1. Basic set theory

- sets
- mathematical induction
- functions
- cardinality

Sets

Definition 1.1 A **set** is a collection of objects called elements or members. A set with no objects is called the **empty set** and is denoted by $\emptyset$ (or sometimes by $\{\}$).

notation:

- $a \in S$ means that 'a is an element in S'
- $a \notin S$ means that 'a is not an element in S'
- $\forall$ means 'for all'
- $\exists$ means 'there exists'
- $\exists!$ means 'there exists a unique'
- $\implies$ means 'implies'
- $\iff$ means 'if and only if'

Definition 1.2

- A set A is a **subset** of a set B if $x \in A$ implies $x \in B$, denoted as $A \subseteq B$.
- Two sets A and B are **equal** if $A \subseteq B$ and $B \subseteq A$, denoted as $A = B$.
- A set A is a **proper subset** of B if $A \subseteq B$ and $A \neq B$, denoted as $A \subsetneq B$.

set building notation: we write

$$\{x \in A \mid P(x)\} \quad \text{or} \quad \{x \mid P(x)\}$$

to mean 'all $x \in A$ that satisfies property $P(x)$'

examples:

- $\mathbf{N} = \{1, 2, 3, 4, \ldots\}$: the set of natural numbers
- $\mathbf{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$: the set of integers
- $\mathbf{Q} = \{m/n \mid m, n \in \mathbf{Z},\ n \neq 0\}$: the set of rational numbers
- $\mathbf{R}$: the set of real numbers

it follows that $\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R}$

Definition 1.3 Given sets A and B:

- The **union** of A and B is the set $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$.
- The **intersection** of A and B is the set $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.
- The **set difference** of A and B is the set $A \setminus B = \{x \in A \mid x \notin B\}$.
- The complement of A is the set $A^c = \{x \mid x \notin A\}$.
- A and B are **disjoint** if $A \cap B = \emptyset$.

Theorem 1.4 *De Morgan's Laws.* If A, B, C are sets, then

- $(B \cup C)^c = B^c \cap C^c$;
- $(B \cap C)^c = B^c \cup C^c$;
- $A \setminus (B \cup C) = A \setminus B \cap A \setminus C$;
- $A \setminus (B \cap C) = A \setminus B \cup A \setminus C$.

we prove the first statement:

- let B, C be sets, we need to show that

$$(B \cup C)^c \subseteq B^c \cap C^c \quad \text{and} \quad B^c \cap C^c \subseteq (B \cup C)^c$$

- $x \in (B \cup C)^c \implies x \notin B \cup C \implies x \notin B$ and $x \notin C$
  $\implies x \in B^c$ and $x \in C^c \implies x \in B^c \cap C^c \implies (B \cup C)^c \subseteq B^c \cap C^c$

- $x \in B^c \cap C^c \implies x \in B^c$ and $x \in C^c \implies x \notin B$ and $x \notin C$
  $\implies x \notin B \cup C \implies x \in (B \cup C)^c \implies B^c \cap C^c \subseteq (B \cup C)^c$

Mathematical induction

Axiom 1.5 *Well ordering property.* If the set $S \subseteq \mathbf{N}$ is nonempty, then there exists some $x \in S$ such that $x \leq y$ for all $y \in S$, *i.e.*, the set S always has a **least element**.

Theorem 1.6 *Induction.* Let $P(n)$ be a statement depending on $n \in \mathbf{N}$. Assume that we have:

1. *Base case.* The statement $P(1)$ is true.
2. *Inductive step.* If $P(m)$ is true then $P(m+1)$ is true.

Then, $P(n)$ is true for all $n \in \mathbf{N}$.

proof:

- suppose $S \neq \emptyset$, then S has a least element $m \in S$
- since $P(1)$ is true, we have $m \neq 1$, *i.e.*, $m > 1$
- since m is a least element, we have $m - 1 \notin S \implies P(m-1)$ is true
- this implies that $P(m)$ is true $\implies m \notin S$, which is a contradiction
- hence, $S = \emptyset$, *i.e.*, $P(n)$ is true for all $n \in \mathbf{N}$

Example 1.7 For all $c \in \mathbf{R}$, $c \neq 1$, and for all $n \in \mathbf{N}$,

$$1 + c + c^2 + \cdots + c^n = \frac{1 - c^{n+1}}{1 - c}.$$

proof:

- the base case ($n = 1$): the left hand side of the equation is $1 + c$; the right hand side is $\frac{1-c^2}{1-c} = \frac{(1+c)(1-c)}{1-c} = 1 + c$, which equals to the left hand side
- the inductive step: assume that the equation is true for $k \in \mathbf{N}$, *i.e.*,

  $$1 + c + c^2 + \cdots + c^k = \frac{1 - c^{k+1}}{1 - c},$$

  we have

  $$\begin{aligned} 1 + c + c^2 + \cdots + c^k + c^{k+1} &= \frac{1 - c^{k+1}}{1 - c} + c^{k+1} \\ &= \frac{1 - c^{k+1} + c^{k+1} - c^{(k+1)+1}}{1 - c} = \frac{1 - c^{(k+1)+1}}{1 - c} \end{aligned}$$

Example 1.8 *Bernoulli's inequality.* For all $c \geq -1$, $(1+c)^n \geq 1+nc$ for all $n \in \mathbf{N}$.

proof:

- for the base case $(n = 1)$, we have $(1+c)^1 \geq 1 + 1 \cdot c$

- the inductive step: suppose $m \in \mathbf{N}$, $m > 1$ and $(1+c)^m \geq 1+mc$, then

$$(1+c)^{m+1} \geq (1+mc)(1+c) = 1 + (m+1)c + mc^2 \geq 1 + (m+1)c$$

Functions

Definition 1.9 If A and B are sets, a **function** $f\colon A \to B$ is a mapping that assigns each $x \in A$ to a unique element in B denoted $f(x)$.

Definition 1.10 Consider a function $f\colon A \to B$. Define the **image** (or direct image) of a subset $C \subseteq A$ as

$$f(C) = \{f(x) \in B \mid x \in C\}.$$

Define the **inverse image** of a subset $D \subseteq B$ as

$$f^{-1}(D) = \{x \in A \mid f(x) \in D\}.$$

---

examples:

- $f\colon \{1,2,3,4\} \to \{a,b\}$ where $f(1) = f(2) = a$, $f(3) = f(4) = b$, we have $f(\{1,2\}) = \{a\}$, $f^{-1}(\{b\}) = \{3,4\}$
- $f\colon \mathbf{R} \to \mathbf{R}$ where $f(x) = \sin(\pi x)$, we have $f([0,1/2]) = [0,1]$, $f^{-1}(\{0\}) = \mathbf{Z}$

Definition 1.11 Let $f\colon A \to B$ be a function.

- The function f is **injective** or **one-to-one** if $f(x_1) = f(x_2)$ implies $x_1 = x_2$.
- The function f is **surjective** or **onto** if $f(A) = B$.
- The function f is **bijective** if f is both surjective and injective. In this case, the function $f^{-1}\colon B \to A$ is the **inverse function** of f, which assigns each $y \in B$ to the unique $x \in A$ such that $f(x) = y$.

- if the function f is a bijection, then $f(f^{-1}(x)) = x$
- example: for the bijection $f\colon \mathbf{R} \to \mathbf{R}$ given by $f(x) = x^3$, we have $f^{-1}(x) = \sqrt[3]{x}$

Definition 1.12 Consider $f\colon A \to B$ and $g\colon B \to C$. The **composition** of the functions f and g is the function $g \circ f\colon A \to C$ defined as

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

- example: if $f(x) = x^3$ and $g(y) = \sin(y)$, then $(g \circ f)(x) = \sin(x^3)$

Cardinality

Definition 1.13 We state that the two sets A and B have the same **cardinality** if there exists a bijection $f\colon A \to B$.

notation:

- $|A|$ denotes the cardinality of the set A
- $|A| = |B|$ if the sets A and B have the same cardinality
- $|A| = n$ if $|A| = |\{1, \ldots, n\}|$
- $|A| \leq |B|$ if there exists an injection $f\colon A \to B$
- $|A| < |B|$ if $|A| \leq |B|$ and $|A| \neq |B|$

Theorem 1.14

- If $|A| = |B|$, then $|B| = |A|$.
- If $|A| = |B|$, and $|B| = |C|$, then $|A| = |C|$.

proof:

- show that the inverse function $f^{-1}\colon B \to A$ of $f\colon A \to B$ is a bijection
- show that the composition $g \circ f\colon A \to C$ of functions $f\colon A \to B$ and $g\colon B \to C$ is a bijection

Theorem 1.15 *Cantor-Schröder-Bernstein.* If $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$.

Definition 1.16 The set A is **countably finite** if $|A| = |\mathbf{N}|$. Specifically, the set A is **finite** if $|A| = n \in \mathbf{N}$. The set A is **countable** if A is finite or countably infinite. Otherwise, we say A is **uncountable**.

Example 1.17 The set of even natural numbers and the set of odd natural numbers have the same cardinality as $\mathbf{N}$, *i.e.*, $|\{2n \mid n \in \mathbf{N}\}| = |\{2n-1 \mid n \in \mathbf{N}\}| = |\mathbf{N}|$.

proof: consider the bijection $f\colon \mathbf{N} \to \{2n \mid n \in \mathbf{N}\}$ given by $f(n) = 2n$ and $g\colon \mathbf{N} \to \{2n-1 \mid n \in \mathbf{N}\}$ given by $g(n) = 2n-1$

Example 1.18 The set of all integers has the same cardinality as $\mathbf{N}$, *i.e.*, $|\mathbf{Z}| = |\mathbf{N}|$.

proof: consider the bijection $f\colon \mathbf{Z} \to \mathbf{N}$ given by

$$f(n) = \begin{cases} 2n & n \geq 0 \\ -(2n+1) & n < 0 \end{cases}$$

Definition 1.19 The **powerset** of a set A, denoted by $\mathcal{P}(A)$, is the set of all subsets of A, *i.e.*, $\mathcal{P}(A) = \{B \mid B \subseteq A\}$.

- for a finite set A of cardinality n, the cardinality of $\mathcal{P}(A)$ is 2^n

examples:

- $A = \emptyset$ then $\mathcal{P}(A) = \{\emptyset\}$
- $A = \{1\}$ then $\mathcal{P}(A) = \{\emptyset, \{1\}\}$
- $A = \{1, 2\}$ then $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$

Theorem 1.20 *Cantor.* If A is a set, then $|A| < |\mathcal{P}(A)|$.

- therefore, $|\mathbf{N}| < |\mathcal{P}(\mathbf{N})| < |\mathcal{P}(\mathcal{P}(\mathbf{N}))| < \cdots$, *i.e.*, there are infinite number of infinite sets

proof:

we first show that $|A| \leq |\mathcal{P}(A)|$

- consider the function $f\colon A \to \mathcal{P}(A)$ given by $f(x) = \{x\}$
- the function f is a injection since

$$f(x_1) = f(x_2) \implies \{x_1\} = \{x_2\} \implies x_1 = x_2$$

we now show that $|A| \neq |\mathcal{P}(A)|$ by contradiction

- suppose $|A| = |\mathcal{P}(A)|$, then there is a surjection $g\colon A \to \mathcal{P}(A)$
- consider the set $B \subseteq A$ given by

$$B = \{x \in A \mid x \notin g(x)\} \in \mathcal{P}(A)$$

- since g is surjective and $B \in \mathcal{P}(A)$, there exists a $b \in A$ such that $g(b) = B$
- there are two cases
  1. $b \in B \implies b \notin g(b) \implies b \notin B$
  2. $b \notin B \implies b \notin g(b) \implies b \in B$

  where in either case we obtain a contradiction
- hence, g is not surjective $\implies |A| \neq |\mathcal{P}(A)|$

Corollary 1.21 For all $n \in \mathbf{N} \cup \{0\}$, $n < 2^n$.
