CH 3 $x \in S$ or $x \notin S$

Set Theory

Def:
- Empty set: $\forall x (x \notin \emptyset)$
- Power set: $P(A) = \{S \mid S \subseteq A\}$
- Equal: $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$
- Subset: $A \subseteq B \Leftrightarrow \forall x (x \in A \to x \in B)$
  - $\subseteq$ is transitive
- $A \cup B = \{x \mid x \in A \vee x \in B\}$
- $A \cap B = \{x \mid x \in A \wedge x \in B\}$
- $B \setminus A = \{x \in B \mid x \notin A\}$
- $A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$
- $|P(A)| = 2^{|A|}$, $|A \times B| = |A| \cdot |B|$

Laws: Idempotence, Comm., Assoc, Absorp., Distr., Consistency: $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$

Lemmas:
- $\emptyset$ is unique. S: $\emptyset \subseteq \emptyset' \wedge \emptyset' \subseteq \emptyset$
- $\emptyset$ is $\subseteq \forall$ sets. S: by contradiction.

Relations:

Def: $\rho \subseteq A \times B$
- $id_A = \{(a,a) \mid a \in A\}$ (all of them)
- $|\rho| \leq 2^{n \cdot m}$ • $\hat{\rho} = \{(b,a) \mid (a,b) \in \rho\}$
- $\rho_1 \circ \rho_2 = \{(a,c) \mid \exists b (a \rho_1 b \wedge b \rho_2 c)\}$

Types:
- Refl.: $id \subseteq \rho$ or $\forall a \in A (a \rho a)$
- Irrefl: $id \cap \rho = \emptyset$
- Symmetric: $a \rho b \Leftrightarrow b \rho a$ or $\rho = \hat{\rho}$
- Antisym.: $a \rho b \wedge b \rho a \Rightarrow a = b$ or $\rho \cap \hat{\rho} \subseteq id$
- Trans: $a \rho b \wedge b \rho c \Rightarrow a \rho c$

Lemmas:
- ρ is trans. iff $\rho^2 \subseteq \rho$
  - ($\Leftarrow$): Assume $\rho^2 \subseteq \rho$ ie. $a \rho^2 b \Rightarrow a \rho b$. If $a \rho b \wedge b \rho c \Rightarrow a \rho^2 c \Rightarrow a \rho c$. ✓
  - ($\Rightarrow$): Assume ρ trans. Then $a \rho^2 c \Rightarrow \exists b (a \rho b \wedge b \rho c) \Rightarrow a \rho c. \Rightarrow \rho^2 \subseteq \rho$. ✓
- If ρ trans: $\rho^n \subseteq \rho$, $\forall$: Induction.

Equivalence Relations

Def: ρ that is 1) refl 2) sym 3) trans
- Equivalence class: $[a]_\rho = \{b \in A \mid a \rho b\}$
- Partition: $A = \bigcup S_i \wedge S_i \cap S_j = \emptyset$
- Quotient set: $A/\rho = \{[a]_\rho \mid a \in A\}$
  - Thm: A/ρ is a partion of A.

Poset

Def: ρ that is 1) refl 2) antisym 3) trans
- $a \not< b$ if $a \rho b$. $a < b$ if $a \rho b \wedge a \neq b$
- Comparable: a, b are... if $a \rho b \vee b \rho a$
- Totally ordered: If any 2 elem are comparable.

Hasse Diagram:
- Covers: $b \ldots a$ if $a < b \wedge \neg(\exists c (a < c \wedge c < b))$
- H.D: A digraph of a finite poset where $a \to b$ if b covers a.

Lex Ord: For $(A, \leq_1) \times (B, \leq_2)$:
$(a_1, b_1) \leq_{Lex} (a_2, b_2) \Leftrightarrow a_1 \leq_1 a_2 \wedge b_1 \leq_2 b_2$
- This is a poset.
- Lex ord: $(a_1, b_1) \leq_{Lex} (a_2, b_2) \Leftrightarrow a_1 <_1 a_2 \vee (a_1 = a_2 \wedge b_1 \leq_2 b_2)$

Special Elems: $S \subseteq A$
- Minimal/Maximal: No elem of A is strictly smaller/larger than a.
  - Need not compare with all
  - Can be many. At least 1 if poset is finite and smallest/Largest. Unique if exists.
- Least/Greatest: Comparable to all and smallest/Largest. Unique if exists.
- Lower/Upper of S: Least/Greatest of S.
- GLB/LUB of S: Largest/Smallest elem bounding from below/above in A.
- Well-Ordered if totally ordered and $\emptyset \neq S \subseteq A$ has a least element.

Meet/Join/Lattice:
- Meet: If $\{a,b\}$ has glb. $a \wedge b$
- Join: If $\{a,b\}$ has lub. $a \vee b$
- Lattice: Every pair is a meet and join.

Functions:

$f: A \to B$
1. Totally Def: $\forall a \exists b\, f(a) = b$ (min 1 elem).
2. Well Def: $\forall a \forall b, b' (f(a) = b \wedge f(a) = b' \Rightarrow b = b')$ (max 1 elem)
- $|B|^{|A|}$ possible functions. ← partial func

Img/Preimg:
- $S \subseteq A \Rightarrow f(S) = \{f(a) \mid a \in S\}$; $Im(f) = f(A) \subseteq B$
- $T \subseteq B \Rightarrow f^{-1}(T) = \{a \mid f(a) \in T\}$ (Preimg)

Properties:
- Injective: $a \neq a' \Rightarrow f(a) \neq f(a')$ (unique map)
- Surjective: $Im(f) = B$ (every b can be reached)
- Bijective: Injective and Surjective

Countability

Def:
- $A \sim B$ if exists bijection $A \to B$
- $A \lesssim B$ if 1) $A \sim C \wedge C \subseteq B$ or 2) exists injection $A \to B$
- Countable: $A \lesssim \mathbb{N}$.

Lemmas:
- $\sim$ is an equivalence rel.
- $\lesssim$ is trans. • $A \subseteq B \Rightarrow A \lesssim B$
- A is countable if finite or $A \sim \mathbb{N}$
1. A countable $\Rightarrow A^n$ countable
2. $\bigcup A_i$ countable if all A_i countable
3. A^* is countable if A countable

Countable:
- $\{0,1\}^* \mapsto dec(\text{'1'} + Seq)$
- $\mathbb{N}^2 : (a,b) \mapsto 0^{|a|} \| 1 \| a \| b$
- $\mathbb{Z} \sim \mathbb{N}$ • $\mathbb{Q} \sim \mathbb{Z} \times \mathbb{N} \sim \mathbb{N}$

Uncountable:
- Infinite sequences (gen by $f: \mathbb{N} \to \{0,1,-\}$) by Cantors diag. (Cont. assumes bijection)

Approach:

Proof Uncount:
1. Find injection $f: \{0,1\}^\infty \to A$
2. Show f is a function. 1) Totally def 2) well def 3) $Im(f) \subseteq A$?
3. Prove inj. 1) $a, b \in \{0,1\}^\infty, a \neq b \Rightarrow \ldots \Rightarrow f(a) \neq f(b)$ or $f(a) = f(b) \Rightarrow \ldots \Rightarrow a = b$
4. We showed $\{0,1\}^\infty \lesssim A$ but formaly say $A \not\sim \mathbb{N}$ by transitivity.

Tricks:
- Complement: Find uncountable B s.t. $A \subseteq B$. Show $B \setminus A$ is countable. Sound since by contradiction $\underbrace{A}_{\text{count}} \cup \underbrace{(B \setminus A)}_{\text{count}} = \underbrace{B}_{\text{uncount}}$
- FTA: e.g. $f: \mathbb{N}^2 \to \mathbb{N} : (a,b) \mapsto 2^a 3^b$. Injective due to unique prime fact.

CH 4

- $a \mid b \Leftrightarrow \exists c (a \cdot c = b)$
- $\forall a \in \mathbb{Z}$ and $d \neq 0, \exists q, r$ s.t. $a = dq + r$ and $0 \leq r < |d|$

Def:
- GCD: for $a \neq 0, b \neq 0$ $gcd(a,b) = d \Leftrightarrow d \mid a \wedge d \mid b \wedge \forall c ((c \mid a \wedge c \mid b) \to c \mid d)$
- LCM: for $a \neq 0, b \neq 0$ $lcm(a,b) = L \Leftrightarrow a \mid L \wedge b \mid L \wedge \forall m ((a \mid m \wedge b \mid m) \to L \mid m)$
- Ideal: $a, b \in \mathbb{Z}$ $(a,b) = \{ua + vb \mid u, v \in \mathbb{Z}\}$
- Congruent: $a \equiv_n b \Leftrightarrow n \mid (a - b)$
- Equality: $a = b \Rightarrow a \equiv_n b$
- If $gcd(a,m) = 1$, then $ax \equiv_n 1$ Else no multiplicative inverse
- FTA: Any number can be decomposed into primes.

Lemmas:
- $gcd(m, n - qm) = gcd(m,n) = gcd(m, R_m(n))$
- $\forall a, b \exists d ((a,b) = (d))$
- for $a, b \in \mathbb{Z}$ (not both 0) $\exists d$ in $\mathbb{Z}$ $(a,b) = (d)$ $\to d = gcd(a,b)$
- for $a, b \in \mathbb{Z}$ (not both 0) $gcd(a,b) = ua + vb$
- $gcd(a,b) \cdot lcm(a,b) = a \cdot b$
- Every composite n has a prime div $\leq \sqrt{n}$

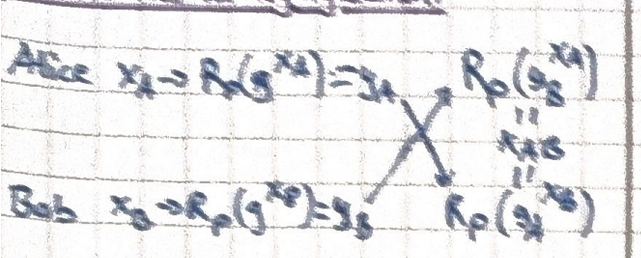
Modular Arithmetics

- If $a \equiv_n b \wedge c \equiv_n d$ then 1) $a + c \equiv_n b + d$ and 2) $ac \equiv_n bd$
- If $a_i \equiv_n b_i$ then $f(a_i \cdots) \equiv_n f(b_i \cdots)$
- 1) $a \equiv_n R_n(a)$ 2) $a \equiv_n b \Leftrightarrow R_n(a) = R_n(b)$
- $R_n(f(R_n(a_i))) = R_n(f(a_i))$
- $ax \equiv_n 1$ has a unique sol if $gcd(a,n) = 1$
- $\bigvee_{0}$ $gcd(a,m) = 1 \Rightarrow R_m(a^{\varphi(m)-1}) = R_m(a^{-1})$

CRT

- $x \equiv_{m_1} a_1, \ldots, x \equiv_{m_r} a_r$
- For rel prime $m_1, m_2, \ldots$ $n = \prod m_i$
- $M_i = M / m_i$. $M_i N_i \equiv_{m_i} 1$. N_i is mult. inv.
- Sol: $x = R_M\left(\sum_{i=1}^{m_i} a_i M_i N_i\right)$

Diffie-Hellman Key Agreement



$x_A, x_B \in \{0, \dots, p-2\}$. g is generator. Requires group $\mathbb{Z}_p^*$. Diff due to disc. log problem.

CHJ

- Operation: a func $S^n \to S$
- Algebra: $\langle S; \Omega \rangle$
  S: Carrier of Algebra
  Ω: List of opers S

		Monoid	Group	Abelian Group	Ring	Commutative R	Integral Domain	Field
Multiplicative	Closure	•	•	•	•	•	•	•
	Associative	•	•	•	•	•	•	•
	Identity	•	•	•	•	•	•	•
	Inverse		•	•	•	•	•	•
	Commutative			•	•	•	•	•
Additive	Closure				•	•	•	•
	Associative				•	•	•	•
	Distributive				•	•	•	•
	Commutative					•	•	•
	Identity						•	•
	No zero-divisors						•	•
	Inverse							•

Monoid

Neutral Elements:
- LN: $e*a = a$ · RN: $a*e = a$
- If $e*a = a*e = a$: Just neutral elem.
- If LN ∧ RN ⇒ LN = RN

Associative:
$(a*(b*c)) = ((a*b)*c)$

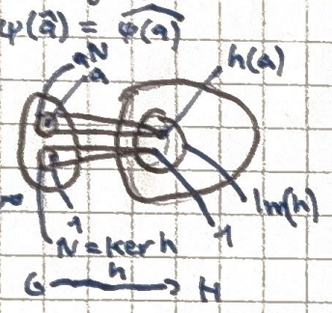
Group

Inverse:
- LI: $b*a = e$ · RI: $a*b = e$
- Inverse if $a*b = b*a = e$
- If LI ∧ RI ⇒ LI = RI. ($b = b*e = b*(a*a') \dots$)
- The inverse is unique

Group Axioms:
For any group: (Lemma)
1. $\hat{\hat{a}} = a$
2. $\widehat{a*b} = \hat{b}*\hat{a}$
3. Left cancel: $a*b = a*c \Rightarrow b = c$
   Right cancel: $b*a = c*a \Rightarrow b = c$
4. $a*x = b$ and $x*a = b$ both have unique sol.

Minimal Axioms:
- G1: assoc, G2': RN, G3': RI
- Prove G3 before G2.
- G3: S: $\hat{a}\cdot a = (\hat{a}\cdot a)\cdot e = (\hat{a}\cdot a)\cdot(\hat{a}\cdot\hat{\hat{a}}) \dots$
- G2: $a\cdot e = a\cdot(\hat{a}\cdot a) = (a\cdot\hat{a})\cdot a = e\cdot a$

Homomorphism:
- Group Homomorphism: func φ from $G \to H$ s.t. $\forall a \forall b\ \varphi(a *_G b) = \varphi(a) *_H \varphi(b)$
- Isomorphism: φ is bijective
- 1) $\varphi(e_G) = e_H$ 2) $\varphi(\hat{a}) = \widehat{\varphi(a)}$



Note: φ need not be injective (if there is a non-zero kernel)

Proving Isomorphism:
1. Define mapping φ suspected of being an isomorphism
2. Check map is well defined (maps to 1 elem max)
3. Check is totally def (maps to at least 1 elem)
4. Verify $\forall g \in G\ \varphi(g) \in H$.
5. Check homomorphism: $\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$
6. Check Inj: $\varphi(g_1) = \varphi(g_2) \Rightarrow g_1 = g_2$ or contrapos.
7. Show surj: S: $\forall h \exists g\ (\varphi(g) = h)$
8. Conclude Isomorphism.

Subgroups:
$H \leq G$ if 1) $\forall a,b \in H\ a\cdot b \in H$ 2) $e \in H$ 3) $\forall a \in H\ \hat{a} \in H$

Order:

- Order { group: $|G|$ for finite groups
  elem: for $a \in G$, ord(a) is the least $m \neq 1$ s.t. $a^m = e$
  ↳ $\text{ord}(a) = \infty$ if $\nexists m$ ↳ $\text{ord}(a) \neq 1$
  ↳ $\text{ord}(a) = 2 \iff a = a^{-1}$
- Cyclic group: $G = \langle g \rangle = \{e, g, g^2, \dots, g^{\text{ord}(g)-1}, \dots\}$
- For $\langle \mathbb{Z}_n; + \rangle$ all g s.t. $\gcd(n,g) = 1$ are generators.
- A cyclic group of order n. is always isomorphic to $\langle \mathbb{Z}_n; + \rangle$ and hence commutative.

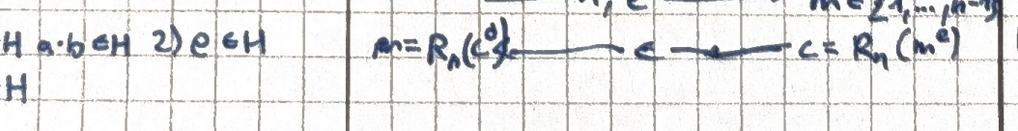
Lagrange and order of subgroups:
- $H \leq G \Rightarrow |H| \mid |G|$
  ↳ for every finite group $\forall a \in G\ \text{ord}(a) \mid |G|$
  ↳ for fin. groups: $\forall a \in G\ a^{|G|} = e$
  ↳ Every group of prime order is cyclic, and every elem except e is a generator.

- $\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid \gcd(a,m) = 1\}$
- $\varphi(m) = |\mathbb{Z}_m^*|$ · $\langle \mathbb{Z}_m^*; \cdot, ^{-1}, 1 \rangle$ is group
- $m = \prod p_i^{e_i} \Rightarrow \varphi(m) = \prod (p_i^{e_i} - p_i^{e_i - 1})$

Fermat/Euler:
1. $\forall m \geq 2\ \wedge \gcd(a,m) = 1$: $a^{\varphi(m)} \equiv_m 1$
2. $a^{p-1} \equiv_p 1 \iff a^p \equiv_p a$.
- Thm: $\mathbb{Z}_m^*$ is cyclic iff $m = 2$, $m = q$, $m = p^e$, or $m = 2p^e$, where p is odd prime

RSA

- Let G be a finite group of ord $n = p \cdot q$
- Let $f = |\mathbb{Z}_n^*| = (p-1)(q-1)$
- Chose $e \neq p, q, pq$ in group $\mathbb{Z}$ (rel. prime to n)
- $x \mapsto x^e$ is a bijection
- Choose $d \equiv_f e^{-1}$ (use ext. ggcd algo)
- Make n, e public.
- Encrypt $m \mapsto c = R_n(m^e)$
- Decrypt $c \mapsto m = R_n(c^d)$



Ring

Lemma:
1. $0a = a0 = 0$. S: $0a = -(a0) + a0 = -(a0) + a(0+0) = -(a0) + a0 + a0 = 0$
2. $(-a)b = -ab$ S: $(-a)b + ab = (-a+a)b = 0b = 0 \Rightarrow (-a)b = -(ab)$
3. $(-a)(-b) = ab$ S: $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$
4. If $|R| > 1 \Rightarrow 1 \neq 0$. Let $a \neq b$. $a = a \cdot 1 = a \cdot 0 = 0$. $b = \dots = 0$. $\Rightarrow 1 \neq 0$.

- Characteristic of a ring: { order of 1 in add. group if fin.; 0 otherwise

Units:

- A elem $u \in R$ is called unit if it's invertible.
  ↳ 0 is never invertible (mult. group).
- R^* is a mul. group. S: $\forall u, v\ \exists y: y = (uv)^{-1}$ ($\Rightarrow y = v^{-1}u^{-1}$). $1 \in R^*$ since $1 = 1^{-1}$. Assoc. is inherited from R.

(set of units)

Divisors:

- $a \mid b$: $\exists c$: $R(ac = b)$ where R is comm ring
- Lemma: 1) $\mid$ is trans 2) $a \mid b \Rightarrow a \mid (bc)$ 3) $a \mid b \wedge a \mid c \Rightarrow a \mid (b+c)$

Integral Domains

- Zero div: a where $a \neq 0$ and $ab = 0$ for some $b \neq 0$.
- Integral Domain: A non-trivial ($1 \neq 0$) comm R without zero-divs.
  ↳ $ab = 0 \Rightarrow a = 0 \vee b = 0$ ↳ $c = \frac{a}{a}$ is unique.

Polynomial Rings:

- For any comm. R, R[x] is a comm R too.

Lemma: Let D be an ID.
1. D[x] is an ID. Only if we had zero-div could $p(x)q(x) = 0$. Look at coefficients.
2. $\deg(ab) = \deg(a) + \deg(b)$. Similar to (1), higest deg can't dissapear since no zero-div
3. Units of D[x] are const. polynoms that are units of D. $D[x]^* = D^*$

Remark: $\mathbb{R}[x]_{x^2+1}$ is isomorphic to $\mathbb{C}$

Field

- Def: A non-trivial comm R where every non-zero elem is a unit (invertible).
  ↳ $F^* = F \setminus \{0\}$ ↳ $(F \setminus \{0\}, \cdot, {}^{-1}, 1)$ is a comm. G.
  ↳ $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ are fields ($\mathbb{Z}, \mathbb{R}[x]$ are not)
- A field is an I.D. S: It suffice to show that for units $u \cdot v = 0 \Rightarrow u^{-1}uv = v = 0$.
- $GF(p)$ is a field of p elems $\sim \mathbb{Z}_p^*$ for prime

Polys:

- Monic: $a(x) \in F[x]$ with leading coeff = 1.
- Irreducible: a poly $a(x)$ w/ $\deg(a(x)) \geq 1$, divisible by only consts or const multiples
- $\gcd(a(x), b(x))$: monic $g(x)$ of largest deg s.t. $g(x) \mid a(x) \wedge g(x) \mid b(x)$

Roots:

- Root: $\alpha \in R$ s.t. $\forall q(x) \in R[x]$ s.t. $q(\alpha) = 0$.

Lemma: $\alpha \in F$. $a(\alpha) = 0 \iff (x - \alpha) \mid a(x)$

↳ irred. poly of deg ≥ 2 has no roots

↳ An irred poly of deg = 2 v 3 is irred. iff it has no roots. S: Since otherwise it must have a factor of deg = 1.

Finite Fields:

- $|F[x]_{m(x)}| = |F|^{\deg(m(x))}$
- $a(x) b(x) \equiv_{m(x)} 1$ has unique sol iff $\gcd(a(x), b(x)) = 1$.
- A ring $F[x]_{m(x)}$ is a field iff $m(x)$ is irred.

Error Correcting Codes

- Let a (n,k)-encoding func $E: A^k \to A^n$. Compute by constructing $a(x)$ with deg k with coefficients $M \in A^k$. Eval $n > k$ points $= C$. Output c is called 'codeword'
- $|m(E)| = |C|$ = codeword space is called an error correcting code. $|C| = |A|^k$.
- Hamming Dist: Char diff.
- $d_{min}(C)$ is min/smallest ham. dist. bet. any two codewords.
- A decoding func $D: A^n \to A^k$ is t error correcting, for any $M \in A^k$. D inverts E for any input w/ at most t Hamming D.
- A code C with $d_{min}(C) = d$ is t-error correcting iff $d \geq 2t+1$.

Polynomial Interpolation:

- A polynomial $a(x) \in F[x]$ can of deg d can be uniquely determined by $d+1$ points
- Assume $\beta_i = a(\alpha_i)$ for $i \in [1, d+1]$
- $a(x) = \sum_{i=1}^{d+1} \beta_i v_i(x)$
- $v_i(x) = \frac{x-\alpha_1}{\alpha_i - \alpha_1} \cdot \ldots \cdot \frac{x-\alpha_{i-1}}{\alpha_i - \alpha_{i-1}} \cdot \frac{x-\alpha_{i+1}}{\alpha_i - \alpha_{i+1}} \cdot \ldots \cdot \frac{x-\alpha_{d+1}}{\alpha_i - \alpha_{d+1}}$
- Uniqueness. Assume $a = a' \wedge \in O(x^d)$ are interpolated by α_i s.t. $i \in [1, d+1]$ $b = a - a'$ has $d+1$ roots (α_i) $\lightning$ By contra. $b = 0 \Rightarrow a = a'$.

CHG

- Set of statements: $S \subseteq \Sigma^*$
- Set of proofs: $P \subseteq \Sigma^*$
- Truth function: $\tau: S \to \{0,1\}$ assigns each $s \in S$ to a truth value and defines semantics of objs of S.
- Verification function: $\phi: S \times P \to \{0,1\}$ checks if p is a valid proof to s.
  ↳ has to be efficiently compute.
- Proof Sys: $\Pi = (S, P, \tau, \phi)$
- Soundness: $\forall s \exists p\ \phi(s,p) = 1 \Rightarrow \tau(s) = 1$
- Completeness: $\forall s\ \tau(s) = 1 \Rightarrow \exists p: \phi(s,p) = 1$
- Syntax: Defines alphabet Λ and specifies which strings Λ^* are formulas.
- Semantics: defines
  1) a func FREE that assigns $F \in \Lambda^*$ a subset of indices of freely occuring variables
  2) a func σ that assigns each formula F and interpretation A suit. for F a truth val. $\sigma(F, A) \in \{0,1\} = A(F)$.
- Interpretation: a set $Z \subseteq \Lambda$ of symbols, a domain for each symbol and func to assign values.
  ↳ suitable if each free var is given a val.
- Model: A suit. intp. A for which F is true. $A(F) = 1$. or $A \models F$. $A \models M$.
- Satisfiable: $\exists$ model for F
- Unsatisfiable: $\nexists$ model for F. $\bot$
- Tautology/Valid: The formula is true $\forall$ inter suit. intp. T. or $\models F$.
- Logical consequence: $F \models G$ if $\forall A$ suit. for F, G $A(F) = 1 \Rightarrow A(G) = 1$
- Equivalent: $F \equiv G \iff F \models G \wedge G \models F$

Lemmas:

- F is taut. if $\neg F$ is unsat.
- Following are equiv:
  1. $\{F_1, \ldots, F_k\} \models G$
  2. $(F_1 \wedge \ldots \wedge F_k) \to G$ is tautology.
  3. $\{F_1, \ldots, F_k, \neg G\}$ is unsat.

Logical Operators:

If F, G are formulas, $\neg F, (F \wedge G), (F \vee G)$ are formulas too:

- $A(F \vee G) = 1 \iff A(F) = 1$ or $A(G) = 1$
- $A(F \wedge G) = 1 \iff A(F) = 1$ and $A(G) = 1$.
- $A(\neg F) = 1 \iff A(F) = 0$.

Logic Calculi

- Derivation rule: $\{F_1, \ldots, F_k\} \vdash_R G$
  Application: (1) select $N \subseteq M$ (2) $N \vdash_R G$ (3) $M \leftarrow M \cup \{G\}$
- Calculus: A set of derivation rules $K = \{R_1, \ldots, R_m\}$
- Derivation of G from M in calc K: finite seq of derivations.
- Correct derivation rule: $M \vdash_K F \Rightarrow M \models F$
- Sound/Correct calc: $M \vdash_K F \Rightarrow M \models F$
- Complete calc: $M \models F \Rightarrow M \vdash_K F$

Normal Forms:

Prenex Normal Form:

Quantifiers at beginning. Make tree and bubble up.

Skolem Normal Form:

Doesn't preserve logical equivalence, but preserves satisfiability. Elim $\exists$ quant

1. Convert to PNF
2. $\forall a,b,c,\ldots\ \exists y \to \text{repl}^{ce}_{y, f(a,b,c,\ldots)}$

CNF (Conjunctive Normal Form):

$F = (a \vee b \vee c) \wedge (\ldots) \ldots$

Take neg of zero rows. $(a=0, b=1 \equiv 0)$
$\Rightarrow (a \vee \neg b) \wedge (\ldots)$

DNF (Disjunctive Normal Form):

$F = (a \wedge b \wedge c) \vee (\ldots) \ldots$

Take true rows $(a=0, b=1 \equiv 1)$
$\Rightarrow (\neg a \wedge b) \vee (\ldots) \ldots$

Resolution Calculus

- Clause: Set of literals. Can be empty.
- If $F = (L_1 \vee L_2) \wedge \ldots \wedge (L_3 \vee L_4)$ in CNF
  $K(F) = \{\{L_1, L_2\}, \ldots, \{L_3, L_4\}\}$
  $K(M) = \bigcup K(n_i)$
- Resolvent: $L \in K_1, \neg L \in K_2 \to K = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\neg L\})$
  ↳ $\{K_1, K_2\} \vdash_{res} K$
  ↳ only 1 rule $\{res\}$
  ↳ sound but not complete.

Application:

- Unsat: M is unsat $\iff K(M) \vdash_{res} \phi$
- Tautology: M is T $\iff K(\neg M) \vdash_{res} \phi$
- Logical Consequence: $M \models F \iff K(M \cup \{\neg F\}) \vdash_{res} \phi$

Predicate Logic

Syntax:

1) Variable symbol X_i
2) function symbol f_i^k (const if $k = c$)
3) Predicate symbol P_i^k
4) Term: I) Variable II) $f_i^k(t_1, \ldots, t_k)$
5) formula: I) $P_i^k(t_1, \ldots, t_k)$ II) $\neg F, F \wedge G, F \vee G$
   III) $\forall x\ F, \exists x\ F$

- Bound: If var x occurs in $\forall x\ G$ or $\exists x\ G$
  ↳ free otherwise.
- Closed: No free vars.
- $F[x/t]$: Subst. free occurrences of x in F by t

Semantics I:

In Intp. $A = (U^A, \phi, \psi, \xi)$
- ↳ U is a non-empty set
- ↳ ϕ assigns a func. to each func.
- ↳ ψ assigns a func to each pred.
- ↳ ξ assigns each free var a value.

• Suitable: If all funcs, predicates, vars have been assigned a value/func.

Semantics II:

$A(t)$ if t is a term:
- t is a var $\Rightarrow A(t) = t^A$
- t is a func $\Rightarrow A(f(t_1,\dots,t_k)) = A(f^A(A(t_1),\dots,A(t_k)))$

$A(F)$ truth value is recursively def:
- F is predicate $\Rightarrow A(P(t_1,\dots,t_k)) = A(P^A(A(t_1),\dots,A(t_k)))$
- $A(\forall x\, G) = \begin{cases} 1 \text{ if } A_{[x\to u]}(G)=1 \text{ for all } u\in U \\ 0 \text{ otherwise.} \end{cases}$
- $A(\exists x\, G) = \begin{cases} 1 \text{ if } A_{[x\to u]}(G)=1 \text{ for some } u\in U \\ 0 \text{ otherwise} \end{cases}$

• Universal Instantiation: $\forall x F \models F[x/t]$

Lemmas:

Equivalences:

1) $F \wedge F \equiv F$, $F \vee F \equiv F$ (idempotence)
2) $F \wedge G \equiv G \wedge F$, $F \vee G \equiv G \vee F$ (commutative)
3) $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$, $(F \vee G) \vee H \equiv F \vee (G \vee H)$ (assoc.)
4) $F \wedge (F \vee G) \equiv F$, $F \vee (F \wedge G) \equiv F$ (absorp.)
5) $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$ (distr. law)
6) $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$ (distr. law)
7) $\neg\neg F \equiv F$ (double neg.)
8) $\neg(F \wedge G) \equiv \neg F \vee \neg G$, $\neg(F \vee G) \equiv \neg F \wedge \neg G$ (de M.)
9) $F \vee T \equiv T$, $F \wedge T \equiv F$ (tautology rules)
10) $F \vee \bot \equiv F$, $F \wedge \bot \equiv \bot$ (unsat. rules)
11) $F \vee \neg F \equiv T$, $F \wedge \neg F \equiv \bot$

For any formula F, G, H & where x doesn't occur free
1) $\neg(\forall x F) \equiv \exists x \neg F$
2) $\neg(\exists x F) \equiv \forall x \neg F$
3) $(\forall x F) \wedge (\forall x G) \equiv \forall x (F \wedge G)$
4) $(\exists x F) \vee (\exists x G) \equiv \exists x (F \vee G)$
5) $\forall x \forall y F \equiv \forall y \forall x F$
6) $\exists x \exists y F \equiv \exists y \exists x F$
7) $(\forall x F) \wedge H \equiv \forall x (F \wedge H)$
8) $(\forall x F) \vee H \equiv \forall x (F \vee H)$
9) $(\exists x F) \wedge H \equiv \exists x (F \wedge H)$
10) $(\exists x F) \vee H \equiv \exists x (F \vee H)$

• Changing subformula with equivalent subformula, remain equivalent.
• For G where y doesn't occur:
- $\forall x\, G \equiv \forall y\, G[x/y]$
- $\exists x\, G \equiv \exists y\, G[x/y]$

Special Thm: $\neg\exists x \forall y (P(y,x) \leftrightarrow \neg P(y,y))$

Proof Patterns

Proof of $\Rightarrow$:
1) Composition of implications: $(a \Rightarrow b) \wedge (b \Rightarrow c) \models a \Rightarrow c$
2) Direct Proof of Impl.: Assume S and show $S \Rightarrow T$
3) Indirect Proof: $\neg b \Rightarrow \neg a \models a \Rightarrow b$

Proof of statements:
1) Modus Ponens: $A \wedge (A \Rightarrow B) \models B$
2) Case Distinction: $(a \vee b \vee \dots \vee c) \wedge (a \Rightarrow x) \wedge (b \Rightarrow x) \wedge \dots \wedge (c \Rightarrow x) \models x$
3) Proof by contradiction: Find T and show $\neg T$. Show $\neg S \Rightarrow T$. $(\neg S \Rightarrow T) \wedge \neg T \models S$

Existence Proofs:
1) Proof by counter-example: $\exists x \in X\, (\neg S_x)$
2) Pigeonhole: If n obj. are partitioned into $k<n$ sets, then atleast one must contain $\lceil \frac{n}{k} \rceil$.

Induction: $P(0) \wedge \forall n (P(n) \Rightarrow P(n+1)) \models \forall n\, P(n)$

Extras

Eulers Totient Table

t	1	2	3	4	5	6	7	8	9	10
0	1	1	2	2	4	2	6	4	6	4
10	10	4	12	6	8	8	16	6	18	8
20	12	10	22	8	20	12	18	12	28	8
30	30	16	20	16	24	12	36	18	24	16
40	40	12	42	20	24	22	46	16	42	20
50	32	24	52	18	40	24	36	28	58	16
60	60	30	36	32	48	20	66	32	44	24
70	70	24	72	36	40	36	60	24	78	32
80	54	40	82	24	64	42	56	40	88	24
90	72	44	60	46	72	32	96	42	60	40

Inverse mod b Table

b	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	1	X																		
3	1	2																		
4	1	X	3																	
5	1	3	2	4																
6	1	X	X	X	5															
7	1	4	5	2	3	6														
8	1	X	3	X	5	X	7													
9	1	5	X	7	2	X	4	8												
10	1	X	7	X	X	X	3	X	9											
11	1	6	4	3	9	2	8	7	5	10										
12	1	X	X	X	5	X	7	X	X	X	11									
13	1	7	9	10	8	11	2	5	3	4	6	12								
14	1	X	5	X	3	X	X	X	11	X	9	X	13							
15	1	8	X	4	X	X	13	2	X	X	11	X	7	14						
16	1	X	11	X	13	X	7	X	9	X	3	X	5	X	15					
17	1	9	6	13	7	3	5	15	2	12	14	10	4	11	8	16				
18	1	X	X	X	11	X	13	X	X	X	5	X	7	X	X	X	17			
19	1	10	13	5	4	16	11	12	12	2	7	8	3	15	14	6	9	18		
20	1	X	7	X	X	X	3	X	9	X	11	X	17	X	X	X	13	X	19	X

Primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 79, 83, 89, 97, 101, 103, 107, ...

Irreducibles

GF(2)[x]:
10, 11, 111, 1011, 1101, 10011, 11001, 11111

GF(3)[x]:
10, 11, 12, 101, 112, 122, 1021, 1102, 1112, 1121, 1201, 1211, 1222, 10012

GF(5)[x]:
10, 11, 12, 14, 102, 103, 111, 112, 123, 124, 133, 134, 141, 142, 1011, 1013, 1021, 1024, 1032, 1033, 1042, 1044, ...

GF(7)[x]:
10, 11, 12, 13, 14, 15, 16, 101, 102, 104, 113, 114, 116, 122, 123, 125, 131, 135, 136, 140, 141, 145, 146, 152, 153, 155, 163, 164, 166, 1002, 1003, 1004, 1005, 1011, 1015, 1021, 1026, 1032, 1035, 1041, 1046, 1052, 1055, 1062, 1065, 1101

Other

- Zero divs of $GF(3)_{x^2+2}$ - If $a(x)$ is 20 $a(x)|0 \equiv x^2+2 \rightarrow$ factor x^2+2 by roots
- Bezout: $\gcd(x,y) = ax+by$ (ideal)
- $\langle \mathbb{Z}_{29}, \cdot, 1 \rangle$ has 28 generators.
- $\langle \mathbb{Z}_{29}^*, \cdot \rangle$ has $\phi(28) = 12$ generators
- $\text{ord}(x \in G) = 36$. $\text{Ord}((x^6, x^{15}))$?
  - ↳ $\gcd(6,36) = 6 \rightarrow \frac{36}{6} = 6$
    $\gcd(16,36) = 4 \rightarrow \frac{36}{4} = 9$
    $\text{ord} = \text{lcm}(9,6) = 18$.
- Order of inverse is same
- Lcm $p^{\max(e_1,e_2)}$ ...
  Gcd $p^{\min(e_1,e_2)}$ ...

Other

- Zero divs of $GF(3)_{x^2+2}$ - If $a(x)$ is 20 $a(x)|0 \equiv x^2+2 \rightarrow$ factor x^2+2 by roots
- Bezout: $\gcd(x,y) = ax+by$ (ideal)
- $\langle \mathbb{Z}_{29}, \cdot, 1 \rangle$ has 28 generators.
- $\langle \mathbb{Z}_{29}^*, \cdot \rangle$ has $\phi(28) = 12$ generators
- $\text{ord}(x \in G) = 36$. $\text{Ord}((x^6, x^{15}))$?
  - ↳ $\gcd(6,36) = 6 \rightarrow \frac{36}{6} = 6$
    $\gcd(16,36) = 4 \rightarrow \frac{36}{4} = 9$
    $\text{ord} = \text{lcm}(9,6) = 18$.
- Order of inverse is same
- Lcm $p^{\max(e_1,e_2)}$ ...
  Gcd $p^{\min(e_1,e_2)}$ ...

$\mathbb{Z}_n^*$ and generators

- Q: Compute # of (diff.) isomorphisms betw. 2 groups of order 19.
  A: $6 = \varphi(19)$, because isomorphism map generators.
- Q: Free symbols. A: Include vars, funcs, predicates!

2	1
3	1 2
4	1 3
5	1 2 3 4
6	1 5
7	1 2 3 4 5 6
8	1 3 5 7
9	1 2 4 5 7 8
10	1 3 7 9
11	1 2 3 4 5 6 7 8 9 10
12	1 5 7 11
13	1 2 3 4 5 6 7 8 9 10 11 12
14	1 3 5 9 11 13
15	1 2 4 7 8 11 13 14
16	1 3 5 7 9 11 13 15
17	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
18	1 5 7 11 13 17
19	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
20	1 2 7 9 11 13 17 19
21	1 2 4 5 8 10 11 13 16 17 19 20
22	1 3 5 7 9 13 15 17 19 21
23	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22
24	1 5 7 11 13 14 19 23
25	1 2 3 4 6 7 8 9 11 12 13 14 16 17 18 19 21 22 23 24
26	1 3 5 7 9 11 15 17 19 21 23 25
27	[illegible] 1 2 4 5 7 8 10 11 13 14 16 17 19 20 22 23 25 26
28	1 3 5 9 11 13 15 17 19 23 25 27
29	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
30	1 7 11 13 17 19 23 29