1 Sets

1.1 Definitions and Notations

Set: A collection of objects, called *elements*.

- **Notation**: Sets are represented by uppercase letters; elements by lowercase letters.
- Example: If a is in set A, we write $a \in A$. If not, $a \notin A$.

Subset: A set B is a subset of A if every element in B is also in A.

- **Notation**: $B \subseteq A$.
- **Extensionality Principle**: Two sets are equal if they contain the same elements.
- Equality: $A = B$ if $A \subseteq B$ and $B \subseteq A$.

Set Representation:

- **Listing Elements**: $\{a_1, a_2, \ldots, a_n\}$.
- **Describing by Properties**: $\{x \mid x \text{ satisfies } P\}$.

1.2 Set Operations

- **Union** ($A \cup B$): Elements in A or B.
- **Intersection** ($A \cap B$): Elements in both A and B.
- **Difference** ($A \setminus B$): Elements in A but not in B.
- **Symmetric Difference** ($A \Delta B$): Elements in either A or B, but not in both.

Properties of Set Operations:

- **Associative**: $(A \cup B) \cup C = A \cup (B \cup C)$
- **Commutative**: $A \cup B = B \cup A$
- **Distributive**: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

1.3 Important Set Types

- **Empty Set** ($\emptyset$): The unique set with no elements.
- **Singleton**: A set with only one element.
- **Universal Set** (V): The fixed larger set within which all sets are considered.
- **Complement**: For a set A in the universal set V, the complement $\overline{A} = V \setminus A$.

Complement Properties:

- **Identity**: $A \cup \emptyset = A$, $A \cap V = A$.
- **Double Complement**: $\overline{(\overline{A})} = A$.
- **De Morgan's Laws**:
  - $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
  - $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

1.4 Families of Sets

Definition: A collection of sets, often denoted as $\mathcal{A}, \mathcal{B}$, etc.

- **Union of Families**: $\bigcup \mathcal{A} = \{x \mid \exists A \in \mathcal{A} : x \in A\}$.
- **Intersection of Families**: $\bigcap \mathcal{A} = \{x \mid \forall A \in \mathcal{A} : x \in A\}$.

1.5 Power Set

Definition: The set of all subsets of a set A, including $\emptyset$ and A itself.

- **Notation**: 2^A or $\mathcal{P}(A)$.
- **Example**: For $A = \{0, 1\}$, $\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.

1.6 Cartesian Product

Definition: An ordered pair where order matters, denoted as (a, b).

- For sets $A_1, \ldots, A_n$, the **Cartesian product** is $A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) \mid a_i \in A_i\}$.
- **Example**: If $A = \{1, 2\}$ and $B = \{x, y\}$, $A \times B = \{(1, x), (1, y), (2, x), (2, y)\}$.

2 Relations and Functions

2.1 Relations and Functions

Relation

Definition: A relation between two sets A and B is a subset of their Cartesian product $A \times B$. Denoted as $R \subseteq A \times B$.

- **Notation**: If $(a, b) \in R$, write it as aRb.
- **Example**: A relation from the set of integers to the set of natural numbers.

Domain and Range:

- **Domain**: Set of all elements in A that relate to some element in B.
- **Range**: Set of all elements in B related to at least one element in A.

Inverse Relation:

- **Definition**: For a relation $R \subseteq A \times B$, its inverse is $R^{-1} \subseteq B \times A$.

Equipotent Relation:

- **Definition**: A relation $R \subseteq A \times B$ is equipotent if there exists a bijection between A and B.

Properties of Relations

- **Reflexive**: aRa for all $a \in A$.
- **Symmetric**: aRb implies bRa.
- **Transitive**: aRb and bRc imply aRc.
- **Antisymmetric**: aRb and bRa imply $a = b$.
- **Compositional Relations**: If $R \subseteq A \times B$ and $S \subseteq B \times C$, then the composition is $S \circ R \subseteq A \times C$.

Functions

Definition: A relation $F \subseteq A \times B$ is a function if for all $a \in A$, there exists a unique $b \in B$.

- **Injective (One-to-one)**: $F(a) = F(a')$ implies $a = a'$.
- **Surjective (Onto)**: For every $b \in B$, there is some $a \in A$ such that $F(a) = b$.
- **Bijective**: Both injective and surjective.

2.2 Equivalence Relations

Definition

A relation $R \subseteq A \times A$ is an **equivalence relation** if it is:

- **Reflexive**: xRx for all $x \in A$.
- **Symmetric**: xRy implies yRx.
- **Transitive**: xRy and yRz imply xRz.

Equivalence Class: The set of all elements in A that are equivalent to a. Defined as $[a] = \{b \in A \mid a \sim b\}$.

Quotient Set: The set of all equivalence classes. Defined as $A/\sim = \{[a] \mid a \in A\}$.

Properties of Equivalence Relations:

- $\forall a \in A : a \in [a]$.
- $\forall a \in A : [a] \neq \emptyset$ and $\bigcup\limits_{a \in A} [a] = A$.
- $\forall a, b \in A : [a] = [b] \iff a \sim b$.
- $\forall a, b \in A : [a] \cap [b] = \emptyset$ if $[a] \neq [b]$.

Partitioning

A partition $\mathscr{A} \subseteq 2^A$ is a partition of A if:

- $\forall X \in \mathscr{A} : X \neq \emptyset$.
- $\forall X, Y \in \mathscr{A} : X \cap Y = \emptyset$ if $X \neq Y$.
- $\bigcup_{X \in \mathscr{A}} X = A$.

2.3 Partial and Total Orderings

Partial Order

- **Definition**: A partial order is a relation $R \subseteq A \times A$ that is **reflexive**, **transitive**, and **antisymmetric**.
- **Example**: $\leq$ on the set of real numbers.

Key Terms:

- **Majorant**: $m \in A$ is a majorant of $X \subseteq A$ if $\forall x \in X : x \leq m$.
- **Minorant**: $m \in A$ is a minorant of $X \subseteq A$ if $\forall x \in X : x \geq m$.
- **Supremum**: The least upper bound of a set $X \subseteq A$.
- **Infimum**: The greatest lower bound of a set $X \subseteq A$.

Total Order

Definition: A total order requires that for each pair of elements $x, y \in A$, either xRy or yRx.

Hasse Diagrams

Definition: A Hasse diagram is a simplified graph representing a finite poset, showing the partial order without reflexive, transitive, or redundant relations.

Construction Steps: 1. **Start with a Poset**: Identify the set A and the partial order R. 2. **Simplify Relations**: Remove reflexive and transitive edges. 3. **Arrange Vertically**: Position elements so aRb implies a is below b. 4. **Draw Edges**: Connect elements with direct relations.

Example: For $A = \{1, 2, 3, 4\}$ with R defined by divisibility: - $1 \mid 2, 1 \mid 3, 1 \mid 4, 2 \mid 4$. - The diagram shows $1 \to 2 \to 4$ and $1 \to 3$.

Key Features: - Highlights immediate relations. - Simplifies hierarchy visualization. - Useful for subsets, divisibility, and dependency graphs.

3 Proof Techniques

Definition of a Proof

Definition 3.1 (Informal Definition): A proof of a mathematical statement is a sequence of valid arguments demonstrating its truth. These arguments must be sufficiently detailed to convince the intended audience.

Trivial Proof

Definition: A proof requiring no further work. This might arise if the statement follows directly from the given information or from the principle: *Anything follows from a falsehood.*

- If $P \implies Q$ and P is false, Q is true.

Examples:

- If $x^2 + 1 = 0$, then $x^4 = 0$.
- Every human with five heads is a genius.
- If $n > 0$ and n is even, then $n > 0$.

Direct Proof

Method: To prove a statement S_n, find a sequence $S_1, S_2, \ldots, S_{n-1}, S_n$ where each S_k follows logically from the preceding statements and known hypotheses. **Example 3.3:** If n is composite, it has at least one prime factor p such that $p \leq \sqrt{n}$.

Proof. Since n is composite, there exist integers $a, b > 1$ such that $n = ab$. Assume $a \leq b$. Then $n = ab \geq a^2$, so $a \leq \sqrt{n}$. If a is prime, we are done. Otherwise, a has a prime divisor p such that $p \leq a \leq \sqrt{n}$. □

Proof by Contraposition

Method: To prove $P \implies Q$, prove its contrapositive $\neg Q \implies \neg P$. **Example 3.4:** If $p > 1$ is an integer with no divisor d such that $1 < d \leq \sqrt{p}$, then p is prime.

Proof. This is the contrapositive of Example 3.3 and was proven earlier. □

Proof by Contradiction

Method: Assume the negation of the statement to be proven. If this assumption leads to a contradiction, the original statement is true. **Example 3.5:** $\sqrt{2}$ is irrational.

Proof. Assume $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{a}{b}$ with integers a, b (where $\gcd(a, b) = 1$). Squaring both sides gives $2b^2 = a^2$, so a^2 is even. This implies a is even, say $a = 2c$. Substituting gives $2b^2 = 4c^2 \implies b^2 = 2c^2$, so b^2 is even, and hence b is even. This contradicts $\gcd(a, b) = 1$. □

Proof by Cases

Method: Divide the statement into exhaustive cases and prove each separately. **Example 3.6:** For all integers n, $n^3 - n$ is divisible by 2.

Proof.

- If n is even, $n = 2k$ for some integer k. Then $n^3 - n = 2k(4k^2 - 1)$, which is even.
- If n is odd, $n = 2k+1$. Then $n^3 - n = 2(4k^3 + 6k^2 + 2k)$, which is even.

□

Proof by Induction

Principle: To prove $P(n)$ for all $n \geq n_0$:

- Base Case: Prove $P(n_0)$.
- Inductive Step: Assume $P(k)$ is true (induction hypothesis). Prove $P(k+1)$.

Example 3.9: The sum of the first n positive integers is $\frac{n(n+1)}{2}$.

Proof. Base Case: For $n = 1$, $1 = \frac{1(1+1)}{2}$. Inductive Step: Assume $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$. Then

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

□

4 Counting

4.1 Basic Techniques

Sum Rule

Property 4.1 (Sum Rule): If there are $n(A)$ ways to perform A and $n(B)$ ways to perform B, then the total number of ways to perform A **or** B is $n(A) + n(B)$. This extends to multiple events:

- $n(A) + n(B) + n(C)$ ways to perform A, B, or C, etc.

Product Rule

Property 4.2 (Product Rule): If there are $n(A)$ ways to perform A and $n(B)$ ways to perform B, and these are independent, the total number of ways to perform A **and** B is $n(A) \cdot n(B)$. This generalizes as:

- $n(A) \cdot n(B) \cdot n(C)$ ways to perform A, B, and C, etc.

Division Rule

Property 4.3 (Division Rule): If there is a k-to-1 correspondence between objects of type A and type B, and there are $n(A)$ objects of type A, then there are $n(B) = \frac{n(A)}{k}$ objects of type B.

4.2 Inclusion-Exclusion Principle

Example 4.4: In a class, 20 students have a driver's license, 16 have a bus pass, and 7 have both. How many students have a bus pass or a driver's license?

- Add 20 and 16, then subtract the overlap: $20+16-7 = 29$.

Property 4.5 (Inclusion-Exclusion for 2 Sets):

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Property 4.6 (Inclusion-Exclusion for 3 Sets):

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

For n sets, a generalization is:

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \cdots + (-1)^{n-1} \left|\bigcap_{i=1}^{n} A_i\right|.$$

4.3 Decision Trees

Example 4.8: A staircase has 4 steps. How many ways can you climb it, taking 1, 2, 3, or 4 steps at a time?

- Draw a tree for possibilities. Each complete path to the top corresponds to a way. Total: 8 ways.

4.4 Permutations and Combinations

Variations

Definition 4.9: A variation of k objects from n is an ordered selection of k objects from n, without repetition. If $n = k$, it's a permutation.

- Number of variations:

$$V_k^n = \frac{n!}{(n-k)!}$$

- Permutations: $P_n = n!$

Combinations

Definition 4.11: A combination of k objects from n is a selection of k objects without regard to order, without repetition.

- Number of combinations:

$$C_k^n = \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Generalizations

Definition 4.12: Allowing repetitions:

$$D_k^n = C_k^n = \binom{n+k-1}{k}$$

5 Probability

Basics

Fundamental Rules

- For any event A: $0 \leq P(A) \leq 1$
- Complement: $P(A^c) = 1 - P(A)$
- Conditional Probability: $P(A|B) = \frac{P(A \cap B)}{P(B)}, \quad P(B) > 0$
- Independence: $P(A|B) = P(A)$

Set Operations

- Intersection: $P(A \cap B) = P(A|B)P(B) = P(B|A)P(A)$
- Union: $P(A \cup B) = P(A) + P(B) - P(A \cap B)$
- General Union: $P(\bigcup_{i=1}^{n} A_i) = \sum_{i=1}^{n} P(A_i) - \sum_{i<j} P(A_i \cap A_j) + \cdots$

Bayes' Theorem

- Basic form: $P(A|B) = \frac{P(B|A)P(A)}{P(B)}$
- Partition form: $P(A_i|B) = \frac{P(A_i)P(B|A_i)}{\sum_{j=1}^{n} P(A_j)P(B|A_j)}$

Discrete Distributions

Uniform Distribution

$P(X = x) = \frac{1}{n}, \quad x \in \{x_1, \ldots, x_n\}$ $E[X] = \frac{a+b}{2}, \quad Var(X) = \frac{(b-a+1)^2-1}{12}$

Binomial Distribution

$X \sim B(n, p)$ $P(X = k) = \binom{n}{k} p^k (1-p)^{n-k}$ $E[X] = np, \quad Var(X) = np(1-p)$

Poisson Distribution

$X \sim Pois(\lambda)$ $P(X = k) = \frac{e^{-\lambda}\lambda^k}{k!}, \quad k \geq 0$ $E[X] = Var(X) = \lambda$

Negative Binomial

$X \sim NB(r, p)$ $P(X = k) = \binom{k-1}{r-1} p^r (1-p)^{k-r}$ $E[X] = \frac{r}{p}, \quad Var(X) = \frac{r(1-p)}{p^2}$

Continuous Distributions

Normal Distribution

$X \sim N(\mu, \sigma^2)$ $f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$ $Z = \frac{X-\mu}{\sigma} \sim N(0, 1)$

Exponential Distribution

$X \sim Exp(\lambda)$ $f(x) = \lambda e^{-\lambda x}, \quad x \geq 0$ $E[X] = \frac{1}{\lambda}, \quad Var(X) = \frac{1}{\lambda^2}$

Properties

Expected Value

- Linearity: $E[aX + b] = aE[X] + b$
- Product: $E[XY] = E[X]E[Y]$ if independent

Variance

- Definition: $Var(X) = E[X^2] - (E[X])^2$
- Properties: $Var(aX + b) = a^2 Var(X)$ $Var(X + Y) = Var(X) + Var(Y)$ if independent

6 boolean algebra

Boolean expressions

$\overline{\overline{x}} = x$ Law of double complement
$x + x = x$ $+$ is idempotent
$x \cdot x = x$ $\cdot$ is idempotent
$x + 0 = x$ Identity law
$x \cdot 1 = x$ Identity law
$x + 1 = 1$ 1 absorbing element for $+$
$x \cdot 0 = 0$ 0 absorbing element for $\cdot$
$x + y = y + x$
$x \cdot y = y \cdot x$ Commutativity
$x + (y + z) = (x + y) + z$
$x(yz) = (xy)z$ Associativity
$x + yz = (x + y)(x + z)$
$x(y + z) = xy + xz$ Distributivity
$\overline{xy} = \overline{x} + \overline{y}$
$\overline{x + y} = \overline{x} \cdot \overline{y}$ De Morgan's law
$x + xy = x$
$x(x + y) = x$ Absorption law
$x + \overline{x} = 1$
$x \cdot \overline{x} = 0$ Unity law

DNF and CNF

Disjunctive Normal Form (DNF): A Boolean expression is in DNF if it is a disjunction (OR, $+$) of conjunctions (AND, $\cdot$) of literals. Example:

$$(A \cdot B) + (\overline{A} \cdot C) + (\overline{B} \cdot \overline{C})$$

Conjunctive Normal Form (CNF): A Boolean expression is in CNF if it is a conjunction (AND, $\cdot$) of disjunctions (OR, $+$) of literals. Example:

$$(A + \overline{B}) \cdot (B + C + \overline{D}) \cdot (\overline{A} + D)$$

Key Differences:

- **DNF**: OR of ANDs (Sum of Products).
- **CNF**: AND of ORs (Product of Sums).

7 Generating Functions

Definitions and Concepts

Generating Function for a Sequence: Given a sequence $a_0, a_1, a_2, \dots$, the generating function $G(x)$ is defined as:

$$G(x) = a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{n=0}^{\infty} a_n x^n.$$

Formal Power Series: A formal power series is an expression of the form:

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots,$$

where coefficients a_n are given but the series may not converge.

Useful Generating Functions

- **Geometric Series:**

$$\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}, \quad |x| < 1.$$

- **Generalized Geometric Series:**

$$\sum_{n=0}^{\infty} c^n x^n = \frac{1}{1-cx}, \quad |cx| < 1.$$

- **Powers of $(1-x)^{-m}$:**

$$\frac{1}{(1-x)^m} = \sum_{n=0}^{\infty} \binom{n+m-1}{m-1} x^n, \quad |x| < 1.$$

- **Derivative Formulas:**

$$\frac{x}{(1-x)^2} = \sum_{n=1}^{\infty} n x^n,$$

$$\frac{1}{(1-x)^2} = \sum_{n=0}^{\infty} (n+1) x^n.$$

- **Exponential Generating Function:**

$$\sum_{n=0}^{\infty} \frac{x^n}{n!} = e^x.$$

- **Alternate Series:**

$$\sum_{n=0}^{\infty} (-1)^n x^n = \frac{1}{1+x}.$$

Examples

Example 1: Fruit Selection

Given a fruit basket with 2 apples, 1 pear, 1 plum, and 1 banana, the generating function is:

$G(x) = (1 + x + x^2)(1 + x)(1 + x)(1 + x).$

The coefficient of x^2 in $G(x)$ gives the number of ways to choose 2 fruits.

Example 2: Pastries

For 3 cheese pastries, 2 apricot pastries, and 4 strawberry pastries, the generating function is:

$G(x) = (1 + x + x^2 + x^3)(1 + x + x^2)(1 + x + x^2 + x^3 + x^4).$

Operations on Generating Functions

Addition: If $A(x)$ and $B(x)$ are generating functions, their sum corresponds to termwise addition of coefficients:

$$(a_0 + a_1 x + \dots) + (b_0 + b_1 x + \dots) = (a_0 + b_0) + (a_1 + b_1) x + \dots.$$

Multiplication: The product of generating functions corresponds to convolution of coefficients:

$$A(x)B(x) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n.$$

Inverse Generating Functions

A generating function $S(x)$ with $S(0) \neq 0$ has an inverse $T(x)$ such that:

$$S(x)T(x) = 1.$$

Example:

$$S(x) = 1 + 2x + 3x^2 + \cdots \implies T(x) = 1 - 2x + x^2.$$

Applications

Solving Recurrence Relations: Generating functions can transform recurrence relations into algebraic equations. For example:

$$h_n = 2h_{n-1} + 1, \quad h_0 = 0.$$

$$\text{Generating function: } H(x) = \frac{x}{(1-x)(1-2x)}.$$

Finding Closed Forms: For a recurrence $s_n = -s_{n-1} + 6s_{n-2}$ with $s_0 = 1, s_1 = 1$, we get:

$$S(x) = \frac{1+2x}{(1+3x)(1-2x)}.$$