Discrete Math Notes

Alex Feng

July 2023

1 Set Theory

Standard Symbols

$\mathbb{P} = \{1, 2, 3, 4, \dots\}$
$\mathbb{N} = \{0, 1, 2, 3, \dots\}$ (Natural Numbers, depends on definition)
$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
$\mathbb{Q}$: the rational numbers
$\mathbb{R}$: the real numbers
$\mathbb{C}$: the complex numbers

Definition: Finite Set

A set is a finite set if it has a finite number of elements. Any set that isn't finite is an infinite set.

Definition: Cardinality

The number of different elements in a finite set A is called its cardinality. The cardinality of A is denoted by $|A|$.

Definition: Subset

Let A and B be sets. $A \subseteq B$ (A is a subset of B) iff every element of A is an element of B. (Additionally, iff $A \neq B$ and $A \subseteq B$, A is a proper subset of B. A is an improper subset of A)

Definition: Set Equality

Let A and B be sets. $A = B$ iff $A \subseteq B$ and $B \subseteq A$

Definition: Intersection

For sets A and B, $A \cap B = \{x : x \in A \text{ and } x \in B\}$ intersection of A and B.

Definition: Disjoint Sets

Sets A and B are disjoint if $A \cap B = \emptyset$

Definition: Union

The union of sets A and B is $A \cup B = \{x : x \in A \text{ or } x \in B\}$

Definition: Universe

The universal set, U, is the set of all elements under discussion for possible membership in a set.

Definition: Complement of a set

The complement of sets A relative to B is $B - A = \{x : x \in B \text{ and } x \notin A\}$. The complement of A is $A^c = U - A = \{x \in U : x \notin A\}$

Definition: Symmetric Difference

The symmetric difference of sets A and B is $A \oplus B = (A \cup B) - (A \cap B)$

Definition: Cartesian Products

The Cartesian product of sets A and B is $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$

Definition: Power Set

The power set of any set A is the set of all subsets of A, denoted $\mathcal{P}(A)$.

Definition: Generalized Set Operations

For sets $A_1, A_2, \ldots, A_n$

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$$

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$$

$$A_1 \times A_2 \times \cdots \times A_n = \bigtimes_{i=1}^{n} A_i$$

$$A_1 \oplus A_2 \oplus \cdots \oplus A_n = \bigoplus_{i=1}^{n} A_i$$

2 Combinatorics

Theorem: Power Set Cardinality

For a finite set A, $|\mathcal{P}(A)| = 2^{|A|}$

Definition: Permutation

An ordered arrangement of k elements selected from a set of n elements, $0 \leq k \leq n$, where no two elements of the arrangement are the same, is called a permutation of n objects taken k at a time. The total number of such permutations is denoted by $P(n, k)$

Theorem: Permutation Counting Formula

$$P(n,k) = \prod_{j=0}^{k-1}(n-j) = \frac{n!}{(n-k)!}$$

Definition: Partition

A partition of set A is a set of one or more nonempty subsets of A, $A_1, A_2, A_3, \ldots$, such that

$$A_1 \cup A_2 \cup A_3 \cup \cdots = A$$

$$\text{If } i \neq j \text{ then } A_1 \cap A_j = \emptyset$$

Theorem: The Basic Law of Addition

If $\{A_1, A_2, \ldots, A_n\}$ is the partition of a finite set A, then

$$|A| = \sum_{k=1}^{n} |A_k|$$

Theorem: Laws of Inclusion-Exclusion

Given finite sets A_1, A_2, A_3, then

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) + |A_1 \cap A_2 \cap A_3|$$

Definition: Binomial Coefficient

Let n and k be nonnegative integers. The binomial coefficient $\binom{n}{k}$ represents the number of combinations of n objects taken k at a time, and is read "n choose k"

Theorem: Binomial Coefficient Formula

If n and k are nonnegative integers with $0 \leq k \leq n$, then the number k-element subsets of an n element set is equal to

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

Theorem: The Binomial Theorem

If $n \geq 0$ and x and y are numbers, then

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

3 Logic

Definition: Proposition

A proposition is a sentence to which one and only one of the terms true or false can be meaningfully applied.

Definition: Logical Conjunction

If p and q are propositions, their conjunction, p and q (denoted $p \wedge q$), is defined by the truth table

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

Definition: Logical Disjunction

If p and q are propositions, their disjuction, p or q (denoted $p \vee q$), is defined by the truth table

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

Definition: Logical Negation

If p is a proposition, its negation, not p, denoted $\neg p$, and is defined by the truth table

p	$\neg p$
0	1
1	0

Definition: Conditional Statement

The conditional statement "If p then q," denoted $p \to q$, is defined by the truth table

p	q	$p \to q$
0	0	1
0	1	1
1	0	0
1	1	1

Definition: Converse

the converse of the proposition $p \to q$ is the proposition $q \to p$

Definition: Contrapositive

The contrapositive of the proposition $p \to q$ is the proposition $\neg q \to \neg p$

Definition: Logical Inverse

The inverse of the proposition $p \to q$ is the proposition $\neg p \to \neg q$

Definition: Biconditional Proposition

If p and q are propositions, the biconditional statement "p if and only if q," denoted $p \leftrightarrow q$, is defined by the truth table

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Definition: Proposition Generated by a Set

Let S be any set of propositions. A proposition generated by S is any valid combination of propositions in S with conjunction, disjunction, and negation. More precisely,

a. If $p \in S$, then p is a proposition generated by S
b. If x and y are propositions generated by S, then so are

$$(x), \neg x, x \vee y, \text{ and } x \wedge y$$

Definition: Tautology

An expression involving logical variables that is true in all cases is a tautology. The number 1 is used to symbolize a tautology.

Definition: Contradiction

An expression involving logical variables that is false for all cases is called a contradiction. The number 0 is used to symbolize a contradiction.

Definition: Equivalence

Let S be a set of propositions and let r and s be propositions generated by S. r and s are equivalent iff $r \leftrightarrow s$ is a tautology. The equivalence of r and s is denoted $r \iff s$.

Definition: Implication

Let S be a set of propositions and let r and s be propositions generated by S. We say that r implies s if $r \rightarrow s$ is a tautology. We write $r \implies s$ to indicate this implication.

Definition: The Sheffer Stroke

The Sheffer Stroke is the logical operator defined by the following truth table:

p	q	$p \mid q$
0	0	1
0	1	1
1	0	1
1	1	0

Definition: Mathematical System

A mathematical system consists of:

1. A set or universe, U.

2. Definitions: sentences that explain the meaning of concepts that relate to the universe. Any term used in describing the universe itself is said to be undefined. All definitions are given in terms of these undefined concepts of objects.

3. Axioms: assertions about the properties of the universe and rules for creating and justifying more assertions. these rules always include the system of logic that we have developed to this point.

4. Theorems: the additional assertions mentioned above.

Definition: Theorem

A true proposition derived from the axioms of a mathematical system is called a theorem.

Definition: Proof

A proof of a theorem is a finite sequence of logically valid steps that demonstrate that the premises of a theorem imply its conclusion.

Definition: Proposition over a Universe

Let U be a nonempty set. A proposition over U is a sentence that contains a variable that can take on any value in U and that has a definite truth value as a result of any such substitution.

Definition: Truth Set

If p is a proposition over U, the truth set of p is $T_p = \{a \in U \mid p(a) \text{ is true } \}$.

Definition: Tautologies and Contradictions over a Universe

A proposition over U is a tautology if its truth set is U. It is a contradiction if its truth set is empty.

Definition: Equivalence of propositions over a universe

For two propositions p and q, if $p \iff q$ then $T_p = T_q$

Definition: Implication for propositions over a universe

If p and q are propositions over U, $p \implies q$ if $p \to q$

Theorem: The Principle of Mathematical Induction

Let $p(n)$ be a proposition over the positive integers. If
1. $p(1)$ is true, and
2. for all $n \geq 1$, $p(n) \implies p(n+1)$

then $p(n)$ is a tautology.

Definition: The Existential Quantifier

If $p(n)$ is a proposition over U with $T_p \neq \emptyset$, we abbreviate "There exists an n in U such that $p(n)$ (is true)" using $(\exists n)(p(n))$

Definition: The Universal Quantifier

"For all n in U, $p(n)$ (a proposition over U with $T_p = U$)" can be abbreviated using $(\forall n)(p(n))$

4 Relations

Definition: Relation

A relation from sets A into B is any subset of $A \times B$.

Definition: Relation on a Set

A relation from a set A into itself is called a relation on A.

Definition: Divides

$a, b \in \mathbb{Z}, a \neq 0$. a divides b, $a \mid b \iff \exists k \in \mathbb{Z}, ak = b$

Definition: Composition of Relations

Let r be a relation from a set A into a set B, and let s be a relation from B into a set C. The composition of r with s, written rs, is the set of pairs of the form $(a, c) \in A \times C$, where $(a, c) \in rs \iff \exists b \in B, (a, b) \in r \wedge (b, c) \in s$.

Definition: Reflexive Relation

Let A be a set and let r be a relation on A. Then r is reflexive iff $\forall a \in A, ara$.

Definition: Antisymmetric Relation

Let A be a set and let r be a relation on A. Then r is antisymmetric iff $arb \wedge a \neq b \implies \neg bra$.

Definition: Transitive Relation

Let A be a set and let r be a relation on A. r is transitive iff $arb \wedge brc \implies arc$

Definition: Partial Ordering

A relation on a set A that is reflexive, antisymmetric, and transitive is called a partial ordering on A. A set on which there is a partial ordering relation defined is called a partially ordered set or poset.

Definition: Symmetric Relation

let r be a relation on a set A. r is symmetric iff $arb \implies bra$.

Definition: Equivalence Relation

A relation r on a set A is called an equivalence relation iff it is reflexive, symmetric, and transitive.

Definition: Equivalence Classes

Let r be an equivalence relation on A, and $a \in A$. The equivalence class of a is the set, $[a]$, of all elements to which a is related.

$$[a] = \{b \in A : arb\}$$

The set of all equivalence classes with respect to r is denoted A/r, read "A mod r."

Theorem: Equivalence Class Partition

Let r be an equivalence relation on A. Then the set of all distinct equivalence classes determined by r form a partition of A denoted A/r and read "A mod r."

Definition: Congruence Modulo n

Let $n \in Z^+, n \geq 2$. We define congruence modulo n to be the relation $\equiv_n$ defined on the integers by

$$a \equiv_n b \iff n \mid (a - b)$$

5 Functions

Definition: Function

A function from a set A into a set B is a relation from A into B such that each element of A is related to exactly one element of the set B. The set A is called the domain of the function and the set B is called the codomain.

Definition: The Set of Functions Between Two Sets

Given two sets, A and B, the set of all functions from A into B is denoted B^A.

Definition: Image of an element under a function

Let $f : A \to B$, read "Let f be a function from the set A into the set B." If $a \in A$, then $f(a)$ is used to denote that element of B to which a is related. $f(a)$ is called the image of a, or, more precisely, the image of a under f. We write $f(a) = b$ to indicate that the image of a is under b.

Definition: Range of a Function

If $f : X \to Y$, then the range of f, is

$$f(X) = \{f(a) \mid a \in X\} = \{b \in Y \mid \exists a \in X, f(a) = b\}$$

Definition: Injection

A function $f : A \to B$ is injective (one-to-one) if

$$\forall a, b \in A, a \neq b \implies f(a) \neq f(b)$$

Definition: Surjection

A function $f : A \to B$ is surjective (onto) if

$$f(A) = B$$

which is equivalent to

$$\forall b \in B, \exists a \in A, f(a) = b$$

Definition: Bijection

A function $f : A \to B$ is bijective (one-to-one and onto) if it is both injective and surjective.

Definition: Cardinality

Two sets are said to have the same cardinality if there exists a bijection between them. If a set has the same cardinality as the set $\{1, 2, 3, \ldots n\}$, then we say its cardinality is n.

Definition: Countable Set

If a set is finite or has the same cardinality as the set of positive integers, it is called a countable set.

Theorem: The Pigeonhole Principle

let f be a function from a finite set X into a finite set Y. If $n \geq 1$ and $|X| > n|Y|$, then there exists an element of Y that is the image under f of at least $n + 1$ elements of X.

Definition: Equality of Functions

let $f, g : A \to B$.

$$f = g \iff \forall x \in A, f(x) = g(x)$$

Definition: Composition of Functions

let $f : A \to B$ and $g : B \to C$. The composition of f followed by g, written $g \circ f$, is a function from A into C defined by $(g \circ f)(x) = g(f(x))$, which is read "g of f of x."

Theorem: Function Composition Associativity

If $f : A \to B, g : B \to C,$ and $h : C \to D$, then $h \circ (g \circ f) = (h \circ g) \circ f$.

Definition: Powers of Functions

Let $f : A \to A$.

$$f^1 = f, \text{ that is, } \forall a \in A, f^1(a) = f(a)$$
$$\text{For } n \geq 1, f^{n+1} = f \circ f^n$$

Theorem: Composition of Injections

If $f : A \to B$ and $g : B \to C$ are injections, then $g \circ f : A \to C$ is an injection.

Theorem: Composition of Surjections

If $f : A \to B$ and $g : B \to C$ are surjections, then $g \circ f : A \to C$ is a surjection.

Definition: Identity Function

For any set A, the identity function on A is a function from A onto A, denoted i (or, more specifically, i_A) such that $\forall a \in A, i(a) = a$

Definition: Inverse of a Function on a Set

Let $f : A \to A$. If there exists a function $g : A \to A$ such that $g \circ f = f \circ g = i$, then g is called the inverse of f and denoted by f^{-1}, read "f inverse."

Theorem: Bijection Inverse

Let $f : A \to A$. f^{-1} exists iff f is a bijection.

Definition: Permutation

A bijection of a set A into itself is called a permutation of A.

Definition: Inverse of a Function (General Case)

Let $f : A \to B$. If there exists a function $g : B \to A$ such that $g \circ f = i_A$ and $f \circ g = i_B$, then g is called the inverse of f and is denoted by f^{-1}, read "f inverse."

Theorem: Existence of Inverse

Let $f : A \to B$. f^{-1} exists iff f is a bijection.