COMP2121 Discrete Mathematics
Revision Notes

Jacob Shing

1 Sept 2025

Contents

1 Logic & Proofs

1.1 Propositional Logic

Definition 1.1 (Proposition)**.** A statement that can be **unambiguously** determined to be either true of false.

Definition 1.2 (Logical Operators)**.** The commonly used logical operators are:

- **Negation**: $\neg P$
- **Conjunction** (AND): $P \wedge Q$
- **Disjunction** (OR): $P \vee Q$
- **Exclusive OR** (XOR): $P \oplus Q$
- **Implication/Conditional** (if ..., then ...): $P \to Q$
- **Biconditional** (if and only if): $P \leftrightarrow Q$

where P and Q are propositions.

Remark. The truth tables for the conditional and biconditional operators are as follows:

P	Q	$\boldsymbol{P \to Q}$	$\boldsymbol{P \leftrightarrow Q}$
F	F	T	T
F	T	T	F
T	F	F	F
T	T	T	T

Note that the "implication" operator is distinct from the "implication" used in natural language. $P \to Q$ does not contain cause-and-effect information.

Definition 1.3 (Sufficiency and Necessity)**.** When $P \to Q$ is true, we say that:

- P is a **sufficient** condition for Q.
- Q is a **necessary** condition for P.

Remark (Common Natural Language Phrases Involving Implication)**.** It is useful to note that the following phrases are logically equivalent to $P \to Q$:

- "If P, then Q"
- "P only if Q"
- "Q if P"
- "Q whenever P"
- "P implies Q"
- "P is sufficient for Q"
- "Q is necessary for P"
- "Q follows from P"
- "Q provided that P"
- "Q unless $\neg P$"

1.1.1 Boolean Algebra

The truth value of a proposition P is denoted by $\mathrm{w}(P)$. For composite propositions, we often need to simplify the expression.

Definition 1.4 (Algebraic Rules for Boolean Algebra)**.** Consider two propositions P and Q, and denote true by 1 and false by 0, we have:

1. $\mathrm{w}(\neg P) = \mathrm{w}(P) \oplus 1$
2. $\mathrm{w}(P \wedge Q) = \mathrm{w}(P)\mathrm{w}(Q)$
3. $\mathrm{w}(P \oplus Q) = \mathrm{w}(P) \oplus \mathrm{w}(Q)$
4. $\mathrm{w}(P \vee Q) = \mathrm{w}(P) \oplus \mathrm{w}(Q) \oplus \mathrm{w}(P)\mathrm{w}(Q)$
5. $\mathrm{w}(P \leftrightarrow Q) = \mathrm{w}(P) \oplus \mathrm{w}(Q) \oplus 1$
6. $\mathrm{w}(P \to Q) = \mathrm{w}(P)\mathrm{w}(Q) \oplus \mathrm{w}(P) \oplus 1$

Example. Question: Compute the truth values of $(P \to Q) \wedge (Q \to P)$ as a function of $\mathrm{w}(P)$ and $\mathrm{w}(Q)$.

Solution: Denote $x = \mathrm{w}(P)$ and $y = \mathrm{w}(Q)$, we have:

$$\begin{aligned}
&\mathrm{w}((P \to Q) \wedge (Q \to P)) \\
&= (xy \oplus x \oplus 1) \wedge (yx \oplus y \oplus 1) \qquad \text{(Rule \#6)} \\
&= (xy \oplus x \oplus 1)(xy \oplus y \oplus 1) \qquad \text{(Rule \#2)} \\
&= x^2y^2 \oplus xy^2 \oplus xy \oplus x^2y \oplus xy \oplus x \oplus xy \oplus y \oplus 1 \\
&= xy \oplus xy \oplus xy \oplus xy \oplus xy \oplus x \oplus xy \oplus y \oplus 1 \qquad (\forall b \in \{0,1\} : (b^2 = b)) \\
&= \boxed{x \oplus y \oplus 1}
\end{aligned}$$

Note that this expression is equivalent to $P \leftrightarrow Q$ (by Rule #5).

1.1.2 Logical Equivalence

Definition 1.5 (Tautology and Contradiction)**.** A **tautology** is a proposition that is always true, denoted by T. A **contradiction** is a proposition that is always false, denoted by F.

Definition 1.6 (Logical Equivalence)**.** Two propositions P and Q are said to be logically equivalent if $P \leftrightarrow Q$ is a tautology, denoted as $P \equiv Q$ or $P \Leftrightarrow Q$.

Theorem 1.7 (Important Laws of Logical Equivalence)**.** These are some important laws for simplifying composite logics:

1. **Double Negation Law**: $\neg(\neg P) \equiv Q$
2. **Identity Laws**: $P \wedge T \equiv P$ and $P \vee F \equiv P$
3. **Domination Laws**: $P \vee T \equiv T$ and $P \wedge F \equiv F$
4. **Idempotent Laws**: $P \wedge P \equiv P$ and $P \vee P \equiv P$
5. **Negation Laws**: $P \wedge \neg P \equiv F$ and $P \vee \neg P \equiv T$
6. **Biconditional Law**: $(P \leftrightarrow Q) \equiv (P \to Q) \wedge (Q \to P)$
7. **Implication Law**: $(P \to Q) \equiv (\neg P \vee Q)$
8. **Contraposition Law**: $(P \to Q) \equiv (\neg Q \to \neg P)$
9. **De Morgan's Laws**:
   (a) $\neg(P \wedge Q \wedge R \wedge \cdots) \equiv \neg P \vee \neg Q \vee \neg R \vee \cdots$
   (b) $\neg(P \vee Q \vee R \vee \cdots) \equiv \neg P \wedge \neg Q \wedge \neg R \wedge \cdots$
10. **Distributivity Laws**:
    (a) $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
    (b) $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
11. **Absorption Laws**:
    (a) $P \vee (P \wedge Q) \equiv P$
    (b) $P \wedge (P \vee Q) \equiv P$

Remark. Other important logical equivalences involving Biconditional and Exclusive Or

1. **Biconditional**:
   (a) $P \leftrightarrow Q \equiv \neg P \leftrightarrow \neg Q$
   (b) $P \leftrightarrow Q \equiv (P \wedge Q) \vee (\neg P \wedge \neg Q)$
   (c) $\neg(P \leftrightarrow Q) \equiv P \leftrightarrow \neg Q$
2. **Exclusive Or**:
   (a) $P \oplus Q \equiv (P \vee Q) \wedge \neg(P \wedge Q)$
   (b) $P \leftrightarrow Q \equiv \neg P \oplus Q \equiv P \oplus \neg Q$
   (c) $P \vee Q \equiv (P \wedge Q) \oplus (P \oplus Q)$
   (d) $P \oplus \boldsymbol{T} \equiv \neg P$ and $P \oplus \boldsymbol{F} \equiv P$

1.2 Predicate Logic

Definition 1.8 (Universe of Discourse)**.** For a variable x, the set of values under consideration is called the **Universe of Discourse**, or the **Domain**.

Definition 1.9 (Predicate)**.** A predicate $P(x)$ is a statement that depends on a variable x so that $P(x)$ is a proposition for every x in the universe of discourse.

Definition 1.10 (The Universal Quantifier and The Existential Quantifier)**.** The notation $\forall \boldsymbol{x} \boldsymbol{P}(\boldsymbol{x})$ denotes "$P(x)$ holds **for every** $\boldsymbol{x}$ in the universe of discourse". Consider its logical equivalence:–

$$\forall x P(x) \equiv P(x_0) \wedge P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n)$$

where $\{x_0, x_1, x_2, \cdots, x_n\}$ is the universe of discourse.
Similarly, the notation $\exists \boldsymbol{x} \boldsymbol{P}(\boldsymbol{x})$ denotes "$P(x)$ holds for **at least one** $\boldsymbol{x}$ in the universe of discourse", and has the logical equivalence of:–

$$\exists x P(x) \equiv P(x_0) \vee P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n)$$

.

Theorem 1.11 (Examples and Counterexamples)**.** To guarantee that the proposition $\forall x P(x)$ is false, it is enough to find one **counterexample** x_0 such that $P(x_0)$ is false. To guarantee that the proposition $\exists x P(x)$ is true, it is enough to find one **example** x_0 such that $P(x_0)$ is true.

Theorem 1.12 (Negations of $\forall$ and $\exists$ Predicates)**.** Predicates involving $\forall$ and $\exists$ can be negated as:

1. $\neg(\forall x P(x)) \equiv \exists x \neg P(x)$
2. $\neg(\exists x P(x)) \equiv \forall x \neg P(x)$

Remark. Quantifiers cannot be exchanged:

$$\forall y[\exists x : P(x, y)] \not\equiv \exists x[\forall y : P(x, y)]$$

Let $P(x, y)$ be "x opens y", $x \in \{\text{all keys in the world}\}$, and $y \in \{\text{all doors in the world}\}$. The left hand side means "for every door, there exists at least one key that opens the door" while the right hand side means "there exists at least one key that opens every door."

Remark. Quantifiers are only distributive with respect to certain operators:

$$\forall x[P(x) \wedge Q(x)] \equiv [\forall x P(x)] \wedge [\forall y Q(y)]$$
$$\exists x[P(x) \vee Q(x)] \equiv [\exists x P(x)] \vee [\exists y Q(y)]$$

Other combinations do not work.

1.3 Proofs

Definition 1.13 (Valid Argument)**.** An argument is said to be valid if it is impossible for the conclusion to be $\boldsymbol{F}$ when all its premises are $\boldsymbol{T}$.

Definition 1.14 (Logical Implication)**.** P is said to be logically implying Q if $P \to Q$ is a tautology, denoted as $P \Rightarrow Q$.

Definition 1.15 (Open Problems)**.** When the proof of a statement remains unknown, the statement is called an **open problem**. Once a proof is found, the problem no longer remains open.

Theorem 1.16 (Rules of Inference in Propositional Logic)**.**

Name	Logical Implication
Modus ponens	$((P \to Q) \wedge P) \Rightarrow Q$
Modus tollens	$((P \to Q) \wedge \neg Q) \Rightarrow \neg P$
Hypothetical syllogism	$((P \to Q) \wedge (Q \to R)) \Rightarrow (P \to R)$
Disjunctive syllogism	$((P \vee Q) \wedge \neg P) \Rightarrow Q$
Addition	$P \Rightarrow (P \vee Q)$
Simplification	$(P \wedge Q) \Rightarrow P$
Resolution	$((P \vee Q) \wedge (\neg P \vee R) \Rightarrow (Q \vee R))$

Theorem 1.17 (Rules of Inference in Predicate Logic)**.**

Name	Logical Implication
Universal instantiation	$(\forall x P(x)) \Rightarrow P(c)$ for any arbitrary c
Universal generalization	$P(c) \Rightarrow (\forall x P(x))$ for any arbitrary c
Existential instantiation	$(\exists x P(x)) \Rightarrow P(c)$ for some c
Existential generalization	$P(c) \Rightarrow (\exists x P(x))$ for some c

Theorem 1.18 (Combining Rules of Inference)**.**

Name	Logical Implication
Universal *modus ponens*	$((\forall x(P(x) \to Q(x))) \wedge P(a)) \Rightarrow Q(a)$ for a particular a
Universal *modus tollens*	$((\forall x(P(x) \to Q(x))) \wedge \neg Q(a)) \Rightarrow \neg P(a)$ for a particular a

Several methods for proving statements are introduced below.

1.3.1 Direct Proof

A **direct proof** of a statement $P \to Q$ starts with the assumption that P is true, and uses a sequence of logical implications to arrive at the conclusion that Q is true.

Example.
Thesis: If n is an odd integer, then n^2 is an odd integer.

Proof.
Assume n to be an odd integer, then, by definition, for some integer k, $n = 2k + 1$.
Then, we have $n^2 = (2k + 1)^2 = 2(2k^2 + 1) + 1$. Since k is an integer, $2k^2 + 1$ is an integer.
By definition of an odd number, $n^2 = 2(2k^2 + 1) + 1$ is an odd integer.
Q.E.D.

1.3.2 Proof by Contraposition

Recall the Contraposition Law: $P \to Q \equiv \neg Q \to \neg P$. To prove $P \to Q$ by contraposition, we first assume that the conclusion, namely Q, is false, and then show that the premise P must also be false.

Example.
Thesis: For every integer n, n is even if n^2 is even.

Proof.
Denote P : "n^2 is even" and Q : "n is even". The thesis is equivalent to $P \to Q$. To prove by contraposition, we prove $\neg Q \to \neg P$, i.e., "If n is odd, then n^2 is odd".
Note that this is exactly the same as the previous example, which has already been proven true.
Therefore, when Q is false (i.e., n is odd), P must also be false (i.e., n^2 is odd), and this shows that $P \Rightarrow Q$.
Q.E.D.

1.3.3 Proof by Contradiction

Suppose we would like to prove P is true, and we can find a contradiction $\boldsymbol{F}$, such that $\neg P \Rightarrow \boldsymbol{F}$. Because $\neg P \to \boldsymbol{F}$ is true, but the consequence is $\boldsymbol{F}$, for the conditional to be true, the premise $\neg P$ must be false, i.e., P must be true.

Example.
Thesis: $\exists x \in \mathbb{R}(x^2 + 1 = 0)$ is false.

Proof.
We start by assuming the negation of the thesis, namely $\exists x \in \mathbb{R}(x^2 + 1 = 0)$ is true.
Consider the fact that $\forall x_0 \in \mathbb{R}(x_0^2 \geq 0)$, which also implies $x_0^2 + 1 \geq 1$.
Combined with the assumption, we have $x_0^2 + 1 = 0 \geq 1$, which is a contradition.
Therefore, the negation of the thesis is false, and the thesis must be true.
Q.E.D.

1.3.4 Proof by Cases

Consider the logical equivalence:

$$(P_1 \vee P_2 \vee \cdots \vee P_n) \to Q \equiv (P_1 \to Q) \wedge (P_2 \to Q) \wedge \cdots \wedge (P_n \to Q)$$

To prove $P \to Q$, where $P \equiv P_1 \vee P_2 \vee \cdots \vee P_n$, we can prove $P_i \to Q$ for each $i = 1, 2, \ldots, n$.

1.3.5 Equivalence Proof

To prove $P \equiv Q$, we can prove both the sufficiency $P \to Q$ and the necessity $Q \to P$.

2 Sets, Relations, & Functions

Remark. The logical expressions given in this section are very important for proofs in assignments and exams.

2.1 Sets

2.1.1 Basics on Sets

Definition 2.1 (Set)**.** A **set** is a collection of **unordered**, **distinct** objects, considered as an object in its own right. The objects are called the **elements** or **members** of the set.

Definition 2.2 (Belonging to a Set)**.** An object x within A is said to **belong** to a set A, denoted by $x \in A$. If x does not belong to A, we write $x \notin A$.

Definition 2.3 (Cardinality)**.** The **cardinality** of a set A, denoted by $|A|$, is the number of elements in A.

Definition 2.4 (Empty Set)**.** The **empty set**, denoted by $\varnothing$, is the set with no elements. Its cardinality is 0, i.e. $|\varnothing| = 0$.

Remark. Sets can be defined in two ways:

1. **Roster form**: Explicitly list all elements of the set. (e.g. $A = \{1, 2, 3\}$)
2. **Set-builder form**: Describe the properties of the elements of the set. (e.g. $A = \{x \mid x \text{ is a positive integer less than } 4\} = \{1, 2, 3\}$)

Definition 2.5 (Power Set)**.** A power set of a set A, denoted by $\mathcal{P}(A)$, is the set of all subsets of A, i.e. all the possible combinations of elements in A.
Note that $\varnothing \in \mathcal{P}(A)$ and $A \in \mathcal{P}(A)$ are tautologies. We also have $|\mathcal{P}(A)| = 2^{|A|}$, provided that A is finite.

Remark. Common sets: (1) Natural numbers: $\mathbb{N} = \{0, 1, 2, \ldots\}$ *in the field of Computer Science,* $0 \in \mathbb{N}$*, while in some other fields,* $0 \notin \mathbb{N}$; (2) Integers: $\mathbb{Z}$, Positive integers: $\mathbb{Z}^+$; (3) Rational numbers: $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$; (4) Real numbers: $\mathbb{R}$; (5) Complex numbers: $\mathbb{C} = \{a + b\mathrm{i} \mid a, b \in \mathbb{R}, \mathrm{i}^2 = -1\}$.

2.1.2 Relationships of Sets

Definition 2.6 (Subset)**.** A set A is a **subset** of a set B, denoted by $A \subseteq B$, if every element of A is also an element of B, or, by logical expression,

$$A \subseteq B \equiv \forall x(x \in A \to x \in B)$$

Conversely, if $\exists x(x \in A \wedge x \notin B)$, then A is not a subset of B, denoted by $A \nsubseteq B$.

Definition 2.7 (Proper Subset)**.** A set A is a **proper subset** of a set B, denoted by $A \subset B$, if $A \subseteq B$ and $A \neq B$, or, by logical expression,

$$A \subset B \equiv [\forall x(x \in A \to x \in B)] \wedge [\exists y(y \in B \wedge \neg(y \in A))]$$

Definition 2.8 (Equality of Sets)**.** Two sets A and B are **equal**, denoted by $A = B$, if for every element x in A, x is also in B, and vice versa, or, by logical expression

$$A = B \equiv \forall x(x \in A \leftrightarrow x \in B)$$

2.1.3 Set Operations

Definition 2.9 (Intersection $\cap$)**.** The **intersection** of two sets A and B, denoted by $A \cap B$, is the set of elements that are in both A and B, or, by logical expression,

$$x \in A \cap B \equiv (x \in A) \wedge (x \in B)$$

Definition 2.10 (Union $\cup$)**.** The **union** of two sets A and B, denoted by $A \cup B$, is the set of elements that are in either A or B (or in both), or, by logical expression,

$$x \in A \cup B \equiv (x \in A) \vee (x \in B)$$

Definition 2.11 (Difference $-$)**.** The **difference** of two sets A and B, denoted by $A - B$, is the set of elements that are in A but not in B, or, by logical expression,

$$x \in A - B \equiv (x \in A) \wedge (x \notin B)$$

Definition 2.12 (Complement $\overline{S}$)**.** The **complement** of a set A in the universal set U, denoted by $\overline{A}$, is the set of elements that are not in A, or, by logical expression,

$$x \in \overline{A} \equiv x \notin A$$

Note that we have $\overline{A} = U - A$.

Definition 2.13 (Cartesian Product $\times$)**.** The **Cartesian product** of two sets A and B, denoted by $A \times B$, is the set of all **ordered pairs** (a, b) where $a \in A$ and $b \in B$.

Remark. Note that $A \times B \neq B \times A$ for non-empty sets A and B. Generally, we have $A \times \varnothing = \varnothing \times A = \varnothing$.

2.1.4 Set Theory & Logic

Sets are in one-to-one correspondence with predicates.

Theorem 2.14 (Sets and Predicates)**.** Let U be the set of all possible values of x, then this universal set is equivalent to the universe of discourse for predicate logics.
For every set $A \subseteq U$, we can define a predicate that depends on A:

$$P_A(x) : (x \in A)$$

Similarly, for every predicate $P(x)$, we can define a truth set A:

$$A := \{x \in U \mid P(x)\}$$

2.2 Relations

2.2.1 Definition & Properties of Relations

Definition 2.15 (Relation)**.** A **relation** from a set A to a set B is a subset of $A \times B$, denoted by $R \subseteq A \times B$.
When element a is in relation with element b by R, we write aRb, i.e.,

$$a \ R \ b \equiv (a, b) \in R$$

Otherwise, we write $a \not R \ b$.

There are several special types of relations when we discuss relations on a set A itself, i.e. $R \subseteq A \times A$.

Definition 2.16 (Reflexive Relation)**.** A **reflexive relation** is defined to be:

$$\forall x \in A(x \ R \ x)$$

Example. Let A be the set of all people and define $x \ R \ y$: "x has a biological father y". Since everyone must be born from a biological father (regardless of whether they know who he is, or whether the father is still alive), we have $\forall x \in A(x \ R \ x)$. Thus, this relation is reflexive.

Definition 2.17 (Symmetric Relation)**.** A **symmetric relation** is defined to be:

$$\forall x, y \in A(x \ R \ y \to y \ R \ x)$$

Example. Continue to let A be the set of all people and redefine $x \ R \ y$: "x is married to y". Since if x is married to y, then y must be married to x, we have $\forall x, y \in A(x \ R \ y \to y \ R \ x)$. Thus, this relation is symmetric.

Remark. It does not matter if $\exists x_0, y_0 \in A$ who are single and not married to anyone, since when $(x_0, y_0) \notin R$, the implication $(x_0 \ R \ y_0) \to (y_0 \ R \ x_0)$ is still true.

Definition 2.18 (Transitive Relation)**.** A **transitive relation** is defined to be:

$$\forall x, y, z \in A[(x \ R \ y) \wedge (y \ R \ z) \to (x \ R \ z)]$$

Example. Let A be the set of all people in Hong Kong, and define $x \ R \ y$: "x studies in the same university as y". Since if x studies in the same university as y, and y studies in the same university as z, then x must study in the same university as z, we have $\forall x, y, z \in A[(x \ R \ y) \wedge (y \ R \ z) \to (x \ R \ z)]$. Thus, this relation is transitive.

Remark. It does not matter if $\exists x, y_0, z \in A$, where y_0 studies in a different university from x and z, since when $(x \ R \ y_0) \wedge (y_0 \ R \ z)$ is false, the implication $[(x \ R \ y_0) \wedge (y_0 \ R \ z)] \to (x \ R \ z)$ is still true.

Definition 2.19 (Equivalence Relation)**.** An **equivalence relation** is a relation that is reflexive, symmetric, and transitive.

2.2.2 Equivalence Classes & Partitions

Lemma 2.20 (Equivalence of Elements)**.** Let R be an equivalence relation on a set A. Two elements $x, y \in A$ are said to be **equivalent** if $x \; R \; y$.

Definition 2.21 (Equivalence Class)**.** The **equivalence class** of an element $x \in A$ is the set of all elements in A that are equivalent to x, denoted by $[x]$, or, more formally,

$$[x] := \{y \in A \mid x \; R \; y\}$$

Every element of $[x]$ is said to be a **representative** of the equivalence class $[x]$.

Example. Let $A = \mathbb{Z}^+$, and define $x \; R \; y$: "$x - y$ is even". Observe that any integer subtracted by itself is 0, which is even, so the relation is reflexive. Also, when $x - y$ is even, then $y - x = -(x - y)$ is also even, so the relation is symmetric. Finally, when $x - y$ and $y - z$ are both even, then $x - z = (x - y) + (y - z)$ is also even, so the relation is transitive. Thus, this relation is an equivalence relation.
Easily, we have $[1] = \{1, 3, 5, 7, \ldots\}$ and $[2] = \{2, 4, 6, 8, \ldots\}$.

Lemma 2.22 (Disjoint Sets)**.** Two sets A_1 and A_2 are said to be **disjoint** if $A_1 \cap A_2 = \varnothing$, i.e. they have no elements in common.

Theorem 2.23 (Distinct Equivalence Classes are Disjoint)**.** If $[x] \cup [y] \neq \varnothing$, then $[x] = [y]$.

Definition 2.24 (Partition of a Set)**.** A list of subsets $A_1, A_2, \ldots, A_k \subseteq A$ forms a **partition** of A if the following conditions are satisfied:

1. $\bigcup_{i=1}^{k} A_i = A$
2. $\forall i \neq j : A_i \cap A_j = \varnothing$

Example. Let A be the set of all people, and define $x \; R \; y$: "x and y are born in the same month". We skip the verification that this is an equivalence relation.
The equivalence classes are: [People born in Jan], [People born in Feb], ..., [People born in Dec].
Observe that the union of all these equivalence classes must be A, since everyone must be born in some month, and any two equivalence classes are disjoint, since no one can be born in two different months. Thus, these equivalence classes form a partition of A.

2.3 Functions

2.3.1 Definition & Terminology

Definition 2.25 (Function)**.** A **function** is a special type of relation from a set A to a set B with the property that for every $a \in A$, there is exactly one $b \in B$ such that a is related to b.
Explicitly, a relation R from A to B is a function if it satisfies:

1. $\forall a \in A, \exists b \in B : a \; R \; b$
2. $\forall a \in A, \forall b_1, b_2 \in B : (a \; R \; b_1) \wedge (a \; R \; b_2) \to (b_1 = b_2)$

Notation: For a relation R that is a function, we write $y = f(x)$.
Complete Notation of a Function: To completely define a function, we write it in the form:

$$f : A \to B \quad f(x) = (\text{the rule to get } y \text{ from } x)$$

Definition 2.26 (Domain, Codomain, Preimage & Image)**.** For a function $y = f(x)$, or $R : A \to B$, we have:

1. The set A is called the **domain** of f;
2. The elements $x \in A$ are called the **preimages**;
3. The set B is called the **codomain** of f;
4. The elements $y \in B$ are called the **images**;

Definition 2.27 (Range)**.** The **range** of a function $f : A \to B$ is the set of all elements in B that are images of elements in A, i.e.

$$f(A) := \{y \in B \mid \exists x \in A(y = f(x))\}$$

Note that we have the property $f(A) \subseteq B$, i.e. the range of f is not necessarily the same as the codomain of f.

2.3.2 Types of Functions

Definition 2.28 (Injective Function)**.** A function $f : A \to B$ is said to be **injective** (one-to-one) if

$$\forall x_1, x_2 \in A[(x_1 \neq x_2) \to (f(x_1) \neq f(x_2))]$$

Example. $f : \mathbb{R} \to \mathbb{R} \quad f(x) = x^2$ is not injective, since $f(1) = f(-1) = 1$, while $f : \mathbb{R}^+ \to \mathbb{R} \quad f(x) = x^2$ is injective.

Definition 2.29 (Surjective Function)**.** A function $f : A \to B$ is said to be **surjective** (onto) if

$$\forall y \in B, \exists x \in A : f(x) = y$$

Consequently, we have $f(A) = B$ for any surjective $f : A \to B$.

Definition 2.30 (Bijective Function)**.** A function $f : A \to B$ is said to be **bijective** if it is both injective and surjective. In other words, for every $y \in B$, there exists a unique $x \in A$ such that $f(x) = y$.

2.3.3 Operations on Functions

Definition 2.31 (Composition of Functions)**.** Given two functions $f : A \to B$ and $g : B \to C$, we can define $g \circ f : A \to C$ by

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

Definition 2.32 (Inverse of a Function)**.** Let $f : A \to B$ be a bijective function. Then there exists a function $g : B \to A$ such that

$$\forall x \in A \quad (g \circ f)(x) = x$$

and

$$\forall y \in B \quad (f \circ g)(y) = y$$

This function g is called the **inverse** of f, denoted by f^{-1}.

2.3.4 Real-valued Functions

Definition 2.33 (Real-valued Function)**.** A function $f : A \to B$ is said to be a **real-valued function** if $B \subseteq \mathbb{R}$.

Theorem 2.34. Let $A, B \subseteq \mathbb{R}$, we say $f : A \to B$ to be:

1. **strictly increasing** if $\forall x_1, x_2 \in A[(x_1 < x_2) \to (f(x_1) < f(x_2))]$;
2. **strictly decreasing** if $\forall x_1, x_2 \in A[(x_1 < x_2) \to (f(x_1) > f(x_2))]$;
3. **non-increasing** if $\forall x_1, x_2 \in A[(x_1 < x_2) \to (f(x_1) \geq f(x_2))]$;
4. **non-decreasing** if $\forall x_1, x_2 \in A[(x_1 < x_2) \to (f(x_1) \leq f(x_2))]$.

Remark. Note that "not non-decreasing" does not imply "decreasing". For example, $f : \mathbb{R} \to \mathbb{R} \quad f(x) = x^2$ is not non-decreasing, but it is not decreasing either.

2.3.5 Growth of Functions

Definition 2.35 (Big-$\mathcal{O}$ Notation)**.** Let $g : \mathbb{N} \to \mathbb{R}^+$ be a function. The set $\mathcal{O}(g)$ is defined as

$$\mathcal{O}(g) := \{f : \mathbb{N} \to \mathbb{R}^+ \mid \exists c > 0, \exists n_0 \in \mathbb{N}, \forall n \geq n_0 (f(n) \leq cg(n))\}$$

That is, a set of functions, that for some scalar c and some threshold n_0, $f(n)$ is eventually upper-bounded by $cg(n)$. $\mathcal{O}(g)$ contains all the functions that grow slower than g, and for $f \in \mathcal{O}(g)$, we say that g is the **asymptotic upper bound** of f.

Remark. Often, we write $f(n) = \mathcal{O}(g(n))$ instead of $f \in \mathcal{O}(g)$ and $f_1(n) = f_2(n) + \mathcal{O}(g(n))$ instead of $f_1(n) = f_2(n) + h(n)$ for some $h \in \mathcal{O}(g)$.

Definition 2.36 (Big-Ω Notation)**.** Let $g : \mathbb{N} \to \mathbb{R}^+$ be a function. The set $\Omega(g)$ is defined as

$$\Omega(g) := \{f : \mathbb{N} \to \mathbb{R}^+ \mid \exists c > 0, \exists n_0 \in \mathbb{N}, \forall n \geq n_0 (f(n) \geq cg(n))\}$$

That is, a set of functions, that for some scalar c and some threshold n_0, $f(n)$ is eventually lower-bounded by $cg(n)$. $\Omega(g)$ contains all the functions that grow at least as fast as g, and for $f \in \Omega(g)$, we say that g is the **asymptotic lower bound** of f.

Theorem 2.37 (Duality of Big-$\mathcal{O}$ and Big-Ω)**.** For any functions $f : \mathbb{N} \to \mathbb{R}^+$ and $g : \mathbb{N} \to \mathbb{R}^+$, we have

$$f \in \mathcal{O}(g) \leftrightarrow g \in \Omega(f)$$

Definition 2.38 (Big-Θ Notation)**.** Let $f, g : \mathbb{N} \to \mathbb{R}^+$ be two functions. We have:

$$f \in \Theta(g) \equiv f \in \mathcal{O}(g) \wedge f \in \Omega(g)$$

Or, using the previous form of definition,

$$\Theta(g) := \{f : \mathbb{N} \to \mathbb{R}^+ \mid \exists c_1, c_2 > 0, \exists n_0 \in \mathbb{N}, \forall n \geq n_0 (c_1 g(n) \leq f(n) \leq c_2 g(n))\}$$

We say that g is the **asymptotic tight bound** of f.
Symmetric Property: $f \in \Theta(g) \leftrightarrow g \in \Theta(f)$.

Remark. The relation $f \; R \; g : f \in \Theta(g)$ is an equivalence relation.

Remark. To determine whether $f \in \mathcal{O}(g)$, $\Omega(g)$ or $\Theta(g)$, we can use the limit test:

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = \begin{cases} 0 & \Rightarrow f \in \mathcal{O}(g) \text{ but } f \notin \Omega(g) \\ c \in \mathbb{R}^+ & \Rightarrow f \in \Theta(g) \\ \infty & \Rightarrow f \in \Omega(g) \text{ but } f \notin \mathcal{O}(g) \end{cases}$$

Further, when $\lim_{n\to\infty} \frac{f(n)}{g(n)} = c \in \mathbb{R}^+$, such constant c can be used as c_1 or c_2 in the definition of Θ.

3 Counting & Probability

3.1 Fundamentals of Counting

Theorem 3.1 (Product Rule)**.** If a procedure can be broken down into k tasks, where the first task can be done in n_1 ways, and for each way of doing the first task the second task can be done in n_2 ways, and so on, then the entire procedure can be done in $n_1 n_2 \cdots n_k$ ways.

Theorem 3.2 (Product Rule for Finite Sets)**.** For some finite sets $A_1, A_2, \ldots, A_k$, the number of **ordered list** $(a_1, a_2, \ldots, a_k)$ where $a_i \in A_i$ for $i = 1, 2, \ldots, k$ is

$$|A_1| \cdot |A_2| \cdots |A_k| = \prod_{i=1}^{k} |A_i|$$

Corollary 3.3. For some finite sets $A_1, A_2, \ldots, A_k$, if all of them are identical, say, A, then a **sequence of length n with entries from A** is an ordered list $(a_1, a_2, \ldots, a_k)$ where $a_i \in A$ for $i = 1, 2, \ldots, k$. The number of such n-sequences is

$$|A|^n$$

With the Product Rule, we can solve problems like:

Example (Counting Functions)**.** Find the number of functions $f : A \to B$, provided that A and B are finite sets.
Solution: A function $f : A \to B$ can be constructed by assigning each element in A to an element in B. This can be broken down into $|A|$ tasks, where the i-th task is to assign $f(a_i) \in B$ for some $a_i \in A$. The i-th task can be done in $|B|$ ways.
By the Product Rule, the total number of ways to construct such function is

$$\boxed{|B|^{|A|}}$$

Example (Counting Injective Functions)**.** Find the number of injective functions $f : A \to B$, provided that A and B are finite sets.
Solution: First, note that if $|A| > |B|$, then there is no injective function from A to B. Now, suppose $|A| \leq |B|$. An injective function $f : A \to B$ can be constructed by several steps. First, we choose an element $a_1 \in A$. There are $|B|$ ways to choose a $f(a_1) \in B$. Next, we choose another element $a_2 \in A$. Since f is injective, there are $|B| - 1$ ways to

choose $f(a_2) \in B$. Continuing this way, we can see that the i-th task can be done in $|B| - i + 1$ ways. Therefore, the number of injective functions from A to B is

$$\boxed{|B|\,(|B|-1)(|B|-2)\cdots(|B|-|A|+1) = \frac{|B|!}{(|B|-|A|)!}}$$

provided that $|A| \leq |B|$.

Theorem 3.4 (Inclusion-Exclusion Principle)**.** For some sets $A_1, A_2, \ldots, A_n$,

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|$$

3.2 Permutations and Combinations

Definition 3.5 (Permutation)**.** A **permutation** of a set A is an ordered arrangement of all the elements of A. The number of permutations of a set with n elements is $n!$.

Definition 3.6 (r-Permutation)**.** An ***r*-permutation** of a set A is an ordered arrangement of r elements of A. The number of r-permutations of a set with n elements is denoted by

$$P(n,r) = \frac{n!}{(n-r)!}, \quad r \in [0,n]$$

Definition 3.7 (r-Combination)**.** An ***r*-combination** of a set A is an unordered selection of r elements of A. Thus, an r-combination is simply a subset of A with r elements. The number of r-combinations of a set with n elements is denoted by

$$C(n,r) = \binom{n}{r} = \frac{n!}{r!(n-r)!}, \quad r \in [0,n]$$

The notation $\binom{n}{r}$ is called a **binomial coefficient**.

Below are some useful properties of binomial coefficients:

Corollary 3.8 (Symmetry of Binomial Coefficients)**.** Let n and r be nonnegative integers with $r \leq n$. Then

$$\binom{n}{r} = \binom{n}{n-r}$$

Corollary 3.9 (Sum of Binomial Coefficients)**.** Let n be a nonnegative integer. Then

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

Corollary 3.10 (Recursive Formula of Binomial Coefficients)**.** Let $n > m \geq 1$ be integers. Then

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

Theorem 3.11 (Vandermonde's Identity)**.** Let m, n and r be nonnegative integers with r not exceeding either m or n. Then

$$\sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k} = \binom{m+n}{r}$$

Definition 3.12 (Equivalence Upon Reshuffling)**.** Two permutations are said to be **equivalent upon reshuffling** if they correspond to the same combination. For example, the permutations (a,b,c), (b,c,a) and (c,a,b) are equivalent upon reshuffling, since they correspond to the same combination $\{a,b,c\}$. The number of k-permutations that are equivalent upon reshuffling is $k!$.

3.2.1 Permutations and Combinations with Repetitions

Theorem 3.13 (r-Permutations with Repetitions)**.** The number of r-permutations of a set with n elements when repetitions are allowed is

$$n^r$$

Theorem 3.14 (Combinations with Repetitions)**.** The number of r-combinations of a set with n elements when repetitions are allowed is

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

Corollary 3.15 (Permutations of Indistinguishable Objects)**.** The number of different permutations of n objects, where there are n_1 indistinguishable objects of type 1, n_2 indistinguishable objects of type 2, ..., and n_k indistinguishable objects of type k, is

$$\prod_{i=1}^{k} \binom{n - \sum_{j=1}^{i-1} n_j}{n_i} = \frac{n!}{\prod_{i=1}^{k} n_i!}$$

or in simpler form,

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\cdots\binom{n-n_1-\cdots-n_{k-1}}{n_k} = \frac{n!}{n_1!n_2!\cdots n_k!}$$

where $\sum_{i=1}^{k} n_i = n$.

3.3 Pigeonhole Principle

Theorem 3.16 (Pigeonhole Principle)**.** If n objects are to be put into m containers, with $n > m$, then at least one container must contain more than one object.

Corollary 3.17 (Generalised Pigeonhole Principle)**.** If n objects are to be put into m containers, then at least one container must contain at least $\left\lceil \frac{n}{m} \right\rceil$ objects.

Example (Application of Pigeonhole Principle)**.** During a month of 30 days, a team plays at least one game a day, but no more than 45 games in total.
Thesis: There must exist a period of some consecutive days during which exactly 14 games are played.

Proof.
Let a_i be the number total games played before the end of the i-th day, then we have a distinct increasing sequence of integers $1 \leq a_1 < a_2 < \cdots < a_{30} \leq 45$. We also let $a_j := a_i + 14$, then we have another sequence of distinct increasing integers $15 \leq a_1 + 14 < a_2 + 14 < \ldots < a_{30} + 14 \leq 59$. Now, we have 60 integers $a_1, a_2, \ldots, a_{30}, a_1 + 14, a_2 + 14, \ldots, a_{30} + 14$ whose values are in the range of $[1, 59]$. Since there are 60 integers but only 59 possible values, by the Pigeonhole Principle, at least two of the integers are the same. Also, as the integers $a_1, a_2, \ldots, a_30$ are distinct, as so are the integers $a_1 + 14, a_2 + 14, \ldots, a_{30} + 14$, the two identical integers must be from different sequences, i.e., there exist indices i and j, such that $a_i = a_j + 14$. This means that exactly 14 games were played from the $(j+1)$-th day to the i-th day.

Q.E.D.

3.4 Fundamental Probability

Definition 3.18 (Probability Distribution)**.** Let S be a finite set, or we call the **sample space**. A **probability distribution** on S is a function $p : S \to [0, 1]$ that maps each **outcome** $x \in S$ to its probability $p(x)$, such that it satisfies:

$$\sum_{x \in S} p(x) = 1$$

Definition 3.19 (Probability of Subsets)**.** Let $p : S \to [0, 1]$ be a probability distribution on S, and let $A \subseteq S$ be a subset of S. A is also called an **event**. The **probability** of the event A is defined as

$$P(A) = \sum_{x \in A} p(x)$$

Remark. We have the following facts: (1) $P(\varnothing) = 0$ and $P(S) = 1$; (2) $P(\{x\}) = p(x)$; (3) $A \subseteq S \Rightarrow P(A) \leq P(S)$;

Definition 3.20 (Uniform Probability Distribution)**.** Let S be a finite sample space. The **uniform probability distribution** on S is defined as

$$p(x) = \frac{1}{|S|}, \quad \forall x \in S$$

Note that we have $\forall A \subseteq S : P(A) = \frac{|A|}{|S|}$. Under uniform probability distribution, to compute the probability of an event, it is equivalent to counting.

Definition 3.21 (Equal Probability Assumption)**.** Let S be a finite sample space, in the absence of any additional information, we assume that all outcomes in S are equally likely. This is called the **equal probability assumption**.

4 Graphs