Proof Patterns

- $S \Rightarrow T$: direct, indirect
- S: modus ponens (prove some R and $R \Rightarrow S$), case distinction (prove that some R_i always occurs, R_i is true, and $R_i \Rightarrow S$), contradiction (disprove some R, assume S is false and prove R)
- S_x for at least one x: constructive, none-constructive, pidgeonhole principle (partition $\wedge$ objects in k sets, at least set contains at least $\lceil \frac{t}{k} \rceil$ objects)
- S_x not for all x: counterexample

Set Theory

D3.2) $A = B \overset{\text{def}}{\Leftrightarrow} \forall x (x \in A \Leftrightarrow x \in B)$
L3.1) $\{a\} = \{b\} \Rightarrow a = b$
D3.3) $A \subseteq B \overset{\text{def}}{\Leftrightarrow} \forall x (x \in A \Rightarrow x \in B)$
D3.4) $\emptyset$ means $\forall x (x \notin \emptyset)$
L3.3) $\forall A (\emptyset \subseteq A)$
D3.5) power set $\mathcal{P}(A) \overset{\text{def}}{=} \{S \mid S \subseteq A\}$
3.1.9 has cardinality $2^{|A|}$ hence $\mathcal{P}(A) \overset{\text{def.}}{=} 2^A$
D3.6) $A \cup B \overset{\text{def}}{=} \{x \mid x \in A \vee x \in B\}$ union
$A \cap B \overset{\text{def}}{=} \{x \mid x \in A \wedge x \in B\}$ intersect.
D3.7) $A \subseteq U$: $\overline{A} \overset{\text{def}}{=} \{x \in U \mid x \notin A\}$
D3.8) $B \setminus A \overset{\text{def}}{=} \{x \in B \mid x \notin A\}$
T3.4) idempotence, commutativity, associativity, absorption, distributivity, ¶

$=$ is $\subseteq \& \supseteq$

consistency ($A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$)

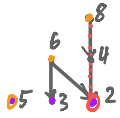
D3.9) $A \times B \overset{\text{def}}{=} \{(a,b) \mid a \in A \wedge b \in B\}$
3.1.11 $|A \times B| = |A| \cdot |B|$
3.1.12 Russell's Paradox $R = \{A \mid A \notin A\}$
↳ $\{x \mid P(x)\}$ is undefined without a universe
↳ the universe itself is not a set

Relations

D3.10) relation ρ from A to B: $\rho \subseteq A \times B$
$B = A$: relation on A
D3.11) $\mathrm{id}_A \overset{\text{def}}{=} \{(a,a) \mid a \in A\}$
3.2.1 There are $2^{(n^2)}$ relations on A
D3.12) $\hat{\rho} \overset{\text{def}}{=} \{(a,b) \mid (b,a) \in \rho\}$
↳ $a \rho b \Leftrightarrow b \hat{\rho} a$
D3.13) $\rho \circ \tau \overset{\text{def}}{=} \{(a,c) \mid \exists b \in B ((a,b) \in \rho \wedge (b,c) \in \tau)\}$
L3.5) associativity $\rho \circ (\tau \circ \phi) = (\rho \circ \tau) \circ \phi$
L3.6) $\widehat{\rho \tau} = \hat{\tau} \hat{\rho}$
D3.14) ρ reflexive $\overset{\text{def}}{\Leftrightarrow}$ $a \rho a$ for all $a \in A$
$\Leftrightarrow \mathrm{id} \subseteq \rho$
D3.15) ρ irreflexive $\overset{\text{def}}{\Leftrightarrow}$ $a \not\rho a$ for all $a \in A$
$\Leftrightarrow \rho \cap \mathrm{id} = \emptyset$
D3.16) ρ symmetric $\overset{\text{def}}{\Leftrightarrow} (a \rho b \Leftrightarrow b \rho a)$
$\Leftrightarrow \rho = \hat{\rho}$
D3.17) ρ antisymmetric $\overset{\text{def}}{\Leftrightarrow} ((a \rho b) \wedge (b \rho a) \Rightarrow a = b)$
$\Leftrightarrow \rho \cap \hat{\rho} = \mathrm{id}$
D3.18) ρ transitive $\overset{\text{def}}{\Leftrightarrow} ((a \rho b) \wedge (b \rho c) \Rightarrow a \rho c)$
L3.7) $\Leftrightarrow \rho^2 \subseteq \rho$

D3.19) transitive closure $\rho^* = \bigcup_{n \in \mathbb{N} \setminus \{0\}} \rho^n$
↳ $a \rho^* b \Leftrightarrow$ "by chaining ρ some finite number of times, a reaches b"
D3.20) equivalence relation: - reflexive
- symmetric
- transitive
D3.21) $[a]_\theta \overset{\text{def}}{=} \{b \in A \mid b \theta a\}$
equivalence class of a
L3.8) θ_1, θ_2 equivalence relations $\Rightarrow \theta_1 \cap \theta_2$ equivalence relation
D3.22) partition $\{S_i \mid i \in I\}$ of A if $S_i \cap S_j = \emptyset$ for $i \neq j$ and $\bigcup_{i \in I} S_i = A$
D3.23) $A/\theta \overset{\text{def}}{=} \{[a]_\theta \mid a \in A\}$
T3.9) θ equivalence relation on A $\Leftrightarrow$ A/θ partition of A
D3.24) partial order: - reflexive
- antisymmetric
- transitive
$(A; \preceq)$ p(artially) o(rdered) set
D3.25) $a, b \in (A; \preceq)$ comparable $\Leftrightarrow a \preceq b$ or $b \preceq a$
D3.26) A totally ordered by $\preceq$ $\Leftrightarrow$ all $a, b \in (A; \preceq)$ comparable
3.4.1 $a \prec b \overset{\text{def}}{\Leftrightarrow} a \preceq b \wedge a \neq b$
D3.27) $a, b \in (A; \preceq)$: b covers a $\Leftrightarrow$ $a \prec b$ and there is no c with $a \prec c$ and $c \prec b$

D3.28) Hasse diagram: directed graph of elements in $(A; \preceq)$ with edges (a,b) for a covers b



E3.30) $(\{2,3,4,5,6,8\}; |)$

T3.10) For $(A; \preceq)$ and $(B; \sqsubseteq)$, $(A \times B; \leq)$ with $(a_1, b_1) \leq (a_2, b_2) \overset{\text{def}}{\Leftrightarrow} a_1 \preceq a_2 \wedge b_1 \sqsubseteq b_2$ is a poset.

T3.11) Lexicographical order with $(a_1, b_1) \leq_{\text{lex}} (a_2, b_2) \overset{\text{def}}{\Leftrightarrow} a_1 \prec a_2 \vee (a_1 = a_2 \wedge b_1 \sqsubseteq b_2)$ is a partial order relation.

3.4.3 $(A; \preceq)$ and $(B; \sqsubseteq)$ totally ordered $\Rightarrow$ $(A \times B; \leq_{\text{lex}})$ totally ordered

D3.29) For $(A; \preceq)$ and $S \subseteq A$, $a \in A$ is
- minimal*/maximal* if no $b \in A$ exists with $b \prec a$ / $b \succ a$
- least/greatest if for all $b \in A$ it is $a \preceq b$ / $a \succeq b$
- lower/upper bound of S if for all $b \in S$ it is $a \preceq b$ / $a \succeq b$
- greatest lower*/least upper bound of S

D3.30) $(A;\preceq)$ well-ordered
$\Leftrightarrow$ totally ordered and every non-empty subset has least element

3.4.4 $\Leftarrow$ totally ordered and finite

D3.31) $\{a,b\} \subseteq A$ in poset $(A;\preceq)$ might have a
- meet $a \wedge b$ (greatest lower bound)
- join $a \vee b$ (least upper bound)

D3.32) $(A;\preceq)$ is a lattice
$\Leftrightarrow$ every element pair has meet and join

Functions

D3.33) function $f: A \to B$ from domain A to codomain B, a relation which is
- totally defined $\forall a \in A\ \exists b \in B\ a f b$
- well-defined
$\forall a \in A\ \forall b,b' \in B\ (a f b \wedge a f b' \to b = b')$

3.5.1 definition $f: x \mapsto$ "expression in x"

D3.34) set of all functions $A \to B$ is B^A

D3.35) partial function: non-totally defined function

D3.36) image of f under S: $f(S) \stackrel{def}{=} \{f(a) \mid a \in S\}$

D3.37) image/range of f: $\mathrm{Im}(f) \stackrel{def}{=} f(A)$

D3.38) preimage of $T \subseteq B$: $f^{-1}(T) \stackrel{def}{=} \{a \in A \mid f(a) \in T\}$

D3.39) $f: A \to B$ is called
- injective if $a \neq b \Rightarrow f(a) \neq f(b)$, i.e. $f(a) = f(b) \Rightarrow a = b$
- surjective if $f(A) = B$, i.e. for all $b \in B$, $b = f(a)$ for some $a \in A$
- bijective if both is the case

D3.40) inverse f^{-1} exists $\Leftrightarrow$ f bijective

D3.41) composition of $f: A \to B$ and $g: B \to C$: $(g \circ f)(a) = g(f(a))$! $\neq$ relations !

L3.12) associativity $(h \circ g) \circ f = h \circ (g \circ f)$

Countability

D3.42) A and B equinumerous $(A \sim B)$ if there exists a bijection $A \to B$.

ii B dominates A $(A \preceq B)$ if $A \sim C$ for $C \subseteq B$, i.e. there exists an injective function $A \to B$.

iii A is countable if $A \preceq \mathbb{N}$, and uncountable otherwise

T3.15) A is countable $\Leftrightarrow$ A is finite or $A \sim \mathbb{N}$

L3.13) $\preceq$ is transitive $A \preceq B \wedge B \preceq C \Rightarrow A \preceq C$

ii $A \subseteq B \Rightarrow A \preceq B$

T3.14) $A \preceq B \wedge B \preceq A \Rightarrow A \sim B$

List of countable sets

T3.16) $\{0,1\}^* \stackrel{def}{=} \{\epsilon, 0, 1, 00, 01, 10, 11, \ldots\}$ set of finite binary sequences

T3.17) $\mathbb{N} \times \mathbb{N} = \mathbb{N}^2$

C3.18) $A \times B$ if A and B are countable, i.e. $A \preceq \mathbb{N} \wedge B \preceq \mathbb{N} \Rightarrow A \times B \preceq \mathbb{N}$

C3.19) $\mathbb{Q}$ rational numbers

T3.20) A^n tuples for $n \in \mathbb{N}$ if A is countable

ii $\bigcup_{i \in \mathbb{N}} A_i$ union of countable list $A_0, A_1, A_2, \ldots$ of countable sets

iii A^* finite sequences of elements from countable A

D3.43) $\{0,1\}^\infty$ set of semi-infinite binary sequences

T3.21) is uncountable

D3.44) $f: \mathbb{N} \to \{0,1\}$ is computable if a program exists that outputs $f(n)$ for all $n \in \mathbb{N}$

C3.22) There are uncomputable functions $\mathbb{N} \to \{0,1\}$

Division

D4.1) $a \mid b$
$\Leftrightarrow$ a is a divisor of b
$\Leftrightarrow$ b is a multiple of a
$\Leftrightarrow$ c is the quotient $c = \frac{b}{a}$ or $a = 0$

T4.1) $a = dq + r$ with $0 \leq r < |d|$ for $a, d \neq 0$ (Euclid)

4.2.2 $r =: R_d(a) = a \bmod d$

D4.2) greatest common divisor d for at least one non-zero $a, b \in \mathbb{Z}$: ¶
$d \mid a \wedge d \mid b \wedge \forall c ((c \mid a \wedge c \mid b) \to c \mid d)$

D4.3) $\gcd(a,b) :=$ positive d
a, b relatively prime $\Leftrightarrow \gcd(a,b) = 1$

L4.2) $\gcd(m, n - qm) = \gcd(m,n)$
$\gcd(m, R_m(n)) = \gcd(m,n)$

D4.4) ideal of $a, b \in \mathbb{Z}$
$(a,b) := \{ua + vb \mid u, v \in \mathbb{Z}\}$
ideal of $a \in \mathbb{Z}$
$(a) := \{ua \mid u \in \mathbb{Z}\}$

L4.3) $d \in \mathbb{Z}$ always exists, such that $(a,b) = (d)$

L4.4) d is a greatest common divisor of a and b if at least one a, b non-zero

C4.5) $\Rightarrow \gcd(a,b) = ua + vb$

D4.5) least common multiple l of $a, b \in \mathbb{N}^+$:
$a \mid l \wedge b \mid l \wedge \forall m ((a \mid m \wedge b \mid m) \to l \mid m)$

D4.6) prime $p > 1$ has only positive divisors 1 and p
composite $c > 1$ is non-prime

T4.6) Every positive integer can be written uniquely as the product of primes. (Fundamental Theorem of Arithmetic)

$a = \prod_i p_i^{e_i}$ and $b = \prod_i p_i^{f_i}$

4.3.3 $\gcd(a,b) = \prod_i p_i^{\min(e_i, f_i)}$

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

$\Rightarrow \gcd(a,b) + \operatorname{lcm}(a,b) = ab$

Modular Arithmetic

D4.8) $a \equiv_m b \overset{\text{def}}{\iff} m \mid (a-b)$ congruence modulo $m \geq 1$

L4.13) is an equivalence relation on $\mathbb{Z}$

L4.14) For $a \equiv_m b$ and $c \equiv_m d$, $a+c \equiv_m b+d$ and $ac \equiv_m bd$

C4.15) multi-variate polynomial with integer coefficients. For $a_i \equiv_m b_i$, $f(a_1, \dots, a_n) = f(b_1, \dots, b_n)$

4.5.2 $\mathbb{Z}_m \overset{\text{def}}{=} \{0, \dots, m-1\}$ set of remainders modulo m

L4.16) i $a \equiv_m R_m(a)$

ii $a \equiv_m b \iff R_m(a) = R_m(b)$

C4.17) $R_m(f(a_1, \dots, a_n)) = R_m(f(R_m(a_1), \dots, R_m(a_2)))$ modular arithmetic

L4.18) $\gcd(a,m) = 1 \iff ax \equiv_m 1$ has solution $x \in \mathbb{Z}_m$

D4.9) called multiplicative inverse of a modulo m. $(x \equiv_m a^{-1})$

T4.19) Chinese Remainder Theorem

$m_1, \dots, m_r$ pairwise relatively prime

$M = \prod_{i=1}^{r} m_i$ product of all m_i

$a_1, \dots, a_r$ with $0 \leq a_i < m_i$.

Exactly one x with $0 \leq x < M$ satisfies the system

$x \equiv_{m_1} a_1, \dots, x \equiv_{m_r} a_r$

4.5.4 $x = R_M\left(\sum_{i=1}^{r} a_i M_i N_i\right)$

with $M_i = \frac{M}{m_i}$ and $N_i \equiv_{m_i} M_i^{-1}$

4.6 Diffie-Hellman Key-Agreement

public prime p

public basis $g \in \{2, \dots, p-1\}$

secret random $x_A, x_B \in \{0, \dots, p-2\}$

$y_A := R_p(g^{x_A})$, $y_B := R_p(g^{x_B})$

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

$y_B^{x_A} \equiv_p g^{x_A x_B} \equiv_p y_A^{x_B}$

$\Rightarrow k_{AB} = k_{BA}$

secure since $x \mapsto R_p(g^x)$ is quick to compute (square and multiply) yet hard to reverse (discrete logarithm problem)

Algebra

D5.1) k-ary operation $S^k \to S$ on S

D5.2) algebra $\langle S; \Omega \rangle$ with carrier S and list of operations Ω

D5.3) left/right neutral element e of $\langle S; * \rangle$: $e * a = a$ / $a * e = a$ for all $a \in S$,

L5.1) Same if both exist, i.e. at most 1.

D5.4) $*$ on S is associative $\iff a*(b*c) = (a*b)*c$ for all $a,b,c \in S$

D5.5) monoid $\langle M; *, e \rangle$:
- $*$ is associative
- e is the neutral element

D5.6) left/right inverse b of a in $\langle S; *, e \rangle$: $b*a = e$ / $a*b = e$,

L5.2) in a monoid same if both exist, i.e. at most 1.

D5.7) group $\langle G; *, \hat{}, e \rangle$

(G1) $*$ is associative

(G2) e is the neutral element

(G3) Every $a \in G$ has an inverse $\hat{a}$

L5.3) Then, for all $a,b,c \in G$:

i $\hat{(\hat{a})} = a$

ii $\widehat{a*b} = \hat{b} * \hat{a}$

iii $a*b = a*c \Rightarrow b = c$

iv $b*a = c*a \Rightarrow b = c$

v $a*x = b$ and $x*a = b$ both have a unique solution x

D5.8) group/monoid $\langle S; * \rangle$ abelian $\iff a*b = b*a$

D5.9) direct product $\langle G_1 \times \dots \times G_n; \times \rangle$ of n groups $\langle G_i; *_i \rangle$ has component-wise operation $\times$:

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

L5.4) and is a group itself with component-wise neutral elements and inversion operations.

D5.10) group homomorphism $\psi: G \to H$ from $\langle G; *, \hat{}, e \rangle$ to $\langle H; \star, \tilde{}, e' \rangle$:

$\psi(a*b) = \psi(a) \star \psi(b)$

ψ isomorphism $G \simeq H$ $\iff \psi$ bijection

L5.5) Any homomorphism satisfies

i $\psi(e) = e'$

ii $\psi(\hat{a}) = \widetilde{\psi(a)}$ for all $a \in G$

D5.11) Subgroup $\langle H; *, \hat{}, e \rangle$ of $\langle G; *, \hat{}, e \rangle$:
- $H \subseteq G$
- $a*b \in H$ for all $a,b \in H$
- $e \in H$
- $\hat{a} \in H$ for all $a \in H$

D5.12) order $\operatorname{ord}(a)$ of a in group G is least $m \geq 1$ such that $a^m = e$, otherwise $\operatorname{ord}(a) = \infty$

5.3.4 $\operatorname{ord}(e) := 1$

$\operatorname{ord}(a) = 2 \Rightarrow a^{-1} = a$ self-inverse

L5.6) G is a finite group $\Rightarrow$ all $a \in G$ have finite order

D5.13) order $|G|$ of finite group G

D5.14) group generated by $a \in G$: $\langle a \rangle \overset{def}{=} \{a^n \mid n \in \mathbb{Z}\}$

5.3.5 $\langle a \rangle = \{e, a, a^2, \dots, a^{ord(a)-1}\}$ $\Leftarrow$ G is finite

D5.15) Cyclic group $G = \langle g \rangle$ of generator $g \in G$

T5.7) $\Rightarrow G \simeq \langle \mathbb{Z}_{|G|}; \oplus \rangle$ and hence abelian

T5.8) G finite and H subgroup of G $\Rightarrow |H| \mid |G|$ (Lagrange)

C5.9) $\Rightarrow ord(a) \mid |G|$ for all $a \in G$

C5.10) $\Rightarrow a^{|G|} = e$ for all $a \in G^*$

C5.11) group G with $|G|$ prime $\Rightarrow$ G is cyclic and all elements are generators

D5.16) $\mathbb{Z}_m^* \overset{def}{=} \{a \in \mathbb{Z}_m \mid gcd(a,m) = 1\}$

D5.17) Euler function $\varphi: \mathbb{Z}^+ \to \mathbb{Z}^+$, $\varphi(m) \overset{def}{=} |\mathbb{Z}_m^*|$

L5.12) $\varphi(m) = \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1}$ using prime factorization of m

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

C5.14) For all a and $m \geq 2$,
Euler $gcd(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv_m 1$
Fermat p prime and $p \nmid a \Rightarrow a^{p-1} \equiv_p 1$

T5.15) $\mathbb{Z}_m^*$ is cyclic $\Leftrightarrow$ $m = 2$ or $m = 4$ or with p odd prime and $e \geq 1$ $m = p^e$ or $m = 2p^e$

T5.16) RSA basis
finite $\langle G; \cdot, ^{-1}, 1 \rangle$
some $e \in \mathbb{Z}$ with $gcd(e, |G|) = 1$
function $x \mapsto y = x^e$
reversing it: $x = y^d$ with $d \equiv_{|G|} e^{-1}$, i.e. $ed \equiv_{|G|} 1$

proof $x^{ed} = x^{k|G|+1} = (x^{|G|})^k \cdot x \overset{*}{=} x$

5.4.2 Choice of G: $\mathbb{Z}_n^*$ with $n = pq$ and p, q prime
public n, e
secret $\varphi(n) = |\mathbb{Z}_n^*| = (p-1)(q-1)$
message $m \in \{1, \dots, n-1\}$
$y := R_n(m^e)$ $m = R_n(m^d)$

D5.18) ring $\langle R; +, -, 0, \cdot, 1 \rangle$
(i) $\langle R; +, -, 0 \rangle$ is a commutative group
(ii) $\langle R; \cdot, 1 \rangle$ is a monoid
(iii) left/right distributive laws $a(b+c) = ab + ac$ / $(b+c)a = ba + ca$

L5.17) Then, for all $a, b \in R$,
i $0a = a0 = 0$
ii $(-a)b = -(ab)$
iii $(-a)(-b) = ab$
iv $|R| > 1 \Leftrightarrow 1 \neq 0$

D5.19) characteristic of a ring := $ord(1)$ in additive group / 0 if $ord(1) = \infty$

D5.18) commutative ring R_c $\Leftrightarrow$ $ab = ba$ (for multiplication)

D5.20) $a \mid b$ $(a \neq 0)$
$\Leftrightarrow$ $c \in R_c$ exists with $b = ac$
$\Leftrightarrow$ a is divisor of b
$\Leftrightarrow$ b is multiple of a

L5.18) $a \mid b$ and $b \mid c \Rightarrow a \mid c$
ii $a \mid b \Rightarrow a \mid bc$ for all c
iii $a \mid b$ and $a \mid c \Rightarrow a \mid (b+c)$

D5.21) greatest common divisor

D5.22) $a \in R_c$ is a zerodivisor $\Leftrightarrow$ $b \in R_c$ exists with $ab = 0$ and $a, b \neq 0$

D5.23) $u \in R$ is a unit
$\Leftrightarrow$ u is invertible
$\Leftrightarrow$ $uv = vu = 1$ for some $v \in R$, $v =: u^{-1}$
Set of units R^*

L5.19) is a multiplicative group

D5.24) R_c is an integral domain $\Leftrightarrow$ R_c has no zerodivisors, i.e. $\forall a \forall b\, (ab = 0 \Rightarrow (a = 0 \vee b = 0))$, is commutative and $|R_c| > 1$

L5.20) $\Rightarrow$ unique quotient $c = \frac{b}{a}$ exists for $a \mid b$

D5.25) polynomial $a(x) \overset{def}{=} \sum_{i=0}^{d} a_i x^i$ with $d \geq 0$.
$deg(a(x)) :=$ greatest i, $a_i \neq 0$
$deg(0) := -\infty$
set $R[x]$ of polynomials over R

T5.21) is a ring.

L5.22) D is an integral domain $\Rightarrow$ $D[x]$ is an integral domain
ii The units $D[x]^* = D^*$ constants

D5.26) field $\langle F; +, -, 0, \cdot, 1 \rangle$: nontrivial, commutative ring with $F^* = F \setminus \{0\}$, i.e. $\langle F \setminus \{0\}; \cdot, ^{-1}, 1 \rangle$ is a commutative group

T5.24) $\Rightarrow$ F is integral domain

T5.23) $\mathbb{Z}_p$ is a field $\Leftrightarrow$ p is prime

5.5.5) field $GF(n)$ with n elements

D5.27) $a(x) \in F[x]$ is monic $\Leftrightarrow$ leading coefficient is 1

5.6.1) $a(x) \mid b(x) \Rightarrow v \cdot a(x) \mid b(x)$ for $v \in F$ with $v \neq 0$

D5.28) $a(x) \in F[x]$ is irreducible $\Leftrightarrow$ $deg(a(x)) \geq 1$ and only constants c or $c \cdot a(x)$ divide $a(x)$

5.6.1 $\in$ no irreducible polynomials of degree $\frac{deg(a(x))}{2}$ divide $a(x)$

D5.29) $\gcd(a(x), b(x)) := g(x)$ of largest degree with $g(x) | a(x)$ and $g(x) | b(x)$

T5.25) $a(x) = b(x) \cdot q(x) + r(x)$ for all $a(x)$ with $b(x) \neq 0$, unique monic **quotient** $q(x)$, **remainder** $r(x)$ with $\deg(r(x)) < \deg(b(x))$

5.6.2 $r(x) = R_{b(x)}(a(x))$

D5.33) **root** $\alpha \in \mathbb{R}$ of $a(x) \in \mathbb{R}[x]$: $a(\alpha) = 0$

L5.28) $\alpha \in F$ is root of $a(x) \in F[x]$ $\Leftrightarrow (x-\alpha) | a(x)$

C5.29) $a(x) \in F[x]$ of $\deg(a(x)) = 2/3$ is irreducible $\Leftrightarrow a(x)$ has no roots

D5.34) **root multiplicity**: highest power of $(x-\alpha)$ dividing $a(x) \in F[x]$

T5.30) $a(x) \in F[x]$ has at most $\deg(a(x))$ roots (with multipl.)

L5.31) $a(x) \in F[x]$ is uniquely determined by any $d = \deg(a(x)) + 1$ values $a(d_i)$

5.7.3 lagrange **interpolation**

$$a(x) = \sum_{i=1}^{d+1} a(d_i)\, U_i(x)$$

$$U_i(x) = \prod_{j \in [0; d+1] \setminus i} \frac{x - d_j}{d_i - d_j}$$

L5.32) $\equiv_{m(x)}$ is an equivalence relation, every class has a unique representative of $< \deg(m(x))$

D5.35) $F[x]_{m(x)} \overset{\text{def}}{=} \{ a(x) \in F[x] \mid \deg(a(x)) < \deg(m(x)) \}$

L5.34) is a ring with modulo ops.

L5.33) F finite $\Rightarrow |F[x]_{m(x)}| = |F|^{\deg(m(x))}$

L5.35) $F[x]^*_{m(x)} = \{ a(x) \in F[x]_{m(x)} \mid \gcd(a(x), m(x)) = 1 \}$

T5.36) $F[x]_{m(x)}$ is a field $\Leftrightarrow m(x)$ is irreducible

Error-correcting Codes

D5.36) (n,k)-**encoding function** $E: \mathcal{A}^k \to \mathcal{A}^n$

D5.37) (n,k)-**error-correcting-code** $\subseteq \mathcal{A}^n$ with cardinality $|\mathcal{A}|^k$

D5.38) **Hamming distance**: # different letters

D5.39) **minimum code distance** d: minimum Hamming distance between 2 codewords

D5.40) (n,k)-**decoding function** $D: \mathcal{A}^n \to \mathcal{A}^k$

D5.41) is **t-error-correcting** if for any word, Hamming distance $\leq t$

T5.40) $\Leftrightarrow d \geq 2t+1$

T5.41) $\mathcal{A} = GF(q)$, $\alpha_0, \dots, \alpha_{n-1} \in \mathcal{A}$

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

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

minimum distance $d = n-k+1$

Proof Systems

6.2.1 alphabet Σ, statements $S \subseteq \Sigma^*$, proof strings $P \subseteq \Sigma^*$, truth function $\tau: S \to \{0,1\}$, verification function $\phi: S \times P \to \{0,1\}$

D6.1) **proof system** $\Pi = (S, P, \tau, \phi)$

D6.2) Π **sound** $\Leftrightarrow$ for all $s \in S$ with associated $p \in P$ and $\phi(s,t) = 1$, $\tau(s) = 1$

D6.3) Π **complete** $\Leftrightarrow$ for all $s \in S$ with $\tau(s) = 1$, exists $p \in P$ with $\phi(s,p) = 1$

Logic

D6.4) **syntax** defines alphabet $\mathcal{A}$ and correct formulas in $\mathcal{A}^*$

D6.5) **semantics** defines for each formula $F = \{f_1, \dots, f_k\} \in \mathcal{A}^*$
- function free(F) $\subset \{1, \dots, k\}$
- truth value $\nu(F, \mathcal{A}) = \mathcal{A}(F)$ for each suitable

D6.6) **interpretation** $\mathcal{A}$ with
- domain for $\mathcal{Z} \subseteq \mathcal{A}$
- assignment function $\mathcal{Z} \to$ domain

D6.7) $\mathcal{A}$ **suitable** $\Leftrightarrow$ all symbols in F assigned a value

D6.9) $\mathcal{A}$ is **model** for F/M
$\Leftrightarrow \mathcal{A}(F) = 1$ / for all $F \in M$
$\Leftrightarrow \mathcal{A} \models F / M$

D6.10) F is **satisfiable** $\Leftrightarrow$ model exists
F is unsatisfiable: $F = \bot$

D6.11) F is a **tautology** $\Leftrightarrow F = \top$ $\Leftrightarrow$ every suitable $\mathcal{A}$ is a model

D6.14) $\Leftrightarrow \models F$

D6.12) **logical consequence** $F \models G$: for all suitable $\mathcal{A}$s, if $\mathcal{A}(F) = 1$, then $\mathcal{A}(G) = 1$

D6.13) $F \equiv G \Leftrightarrow F \models G$ and $G \models F$ $\Leftrightarrow F$ and G are **equivalent**

D6.15) $\neg F$, $(F \wedge G)$, $(F \vee G)$ are formulas

D6.16) $\mathcal{A}(F \wedge G) \Leftrightarrow \mathcal{A}(F) = 1$ and $\mathcal{A}(G) = 1$
$\mathcal{A}(F \vee G) \Leftrightarrow$ " or "
$\mathcal{A}(\neg F) \Leftrightarrow \mathcal{A}(F) = 0$

L6.1)

	$F \wedge F \equiv F$	$F \vee F \equiv F$	idempotence
2	$F \wedge G \equiv G \wedge F$	$F \vee G \equiv G \vee F$	commutativity
3	$(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$	$(F \vee G) \vee H \equiv F \vee (G \vee H)$	ass.
4	$F \wedge (F \vee G) \equiv F$	$F \vee (F \wedge G) \equiv F$	absorption
5	$F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$		dist.
6	$F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$		dist.
7	$\neg\neg F \equiv F$		double negation
8	$\neg(F \wedge G) \equiv \neg F \vee \neg G$		de Morgan
	$\neg(F \vee G) \equiv \neg F \wedge \neg G$		de Morgan
9	$F \vee \top \equiv \top$	$F \wedge \top \equiv F$	
10	$F \vee \bot \equiv F$	$F \wedge \bot \equiv \bot$	
11	$F \vee \neg F \equiv \top$	$F \wedge \neg F \equiv \bot$	

L6.2) F is a tautology $\Leftrightarrow \neg F$ is unsatisfiable

L6.3) These are equivalent:
1 $\{F_1, \dots, F_k\} \models G$
2 $(F_1 \wedge \dots \wedge F_k) \Rightarrow G$ is tautology
3 $\{F_1, \dots, F_k, \neg G\}$ is unsatisfiable

6.4.2 Hilbert-Style Calculi

D6.17) **derivation rule** $\{F_1, \dots, F_k\} \vdash_R G$

D6.18) is applied by selecting $N \subseteq M$, specifying formulas in N for $N \vdash_R G$, and adding G to M

D6.19) **calculus** $K = \{R_1, \dots, R_m\}$

D6.20) **derivation** $M \vdash_K G$: finite sequence of rule applications of rules in K leading from formulas M to formula G

D6.21) R **correct**: $M \vdash_R G \Rightarrow M \models G$

D6.22) K **sound**: $M \vdash_K G \Rightarrow M \models G$
6.4.3 $\Leftrightarrow$ every $R \in K$ is correct

D6.22) K **complete**: " $\Leftarrow$ " for all M, G

L6.4) $F \vdash_K G$ holds for sound K $\Rightarrow \models (F \to G)$

6.5 Propositional Logic

D6.23) **Syntax**:
- atomic formulas A_i with $i \in \mathbb{N}$
- D6.15 $(\neg F, (F \wedge G), (F \vee G))$

D6.24) **Semantics**:
- truth assignment $\mathcal{A}: \mathbb{Z} \to \{0,1\}$ for all atomic formulas A_i
- $\mathcal{A}(F) = \mathcal{A}(A_i)$ if $F = A_i$, otherwise D6.16

D6.25) **literal**: A_i or $\neg A_i$

D6.26) **conjunctive normal form CNF**: $(L_1 \vee \dots \vee L_i) \wedge \dots \wedge (L_j \vee \dots \vee L_n)$

D6.27) **disjunctive normal form DNF**: $(L_1 \wedge \dots \wedge L_i) \vee \dots \vee (L_j \wedge \dots \wedge L_n)$

T6.5) Every formula $\equiv$ both NFs

6.5.6 Resolution Calculus

D6.28) **clause** K: set of literals

D6.29) F in CNF as in D6.26 $\Rightarrow K(F) \overset{def}{=} \{\{L_{1,1}, \dots L_{1,i}\}, \dots, \{L_{j,1} \dots L_{j,n}\}\}$
$K(M) \overset{def}{=} \bigcup_{i=1}^{k} K(F_i)$

D6.30) $K = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\neg L\})$ is **resolvent** $\Leftrightarrow L \in K_1, \neg L \in K_2$

6.5.6 $\{K_1, K_2\} \vdash_{res} K$
calculus $Res = \{res\}$

L6.6) is sound

T6.7) M unsatisfiable $\Leftrightarrow K(M) \vdash_{res} \emptyset$

6.6 Predicate Logic

D6.31) **Syntax**:
- variable symbols x_i with $i \in \mathbb{N}$
- function symbols $f_i^{(k)}$ with $i, k \in \mathbb{N}$ and k the number of arguments
- predicate symbols $P_i^{(k)}$ "
- terms: variables or functions using other terms
- atomic formulas: predicates using terms
- D6.15 $(\neg F, (F \wedge G), (F \vee G))$
- $\forall x_i F$ and $\exists x_i F$ are formulas for all i

D6.32) x is **bound** $\Leftrightarrow$ x is not **free**
$\Leftrightarrow$ x occurs in $\forall x G$ or $\exists x G$
F is **closed** $\Leftrightarrow$ F contains no free variables

D6.33) $F[x/t]$: substitute every free occurence of x with t

D6.34) **interpretation** $\mathcal{A} = (U, \phi, \Psi, \xi)$
- non-empty universe U
- function assignments ϕ, i.e. $\phi(f): U^k \to U$
- predicate assignments Ψ, i.e. $\Psi(P): U^k \to \{0,1\}$
- variable assignments ξ, i.e. $\xi(x) \in U$

D6.35) $\mathcal{A}$ **suitable** for F $\Leftrightarrow$ $\mathcal{A}$ defines all symbols and free variables in F

D6.36) **semantics**:
- $\mathcal{A}(t) = \begin{cases} \xi(t) \text{ if } t \text{ is a variable} \\ \phi(f)(\mathcal{A}(t_1), \dots) \text{ else} \end{cases}$
- truth value $\mathcal{A}(F)$: recur as in D6.16,
$\mathcal{A}(P(t_1, \dots)) = \Psi(P)(\mathcal{A}(t_1) \dots)$,
$\mathcal{A}(\forall x G) = \begin{cases} 1 \text{ if } \mathcal{A}_{[x \to u]} = 1 \text{ for all } u \in U \\ 0 \text{ else} \end{cases}$, or
$\mathcal{A}(\exists x G) = \begin{cases} 1 \text{ if } \mathcal{A}_{[x \to u]} = 1 \text{ for some } u \in U \\ 0 \text{ else} \end{cases}$

L6.8) $\neg(\forall x F) \equiv \exists x \neg F$
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 $(\forall x F) \wedge H \equiv \forall x (F \wedge H)$ if x not free
8 " $\forall \vee$ 9 " $\exists \wedge$ 10 " $\exists \vee$

L6.9) $F = \dots G \dots$ and $G \equiv H$ $\Rightarrow F' = \dots H \dots \equiv F$

L6.10) $\forall x G \equiv \forall y G[x/y]$
$\exists x G \equiv \exists y G[x/y]$
if y doesn't occur in G

D6.37) F is **rectified** $\Leftrightarrow$ no variables appear free and bound, and no quantifier has the same variable

L6.11) $\forall x F \models F[x/t]$
universal instantiation

D6.38) $Q_1 x_1 Q_2 x_2 \dots Q_n x_n G$ prenex form

T6.12) always exists

T6.13) $\neg \exists x \forall y (P(y,x) \Leftrightarrow \neg P(y,y))$

C6.14) $\Rightarrow \{S \mid S \notin S\}$ is not a set