Field with p elements

Error-Correcting Codes

(n,k) **encoding function** E for alphabet A is injection that maps a list of information symbols $(a_0, \dots, a_{k-2}) \in A^k$ to a list of (encoded) symbols $(c_0, \dots, c_{n-2}) \in A^n$ of $n > k$.

(n,k) **error-correcting code** over alphabet A is a subset of A^n of cardinality q^k (for $q = |A|$)

Hamming Distance between two strings of equal length over A is the number of positions at which the strings differ

minimum distance $d_{min}(C)$ of error-correcting code C is the minimum Hamming-Distance between any two codewords

decoding function D for an (n,k)-encoding function is $D: A^n \rightarrow A^k$

t-error correcting is a decoding function D for an encoding function E if for any $(a_0, \dots, a_{n-1})$ $D((r_0, \dots, r_{n-2})) = (a_0, \dots, a_{n-1})$ for any $(r_0, \dots, r_{n-2})$ with hamming-distance at most t from $E((a_0, \dots, a_{n-1}))$.
A code C is t-error correcting if such E, D with $C = Im(E)$ exist.

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

T5.42 for $A = GF(q)$ and $\alpha_0, \dots, \alpha_{n-1}$ distinct elements of A. The encoding function $E((a_0, \dots, a_{k-1})) = (a(\alpha_0), \dots, a(\alpha_{n-1}))$ where $a(x)$ is the polynomial:
$a(x) = a_{k-1}x^{k-1} + \dots + a_1 x + a_0$
This code has minimum distance $n-k+1$

Logic

proof system $\Pi = (S, P, T, \phi)$
S: universe of statements
P = universe of proofs
$T(s) = 1$ for $s \in S$ if statement s true
$\phi(s,p) = 1$ for $s \in S$, $p \in P$ if p valid proof for s

sound is proof system if no false statement has a proof ($\phi(s,p) = 1 \rightarrow T(s) = 1$)

complete is proof system if every true statement has a proof ($\forall s\, \exists p\ \phi(s,p) = 1$ (if s true))

"Proof verification has to be computable, T not

Syntax defines alphabet Λ and which strings Λ^* are syntactically correct (are formulas)

semantics defines a "free" - function which specifies, which symbols in a formula are free

interpretation is a set $Z \subseteq \Lambda$ of symbols, a domain of values for each one and a function that assigns each symbol in Z a value in its domain.

suitable is an interpretation for formula F if it assigns a value to all free symbols in F

semantics also def. a function assigning to each formula and interpretation a truth value $\mathcal{A}(F) = 0$ or $\mathcal{A}(F) = 1$

model is a suitable interpretation $\mathcal{A}$ for a formula F for which $\mathcal{A}(F) = 1$.
(we also write $\mathcal{A} \models F$)

Satisfiable is formula $F \leftrightarrow \exists$ model for F, "unsatisfiable" otherwise

tautology is formula true for every suitable interpretation

$F \models G$ = "logical consequence" if for every interpretation suitable for both and a model for F, it is also a model for G

$F \equiv G$ = "equivalent" if every interpr. has same truth value for both:
$F \equiv G \leftrightarrow F \models G$ and $G \models F$

"$F \models$" $\triangleq$ "F tautology"

D6.15 $\neg F$, $F\wedge G$, $F\vee G$ formulas for F,G formulas

$\mathcal{A}(F\vee G)=1 \leftrightarrow \mathcal{A}(F)=1$ or $\mathcal{A}(G)=1$

$\mathcal{A}(F\wedge G)=1 \leftrightarrow \mathcal{A}(F)=1$ and $\mathcal{A}(G)=1$

$\mathcal{A}(\neg F)=1 \leftrightarrow \mathcal{A}(F)=0$

L6.1

idempotence	$F\wedge F=F$	$F\vee F=F$
com.	$F\wedge G=G\wedge F$	$F\vee G=G\vee F$
ass.	$F\wedge(G\wedge H)=(F\wedge G)\wedge H$	(same for $\vee$)
absorption	$F\wedge(F\vee G)=F$	$F\vee(F\wedge G)=F$
distr. laws	$F\wedge(F\vee G)=(F\wedge H)\vee(F\wedge G)$	(same for $\vee,\wedge$ reversed)
double neg	$\neg\neg F=F$	
de morgan	$\neg(A\wedge B)=\neg A\vee\neg B$	$\neg(A\vee B)=\neg A\wedge\neg B$
tautology	$F\vee T=T$	$F\wedge T=F$
unsat.	$F\vee\bot=F$	$F\wedge\bot=\bot$
	$F\vee\neg F=T$	$F\wedge\neg F=\bot$

L6.2 F tautology $\leftrightarrow$ $\neg F$ unsatisfiable

L3.3 $\{F_1,\dots,F_k\}\models G \leftrightarrow$
$(F_1\wedge\dots\wedge F_k)\to G$ tautology $\leftrightarrow$
$\{F_1,\dots,F_k,\neg G\}$ unsatisfiable

Calculi:

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

application of $\vdash_R$ selects $N\subseteq M$ s.t. $N\vdash_R A$ and then adds A to M

calculus = finite set of derivation rules

derivation of formula G from set M is a finite sequence of derivation rules which starts with M and derives G.

$M\vdash_k G$ = $\exists$ derivation of G from M in k(calculus)

correct is derivation rule if: $M\vdash_R F \Rightarrow M\models F$

sound is calculus k if $M\vdash_k F \Rightarrow M\models F$

complete is calculus if $M\models F \Rightarrow M\vdash_k F$

Propositional logic

atomic formula is symbol A_i

- atomic formula is formula
- for F,G formulas $\neg F$, $F\wedge G$, $F\vee G$ are formulas

interpretation is function $\mathcal{A}: Z\to\{0,1\}$ assigning each A_i a value 0 or 1

literal is A_i or $\neg A_i$

CNF = "conjunctive normal form" = $(A\vee\dots\vee B)\wedge(\dots)\wedge\dots\wedge(A\vee\dots\vee v)$

DNF = "disjunctive normal form" = $(A\wedge\dots\wedge B)\vee(\dots)\vee(A\wedge\dots\wedge B)$

T6.4 all formulas have a CNF/DNF

finding CNF: 1) Take truth table 2) negate each symbol for the false columns and combine them with $\wedge$ 3) combine the colums with $\wedge$

finding DNF: 1) Truth table 2) for each $\in$ true column combine its symbols 3) combine them with $\vee$ (the columns)

Resolution Calculus

clause is set of literals

→ for formula $F=(A\vee\dots\vee B)\wedge(C\vee\dots\vee D)\wedge(\dots)$ the clause is set $\{\{A,\dots,B\},\{C,\dots,D\},\{\dots\}\}$

→ The clause set for the set of formulas is the union of their sets

resolvent of clauses k_1 and k_2 if $\exists L$ s.t. $L\in k_1$ and $\neg L\in k_2$ and then $k=(k_1\setminus\{L\})\cup(k_2\setminus\{\neg L\})$ (k = "resolvent")

$\{k_1,k_2\}\vdash_{res} k$

L6.5 Resolution calculus is sound, so $K\vdash_{res} A \Rightarrow K\models A$

T6.6 Set M of formulas unsatisfiable $\leftrightarrow$ $k(M)\vdash_{res}\emptyset$

Predicate Logic

variable symbol x_i

function symbol $f_i^{(h)}$ (h n.o. arguments)

→ for $h=0$ "constants"

predicate symbol $P_i^{(h)}$

term: a variable is a term and $f_i^{(h)}(t_1,\dots,t_h)$ is a term

formula: $P_i^{(h)}(t_1\dots t_h)$ is formula

- for formulas F,G, $\neg F$, $F\wedge G$, $F\vee G$ are formulas
- for formula F, $\forall xF$ and $\forall\exists x_i F$ are formulas

D6.32 Every occurrence of variable in formula is bound or free: If x is in formula G for $\forall xG$ or $\exists xG$ then it is bound, else it is free

closed is formula with no free variables

$F[x/t]$ is formula obtained by substituting every free occurence of x in F with t

Interpretation is tuple $\mathcal{A}=(U,\phi,\psi,\xi)$ with U universe, ϕ assigns function symbols, ψ assigns predicate symbols, ξ assigns variable symbols.

We write $U^{\mathcal{A}}$, $f^{\mathcal{A}}$, $p^{\mathcal{A}}$, $x^{\mathcal{A}}$

suitable for F is interpretation if it defines all free symbols in F

D6.36 semantics

- variables and functions defined recursively

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

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

$\mathcal{A}[x\to u]$ is $\mathcal{A}$ but x replaced by u

L6.7 if x does not occur free in H:

- $\neg(\forall x F)\equiv\exists x(\neg F)$
- $\neg(\exists xF)\equiv\forall x(\neg F)$
- $\forall x(F)\wedge\forall x(G)\equiv\forall x(F\wedge G)$
- $(\exists xF)\vee(\exists xG)\equiv\exists x(F\vee G)$
- $\forall x\forall y F\equiv\forall y\forall x F$, $\exists x\exists y F\equiv\exists y\exists x F$
- $(\forall xF)\wedge H\equiv\forall x(F\wedge H)$
- $(\forall xF)\vee H\equiv\forall x(F\vee H)$
- $(\exists xF)\vee H\equiv\exists x(F\vee H)$
- $(\exists xF)\wedge H\equiv\exists x(F\wedge H)$

L6.8 If we replace sub-formula G of F with equivalent formula, the formula is equivalent

L6.9 $\forall xG\equiv\forall yG[x/y]$, $\exists xG\equiv\exists yG[x/y]$ if y does not occur free in G

rectified is formula in which no variable is both bound and free and and all variables after the quantifiers are distinct

prenex form $Q_1x_1Q_2x_2\dots Q_nx_nG$ where Q_i are all quantifiers in the formula (all quantifiers are at the start)

→ every formula has prenex form

L6.11 $\forall xF\vdash F[x/t]$ for any term t

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1																			
2	1	1																		
3	1	2	1																	
4	1	x	3	1																
5	1	3	2	4	1															
6	1	x	x	x	5	1														
7	1	4	5	2	3	6	1													
8	1	x	3	x	5	x	7	1												
9	1	5	x	7	2	x	4	8	1											
10	1	x	7	x	x	x	3	x	9	1										
11	1	6	4	3	9	2	8	7	5	10	1									
12	1	x	x	x	5	x	7	x	x	x	11	1								
13	1	7	9	10	8	11	2	5	3	4	6	12	1							
14	1	x	5	x	3	x	x	x	11	x	9	x	13	1						
15	1	8	x	4	x	x	13	2	x	x	11	x	7	x	1					
16	1	x	11	x	13	x	7	x	9	x	3	8	5	x	15	1				
17	1	9	6	13	7	3	5	15	2	12	14	10	4	11	8	16	1			
18	1	x	x	x	11	x	7	x	x	x	5	x	7	x	x	x	17	1		
19	1	10	13	5	4	16	11	12	17	2	7	8	3	15	14	6	9	18	1	
20	1	x	7	x	x	x	3	x	9	x	11	x	17	x	x	x	13	x	19	1
(mod)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

multiplicative Inverse modulo that of that

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

computing $R_n(..)$

- get $-1/1$
- euler func φ watch out multiple exponents changes again!
- split pow and compute
- split up and use CRT

CRT

cannot decompose $\equiv_4 \not\Rightarrow \equiv_2$

only if $gcd = 2$

$ord(\mathbb{Z}_m^*) = m$, mod $m-1$

$Ord(F^*) = ord(F) - 2$ (since we preclude 0!)

$Ord(a)$ in $\mathbb{Z}_n = \frac{n}{gcd(a,m)}$

$\mathbb{Z}_n^*$? = cardinality $= \varphi(n)$?

cyclic $= n$ ⊙ $4, 2, p^x, 2p^x$ $p \neq 2$

(x)

Set of subsets

$\mathcal{P}(\emptyset) = \{\emptyset\}$

$\emptyset \times A = \emptyset$

$A \setminus B$ = mus all elements of B and not B?

$|A+B| = |A| \cdot |B|$

$A \times B$ = set of tuples

$|\mathcal{P}(A)| = 2^{|A|}$

work out when negating $\forall x = \exists x$? and so...

- $\mathbb{Z}_n$ has $\varphi(n)$ generators
- an isomorphism is defined uniquely by which generators mapped to one other?
  → then others follow!

don't waste time → skip exercises

groups (non-isomorph)

ord	
1	Z_1
2	Z_2
3	Z_3
4	Z_4, Z_2^2
5	Z_5
6	Z_6, D_6
7	Z_7
8	Z_8, $Z_2 * Z_4$, Z_2^3, D_8, Q_8
9	Z_9, Z_3^2
10	$Z_{10} = Z_2 * Z_5$, D_{10}

Irr. polynomials

GF(2)

x^4	x^3	x^2	x	c
				1 0
				1 1
			1	1 1
	1	0	1	1
	1	1	0	1
1	0	0	1	1
1	1	1	1	1

GF(3)

x^3	x^2	x	c
			1 0
			1 1
			1 2
		1	0 1
		1	1 2
	1	0	2 1
	1	1	0 2

GF(5)

x^3	x^2	x	c
			1 0
			1 1
			1 2
			1 4
		1	0 2
		1	0 3
		1	1 1
		1	2 3
		1	2 4
		1	3 3
		1	3 4
		1	4 1
		1	4 2
	1	0	1 1
	1	0	1 4
	1	2	1
	1	2	3 3
	1	3	3
	1	3	4 2
	1	4	2
	1	4	4 4

GF(7)

x^2	x	c
		1 0
		1 1
		1 2
		1 3
		1 4
		1 5
		1 6
	1	0 1
	1	0 2
	1	0 4
	1	1 3
	1	1 4
	1	1 6
	1	2 2
	1	2 3
	1	2 5
	1	3 1
	1	3 5
	1	3 6
	1	4 1
	1	4 5
	1	4 6
	1	5 2

153	
163	
164	
166	

GF(8)

x^3	x^2	x	c
1	0	0	2
1	0	0	3
1	0	0	4
1	0	0	5
1	0	1	1
1	0	1	6
1	0	2	1
1	0	2	6
1	0	3	2
1	0	3	5
1	0	4	7
1	0	4	6
1	0	5	2
1	0	6	2
1	0	6	5

1101