MATH1064 Study Notes

University of Sydney
Semester 2, 2025
MATH1064

Happy studying!

Contents

1 Introduction to Discrete Maths and Set Theory

1.1 Introduction to Discrete Maths

Discrete maths is the study of "discrete structures", this includes objects which are:

- Countable or listable
- Distinct and unconnected.

There are two objectives of MATH1064:

1. Develop mathematical reasoning skills. This involves using **logic and proofs**, and **rigorously** (exhausting all possibilities) finding solutions to problems.
2. Study **discrete structures** and their properties including:
   - Sets and functions
   - Prime numbers and modular arithmetic
   - Graphs and networks
   - Counting and probability.

1.2 Introduction to Set Theory

1.2.1 Definitions

Definition 1 (Set)**.** A **set** S is a collection of objects, called **elements** of S.

- If x is an element of S, $x \in S$
- If not, then $x \notin S$.

Sets can be finite or infinite:

- Example (finite): $S = \{2, 3, 5\}$
- Example (infinite): $S = \{0, 1, 2, \dots\} = \mathbb{N}$

Definition 2 (Set Equivalence)**.** Two sets S and T are said to be equal if they contain the same elements, regardless of **order** or **repetition**.

- Example 1:

$$S = \{1, 1, 5, 3\}$$
$$T = \{1, 3, 5\}$$
$$S = T$$

- Example 2:

$$\begin{aligned} S &= \{-1, 0, 1, \dots\} \\ T &= \{0, 1, \dots\} \\ S &\neq T \end{aligned}$$

Definition 3 (Empty Set)**.** The **empty set** is a unique set containing no elements. $\varnothing = \{\}$.

Definition 4 (Singlton Set)**.** A **singleton set** has only one element, e.g. $S = \{x\}$ or $S = \{x, x, x\}$

1.2.2 Unpacking Sets

Sets can contain other sets as elements, inner sets are considered distinct elements even if their contents are the same as other elements in the outer set. This is because when we unpack sets, we only remove outer curly braces { }.

$$\begin{aligned} S &= \{1, 2, \{1\}\} \\ |S| &= 3 \text{ distinct elements} \end{aligned}$$

1.2.3 Sets with Properties

We can describe sets using **set builder notion** which indicates the properties of a set.

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

"The set A consists of all elements x of S such that x has property P".

Examples:

$$\begin{aligned} \{x \in \mathbb{N} \mid 3 \leq x \leq 5\} &= \{3, 4, 5\} \\ \{y \in \mathbb{Z} \mid y = 2k \text{ for some } k \in \mathbb{Z}\} &= \{\dots, -2, 0, 2, \dots\} \\ \{2z + 1 \mid z \in \mathbb{N}\} &= \{1, 3, 5, \dots\} \end{aligned}$$

1.2.4 Russel's Paradox

Define a set $T = \{S, set \mid S \notin S\}$. The set T contains any set S which does not contain itself.

Consider if $T \in T$:

- If $T \in T$: T does not satisfy the condition.
- If $T \notin T$: T does satisfy the condition, thus $T \in T$ according to our definition.

This induces a contradiction, hence demonstrating that we need **axioms** which **rigorously** state how to define and build sets.

1.2.5 Operations on Sets

Definition 5 (Union)**.** Given two sets S and T, the **union** of S and T is the set containing all elements from S and T. This is written as $S \cup T$ where $x \in S$ **OR** $x \in T$.

- Example 1: $\{1,2,3\} \cup \{2,5\} = \{1,2,3,5\}$
- Example 2: $\{0,1,2,\dots\} \cup \{0,-1,-2,\dots\} = \mathbb{Z}$

Definition 6 (Intersection)**.** Given two sets S and T, the **intersection** of S and T is the set of elements belonging to both S and T. This is written as $S \cap T$ where $x \in S$ **AND** $x \in T$.

- Example 1: $\{1,2,3\} \cap \{2,5\} = \{2\}$
- Example 2: $\{1,2,3,\dots\} \cap \{-1,-2,-3,\dots\} = \emptyset$

Multiple unions and intersections can be taken at a time.

$$\begin{aligned} \bigcup_{i=1}^{3} \{i, 2i\} &= \{1,2\} \cup \{2,4\} \cup \{3,6\} \\ &= \{1,2,3,4,6\} \end{aligned}$$

$$\begin{aligned} \bigcap_{i=1}^{3} \{i, i+1, i+2\} &= \{1,2,3\} \cap \{2,3,4\} \cap \{3,4,5\} \\ &= \{3\} \end{aligned}$$

Formally, for sets $A_1, A_2, \dots, A_i$ we define the set A_i as:

$$\bigcup_{i=1}^{\infty} A_i = \{x \mid x \in A_k \text{ for SOME } k \geq 1\}$$

That is for an infinite series of unions, x is an element that appears **at least once** in the sets A_k for $k \geq 1$.

And similarly for intersections, we define the set A_i as:

$$\bigcap_{i=1}^{\infty} A_i = \{x \mid x \in A_k \text{ for ALL } k \geq 1\}$$

That is, for an infinite series of intersections, x is an element which appears in **all** sets A_k for $k \geq 1$.

1.2.6 Subsets

Definition 7 (Subsets). A set S is a **subset** of another set T if every element of S is an element of T. This is written as $S \subset T$.

Additionally, if S is a subset of T but is not equal to T, then it is considered a **proper subset**, denoted as $S \subseteq T$.

For example,

$$S = \{2, 4, 6\}$$
$$T = \{2, 4, 6, 8\}$$
$$S \subseteq T, \text{ since } 8 \notin S$$

1.2.7 Proving Subset Relationships

To prove $S \subseteq T$, we need to:

1. Take an arbitrary element of S, which we call x
2. Show that $x \in T$

Example: Let S and T be sets where,

$$S = \{2n \mid n \in \mathbb{N}, n \geq 1\}$$
$$T = \{2^m \mid m \in \mathbb{N}\}$$

Proof. Let $x \in S$, by definition $x = 2^n$ for some $n \geq 1$.

$$x = 2^n$$
$$x = 2(2^{n-1}), \text{ rewriting } x$$

Since $n \geq 1$, $n - 1 \geq 0$ meaning that $n - 1 \in \mathbb{N} \implies 2^{n-1} \in \mathbb{N}$. Because 2^{n-1} is a natural number, we can rewrite $x = 2m$ where $m = 2^{n-1}$ as we know $m \in \mathbb{N}$, $x \in T \implies S \subseteq T$. $\square$

1.2.8 Proving Equality Relationships

To prove that $S = T$, we need a **"double containment proof"** which shows that both sets have the same elements, that is:

1. Every $x \in S$ also satisifes $x \in T$
2. Every $x \in T$ also satisfies $x \in S$

Example: Let S and T be sets where,

$$S = \{2m + 1 \mid m \in \mathbb{Z}\}$$
$$T = \{2r - 1 \mid r \in \mathbb{Z}\}$$

Proof. Show $S \subseteq T$. Let $x \in S$, then $x = 2m + 1$ for some $m \in Z$.
Let $r = m + 1$.

$$\begin{aligned}
x &= 2m + 1 \\
x &= 2m + 2 - 1, \text{ rewriting } x \\
x &= 2(m + 1) - 1, \text{ notice } m + 1 = r \\
x &= 2r - 1, \text{this is the same as } x \in T
\end{aligned}$$

$x = 2r - 1$ for some $r \in \mathbb{Z}$. Thus, $x \in T \implies S \subseteq T$. □

Proof. Show $T \subset S$. Let $x \in T$, then $x = 2r - 1$ for some $r \in \mathbb{Z}$.
Let $m = r - 1$.

$$\begin{aligned}
x &= 2r - 1 \\
x &= 2r - 2 + 1 \\
x &= 2(r - 1) + 1 \\
x &= 2m + 1
\end{aligned}$$

$x = 2m + 1$ for some $m \in \mathbb{Z}$. Thus, $x \in S \implies T \subseteq T$. □

Since $S \subseteq T$ and $T \subseteq S$, the two sets must have the same elements and are equal, $S = T$.

1.3 More Set Theory

1.3.1 Cardinality

The **cardinality** of a set S in a rough sense refers to the size of S, i.e. the no. of elements in S.

- If S is finite, then $|S|$ is the number of distinct elements in S.
- If S is infinite, then we write $|S| = \infty$.

Note that there can be **different infinite cardinalities**, or sizes of infinities. A basic example of this is the set of natural numbers $\mathbb{N}$ compared to the set of real numbers $\mathbb{R}$.

1.3.2 Set Differences

Definition 8 (Set Difference)**.** Given two sets S and T, the **set difference** is the set of elements $x \in S$ and $x \notin S$. This is written as $S \backslash T$ or $S - T$.

- Example 1: $\{1, 2, 3\} \backslash \{2, 5\} = \{1, 3\}$
- Example 2: $\{0, 1, 2, \dots\} \backslash \{0, -1, -2, \dots\} = \{1, 2, \dots\}$
- Example 3: $\mathbb{N} \backslash \mathbb{Z} = \emptyset$

1.3.3 Universal Set

Definition 9 (Universal Set)**.** Let $\mathbb{U}$ be some **universal set** which is the set containing all elements of which other sets are subsets. The universal set is context dependent.

- $\mathbb{U} = \mathbb{Z}$, if working with number theory
- $\mathbb{U} = \mathbb{R}^2$, if working with plane geometry

1.3.4 Complementary Set

Definition 10 (Complement)**.** For a set $S \subseteq \mathbb{U}$, the **complement** of $S \in \mathbb{U}$ is given by $x \in \mathbb{U}$ where $x \notin S$. This is written as $\overline{S}$ or $S^{\complement}$.

In other words, $\overline{S}$ is the set containing all elements not in S, where the range of elements considered is constrained by $\mathbb{U}$. This resolves the Russel Paradox.

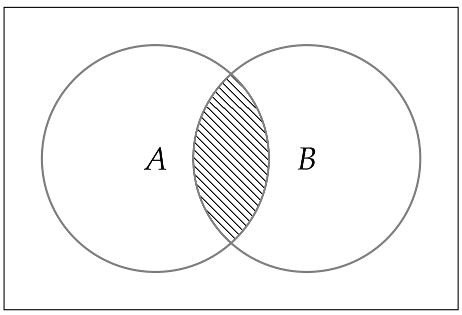
For example, if $\mathbb{U} = \mathbb{Z}$:

- $\overline{\{1, 2, 3\}} = \{\dots, -1, 0, 4, \dots\}$
- $\overline{\{x \in \mathbb{Z} \mid x > 0\}} = \{x \in \mathbb{Z} \mid x < 0\}$
- $\overline{\mathbb{Z}} = \varnothing$

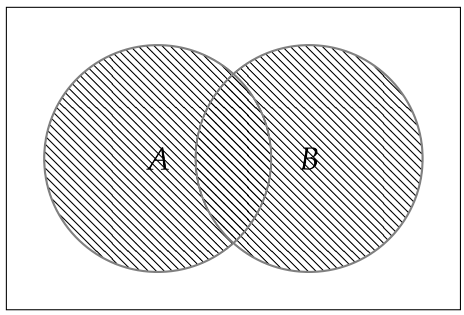
1.3.5 Venn Diagrams

Venn Diagrams are tools used to visualise relationships between sets.

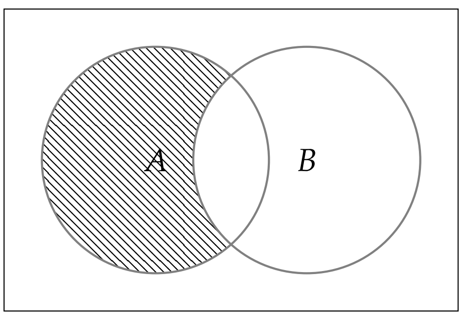
$A \cap B$



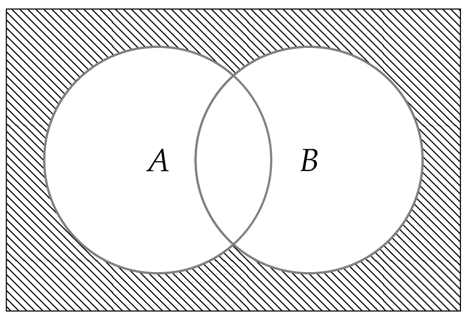
$A \cup B$



$A \backslash B$



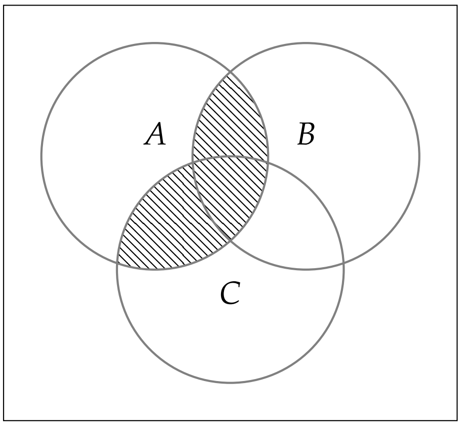
$\overline{A \cup B}$



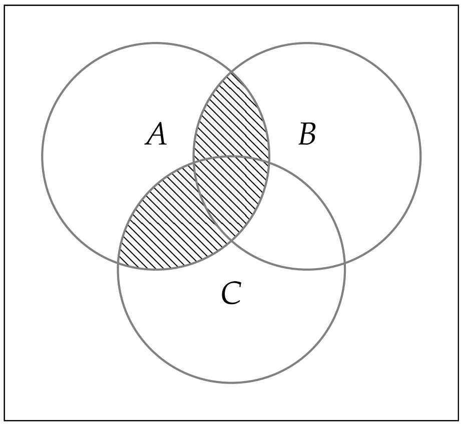
Venn diagrams are useful for intuition and can be used to guide proofs, but are not sufficient as rigorous proofs in of themselves.

Example: Prove if $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

$A \cap (B \cup C)$



$(A \cap B) \cup (A \cap C)$



Proof. Double Containment. First, show $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.
Let $x \in A \cap (B \cup C)$:

$$\begin{aligned} \text{Then } x \in A \text{ and } x \in (B \cup C) \\ x \in (B \cup C) \implies x \in B \text{ or } x \in C \\ \text{if } x \in B, x \in (A \cap B) \implies x \in (A \cap B) \cup (A \cap C) \\ \text{if } x \in C, x \in (A \cap C) \implies x \in (A \cap C) \cup (A \cap B) \\ \implies A \cup (B \cap C) \subseteq (A \cap B) \cup (A \cap C) \end{aligned}$$

This proof works because we know that if $x \in (A \cap B)$, then suppose we expand the set $(A \cap B)$ by including another arbitrary set, say $(A \cap C)$. We can implicitly assume x is an element of $(A \cap B) \cup (A \cap C)$ since we are simply expanding the scope of the set.

Second, show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.
Let $x \in (A \cap B) \cup (A \cap C)$:

$$\begin{aligned} \text{Then } x \in A \text{ and } x \in B \\ \implies x \in (B \cup C) \\ \implies x \in A \cap (B \cup C) \end{aligned}$$

$$
\begin{aligned}
\text{Then } x \in A \text{ and } x \in C \\
\implies x \in (C \cup B) \\
\implies x \in A \cap (C \cup B)
\end{aligned}
$$

Thus, $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$, indicating that both sets are equal.

$\square$

1.3.6 Set Identities

- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- $A \cap (A \cup B) = A$

2 Week 2

2.1 Power Sets and Cartesian Planes

2.1.1 Power Set

Definition 11 (Power Set)**.** For a set S the **power set** of S is the set which contains all possible subsets of S. This is denoted as $P(S) = \{A \mid A \subseteq S\}$.

For example,

- $S = \{a, b\} \implies P(S) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
- $S = \emptyset \implies P(S) = \{\emptyset\}$
- $S = \{1, 2, 3\} \implies P(S) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

Theorem 1 (Cardinality of the Power Set)**.** *Let S be a finite set with $|S| = n$, then $|P(S)| = 2^n$*

2.1.2 Cartesian Product

Definition 12 (Cartesian Product)**.** For two sets A and B, the cartesian product $A \times B$ is given by the set of ordered pairs, $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

Note: in ordered pairs, the order of elements, and repetition matter (like cartesian coordinates).

Example: $A = a, b.B = 1, 2$

- $A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2)\}$
- $B \times A = \{(1, a), (1, b), (2, a), (2, b)\}$

Theorem 2 (Cardinality of Cross Product)**.** *The cardinality of the cross product of two sets A and B is given by $|n \times m|$ where $|A| = n$ and $|B| = m$.*

The cross product of an empty set is always the empty set. For example, if $A = \emptyset$, $B = \{1, 2\}$, then $A \times B = \emptyset$.

$A \times B = B \times A \iff A = B$ or when A or $B = \emptyset$.

Proof. If A or $B = \emptyset$, then there is nothing to prove.

Otherwise, assume $A \times B = B \times A$.

Show $A \subseteq B$.
Let $x \in A$ and choose some $y \in B$:

$$\begin{aligned} \text{Then } & (x,y) \in A \times B \\ A \times B = B \times A \implies & (x,y) \in B \times A \\ \implies & x \in B \\ \implies & A \subseteq B \end{aligned}$$

Show $B \subseteq A$.

$$\begin{aligned} & (y,x) \in B \times A \\ A \times B = B \times A \implies & (y,x) \in A \times B \\ \implies & y \in A \\ \implies & B \subseteq A \end{aligned}$$

Therefore, $A = B$ by double containment.

$\square$

2.1.3 Functions

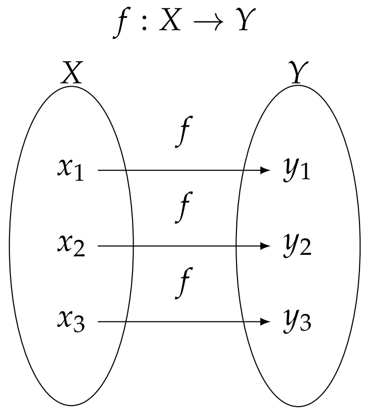
Definition 13 (Function)**.** Given two sets X and Y, the function f from X to Y, written as $f : X \to Y$, maps each $x \in X$ to exactly one $y \in Y$ (see vertical line test).

Important Criteria:

- Every $x \in X$ maps somewhere, i.e. $X \to Y$.
- Every $x \in X$ maps to **at most one** $y \in Y$.

Examples:

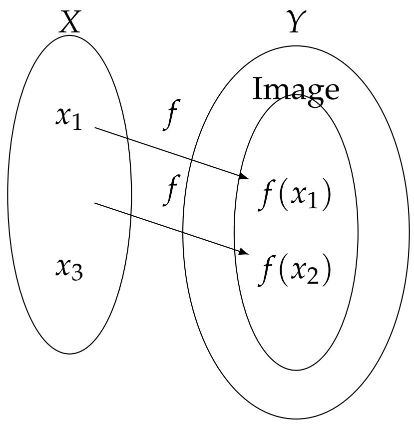
- $f : \mathbb{N} \to \mathbb{N}, f(n) = n!$ is a function
- $f : \mathbb{R} \to \mathbb{R}, f(x) = \ln x$ is not a function as $f(x)$ is undefined for $x < 0$
- $f : \mathbb{Q} \to \mathbb{N}, f(\frac{n}{m}) = n$ is not a function as there are multiple ways to write the same input with different outputs, e.g. $\frac{3}{2} = 3$ but $\frac{6}{4} = 6$.



2.1.4 Function Terminology

Let $f : X \to Y$ be a function. Then we say:

- X is called the **domain** of f
- Y is called the **co-domain** of f
- $f(x) \in Y$ is called the **image** of X (also called range).



Similarly, the **pre-image** of a y is the set of all input values which map to the co-domain Y. This is written as $f^{-1}(y) = \{x \in X \mid f(x) = y\} \subseteq X$. In essence, it explains where does y come from under the function $f(x)$.

2.1.5 Identity Function

Definition 14 (Identity Function)**.** The **identity function** is a function which maps a set to iteself. For any set S, $i_x : X \to X$ is defined by $i_x(a) = a, a \in X$.

2.1.6 Floors and Ceilings

Definition 15 (Floor)**.** For $x \in \mathbb{R}$, the floor of x is the unique integer n such that $n \leq x \leq n+1$. In essence, it is "rounding down" x in terms of value. It is written as $\lfloor x \rfloor$.

Definition 16 (Ceiling)**.** For $x \in \mathbb{R}$, the ceiling of x is the unique integer m such that $m-1 \leq x \leq m$. In essence, it is "rounding up" x in terms of value. It is written as $\lceil x \rceil$.

Note: both floor and ceiling are functions $f : \mathbb{R} \to \mathbb{Z}$. Additionally, for $x < 0$, the rounding up/down of these functions are reversed.

Examples:

- $\lfloor 2.5 \rfloor = 2$
- $\lfloor -2.5 \rfloor = -3$
- $\lceil 2.5 \rceil = 3$
- $\lceil -2.5 \rceil = -2$

3 Week 3

4 Week 4

5 Week 5