Course 50.050/50.550
Advanced Algorithms

Week 1 – Lecture L01.01

SINGAPORE UNIVERSITY OF
TECHNOLOGY AND DESIGN

About this course

This course covers relevant foundations of **discrete mathematics** and other related mathematical areas, so that we can understand **advanced algorithms**, and how diverse mathematical ideas are used in **algorithm design**.

- Emphasis on understanding the underlying mathematics for algorithms beyond those covered in 50.004 (Algorithms).

Course Textbook:

- "Discrete Mathematics and Its Applications" (6th Edition), by Kenneth Rosen

Other Reference Books:

- "Concrete Mathematics: A Foundation for Computer Science" (6th Edition), by Donald Knuth, Oren Patashnik, and Ronald Graham.
- "Mathematics for Computer Science" by Eric Lehman, F. Thomson Leighton, and Albert R. Meyer.

Course materials, such as lecture slides, cohort class slides, and homework, will be available on eDimension.

Teaching Team

Course Instructor:

- Prof. Ernest Chong
  - ernest_chong@sutd.edu.sg

Teaching assistants:

- Benjamin Drabkin (research fellow, voluntary TA role)
  - benjamin_drabkin@sutd.edu.sg
- Tiansi Li (research fellow, voluntary TA role)
  - tiansi_li@sutd.edu.sg
- Jingyi Xu (research fellow, voluntary TA role)
  - jingyi_xu@sutd.edu.sg

We shall be using **Ed Discussion** to help with your questions.

Grading

1D Project:	10% (Week 8)
Homework sets:	20% (for 6 HW sets)
4 Mini-quizzes:	15% (Weeks 3, 6, 10, 12)
Midterm Exam:	25% (Week 8)
Final Exam:	30% (Week 14)

Mini-quizzes:

- Best 3 of 4 mini-quiz scores will be counted towards final grade.
- Each mini-quiz is 15mins long (held during your cohort class).

Homework:

- Typically due on Fridays, 1pm.
- Homework submission is via eDimension.
- Graded homework will be returned one week after submission.
- Suggested solutions to homework will be uploaded onto eDimension shortly before graded homework is returned.

Homework Grading

Each homework set is worth 20 marks.

- You should try your best not to spend more than one full afternoon to complete each homework set.
  - The good thing about homework sets is that you can spend as much time on them as you want.
  - If you are stuck with some homework question, don't give up!
- You are strongly encouraged to discuss the questions with your friends, as well as discuss on **Ed Discussion**. However, you must write up your own solutions.
- See eDimension for details on policy for late HW submission.
- Issues with homework grading must be raised within one week upon receiving the graded homework.

Outline of Lecture

- Sets, set operations
- Injections, surjections and bijections
- Countable sets vs uncountable sets
- Different "sizes" of infinities

What is a set?

A set is a well-defined collection of **distinct** objects.

- **Notation:** Given some distinct objects, we have to place them in between curly brackets $\{\ \}$ to denote the set comprising these objects.
- **Example:** The set of all positive integers strictly below 10:

$$\{1,\quad 2,\quad 3,\quad 4,\quad 5,\quad 6,\quad 7,\quad 8,\quad 9\}$$

- **Example:** The following specific set of ASCII strings:

$$\{\text{'}\texttt{A}\text{'}, \text{'}\texttt{x+y=z}\text{'}, \text{'}\texttt{Advanced Algorithms!}\text{'}, \text{'}\texttt{hello}\text{'}, \text{'}\texttt{ehofsjd}\text{'}\}$$

We can also give a description of the set.

- **Example:** The set of all functions $f : A \to B$ for some fixed sets A and B.
- **Example:** The set of all non-empty ASCII strings.

Question: What is the difference between 0 and $\{0\}$?

Answer: 0 is a number, while $\{0\}$ is a set that contains a single number, the number 0.

Basic properties of sets

A set is **unordered**.

- **Example:** $\{1, 2, 3\}$ and $\{3, 2, 1\}$ are the exact same set!

The objects contained in a set are called elements.

- **Example:** The set $\{2, 3, 5\}$ has three elements.
  - The three elements of this set are $2, 3, 5$.

Elements of a set can be sets themselves.

- **Example:** The set $\{\{2, 3\}, \{5\}\}$ has two elements.
  - Both elements are sets themselves. They are $\{2, 3\}$ and $\{5\}$.
- **Example:** The set $\{1, \{2, 3\}, \{5\}\}$ has three elements.
  - Elements: one number and two sets of numbers.

An empty set, denoted by $\emptyset$ (or $\varnothing$), is a set with no elements.
Question: What is the difference between $\emptyset$ and $\{\emptyset\}$ and $\{\{\emptyset\}\}$?
Answer: $\emptyset$ is a set with no elements.
$\{\emptyset\}$ is a set with one element, the empty set $\emptyset$.
$\{\{\emptyset\}\}$ is a set with one element, the set $\{\emptyset\}$ consisting of the empty set as its single element.

Naming conventions for sets

We can give names to sets.

- **Example:** We can say "Let $X := \{a, b, c\}$ be a set." Then this set X has three elements. They are a, b, c.
  - Here, the symbol "$:=$" indicates we are defining something.
  - Uppercase English letters are usually used to denote sets.
  - Lowercase English letters are usually used to denote elements.

The empty set $\emptyset$ is sometimes also called the null set.

- **Alternative notation:** $\emptyset$ is also sometimes written as $\{\}$.

A set with one element is called a singleton (or singleton set).

- **Example:** $\{\emptyset\}$ is a singleton consisting of the single element $\emptyset$.

A set with two elements is called a pair (or unordered pair).

Warning: Some authors may have different "writing" conventions.

- **Example:** Some authors write $\{1, 1, 2, 2, 3, 3\}$ and $\{1, 2, 3\}$ to mean the exact same set, consisting of three elements $1, 2, 3$.
  - Similar: When you define a Python set and indicate repeated elements, those repeats are automatically ignored.

Basic notation related to sets

Suppose X and Y are sets.

- We write $x \in X$ to mean that x is an element of X.
- We write $x \notin X$ to mean that x is **not** an element of X.
- We write $X \subseteq Y$ to mean that X is a subset of Y.
  - This means that every element of X is also an element of Y.
  - It is possible that $X = Y$, i.e. X and Y could be the same set.
- We write $X \nsubseteq Y$ to mean that X is **not** a subset of Y.
  - This means that there is some element of X that is not an element of Y.
- We write $X \subsetneq Y$ to mean that X is a subset of Y that is not identically Y.
  - Same meaning as $X \subseteq Y$ **and** $X \neq Y$.
  - We say that X is a proper subset of Y.

Warning: Some authors write "$X \subset Y$" instead of "$X \subseteq Y$" to mean the same thing: X is a subset of Y, and possibly $X = Y$.

Set operations

Suppose X and Y are sets.

- **Set union**: $X \cup Y$ is the set containing those elements that are in X or Y or both.
  - e.g. if $X = \{1,2\}$ and $Y = \{2,3\}$, then $X \cup Y = \{1,2,3\}$.
- **Set intersection**: $X \cap Y$ is the set containing only those elements that are in both X and Y.
  - e.g. if $X = \{1,2\}$ and $Y = \{2,3\}$, then $X \cap Y = \{2\}$.
  - We say X and Y are disjoint if $X \cap Y = \emptyset$.
- **Set difference**: $X - Y$ is the set containing those elements in X that are not in Y.
  - e.g. if $X = \{1,2\}$ and $Y = \{2,3\}$, then $X - Y = \{1\}$.
  - Can you see why $X - Y$ and $X - X \cap Y$ are the same set?
- **Set exclusion**: If $Y \subseteq X$, then $X \backslash Y$ is the set $X - Y$.
  - When we write $X \backslash Y$, we are implicitly assuming that $Y \subseteq X$.
  - e.g. if $X = \{a,b,c\}$ and $Y = \{a,c\}$, then $X \backslash Y = \{b\}$.
- **Symmetric difference**: $X \Delta Y$ is the set containing those elements that are in either X or Y, but not in both X and Y.
  - $X \Delta Y$ is exactly the same as $(X \cup Y) \backslash (X \cap Y)$.
  - e.g. if $X = \{1,2\}$ and $Y = \{2,3\}$, then $X \Delta Y = \{1,3\}$.
  - Symmetric difference is also called **disjunctive union**.

Complements of sets

Frequently, we study sets not in isolation, but as subsets of some "bigger" set, which we call the universal set or the ground set.

- What is considered the universal set depends on the context.
- **Example:** If we consider sets consisting of integers, then our universal set could be $\mathbb{Z}$, the set of all integers.

Once it is clear from the context what our universal set U is, then we can consider complements of sets.

Definition: The complement of a set X is the set $U \backslash X$.

- **Notation:** The complement of X is denoted by $\overline{X}$ or X^c.
- **Note:** Complements of sets makes sense only when it is clear what the universal set U is.

Fact: Given any two sets A and B contained in the same universal set, we always have the following two set identities:

- $\overline{A \cup B} = \overline{A} \cap \overline{B}$ and $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
- This is known as **De Morgan's laws** (for sets).

Important examples of sets of numbers

- $\mathbb{Z}$ denotes the set of all **integers**.
  - $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.
- $\mathbb{Z}^+$ denotes the set of all **positive integers**.
  - $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$.
- $\mathbb{N}$ denotes the set of all **natural numbers**.
  - $\mathbb{N}$ is also the set of all **non-negative integers**.
  - $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.
  - **Warning:** Some authors write $\mathbb{N}$ to mean $\mathbb{Z}^+$.
- $\mathbb{Q}$ denotes the set of all **rational numbers**.
  - $\mathbb{Q}^+$ denotes the set of all positive rational numbers.
- $\mathbb{R}$ denotes the set of all **real numbers**.
  - $\mathbb{R}^+$ denotes the set of all positive real numbers.
  - $\mathbb{R}_{\geq 0}$ denotes the set of all non-negative real numbers.
- $\mathbb{C}$ denotes the set of all **complex numbers**.
  - **Warning:** The notation $\mathbb{C}^+$ does not quite make sense.
  - **Note:** "positive" always means "> 0".
  - What does it mean for a complex number $x + iy$ to be positive?

Are there other kinds of numbers? Yes! More in Week 9.

Building new sets from existing sets

Question: How do we "construct" $\mathbb{Q}$?

- We could define $\mathbb{Q}$ as the **set** $\mathbb{Q} := \{\frac{p}{q} | p \in \mathbb{Z}, q \in \mathbb{Z}^+\}$.
  - e.g. we treat $\frac{1}{2}, \frac{2}{4}, \frac{3}{6}$ as being the same element in $\mathbb{Q}$.
- In other words, we built $\mathbb{Q}$ from the two sets $\mathbb{Z}$ and $\mathbb{Z}^+$.

Set-builder notation: We can define a set X via the "format"

$$X := \left\{ \text{what the elements in } X \text{ look like} \middle| \text{what conditions must hold} \right\}$$

- **Example:** $\{x | x \in \mathbb{R}, x > 5\}$ denotes the set of all x such that the conditions "x is a real number", and "$x > 5$" are satisfied.
- We could also write $\{x | x \in \mathbb{R}, x > 5\}$ as $\{x \in \mathbb{R} | x > 5\}$.
- **Example:** $\{x \in \mathbb{Z} | x$ is a multiple of $5\}$ is another set.

For this set-builder notation, we could also use ":" in place of "|".

- **Example:** $\mathbb{R}^+ := \{x : x \in \mathbb{R}, x > 0\} = \{x \in \mathbb{R} : x > 0\}$.
- **Example:** $\mathbb{C} := \{x + y\sqrt{-1} : x, y \in \mathbb{R}\}$.

Power sets

Definition: Given a set X, the power set of X is the set containing all possible subsets of X.

- The power set of X is denoted by $\mathcal{P}(X)$ or 2^X.
- **Example:** The power set of the set $\{1, 2, 3\}$ is

$$\mathcal{P}(\{1,2,3\}) = \Big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\Big\}.$$

Theorem: Let $n \in \mathbb{N}$, and let X be a set with n elements. Then, the power set $\mathcal{P}(X)$ has 2^n elements.

Proof: What could a subset Y of X look like? For every element $x \in X$, either x is in Y or x is not in Y; there are two possibilities for each x. Since X is a set with n elements, there are a total of 2^n different possibilities for what Y could contain. $\square$

- **Example:** $\mathcal{P}(\{1,2,3\})$ has $2^3 = 8$ elements.
- **Example:** $\mathcal{P}(\emptyset) = \{\emptyset\}$ has one element.
- **Example:** $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$ has two elements.

Cardinality of sets

Definition: The cardinality of a set is its number of elements.

- **Notation:** The cardinality of a set X is denoted by $|X|$.
  - The set $\mathcal{P}(\{1,2,3\})$ has cardinality $2^3 = 8$.
  - The set $\{1,2,3,4,5,6,7,8\}$ has cardinality 8.
  - The set $\{0,2,4,6,8,10,12,14\}$ also has cardinality 8.

Question: Given two sets A and B, how to tell whether $|A| = |B|$?

- Intuitively, A and B have the same cardinality if the elements of A "match up" with the elements of B.

$$
\begin{array}{cccccccccc}
\Big\{ & \emptyset, & \{1\}, & \{2\}, & \{3\}, & \{1,2\}, & \{1,3\}, & \{2,3\}, & \{1,2,3\} & \Big\} \\
 & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\
\Big\{ & 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8 & \Big\} \\
 & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\
\Big\{ & 0, & 2, & 4, & 6, & 8, & 10, & 12, & 14 & \Big\}
\end{array}
$$

- We can make this intuitive "matching up" idea precise by considering a **function** $f : A \to B$.

Quick recap: What exactly is a function?

A function can be written in the form $f : X \to Y$.

- X and Y are sets. We give the name "f" to this function.
- We can think of f as a map from set X to set Y.
  - Every element $x \in X$ is mapped to some element in Y that we denote by $f(x)$. We call $f(x)$ the image of f at x, or the value of f at x, or the output of f at x, or the output value of f at x.
  - We say that f is a function from X to Y.
- The **domain** of f is X, while the **codomain** of f is Y.
  - **Note:** The codomain of f may be different from the **range** of f.
  - The range (or image) of f is the set of possible output values of f.

Example: $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ is the square function.

- When defining the mapping of f, we can write $x \mapsto x^2$ to mean exactly the same as $f(x) = x^2$ (for all x in the domain).
- This "maps to" symbol $\mapsto$ allows us to define functions without necessarily having to give a name to the function.
  - $x \mapsto x^2$ with domain $\mathbb{R}$ and codomain $\mathbb{R}$ is the square function.

Note: Two functions with the same domain, codomain and mapping, are the same function, even if they have different names.

Injections, surjections, bijections

Definition: Let $f : X \to Y$ be a function.

- f is surjective (or onto) if its range equals its codomain.
  - i.e. every $y \in Y$ is an output value of f at some $x \in X$.
- f is injective (or one-to-one) if f maps distinct elements of X to distinct elements of Y.
  - i.e. the only way for $f(x_1) = f(x_2)$ to be true is if $x_1 = x_2$.
- f is bijective if f is both injective and surjective.
- An injection/surjection/bijection is a function that is injective/surjective/bijective.

Fact: If f is a bijection from X to Y, then there exists a bijection from Y to X, called the inverse of f. This inverse is denoted by f^{-1}.

Examples:

- $f_1 : \mathbb{R} \to \mathbb{R}$ given by $x \mapsto x^2$ is neither injective nor surjective.
- $f_2 : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ given by $x \mapsto x^2$ is a bijection.
  - Its inverse f_2^{-1} (from $\mathbb{R}_{\geq 0}$ to $\mathbb{R}_{\geq 0}$) is given by $x \mapsto \sqrt{x}$.
- $f_3 : \mathbb{R} \to \mathbb{R}_{\geq 0}$ given by $x \mapsto x^2$ is surjective but not injective.
- $f_4 : \mathbb{R}_{\geq 0} \to \mathbb{R}$ given by $x \mapsto x^2$ is injective but not surjective.

Counting the number of elements in sets

Note: The cardinality of a finite set must be a number in $\mathbb{N}$.

- Conversely, if a set X has cardinality $|X| = n$ for some $n \in \mathbb{N}$, then X must be a finite set.
- Thus, we define a set X to be finite if $|X| = n$ for some $n \in \mathbb{N}$.

Definition: Given $n \in \mathbb{N}$ and a set X, we say X has cardinality n if there exists a **bijection** $f : X \to \{1, 2, \dots, n\}$.

- **Special case:** $X = \emptyset$ is the only possible set with cardinality 0.
- **Note:** The set $\{1, 2, \dots, n\}$ has cardinality n.

Definition: Two sets X and Y are said to have the same cardinality if there exists a **bijection** $f : X \to Y$.

Question: What does it mean when a set is **not** finite?

- A set that is not a finite set is called an infinite set.

Question of the day: Do all infinite sets have the same cardinality?

- Can we say that every infinite set has the same cardinality ∞?

Countably infinite sets

A set is called countably infinite if it has the same cardinality as $\mathbb{N}$.

- Intuitively, a set X is countably infinite if its elements can be matched up exactly with the non-negative integers.
  - We can think of this "matching up" as a sequence $x_0, x_1, x_2, \ldots$ (with indices in $\mathbb{N}$) that has all elements in X, without repeats.

Example: $\mathbb{Z}^+$ is countably infinite, since the function $f : \mathbb{N} \to \mathbb{Z}^+$ given by $x \mapsto x + 1$ is a bijection.

- We can think of a sequence $x_0, x_1, x_2, \ldots$, where $x_k := k + 1$.

More generally, a set X is countably infinite if we can construct a sequence $x_0, x_1, x_2, \ldots$, whose terms are indexed by $\mathbb{N}$, such that:

- Every x_i in this sequence is an element of X.
- Every $x \in X$ is one of the terms of the sequence.
- There are no repeated terms in the sequence.

Remark: Since there is a bijection from $\mathbb{N}$ to $\mathbb{Z}^+$, a set X is countably infinite if we can equivalently construct a sequence $x_1, x_2, x_3, \ldots$, whose terms are indexed by $\mathbb{Z}^+$, such that the above three conditions hold.

Countably infinite and countable sets

Example: Let $A := \{2n+1 : n \in \mathbb{N}\}$ and $B := \{2n : n \in \mathbb{N}\}$.

- $A = \{\text{odd integers in } \mathbb{N}\}$, $B = \{\text{even integers in } \mathbb{N}\}$.
- Both A and B are countably infinite sets.
- **Interesting Fact:** A and B are disjoint subsets of $\mathbb{N}$.
  - A and B have the same cardinality as $\mathbb{N}$, yet both are proper disjoint subsets of $\mathbb{N}$, whose union $A \cup B$ equals $\mathbb{N}$.

Consequence: It is possible for a set X to be partitioned into two disjoint subsets A and B, both with the same cardinality as X.

- i.e. it is possible to split one set into two sets of the same size.
- Counter-intuitive things happen when we deal with infinite sets.

Question: Can you explain why $\mathbb{Z}$ has the same cardinality as $\mathbb{N}$?

- Can you write down an explicit bijection from $\mathbb{N}$ to $\mathbb{Z}$?

Question: Do you think $\mathbb{Q}$ has the same cardinality as $\mathbb{N}$?

Definition: A set is countable if it is finite or countably infinite.

- A set if uncountable if it is not countable.

Question: Are there uncountable sets?

Are there uncountable sets?

Answer: Yes. We claim that the real interval $(0, 1)$ is uncountable.

Suppose on the contrary that $(0, 1)$ is countable. This means we can have a sequence $r_0, r_1, r_2, \ldots$ consisting of all real numbers in $(0, 1)$.

Key Idea 1: Consider the decimal representations of $r_0, r_1, r_2, \ldots$

$$\begin{aligned} r_0 &= 0.d_{0,0}d_{0,1}d_{0,2}d_{0,3}\ldots \\ r_1 &= 0.d_{1,0}d_{1,1}d_{1,2}d_{1,3}\ldots \\ r_2 &= 0.d_{2,0}d_{2,1}d_{2,2}d_{2,3}\ldots \\ r_3 &= 0.d_{3,0}d_{3,1}d_{3,2}d_{3,3}\ldots \\ &\vdots \qquad \vdots \end{aligned}$$

$d_{i,j}$ is the $(j+1)$-th decimal digit of r_i

e.g. if $r_0 = 0.2357\ldots$, then:
$d_{0,0} = 2, d_{0,1} = 3, d_{0,2} = 5, d_{0,3} = 7, \ldots$

Let $r \in (0, 1)$ have decimal representation $r = 0.a_0a_1a_2\ldots$, where

$$a_i = \begin{cases} 2, \text{if } r_{i,i} = 1; \\ 1, \text{if } r_{i,i} \neq 1. \end{cases}$$

Key Idea 2: The $(i+1)$-th decimal digit of r and r_i are different.

- This means that r cannot appear in our sequence, yet r is an element of the real interval $(0, 1)$. Contradiction!

Different sizes for infinity

Definition: Given sets X and Y, we have $|X| \leq |Y|$ if there exists an injection from X to Y.

> ***Remark:*** *To show that $|X| < |Y|$, we must show that there is an injection from X and Y AND show that there is no possible bijection from X to Y.*

So far, we have seen several infinite sets: $\mathbb{N}$, $\mathbb{Z}^+$, etc.

- Countably infinite sets have the same cardinality as $\mathbb{N}$.
- We denote the cardinality $|\mathbb{N}|$ by $\aleph_0$ (read as aleph-nought).

We have also seen that $(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$ is uncountable.

Fact: $\mathbb{R}$ has the same cardinality as the real interval $(0, 1)$.

- The map $x \mapsto \tan(\pi x - \frac{\pi}{2})$ is a bijection from $(0, 1)$ to $\mathbb{R}$.
- **Consequence:** The set $\mathbb{R}$ of real numbers is uncountable.
- We denote the cardinality $|\mathbb{R}|$ by $2^{\aleph_0}$.

The continuum hypothesis is a statement in set theory that says:

$$\text{There is no set } X \text{ satisfying } |\mathbb{N}| < |X| < |\mathbb{R}|.$$

Theorem: (Gödel, 1940) The continuum hypothesis is a statement that **cannot be proven**, i.e. it is not true, and it is not false!

Infinitely many sizes for infinity

Our exploration of infinite sets so far..

- $\mathbb{N}$ has cardinality $\aleph_0$, $\mathbb{R}$ has cardinality $2^{\aleph_0}$. We also know $\aleph_0 < 2^{\aleph_0}$.
- These cardinalities $\aleph_0$ and $2^{\aleph_0}$ are examples of cardinal numbers.

Theorem: The sets $\mathbb{R}$ and $\mathcal{P}(\mathbb{N})$ have the same cardinality.

- Proof is out of syllabus, although not too hard.

Theorem: For any set X, we have $|X| < |\mathcal{P}(X)|$.

- Russell's paradox: The "set of all sets" cannot contain itself.
- More formally, a set cannot possibly contain its power set.

Consequence:

$$|X| < |\mathcal{P}(X)| < |\mathcal{P}(\mathcal{P}(X))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(X)))| < \cdots .$$

Note: The set of cardinal numbers extends the set of natural numbers:
$0, 1, 2, 3, \ldots ; \aleph_0, \aleph_1, \aleph_2, \aleph_3, \ldots$

- Given $n \in \mathbb{N}$, we define $\aleph_{n+1}$ to be the next smallest possible cardinal number after $\aleph_n$.
- The unprovability of the continuum hypothesis implies that we are unable to prove whether "$\aleph_1 = 2^{\aleph_0}$" is true or false.

Summary

- Sets, set operations
- Injections, surjections and bijections
- Countable sets vs uncountable sets
- Different "sizes" of infinities