Rose's Discrete Mathematics

Rose Enos

2025

Adapted from the following sources:

- *Boolean Logic and Discrete Structures*, September 2024 Edition by Sandy Irani
- *An Introduction to Abstract Mathematics*, March 10, 2024 Edition by Neil Donaldson and Alessandra Pantano
- Lectures by Professor Irene Gassko at the University of California, Irvine for I&C SCI 6B and I&C SCI 6D
- Lectures by Professor Neil Donaldson at the University of California, Irvine for MATH 13
- Lectures by Devansh Saluja at the University of California, Irvine for MATH 13

Contents

1 Propositional Logic

1.1 Propositions

Logic is the study of formal reasoning. A **truth value**, or **truth state**, is which describes a statement of true T, false F, unknown, or subjective. A **proposition**, or **statement**, is a sentence with a truth value. A **propositional variable**, or **abstract proposition**, p is a variable that represents a proposition.

A **compound proposition** is a combination of propositions. Compound propositions are constructed by **logical operations**. The **conjunction** $p \wedge q$ of two propositions is true if and only if both propositions are true. The **disjunction**, or **inclusive disjunction**, $p \vee q$ is false if and only if both propositions are false. The **exclusive disjunction** $p \oplus q$ is true if and only if exactly one of the propositions is true. The **negation**, or **complement**, $\neg p$ of a proposition is true if and only if the proposition is false. The **order of precedence** when evaluating logical operations is as follows:

1. Parentheses
2. Quantifiers
3. Negation
4. Conjunction
5. Disjunction
6. Connectives

A **truth table** gives the truth value of a compound proposition based on each combination of truth values of the component propositions. A compound proposition with n component propositions generates a truth table with 2^n rows.

$\cdots$	p	q
$\cdots$	F	F
$\cdots$	F	T
$\cdots$	T	F
$\cdots$	T	T

Table 1: Truth table

The **conditional operation**, or **implication**, $p \implies q$ on two propositions, the **hypothesis**, or **antecedent**, p and the **conclusion**, or **consequent**, q, is false if and only if the hypothesis is true and the conclusion is false. **Lazy evaluation** states that the conditional is true if the hypothesis is false. The **biconditional operation** $p \iff q$ is true if and only if both propositions

Conditional	$p \implies q$
Converse	$q \implies p$
Contrapositive	$\neg q \implies \neg p$
Inverse	$\neg p \implies \neg q$

Table 2: Conditional relationships

have the same truth value. The conditional and biconditional operations are **logical connectives**.

Two propositions are **logically equivalent** $p \equiv q$ if and only if they always have the same truth value regardless of the combination of truth values of their component propositions. A **tautology** is a proposition $p \equiv T$. A **contradiction** is a proposition $p \equiv F$. A **contingency** is a proposition that is neither a tautology nor a contradiction. Equivalent propositions can be **substituted** for each other in a compound proposition of which they are a component.

Idempotent Laws	$p \vee p \equiv p$ $p \wedge p \equiv p$
Associative Laws	$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
Commutative Laws	$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$
Distributive Laws	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
Identity Laws	$p \vee F \equiv p$ $p \wedge T \equiv p$
Domination Laws	$p \wedge F \equiv F$ $p \vee T \equiv T$
Double Negation Law	$\neg\neg p \equiv p$
Complement Laws	$p \wedge \neg p \equiv F$ $p \vee \neg p \equiv T$ $\neg T \equiv F$ $\neg F \equiv T$
De Morgan's Laws	$\neg(p \vee q) \equiv \neg p \wedge \neg q$ $\neg(p \wedge q) \equiv \neg p \vee \neg q$
Absorption Laws	$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$
Conditional Identities	$p \implies q \equiv \neg p \vee q$ $p \iff q \equiv (p \implies q) \wedge (q \implies p)$

Table 3: Laws of propositional logic

1.2 Predicates

A **predicate**, or **propositional function** or **open sentence**, $P(x)$ is a statement P whose truth value depends on one or more variables x. The **domain** of a variable is the set of its possible values. The **universal quantifier** $\forall x$ quantifies all values in the domain of a variable. The **existential quantifier** $\exists x$ quantifies at least one value in the domain of a variable.

A **free variable** is an unquantified variable. A predicate depends on a free variable. A **bound variable** is a quantified variable. A predicate becomes a proposition when its variables are bound.

A predicate with a universally quantified variable is false if and only if it is false for at least one value of the variable, called a **counterexample**, and thus is **vacuously true** when the domain is empty. A predicate with an existentially quantified variable is true if and only if it is true for at least one value of the variable, called an **example**, and thus is **vacuously false** when the domain is empty.

De Morgan's Laws give

$$\neg\forall x P(x) \equiv \exists x \neg P(x)$$
$$\neg\exists x P(x) \equiv \forall x \neg P(x)$$

Nested quantifiers are a series of quantifiers. n nested universal quantifiers quantify every combination of n values in the domains of the quantified variables. n nested existential quantifiers quantify at least one combination of n values in the domains of the quantified variables.

Self exclusion is expressed by nested quantifiers as

$$\exists x \forall y((x \neq y) \implies P(x, y))$$

Uniqueness is expressed by nested quantifiers as

$$\exists x \forall y(P(x) \wedge ((x \neq y) \implies \neg P(y)))$$

1.3 Arguments

An **argument** is a conditional

$$p_1 \wedge \cdots \wedge p_n \implies q$$

and can be expressed

$$\begin{array}{l} p_1 \\ \vdots \\ \underline{p_n} \\ \therefore q \end{array}$$

An argument is **valid** if it is a tautology. An argument is **invalid** if it is not a tautology. An argument is invalid if there is a set of values of its component

propositions for which it is false, called a **counterexample**. The **form** of a natural-language argument is its expression as a logical argument.

An **element** is a value in the domain of a variable. An **arbitrary element** is an element with only properties shared by all elements in the domain. A **particular element** is an element with properties including those shared by all elements in the domain.

Modus Ponens	p $p \implies q$ $\therefore q$
Modus Tollens	$\neg q$ $p \implies q$ $\therefore \neg p$
Addition	p $\therefore p \vee q$
Simplification	$p \wedge q$ $\therefore p$
Conjunction	p q $\therefore p \wedge q$
Hypothetical Syllogism	$p \implies q$ $q \implies r$ $\therefore p \implies r$
Disjunctive Syllogism	$p \vee q$ $\neg p$ $\therefore q$
Resolution	$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$
Universal Instantiation	c is an element $\forall x P(x)$ $\therefore P(c)$
Universal Generalization	c is an arbitrary element $P(c)$ $\therefore \forall x P(x)$
Existential Instantiation	$\exists x P(x)$ $\therefore (c$ is a particular element$) \wedge P(c)$
Existential Generalization	c is an element $P(c)$ $\therefore \exists x P(x)$

Table 4: Rules of Inference

2 Set Theory

2.1 Sets

A **set** S is an unordered collection of objects. An **element** $x \in S$ of a set is an object in the set. A **singleton** is a set of one element. **Roster notation** describes a set by its elements

$$S = \{x_1, \ldots, x_n\}$$

Set builder notation describes a set by the properties of its elements

$$S = \{x | P(x)\}$$

The **empty set**, or **null set**, $\emptyset$ is the set with no elements. A **finite set** is a set with a finite number of elements. An **infinite set** is a set with an infinite number of elements. The **cardinality** $|S|$ of a set is its number of distinct elements.

The **universal set** $\mathcal{U}$ on a domain is the set with all elements in the domain. A **Venn diagram** expresses sets as ellipses within the rectangular universal set.

Subset of a superset	$R \subseteq S \iff \forall x \in R(x \in S) \implies \lvert R\rvert \leq \lvert S\rvert$
Equality	$S = T \iff S \subseteq T \wedge T \subseteq S \implies \lvert S\rvert = \lvert T\rvert$
Proper subset Strict subset	$R \subset S \iff R \subseteq S \wedge S \nsubseteq R \implies \lvert R\rvert < \lvert S\rvert$
Power set	$\mathcal{P}(S) = \{R \mid R \subseteq S\} \implies \lvert\mathcal{P}(S)\rvert = 2^{\lvert S\rvert}$

Table 5: Set relationships

Intersection	$S \cap T = \{x \mid x \in S \wedge x \in T\}$
Union	$S \cup T = \{x \mid x \in S \vee x \in T\}$
Complement	$\bar{S} = S^{\complement} = \{x \mid x \notin S\}$
Set difference Relative complement	$S - T = S \setminus T = \{x \mid x \in S \wedge x \notin T\}$
Symmetric difference	$S \oplus T = \{x \mid (x \in S \wedge x \notin T) \vee (x \in T \wedge x \notin S)\}$

Table 6: Set operations

Two sets are **disjoint** if

$$S \cap T = \emptyset$$

Several sets are **pairwise disjoint**, or **mutually disjoint**, if every combination of two sets are disjoint. A **partition** of a set is one or more sets with the following properties:

1. Every set is a subset of the original set.
2. No set is the empty set.

3. The sets are pairwise disjoint.

4. The union of all the sets is equal to the original set.

Idempotent Laws	$A \cup A = A$ $A \cap A = A$
Associative Laws	$(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$
Commutative Laws	$A \cup B = B \cup A$ $A \cap B = B \cap A$
Distributive Laws	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Identity Laws	$A \cup \emptyset = A$ $A \cap U = A$
Domination Laws	$A \cap \emptyset = \emptyset$ $A \cup U = U$
Double Complement Law	$\bar{\bar{A}} = A$
Complement Laws	$A \cap \bar{A} = \emptyset$ $A \cup \bar{A} = U$ $\bar{U} = \emptyset$ $\bar{\emptyset} = U$
De Morgan's Laws	$\overline{A \cup B} = \bar{A} \cap \bar{B}$ $\overline{A \cap B} = \bar{A} \cup \bar{B}$
Absorption Laws	$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$

Table 7: Set identities

An **interval** is the subset of $\mathbb{R}$ between two endpoints. A **closed** interval

$$[a, b]$$

includes its endpoints. A **half-open** interval

$$[a, b)$$

$$(a, b]$$

includes exactly one of its endpoints. An **infinite**, or **open**, interval

$$(a, b)$$

does not include its endpoints. A subset A of $\mathbb{R}$ is **well ordered** if

$$\forall B \exists x \in B \forall y \in B (B \subseteq A \wedge B \neq \emptyset \implies x \leq y)$$

2.2 Ordered Tuples

An **ordered n-tuple** $S = (x_1, \ldots, x_n)$ is a set of n elements in which the order of elements is fixed. An **ordered pair** is an ordered 2-tuple. An **ordered triple** is an ordered 3-tuple. An **entry** is an element in an ordered n-tuple.

The **Cartesian product** of n sets is

$$S_1 \times \cdots \times S_n = \{(x_1, \ldots, x_n) : x_1 \in S_1 \wedge \cdots \wedge x_n \in S_n\}$$

with

$$|S_1 \times \cdots \times S_n| = |S_1| \cdots |S_n|$$

The **power** of a set is

$$S^k = \underbrace{S \times \cdots \times S}_{n \text{ times}}$$

A **string** is an ordered n-tuple of characters

$$s = (x_1, \ldots, x_n) = x_1 \cdots x_n$$

The **alphabet** of a set of strings is the set of distinct characters contained in any string. The **length** of a string is its cardinality. The **empty string** λ is the string of no characters. The **concatenation** of two strings is

$$st = s_1 \cdots s_n t_1 \cdots t_n$$

The **Kleene closure** of a string is

$$s^* = \lambda \cup s^1 \cup s^2 \cup \cdots$$

The **Kleene plus closure** of a string is

$$s^+ = s^1 \cup s^2 \cup \cdots$$

A **binary string** is a string of alphabet $\{0, 1\}$. A **bit** is a character in a binary string. An **n-bit string** is a binary string of length n. The **parity** of a binary string is the number of bits that are 1.

3 Relations

3.1 Binary Relations

A **binary relation** is a set

$$\mathcal{R} \subseteq A \times B$$

The first entry x in any element of a binary relation is **related** $x\mathcal{R}y$ to the second entry y. The **domain** is

$$\{a \in A : \exists b \in B((a,b) \in \mathcal{R})\}$$

and the **range** is

$$\{b \in B : \exists a \in A((a,b) \in \mathcal{R})\}$$

The **inverse** is

$$\mathcal{R}^{-1} = \{(b,a) \in B \times A : (a,b) \in \mathcal{R}\}$$

The **empty relation** $\emptyset$ is the relation that does not relate any elements to any elements. A **binary relation on a set** is a set

$$\mathcal{R} \subseteq A^2$$

An n**-ary relation** is a subset of the Cartesian product of n sets.

An **arrow diagram** represents a binary relation as arrows from elements in the domain to the elements that the first elements are related to. A **self-loop** is an arrow from an element to itself.

Reflexive	$\forall x \in A(x\mathcal{R}x)$
Anti-reflexive or irreflexive	$\forall x \in A\neg(x\mathcal{R}x)$
Symmetric	$\forall x \in A\forall y \in A(x\mathcal{R}y \iff y\mathcal{R}x)$
Anti-symmetric	$\forall x \in A\forall y \in A(x \neq y \implies \neg(x\mathcal{R}y) \vee \neg(y\mathcal{R}x))$
Transitive	$\forall x \in A\forall y \in A\forall z \in A(x\mathcal{R}y \wedge y\mathcal{R}z \implies x\mathcal{R}z)$

Table 8: Properties of binary relations

The **composition** of two binary relations is defined

$$(a,c) \in S \circ R \iff \exists b \in A(((a,b) \in R) \wedge ((b,c) \in S))$$

The **power** of a binary relation is

$$A^k = \underbrace{A \circ \cdots \circ A}_{k \text{ times}}$$

The **transitive closure** of a binary relation is

$$A^+ = A^1 \cup \cdots \cup A^{|A|}$$

The transitive closure can be found as follows:

1. Identify two elements of the relation where the second entry of the first element is the same as the first entry of the second element, and there is no element in the relation whose first entry is the first entry of the first element and whose second entry is the second entry of the second element.
2. Add the element to the relation whose first entry is the first entry of the first element and whose second entry is the second entry of the second element.
3. Repeat steps 1-2 until there are no two elements in the relation that satisfy step 1.

3.2 Binary Orders

A **partial order** $\preceq$ is a binary relation that is reflexive, anti-symmetric, and transitive. A **partially ordered set**, or **poset**, on a domain A is

$$(A, \preceq)$$

A **Hasse diagram** represents a partially ordered set as elements where a first element is below a second element if the first element is related to the second element, and there is a line between the first element and the second element if there is no element that the first element is related to and that is related to the second element.

A **strict order**, or **precedence relationship**, $\prec$ is a binary relation that is anti-reflexive and transitive (this implies that the relation is anti-symmetric). A **strictly ordered set** on a domain A is

$$(A, \prec)$$

A **minimal element** in an order is an element that no other elements are related to. A **maximal element** in an order is an element that is not related to any other element.

Two elements in an order are **comparable** if they are related to each other in either direction. Two elements in an order are **incomparable** if they are not related to each other in either direction. A **total order** is an order in which all elements are comparable.

An **equivalence relation** $\sim$ is a binary relation that is reflexive, symmetric, and transitive. An **equivalence class** of an equivalence relation on X is

$$[x] = \{y \in X : x \sim y\}$$

where x is a **representative**. Equivalence classes are pairwise disjoint. The **quotient of** X **by** $\sim$, or X **modulo** $\sim$,

$$X/\sim = \{[x] : x \in X\}$$

partitions X. A **canonical map** is a function

$$f : X \to X/\sim$$

3.3 Functions

A **function**, or **well-defined function** or **mapping** or **transformation**, is

$$f : X \to Y$$

where X is the **domain**, Y is the **codomain** or **target**. An element of the domain is related, or **mapped**, to an element of the codomain.

$$(x, y_1) \in f \wedge (x, y_2) \in f \implies y_1 = y_2$$

For $(x, y) \in f$, y is the **image** $f(x)$ of x. The **range** is

$$\{y | (x, y) \in f\}$$

We can also partly define f by the rule

$$f : x \mapsto y$$

The image of a set S is

$$f(S) = \{f(s) \in Y : s \in S\}$$

An **arrow diagram** represents a function as arrows from the first entry to the second entry of each element in the function, with a vertical list of elements in the domain on the left and a vertical list of elements in the codomain on the right.

A function is **one-to-one**, or **injective**, if

$$\forall x_1 \in X \forall x_2 \in X \forall y \in Y((x_1, y) \in f \wedge (x_2, y) \in f \implies x_1 = x_2)$$

Then

$$|X| \leq |Y|$$

A function is **onto**, or **surjective** or **corresponding**, if

$$\forall y \in Y \exists x \in X((x, y) \in f)$$

Then

$$|X| \geq |Y|$$

A function is **bijective**, or **one-to-one corresponding**, if it is one-to-one and onto. Then

$$|X| = |Y|$$

The inverse of a function f is a function if and only if f is a bijection. For $(y, x) \in f^{-1}$, x is the the **inverse image**, or **pre-image**, $f^{-1}(y)$ of y. The inverse image of a set S is

$$f^{-1}(S) = \{x \in X : f(x) \in S\}$$

Given a rule completely defining f, the rule completely defining f^{-1} can be found by converting the rule to an equation with y, solving for x, and converting the equation into a rule for y.

The **composition** of two functions is

$$g \circ f : x \mapsto g(f(x))$$

The **identity function** gives

$$I(x) = x$$

The composition of a bijection and its inverse, or vice versa, is the identity function. The **characteristic function** is the function that maps an indexed subset to the binary string where each bit is 1 if and only if the subset contains the corresponding element of the superset.

Strictly increasing	$\forall x_1 \forall x_2 (x_1 < x_2 \implies f(x_1) < f(x_2))$
Strictly decreasing	$\forall x_1 \forall x_2 (x_1 < x_2 \implies f(x_1) > f(x_2))$
Increasing or nondecreasing	$\forall x_1 \forall x_2 (x_1 \leq x_2 \implies f(x_1) \leq f(x_2))$
Decreasing or nonincreasing	$\forall x_1 \forall x_2 (x_1 \geq x_2 \implies f(x_1) \geq f(x_2))$

Table 9: Properties of functions

3.4 Cardinality

Cantor's definition of cardinality gives

$$|X| \leq |Y| \iff \exists f : X \to Y (f \text{ is injective})$$

$$|X| = |Y| \iff \exists g : X \to Y (g \text{ is bijective})$$

The **cardinal number** of a set describes its number of elements.

A set is **infinite**, or an **infinity**, if it has the same cardinality as a proper subset of itself. The **aleph numbers**

$$\{\aleph_0, \aleph_1, \dots, \}$$

are the cardinal numbers of the infinities in increasing order.

$$\aleph_0 = |\mathbb{N}|$$

The **continuum** is

$$\mathfrak{c} = |\mathbb{R}| > \aleph_0$$

A set is **finite** if

$$|S| < \aleph_0$$

The cardinal number of a finite set is in $\mathbb{N}_0$. A set is **countable** if

$$|S| \leq \aleph_0$$

A set is **countably infinite**, or **denumerable**, if

$$|S| = \aleph_0$$

A set is **uncountable** if

$$|S| > \aleph_0$$

The **Cantor-Schröder-Bernstein theorem** states

$$|S| \leq |T| \wedge |T| \leq |S| \implies |S| = |T|$$

Cantor's theorem states

$$|S| < |\mathcal{P}(S)|$$

It follows that there is no largest cardinality.

The **pigeonhole principle** states that a function with a domain of cardinality at least $n+1$ and a codomain of cardinality at most n cannot be one-to-one. The **generalized pigeonhole principle** states that a function with a domain of cardinality at least n and a codomain of cardinality k maps at least $\lceil \frac{n}{k} \rceil$ elements of the domain to at least 1 element of the codomain. The converse states that if a function maps from a domain of cardinality n to a codomain of cardinality k and maps at least b elements of the domain to at least 1 element of the codomain, then

$$n \geq k(b-1)+1$$

4 Sequences

4.1 Sequences

A **sequence** is a function over an **indexing** set, usually consecutive integers,

$$\{f_k\} = f_i, \ldots, f_n$$

whose input is an **index** and whose output is a **term**. The terms are **indexed**. A **finite sequence** has finitely many terms, an **initial index**, and a **final index**. An **infinite sequence** has infinitely many terms.

A sequence is

- **increasing** if $\forall k(a_k < a_{k+1})$,
- **nondecreasing** if $\forall k(a_k \leq a_{k+1})$,
- **decreasing** if $\forall k(a_k > a_{k+1})$, and
- **nonincreasing** if $\forall k(a_k \geq a_{k+1})$.

The terms of a sequence can be defined by an **explicit formula**. A **geometric sequence** has the explicit formula

$$s_k = s_0 r^k$$

where r is its **common ratio**. An **arithmetic sequence** has the explicit formula

$$t_n = t_0 + dn$$

where d is its **common difference**.

A **recurrence relation** is a sequence whose output depends on previous terms. A **dynamical system** is a system described by a recurrence relation. A **discrete time dynamical system** is a dynamical system described in terms of discrete time.

Summation notation gives

$$\sum_{i=s}^{t} a_i = a_s + \cdots + a_t$$

where i is the **index**, s is the **lower limit**, and t is the **upper limit**. The left expression is in **summation form** and the right expression is in **expanded form**. **Linearity** states

$$\sum_{i=s}^{t}(a_i + b) = \sum_{i=s}^{t} a_i + \sum_{i=s}^{t} b$$

$$\sum_{i=s}^{t} ca_i = c\sum_{i=s}^{t} a_i$$

where c is independent of i.

The **closed form** for the summation of the index is

$$\sum_{i=1}^{n} = \frac{(n+1)n}{2}$$

for an arithmetic sequence is

$$\sum_{k=0}^{n-1}(a+kd) = an + \frac{d(n-1)n}{2}$$

and for a geometric sequence is

$$\sum_{k=0}^{n-1} ar^k = \frac{a(r^n-1)}{r-1}$$

A sequence of sets $\{A_n\}$ over S has union

$$\bigcup_{i=a}^{b} A_i = \{x : \exists i \in S(a \leq i \wedge i \leq b \wedge x \in A_i)\}$$

and intersection

$$\bigcap_{i=1}^{b} A_i = \{x : \forall i \in S(a \leq i \wedge i \leq b \wedge x \in A_i)\}$$

where

$$\bigcup A_n = \bigcup_{i=s_1}^{s_n} A_i$$

and

$$\bigcap A_n = \bigcap_{i=s_1}^{s_n} A_i$$

It follows that for any term A_m,

$$A_m \subseteq \bigcup A_n$$

and

$$\bigcap A_n \subseteq A_m$$

A sequence of sets $\{A_n\}$ over a subset of $\mathbb{N}$ is **nested** if consecutive terms satisfy the same subset relation. If

$$A_n \subseteq A_{n-1} \subseteq \cdots$$

then

$$\bigcup A_n = A_1$$

and for a finite indexing set

$$\bigcap A_n = A_n$$

If

$$A_1 \subseteq A_2 \subseteq \cdots$$

then

$$\bigcap A_n = A_1$$

and for a finite indexing set

$$\bigcup A_n = A_n$$

4.2 Recurrence Relations

Recursion is the process of computing a function by its own output on smaller input. A **recursive definition** for a set is a **basis** of specific elements, a **recursive rule** that constructs elements from existing elements, and an **exclusion statement** that an element is in the set only if it is in the basis or can be constructed by the recursive rule.

A **recurrence relation** is a recursive definition for a sequence. The **solution** of a recurrence relation is a closed-form expression for the sequence. A **homogeneous** recurrence relation describes a term as a combination of only previous terms. A **linear homogeneous** recurrence relation is

$$f_n = c_1 f_{n-1} + \cdots + c_k f_{n-k}$$

where $c_k \neq 0$ and the degree is k. The **characteristic equation** of a linear homogeneous recurrence relation is

$$x^n = c_1 x^{n-1} + \cdots + c_k x^{n-k}$$
$$p(x) = x^k - c_1 x^{k-1} - \cdots - c_k = 0$$

Solutions to the characteristic equation are solutions to the recurrence relation. If the characteristic equation has a root x with multiplicity m, then the recurrence relation has solutions

$$f_n = x^n, \ldots, f_n = n^{m-1} x^n$$

The **general solution** to a linear homogeneous recurrence relation is

$$f_n = t_1 x_1^n + \cdots + t_k x_k^n$$

where $t_1, \ldots, t_k$ are parameters and $x_1, \ldots, x_n$ are solutions to the recurrence relation.

Substituting initial values gives a linear system whose solution gives the values of the parameters for the solution. It follows that a solution requires as many initial values as the degree of the recurrence relation.

A **non-homogeneous linear recurrence relation** is a linear recurrence relation that contains terms that are constant or a function of n. The **associated homogeneous recurrence relation** is the recurrence relation without the non-homogeneous terms.

The **homogeneous solution** $f_n^{(h)}$ is the general solution to the associated homogeneous recurrence relation. A **particular solution** $f_n^{(p)}$ can be guessed and verified by substitution into the recurrence relation. If the non-homogeneous terms are

$$p(n)s^n$$

where $p(n)$ is a polynomial of degree t and s is a constant, then

- if s is not a root of the characteristic equation for the associated homogeneous recurrence relation,

$$f_n^{(p)} = (d_t n^t + \cdots + d_1 n + d_0)s^n$$

- if s is a root of the characteristic equation for the associated homogeneous recurrence relation of multiplicity m,

$$f_n^{(p)} = n^m(d_t n^t + \cdots + d_1 n + d_0)s^n$$

where $d_0, \ldots, d_t$ are constants. The general solution to a non-homogeneous linear recurrence relation is

$$f_n = f_n^{(h)} + f_n^{(p)}$$

5 Number Theory

5.1 Modular Arithmetic

Number theory is the study of integers. A nonzero integer x **divides** another integer y, or x is a factor of y or y is **divisible** by x or y is a **multiple** of x,

$$x \mid y \iff \exists k \in \mathbb{Z}(y = kx)$$

and otherwise x does not divide y

$$x \nmid y \iff \forall k \in \mathbb{Z}(y \neq kx)$$

A **linear combination** of terms $x_1, \ldots, x_n$ is

$$c_1 x_1 + \cdots + c_n x_n$$

where $c_1, \ldots, c_n$ are constants.

$$x \mid y_1 \wedge \cdots \wedge x \mid y_n \implies x \mid (c_1 y_1 + \cdots + c_n y_n)$$

Integer division, or **Euclidean division**, expresses the division of two integers as an integer **quotient** and an integer **remainder**, or **modulus**. The **Division Algorithm** states

$$\begin{aligned}\forall n \in \mathbb{Z} \forall d \in \mathbb{Z}^+ \exists q \in \mathbb{Z} \exists r \in \mathbb{Z} \forall s \in \mathbb{Z} \forall t \in \mathbb{Z} \\ ((0 \leq r \leq d-1 \implies n = qd + r) \\ \wedge (0 \leq t \leq d-1 \wedge (q \neq s \vee r \neq t) \implies n \neq sd + t))\end{aligned}$$

Then

$$\begin{aligned} q &= n \quad \text{div } d \\ r &= n \quad \text{mod } d \end{aligned}$$

where div is the integer division operator and mod is the **modulo** operator, both of which have the same precedence as multiplication. Note the difference between the division operation and traditional division in the case of a negative quotient.

Modular arithmetic is the modulo on arithmetic operations. **Addition modulo** m and **multiplication modulo** m are defined on a set as

$$x \mod m$$

where m is an integer and x is the sum or product, respectively, of two elements.

$$\begin{aligned} ((x \mod m) + (y \mod m)) \mod m &= (x + y) \mod m \\ ((x \mod m)(y \mod m)) \mod m &= (xy) \mod m \end{aligned}$$

where $m > 1$.

A **ring** is

$$\mathbb{Z}_m = \mathbb{Z}/\sim_m$$

where

$$\begin{aligned} \sim_m &= \{(x, y) : x \equiv y \mod m\} \\ [x] +_m [y] &= [x + y] \\ [x] \cdot_m [y] &= [xy] \end{aligned}$$

A **field** is a nonzero ring in which every element has a multiplicative inverse. For a field, m is prime.

Equality modulo m, or **congruence modulo** m, is defined such that x is **congruent** to $y \mod m$

$$x \equiv y \pmod{m} \iff x \mod m = y \mod m$$

where $m > 0$ and

$$x \equiv y \pmod{m} \iff m \mid (x - y)$$

where $m > 1$.

$$x \equiv y \pmod{m} \implies \frac{x}{n} \equiv \frac{y}{n} \pmod{\frac{m}{n}}$$

where n divides x, y, m.

A **pseudo-random number generator** outputs deterministic numbers with relevant statistical properties of random numbers. The **linear congruential generator** is

$$\begin{cases} X_0 \\ X_{n+1} = (aX_n + c) \mod m \quad n \geq 0 \end{cases}$$

where m is the range and a, c are constants chosen for efficiency and utility.

5.2 Factorization

An integer n greater than 1 is **prime** if

$$\forall x \in \mathbb{Z}(x > 1 \wedge x \neq n \implies x \nmid n)$$

and **composite** if

$$\exists m \in \mathbb{Z}(1 < m < n \wedge m \mid n)$$

The **fundamental theorem of arithmetic** states that every prime or composite number can be expressed as its **prime factorization**, a unique product of prime numbers in nondecreasing order. It follows that the prime factorization of a prime number contains one factor and that the prime factorization of a composite number contains more than one factor. The **multiplicity** of a factor in a prime factorization is the number of times the factor appears in the factorization. Factors can be expressed in exponential notation by their multiplicities.

The **greatest common divisor** $\gcd(x, y)$ of integers x and y that are not both zero is the largest positive integer that is a factor of both x and y. The **least common multiple** $\operatorname{lcm}(x, y)$ of nonzero integers x and y is the smallest positive integer that is a multiple of both x and y. Positive integers x and y are **relatively prime**, or **mutually prime** or **coprime**, if

$$\gcd(x, y) = 1$$

If

$$x = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$
$$y = p_1^{\beta_1} \cdots p_r^{\beta_r}$$

where $p_1, \ldots, p_r$ are the distinct prime factors of x or y with nonnegative integer multiplicities $\alpha_1, \ldots, \alpha_r$ in x and $\beta_1, \ldots, \beta_r$ in y, then

$$x \mid y \iff \forall i \in \mathbb{Z}(1 \leq i \leq r \implies \alpha_i \leq \beta_i)$$

and

$$\gcd(x, y) = p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_r^{\min\{\alpha_r, \beta_r\}}$$
$$\operatorname{lcm}(x, y) = p_1^{\max\{\alpha_1, \beta_1\}} \cdots p_r^{\max\{\alpha_r, \beta_r\}}$$

Multiplicative inverse modulo n has output $s \in \{1, \ldots, n-1\}$ where

$$sx \mod n = 1$$

x has an inverse modulo n if and only if x and n are relatively prime.

The **primality** of an integer greater than 1 is its property of prime or composite. A composite number N has a factor greater than 1 and at most $\sqrt{N}$. A brute force primality algorithm must check whether each integer at most $\sqrt{N}$ is a factor of N and thus has time complexity $\Theta(N)$.

There are an infinite number of prime numbers. The **Prime Number Theorem** states

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$$

where $\pi(x)$ is the number of prime numbers in $\{2, \ldots, x\}$.

$$\ln x \approx 2.3d$$

where d is the number of digits in x. It follows that a primality algorithm for N based on random selection has time complexity $\Theta(n)$ where n is the number of digits in N.

Euclid's algorithm calculates $\gcd(x, y)$ by applying

$$\forall x \in \mathbb{Z}^+ \forall y \in \mathbb{Z}^+ (\gcd(x, y) = \gcd(x, y \mod x))$$

repeatedly with $x < y$ in each iteration until $y \mod x = 0$. A **Diophantine equation** has integer coefficients and solutions. **Bézout's identity** states that

$$\gcd(x, y) = sx + ty$$

is Diophantine. It follows that

$$\gcd(a, b) = 1 \wedge a \mid bc \implies a \mid c$$

The **extended Euclidean algorithm** finds s, t in Bézout's Identity by expressing $r = y \mod x = y - (y \operatorname{div} x)x$ for each iteration and substituting the expressions $r = y - dx$ forward into the penultimate expression in reverse order until the initial case.

$$\begin{aligned}
\gcd(x_1, y_1) = r_{n-1} &= y_{n-1} - d_{n-1}x_{n-1} \\
&= y_{n-1} - d_{n-1}r_{n-2} \\
&\vdots \\
&= y_{n-1} - d_{n-1}(y_{n-2} - d_{n-2}(\cdots(y_1 - d_1x_1)\cdots)) \\
&= (1 + d_2 \cdots d_{n-1})y_1 \\
&\quad - (d_1 + (-1)^{n-1}d_1 \cdots d_{n-1} + (-1)^n d_3 \cdots d_{n-1})x_1
\end{aligned}$$

If x has an inverse modulus n, then the Extended Euclidean Algorithm finds integers s, t such that $1 = sx + tn$. Then $(s \mod n)x \mod n = 1$. In fact, if $c = ax + bn$ and $\gcd(x, n) = d \mid c$, then

$$\begin{cases} a = s - \frac{x}{d}k \\ b = t - \frac{y}{d}k \end{cases}$$

for some integer k.

The exponentiation $x^y \mod n$ can be found by expressing y as a sum of powers of 2 up to 2^p. Then find $x^{2^i} \mod n$ for each $i \leq p$ sequentially by squaring the last result and taking the modulus. Then calculate x as a product of the moduli of the exponentiations to the relevant powers of 2 and calculate the final result.

An iterative algorithm for computing x^y has $p = 1, s = x, r = y$ initially and loops while $r > 0$, replacing p with ps if $r \mod 2 = 1$, s with s^2, and r with $r \operatorname{div} 2$. The algorithm iterates the number of bits in the binary expansion of y times, and thus has time complexity $O(\log y)$. An algorithm for $x^y \mod n$ instead replaces p with $ps \mod n$ and s with $s^2 \mod n$.

5.3 Base

For a **base** b greater than 1, every positive integer n has a unique **base** b **expansion of** n

$$n = a_k b^k + \cdots + a_0 b^0 = (a_k \cdots a_0)_b$$

where $a_k, \ldots, a_0$ are the **digits** of the integer in $\{0, \ldots, b-1\}$, $a_k \neq 0$, and k is nonnegative.

Decimal notation represents integers with base 10. **Binary** notation represents integers with base 2 where the digits are **bits** and 8 bits are a **byte**. **Hexadecimal**, or **hex**, notation represents integers with base 16 where the digits are the ten Arabic numerals and the first six Latin script letters.

An integer of base b can be converted to a decimal integer n by its base expansion, which also gives

$$n = (((a_k)b + a_{k-1})b \cdots)b + a_0$$

An decimal integer n can be converted to base b by appending $n \mod b$ to the base b expansion of $n \operatorname{div} b$. The number of digits required for the base b expansion of a positive decimal integer n is

$$k + 1 \geq \lceil \log_b(n+1) \rceil$$

If for bases b and b'

$$b' = b^m$$

for some integer m, then each m digits of the base b representation convert to 1 digit of the base b' representation from the right, with necessary leading zeros.

6 Combinatorics

6.1 Combinatorial Rules

The **product rule** states

$$|S_1 \times \cdots \times S_n| = |S_1| \cdots |S_n|$$

where $S_1, \ldots, S_n$ are finite sets. The **generalized product rule** states that in a set S of all possible sequences of k items, if there are n_1 choices for the first item and n_k choices for the kth item for every possible choice for the first $k-1$ items, then

$$|S| = n_1 \cdots n_k$$

The **principle of inclusion-exclusion** states

$$\begin{aligned} |S_1 \cup \cdots \cup S_n| = &\sum_{j=1}^{n} |S_j| \\ &- \sum_{j=1}^{n} \sum_{k=1}^{j-1} |S_j \cap S_k| - \sum_{j=1}^{n} \sum_{k=j+1}^{n} |S_j \cap S_k| \\ &+ \cdots \\ &+ (-1)^{n+1} |S_1 \cap \cdots \cap S_n| \end{aligned}$$

where $S_1, \ldots, S_n$ are finite sets. The principle of inclusion-exclusion on pairwise disjoint sets gives the **sum rule**:

$$|S_1 \cup \cdots \cup S_n| = |S_1| + \cdots + |S_n|$$

The **bijection rule** states

$$|S| = |T|$$

where S, T are finite sets and there is a bijection

$$f : S \to T$$

A function is k**-to-one** if it maps exactly k elements of the domain X to each element of the codomain Y. Then the k**-to-one rule** states

$$|Y| = \frac{|X|}{k}$$

6.2 Combinations and Permutations

An r**-permutation** is a sequence of r unique elements of a set. The number of r-permutations of a set of n elements is

$$P(n, r) = \frac{n!}{(n-r)!} = n(n-1) \cdots (n-r+1)$$

Then a **permutation** is an n-permutation. A **permutation with repetition** is a sequence of possibly nonunique elements of a set. The number of permutations with repetition of a set of n elements is

$$\frac{n!}{n_1! \cdots n_k!}$$

where n_i is the number of repetitions of the ith element of the set and

$$n = n_1 + \cdots + n_k$$

An **r-subset**, or **r-combination**, is a subset of r elements. The number of r-combinations of a set of n elements is

$$C(n, r) = \binom{n}{r} = \binom{n}{n-r} = \frac{n!}{r!(n-r)!}$$

The **principle of counting by complement** states

$$|P| = |S| - |\bar{P}|$$

where P is the subset of S containing the elements to be counted.

A **multiset** is a collection of possibly nonunique elements. Two multisets are equal if they have the same number of each element. The number of ways to select n total of m different kinds of elements, or n elements into m different categories, is

$$\binom{n+m-1}{m-1}$$

Elements in a set are **indistinguishable** if they are identical, and are otherwise **distinguishable**.

Elements	No restrictions	At most one per category	Same number per category
Indistinguishable	$\binom{n+m-1}{m-1}$	$\binom{m}{n}$	1
Distinguishable	m^n	$P(m, n)$	$\frac{n!}{((\frac{n}{m})!)^m}$

Table 10: Common assignment problems

Binomial coefficients are the coefficients of the expansion of a positive power of a binomial. The **binomial theorem** states

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

where n is a nonnegative integer and a and b are real numbers. It follows that

$$2^n = \sum_{k=0}^{n} \binom{n}{k}$$

and

$$0 = \sum_{k=0}^{n} (-1)^k \binom{n}{k}$$

and from there that

$$\sum_{k=0}^{\frac{n}{2}} \binom{n}{2k} = \sum_{k=0}^{\frac{n}{2}-1} \binom{n}{2k+1}$$

for even n, and

$$\sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k} = \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k+1}$$

for odd n.

Pascal's triangle is a triangular chart where the nth row lists the $n+1$ binomial coefficients $\binom{n}{n-1}, \ldots, \binom{n}{n}$. The 0th and nth coefficients evaluate to 1. The other kth coefficients evaluate by **Pascal's identity**

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

The coefficients of the nth row sum to 2^n.

Lexicographical order orders n-tuples by the first entry by which they differ. To find the next-highest permutation of a set, take the current permutation, find the rightmost entry n_i such that $n_i < n_{i+1}$, swap n_i with the next-highest entry of those to its right, and sort the entries to the right of the former position of n_i. The first permutation is the completely sorted permutation. The last permutation is completely reverse sorted permutation.

Combinations are ordered as sorted n-tuples. To find the next-highest r-combination of a set $\{n_1, \ldots, n_n\}$, take the current r-combination, find the rightmost entry r_i such that $r_i < n_{n-r+i}$, increment r_i, and replace the entries to the right of r_i with the sorted smallest same number of entries that are all greater than r_i. The first r-combination is the set of the first r elements. The last r-combination is the set of the last r elements.

A **generating function** of a sequence $\{f_n\}$ is

$$F(x) = \sum_{i=0}^{\infty} f_i x^i$$

Some generating functions have closed forms that can be found by algebra. Terms of a generating function can represent the number of combinations of the term index size of a set. The product of two generating functions gives the number of combinations of the union of their distinct represented sets.

Infinite indistinguishable elements	$1 + x + x^2 + \cdots = \frac{1}{1-x}$
Finite indistinguishable elements	$1 + x + \cdots + x^n = \frac{1-x^{n+1}}{1-x}$
Infinite groups of k elements	$1 + x^k + x^{2k} + \cdots = \frac{1}{1-x^k}$
2 infinite indistinguishable elements	$1 + 2x + 3x^2 + \cdots = \frac{1}{(1-x)^2}$

Table 11: Generating Functions of Combinations

A Proofs

A **theorem** is a statement that can be logically proven. An **identity** is a theorem that states mathematical equality. A **corollary** is a theorem that follows from another theorem. A **conjecture** is a statement that is unproven. A **proof** is a logical series of justified steps that proves a theorem. A **lemma** is a theorem that exists only to prove another theorem. An **axiom** is a statement that is assumed true. Common axioms are

- Rules of algebra
- Closure of integers under addition and multiplication
- Parity of integers
- Discretion of integers
- Relative order of real numbers
- Positivity of squares of real numbers

The start of a proof should be clearly denoted by the word "Proof". A proof consists of natural-language sentences with integrated mathematics. A proof should provide a roadmap of what is assumed, what will be proved, and what has been proven. Variables and equation blocks should be introduced by natural language. The amount of detail provided in a proof should depend on the experience of the target audience. The end of a proof should be clearly denoted by the acronym "QED" or the tombstone character. Some common keywords in proofs are

- thus/therefore/it follows that/then/hence: connect to the previous few statements
- let/suppose: introduce a new variable
- suppose: introduce a new assumption
- since/because we know that: remind the reader of an earlier statement
- we will prove/we will show: indicate where the proof is going
- by definition: prove a statement from a definition

- by assumption: prove a statement from an assumption
- in other words: rephrase or specify a statement
- gives/yields: connect to the previous equality or inequality
- without loss of generality: apply proof for one case to other cases

A **direct proof** assumes the hypothesis of a theorem and proves its conclusion. A **proof by contrapositive** assumes the negation of the conclusion of a theorem and proves the negation of its hypothesis. A **proof by contradiction** disproves the negation of a theorem. A **proof by cases** proves a theorem for each class of its domain. A **case** is the proof for a single class.

A **proof by exhaustion** proves a theorem for every element in its domain. A **proof by universal generalization** proves a theorem for an arbitrary element in its domain. An **existence proof** proves an existential statement. A **constructive proof of existence** proves an existential statement for a particular element in the domain. A **nonconstructive proof of existence** disproves the negation of an existential statement.

A **base case** is the initial term of a sequence of statements. The **inductive hypothesis**, or **inductive assumption**, is the statement that the term directly preceding another term is true. The **inductive step** is the statement that a term is true if the inductive hypothesis is true.

The **principle of mathematical induction** states that if the base case and the inductive step are true, then all statements in a sequence are true. The **principle of strong induction** describes induction where there may be several statements in the base case and where the inductive hypothesis states that all terms preceding another term are true. **Structural induction** is the process of proving a property of a recursively defined set using its recursive definition.

The **well-ordering principle**, or **least natural number principle**, states that the natural numbers are well ordered. The well-ordering principle implies the principle of mathematical induction. A proof by induction may also be proved by contradiction by considering a **minimal counterexample**, the minimum element of the set of counterexamples.

A **combinatorial proof** uses combinatorics and the bijection rule. A combinatorial proof of identity usually counts by alternate methods to find equivalent expressions.

B Mathematical Definitions

The **natural numbers** are the numbers used for counting:

$$\mathbb{N} = \{0, 1, \ldots\}$$

The **integers** are the natural numbers and their negatives:

$$\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$$

The **rational numbers** are the quotients of integers where the denominator is nonzero:

$$\mathbb{Q} = \left\{ \frac{p}{q} | p \in \mathbb{Z} \wedge q \in \mathbb{Z} \wedge q \neq 0 \right\}$$

The **real numbers** are all numbers including and between integers:

$$\mathbb{R}$$

The **irrational numbers** are the real numbers which are not rational numbers:

$$\mathbb{R} \setminus \mathbb{Q}$$

The **complex numbers** are the sums of real numbers and scalar multiples of $\mathrm{i} = \sqrt{-1}$:

$$\mathbb{C} = \{x + y\mathrm{i} : x \in \mathbb{R} \wedge y \in \mathbb{R}\}$$

The **algebraic numbers** are the solutions to integer-coefficient polynomials:

$$\mathbb{A} = \{x \in \mathbb{C} : \exists p = c_0 x^0 + \cdots + c_n x^n = 0\}$$

The **transcendental numbers** are the complex numbers which are not algebraic numbers:

$$\mathbb{C} \setminus \mathbb{A}$$

The **scalar multiple** of a set of numbers is the set that contains only the multiples of the scalar.

A number is **at least** another number if and only if

$$x = c \vee x > c$$

and **at most** another number if and only if

$$x = c \vee x < c$$

Positive numbers are those greater than zero. **Negative numbers** are those less than zero. **Nonnegative numbers** are those at least zero. **Nonpositive numbers** are those at most zero.

An integer x is **even** if

$$\exists k \in \mathbb{Z}(x = 2k)$$

and **odd** if

$$\exists k \in \mathbb{Z}(x = 2k + 1)$$

The **parity** of an integer is its property of even or odd.

An integer n is the **perfect square** if

$$\exists k \in \mathbb{Z}(n = k^2)$$

Two integers x, y are **consecutive** if

$$x = 1 + y \vee y = 1 + x$$

Two numbers x, y are **distinct** if

$$x \neq y$$

The **factorial** of an integer is

$$n! = \begin{cases} 1 & n = 0 \\ n(n-1)! & n \geq 1 \end{cases}$$

The **floor function** $\lfloor x \rfloor$ maps a real number x to the integer that is closest to it on the negative side. The **ceiling function** $\lceil x \rceil$ maps a real number x to the integer that is closest to it on the positive side. The **absolute value function** gives

$$|x| = \begin{cases} -x & x < 0 \\ x & x \geq 0 \end{cases}$$

The **exponential function** gives

$$b^x = \underbrace{b \cdot b}_{x \text{ times}}$$

where b is the **base** and x is the **exponent**. The properties of exponents are

1. $b^x b^y = b^{x+y}$
2. $(b^x)^y = b^{xy}$
3. $\frac{b^x}{b^y} = b^{x-y}$
4. $(bc)^x = b^x c^x$

The **logarithm function** is the inverse of the exponential function. The properties of logarithms are

1. $\log_b(xy) = \log_b x + \log_b y$
2. $\log_b \left(\frac{x}{y}\right) = \log_b x - \log_b y$
3. $\log_b(x^y) = y \log_b x$
4. $\log_c x = \frac{\log_b x}{\log_b c}, c \neq 1$

The solution to the Fibonacci sequence

$$\begin{cases} f_0 = 0 \\ f_1 = 1 \\ f_n = f_{n-1} + f_{n-2} & n \geq 2 \end{cases}$$

is

$$f_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n \quad n \geq 0$$

The **golden ratio**

$$\phi = \frac{1+\sqrt{5}}{2}$$

describes many natural and artificial proportions.

The **arithmetic mean** of n numbers $x_1, \ldots, x_n$ is

$$\frac{x_1 + \cdots + x_n}{n}$$

and the **geometric mean** where $x_1, \ldots, x_n$ are nonnegative is

$$\sqrt[n]{x_1 \cdots x_n}$$

The **AM-GM Inequality** states

$$\frac{x_1 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 \cdots x_n}$$

$$\frac{x_1 + \cdots + x_n}{n} = \sqrt[n]{x_1 \cdots x_n} \iff x_1 = \cdots = x_n$$