1 Operators

$$a|b :\Leftrightarrow \exists c \; b = ac \text{ for } a \neq 0$$
$$a \equiv_m b :\Leftrightarrow m|(a-b)$$

2 Propositions

$$A \to B \Leftrightarrow \neg A \vee B$$
$$(A \wedge B) \vee C \Leftrightarrow (A \vee C) \wedge (B \vee C)$$
$$(A \vee B) \wedge (C \vee D) \Leftrightarrow (A \wedge C) \vee (A \wedge D) \vee (B \wedge C) \vee (B \wedge D)$$
$$\forall x \; P(x) \wedge \forall x \; Q(x) \Leftrightarrow \forall x \; (P(x) \wedge Q(x))$$
$$\exists x \; (P(x) \wedge Q(x)) \Rightarrow \exists x \; P(x) \wedge \exists x \; Q(x) \quad \text{but not vice versa}$$
$$\neg \forall x \; P(x) \Leftrightarrow \exists x \; \neg P(x)$$
$$\neg \exists x \; P(x) \Leftrightarrow \forall x \; \neg P(x)$$
$$\exists y \; \forall x \; P(x,y) \Rightarrow \forall x \; \exists y \; P(x,y) \quad \text{but not vice versa}$$

3 Proofs

To prove a sentence (either true or false) means to show that it's a tautology. The following **proof patterns** may be used.

3.0.1 Direct Proof of an Implication

Example: $F \to G$

A **direct proof of an implication** works by assuming F and then deriving G from F.

$$F \Rightarrow ... \Rightarrow ... \Rightarrow ... \Rightarrow G$$

3.0.2 Indirect Proof of an Implication

Example: $F \to G$

An **indirect proof of an implication** proceeds by assuming $\neg G$ and deriving $\neg F$ under this assumption.

$$\neg G \Rightarrow ... \Rightarrow ... \Rightarrow ... \Rightarrow \neg F$$

3.0.3 Composition of Implications

Example: $F \to G$ and $G \to H$

1. Prove the statement F
2. Prove the implications $F \Rightarrow G$ and $G \Rightarrow H$

3.0.4 Case Distinction

1. Define a complete list of cases
2. Prove the statement for each case separately

3.0.5 Proof by Contradiction

Assume that the sentence F is false and derive a false statement from it.

$$\neg F \Rightarrow ... \Rightarrow ... \Rightarrow ... \Rightarrow \bot$$

3.0.6 Existence Proof

Example: $\exists x \ P(x)$

Either find a variable which satisfies the sentence (**constructive**) or proof the existence of such a variable without exhibiting it (**non-constructive**).

3.0.7 Proof by Counterexample

Example: $\neg \forall x \ P(x)$

Find a variable such that the sentence is wrong.

3.0.8 Proof by Induction

Example: $\forall n \ P(n)$

1. **Basis step**: Prove $P(0)$
2. Assume $P(n)$
3. **Induction step**: Prove $P(n+1)$

4 Predicate Logic

4.1 Rules

1. $\forall x \ P(x) \land \forall x \ Q(x) \Leftrightarrow \forall x \ (P(x) \land Q(x))$
2. $\exists x \ (P(x) \land Q(x)) \Rightarrow \exists x \ P(x) \land \exists x \ Q(x)$
3. $\neg \forall x \ P(x) \Leftrightarrow \exists x \ \neg P(x)$
4. $\neg \exists x \ P(x) \Leftrightarrow \forall x \ \neg P(x)$
5. $\exists y \forall x \ P(x,y) \Rightarrow \forall x \exists y \ P(x,y)$

5 Sets

$$\begin{aligned} A \subseteq B &:\Leftrightarrow \forall x \ (x \in A \to x \in B) \\ A = B &\Leftrightarrow A \subseteq B \land B \subseteq A \\ P(A) &:= \{S \mid S \subseteq A\} \\ A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \\ A \times B &= \{(a,b) \mid a \in A \land b \in B\} \end{aligned}$$

6 Relations

6.1 Reflexive

Formula: $a\ \rho\ a$
Set: $id \subseteq \rho$
Matrix: Diagonal is all 1
Graph: Every vertex has a loop
Examples: $\leq$, $\geq$, $|$, $\equiv_m$ on $\mathbb{Z}$

6.2 Transitive

Formula: $a\ \rho\ b\ \wedge\ b\ \rho\ c \Rightarrow a\ \rho\ c$
Set: $\rho^2 \subseteq \rho$
Examples: $\leq$, $\geq$, $|$, $<$, $>$, $\equiv_m$ on $\mathbb{Z}$

6.3 Symmetric

Formula: $a\ \rho\ b \Leftrightarrow b\ \rho\ a$
Set: $\rho = \hat{\rho}$
Matrix: Matrix is symmetric
Graph: Undirected graph, possibly with loops
Examples: $\equiv_m$ on $\mathbb{Z}$

6.4 Antisymmetric

Formula: $a\ \rho\ b \wedge b\ \rho\ a \Rightarrow a = b$
Set: $\rho \cap \hat{\rho} \subseteq id$
Graph: No cycle of length 2
Examples: $\leq$, $\geq$ on $\mathbb{Z}$ and $|$ on $\mathbb{N}$

6.4.1 Relations as Sets

$a\ \rho\sigma\ b$**:**	$\exists b \in B : (a\ \rho\ b\ \wedge\ b\ \sigma\ c)$
$a\ (\rho \cup \sigma)\ b$**:**	Either $a\ \rho\ b$ or $a\ \sigma\ b$
$a\ (\rho \cap \sigma)\ b$**:**	$a\ \rho\ b$ and $a\ \sigma\ b$
The empty set $\emptyset$:	symmetric and transitive

6.4.2 Equivalence Relation

Example: $\equiv_m$ on $\mathbb{Z}$
A relation that is reflexive, symmetric, and transitive.

6.5 Partial Order

Example: $\leq$ and $\geq$ on $\mathbb{Z}, \mathbb{Q}, or \mathbb{R}$
A relation that is reflexive, antisymmetric, and transitive.

Special elements in a poset $(A, \preceq)$ with a subset S of A $S \subseteq A$:

minimal (maximal) element:	$a \in S$ if there exists no $b \in S$ with $b \prec a$ $(b \succ a)$
least (greatest) element:	$a \in S$ if $a \preceq b$ $(a \succeq b)$ for all $b \in S$
lower (upper) bound:	$a \in A$ if $a \preceq b$ $(a \succeq b)$ for all $b \in S$
greatest lower (least upper) bound:	$a \in A$ if a is the greatest (least) element of the set of all lower (upper) bounds of S

6.6 Function

injective:	no collisions
surjective:	every value in the codomain is taken on for some argument
bijective:	one-to-one mapping (injective and surjective)

7 Combinatorics

	with repetition	**without repetition**
ordered	n^k	$\frac{n!}{(n-k)!}$
	A passcode of length n with k different digits	How many ways can k places be awarded to n people
unordered	$\binom{n+k-1}{k}$	$\binom{n}{k} = \frac{n!}{k!(n-k)!}$
	Choose k scoops of ice cream from n different flavours	

7.0.1 Countability

same cardinality $A \sim B$**:**	There exists a bijection $A \to B$
B has at least the cardinality of A $A \preceq B$**:**	$A \sim C$ for some subset $C \subseteq B$
B dominates A $A \prec B$**:**	$A \preceq B \wedge A \not\sim B$
countable:	$A \preceq \mathbb{N}$

Hint:
The set $\{0,1\}^* := \{0, 1, 00, 01, ...\}$ of **finite binary sequences** is countable.
The set $\{0,1\}^\infty$ is uncountable (Cantor's diagonalization argument)

8 Graph Theory

walk:	sequence of vertices such that consecutive vertices are connected
tour:	a walk with distinct edges
circuit:	a tour that ends where it started
Hamiltonian cycle:	a circuit that visits all vertices

A **tree** is an *undirected, connected* graph with no cycles and $n-1$ edges.

For *connected, planar* graphs, the following equations hold:

$$\textbf{number of regions } r = |E| - |V| + 2$$
$$\textbf{sum of the degrees of the regions} = 2|E|$$
$$\text{if } |V| \geq 3 \Rightarrow |E| \leq 3|V| - 6$$
$$\text{if } |V| \geq 3 \text{ and bipartite} \Rightarrow |E| \leq 2|V| - 4$$

9 Number Theory

9.1 Division

Hint: Every non-zero integer is a divisor of 0. 1 and -1 are divisors of every integer.

9.2 Greatest Common Divisor

For integers a and b (not both 0), an integer d is called a $gcd(a, b)$ if d divides both a and b and if every common divisor of a and b divides d.

$$d|a \text{ and } d|b \text{ and } c|a \wedge c|b \Rightarrow c|d$$
$$gcd(a, b) :\Leftrightarrow \exists u, v \; ua + vb$$

9.3 Ideal

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

For $a, b \in \mathbb{Z}$ there exists $d \in \mathbb{Z}$ such that $(a, b) = (d)$. This is implies that d is the **gcd** of a and b.

9.4 Least Common Multiple

$l = lcm(a, b)$ is the common multiple of a and b which divides every common multiple of a and b.

$$a|l' \text{ and } b|l' \;\Rightarrow l|l'$$

It follows:

$$gcd(a, b) \cdot lcm(a, b) = ab$$

9.5 Modular Arithmetic

$$R_m(a + b) = R_m(R_m(a) + R_m(b))$$
$$R_m(ab) = R_m(R_m(a) \cdot R_m(b))$$

9.6 Multiplicative Inverses

The **congruence equation** has a solution $x \in \mathbb{Z}_m$ if and only if $gcd(a, m) = 1$. The solution is unique.

$$ax \equiv_m 1$$

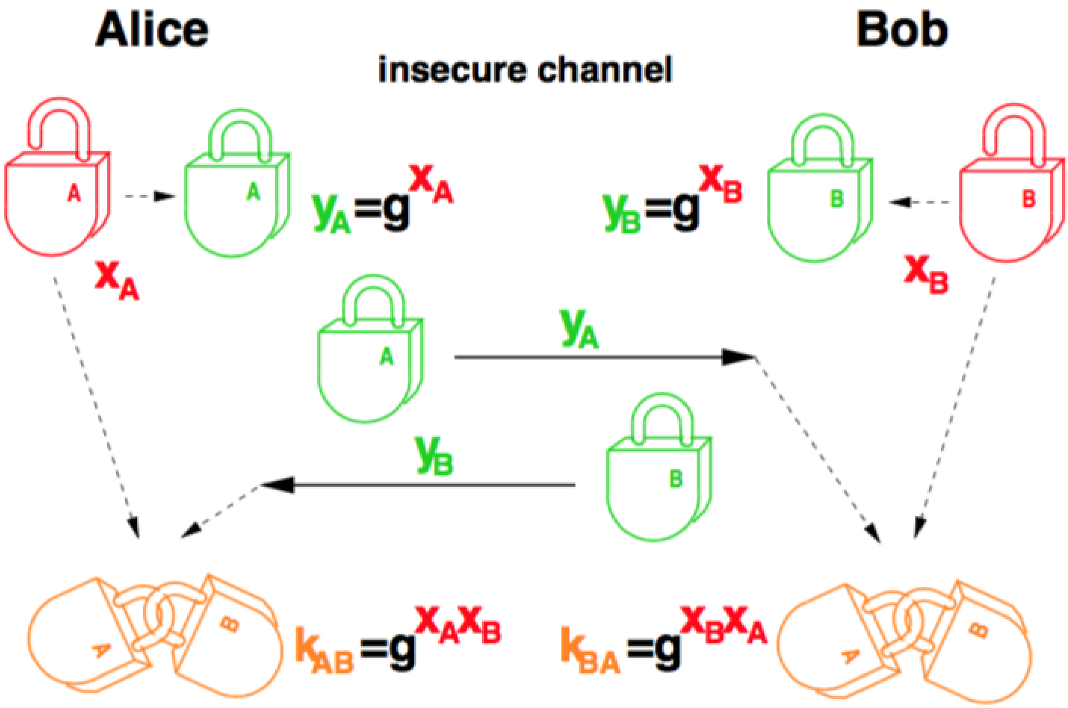
The x satisfying the equation is called the **multiplicative inverse of a modulo m** ($x \equiv_m a^{-1}$ or $x \equiv_m \frac{1}{a}$).

9.7 Diffie-Hellmann Key-Agreement Protocol

The Diffie-Hellmann protocol is based on the **discrete logarithm problem**. Basically, while $y = R_p(g^x)$ can be computed efficiently, it can't be solved for x.

Alice	insecure channel	Bob
select x_A at random from $\{0, \ldots, p-2\}$		select x_B at random from $\{0, \ldots, p-2\}$
$y_A := R_p(g^{x_A})$		$y_B := R_p(g^{x_B})$
	$\xrightarrow{y_A}$	
	$\xleftarrow{y_B}$	
$k_{AB} := R_p(y_B^{x_A})$		$k_{BA} := R_p(y_A^{x_B})$

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



10 Algebra

10.1 Special Properties

Some special properties of an algebra $\langle S; *, e\rangle$ are

neutral element:	$e \in S$ such that $e * a = a * e = a$
associativity:	$*$ is associative if $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$
inverse element:	b is the inverse of a if $b * a = a * b = e$
commutative/abelian:	$a * b = b * a$ for all $a, b \in S$

The **neutral** and **inverse element** can have a left and right version. E.g. $e * a = a$ is the left neutral element. However, there is *always only one* neutral/inverse element.

10.2 Special Algebras

	Notation	Axioms	Examples
Semigroup	$\langle S; * \rangle$	$*$ is associative	
Monoid	$\langle M; *, e \rangle$	$*$ is associative	
		e is the neutral element	
Group	$\langle G; *, \hat{}, e \rangle$	$*$ is associative	$\langle \mathbb{Z}; +, -, 0 \rangle$, $\langle \mathbb{Q} - \{0\}; \cdot, ^{-1}, 1 \rangle$, $\langle \mathbb{R}; +, -, 0 \rangle$
		e is the neutral element	
		every $a \in G$ has an inverse element	
Ring	$\langle R; +, -, 0, \cdot, 1 \rangle$	$\langle R; +, -, 0 \rangle$ is a commutative group	$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (commutative)
		$\langle R; \cdot, 1 \rangle$ is a monoid	
		$a(b+c) = ab + ac$ and $(b+c)a = ba + ca$ for all $a, b, c \in R$	
Integral Domain		cummutative	$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
		no zerodividers $ab = 0 \Rightarrow a = 0 \vee b = 0$	
Field	$\langle F - \{0\}; \cdot, ^{-1}, 1 \rangle$, $GF(p)$	commutative	$\mathbb{Q}, \mathbb{R}, \mathbb{C}$
		every nonzero element is a unit (has an inverse)	

10.3 Groups

10.3.1 Direct Product

The **direct product of n groups** $\langle G_1; *_1 \rangle, ..., \langle G_n; *_n \rangle$ is the group

$$\langle G_1 \times ... \times G_n, \star \rangle$$

where the operation $\star$ is component-wise:

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

10.3.2 Homomorphism

A function ψ from a group $\langle G; *, \hat{}, e \rangle$ to a group $\langle H; \star, \hat{}, e' \rangle$ is a group homomorphism if, for all a and b

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

Furthermore, ψ is an **isomorphism** if it's a bijection.
A group homomorphism satisfies:

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

10.4 Subgroup

A subset $H \subseteq G$ of a group $\langle G; *, \hat{}, e \rangle$ is called a subgroup if $\langle H; *, \hat{}, e \rangle$ is *closed* with respect to all operations.

$$a * b \in H \text{ for all } a, b \in H$$
$$e \in H$$
$$\hat{a} \in H \text{ for all } a \in H$$

The smallest subgroup of a group G containing the element $g \in G$ is the **group generated** by g:

$$\langle g \rangle := \{g^n | n \in \mathbb{Z}\}$$

where the resulting group is called **cyclic**.

Hint: The order of a subgroup of a finite group divides its enclosing group's order $|H|$ divides $|G|$.

10.4.1 Cyclic Group

A **cyclic group** of order n is isomorphic with $\langle \mathbb{Z}_n; \oplus \rangle$.

Hint: Every group of prime order is cyclic, and in such a group every element except the neutral element is a generator.
Hint: $\mathbb{Z}_p^*$ is cyclic if and only if $m = 2$, $m = 4$, $m = p^e$ or $m = 2p^e$, where p is a prime and $e \geq 1$

10.4.2 Order

of a finite group: $|G|$ is the order of G

of an element of G: The order of $a \in G$ is the least $m \geq 1$ such that $a^m = e$ if such an m exists, and $ord(a) = \infty$ otherwise.
Hint: $ord(e) = 1$. If $ord(a) = 2$, then $a^{-1} = a$.

10.5 Group $\mathbb{Z}_m^*$ and Euler's Function

$\langle \mathbb{Z}_m^*; \odot, ^{-1}, 1 \rangle$ is a group with the set

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

The **Euler function** is defined as follows:

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

Hint: If p is a prime, then $\mathbb{Z}_p^* = \{1, ..., p-1\} = \mathbb{Z}_p - \{0\}$

10.6 Error-Correcting Codes

A **(k,n)-error-correcting code** $\mathcal{C}$ over the alphabet $\mathcal{A}$ with $|\mathcal{A}| = q$ is a subset of cardinality q^k of $\mathcal{A}^n$.

Hint: Usually, $\mathcal{A} = \{0, 1\}$ with $q = 2$ is being considered

The **Hamming distance** between two codewords is the number of positions at which the two codewords differ.
The **minimum distance** of an error-correcting code $\mathcal{C}$ is the minimal Hamming distance between any two codewords.
A code $\mathcal{C}$ with minimum distance d can correct t errors if and only if $d \geq 2t + 1$.

11 Logic

11.1 Proof System

A **proof system** is a quadruple $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$ with the following components:

set of statements $\mathcal{S}$:	every $s \in \mathcal{S}$ is either *true* or *false*
set of proofs $\mathcal{P}$:	e.g. strings over some alphabet
truth function τ:	defines the meaning (*semantics*) of objects in $\mathcal{S}$
verification function ϕ:	$\phi(s,p) = 1$ means that p is a valid proof for the statement s

The proof system $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$ is

sound	if no false statement has a proof $\phi(s,p) = 1 \Rightarrow \tau(s) = 1$
complete	if every true statement has a proof $\tau(s) = 1 \Rightarrow \exists p \in (P)\ \phi(s,p) = 1$

11.2 Syntax and Semantics

	Description	Notation
Syntax	alphabet of allowed symbols and which strings are valid	
Interpretation	an assignment to all variable symbols	$\mathcal{A}(A) = \{0,1\}$
Semantics	a function σ assigning to each formula F and each suitable interpretation $\mathcal{A}$ a truth value	$\sigma(F, \mathcal{A}) = \{0,1\}$, $\mathcal{A}(F)$
Model	an interpretation $\mathcal{A}$ for which F is true	$\mathcal{A} \models F$

11.2.1 Structure

A **structure** is a tuple $\mathcal{A} = (U, \phi, \psi, \xi)$ with the following components:

universe U:	nonempty set
function ϕ:	assigns to each function symbol a function $U^k \mapsto U$
function ψ:	assigns to each predicate symbol a function $U^k \mapsto \{0,1\}$
function ξ:	assigns to each variable symbol a value in U

11.3 Calculi

A **derivation rule** is a rule for deriving a formula from a set of formulas. G can be derived from the set $\{F_1, ..., F_k\}$ by rule R:

$$\{F_1, ..., F_k\} \vdash_R G$$

A **calculus** K is a finite set of derivation rules $K = \{R_1, ..., R_m\}$. It is

sound/correct	if and only if every derivation rule is correct
complete	if M is a logical consequence of F, then F can be derived from M using K

11.4 Normal Forms

11.4.1 Conjunctive Normal Form (CNF)

$$F = (L_{11} \vee ... \vee L_{1m_1}) \wedge ... \wedge (L_{n1} \vee ... \vee L_{nm_n})$$

11.4.2 Disjunctive Normal Form (DNF)

$$F = (L_{11} \wedge ... \wedge L_{1m_1}) \vee ... \vee (L_{n1} \wedge ... \wedge L_{nm_n})$$

Hint: Every formula is equivalent to a formula in **CNF** and **DNF**.

11.5 Resolution Calculus

Given a Formula F in CNF, one can transform it into a set of clauses:

$$\mathcal{K}(F) = \{\{L_{11}, ..., L_{1m_1}\}, ..., \{L_{n1}, ..., L_{nm_1}\}\}$$

A clause K is then a **resolvent** of clauses K_1 and K_2 if there is a literal L such that $L \in K_1$ and $\neg L \in K_2$

$$K = (K_1 - \{L\}) \cup (K_2 - \{\neg L\})$$

This derivation is denoted as follows:

$$\{K_1, K_2\} \vdash_{res} K$$

Hint: A set M of formulas is unsatisfiable if and only if $\mathcal{K}(M) \vdash_{res} \emptyset$