Basic Structures: Sets and Functions

1. Sets

Definition 1. A set is an unordered collection of objects. The objects in a set are also called elements or members of the set. They are contained in the set.

Example 1. We’ll use the following symbols to represent their respective sets:
- \( \mathbb{N} = \{0, 1, 2, \ldots\} \), natural numbers
- \( \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \), integers
- \( \mathbb{Z}^+ = \{1, 2, \ldots\} \), positive integers
- \( \mathbb{Q} = \{p/q : p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0\} \), rational numbers
- \( \mathbb{R} \), real numbers

Definition 2. Two sets are equal if and only if they have the same elements.

Definition 3. The set \( A \) is a subset of set \( B \), write \( A \subseteq B \), if and only if every element of \( A \) is also an element of \( B \).

Theorem 1. For any set \( S \):
- \( \emptyset \subseteq S \); and
- \( S \subseteq S \).

Note that when \( A = B \), \( A \subseteq B \) as well. Sometimes we’d like to exclude this case. We write \( A \subset B \) (“\( A \) is a proper subset of \( B \)”)

Definition 4. Let \( S \) be a set. If there are \( n \) distinct elements in \( S \) (\( 0 \leq n < \infty \)), we say \( S \) is a finite set and \( n \) is the cardinality of \( S \). Write \( |S| = n \).

Definition 5. A set is infinite if it is not finite.

Remark. We’ll talk about the cardinality of infinite sets in Section §5.2.

Definition 6. Given a set \( S \), the power set \( \wp(S) \) of \( S \) is the set of all subsets of \( S \). In other words, \( \wp(S) = \{x : x \subseteq S\} \).

Example 2. Compute \( \wp(\emptyset) \) and \( \wp(\{\emptyset\}) \).

Solution. \( \wp(\emptyset) = \{x : x \subseteq \emptyset\} = \{\emptyset\} \). \( \wp(\{\emptyset\}) = \{x : x \subseteq \{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} \). \( \square \)

Definition 7. Let \( A \) and \( B \) be sets. The Cartesian product of \( A \) and \( B \), \( A \times B \), is defined by
\[
A \times B = \{(a, b) : a \in A \land b \in B\}
\]
Cartesian products can be generalized to more than two sets.

Definition 8. The Cartesian product of the sets \( A_0, A_1, \ldots, A_n \), \( A_0 \times A_1 \times \cdots \times A_n \), is defined by
\[
A_0 \times A_1 \times \cdots \times A_n = \{(a_0, a_1, \ldots, a_n) : a_i \in A_i \text{ for } i = 0, 1, \ldots, n\}
\]

Definition 9. Given a predicate \( P \) and a domain \( D \), the truth set of \( P \) is the set of elements \( x \in D \) such that \( P(x) \) is true. The truth set of \( P(x) \) is denoted by \( \{x \in D : P(x)\} \).

2. Set Operations

Definition 10. Let \( A \) and \( B \) be sets. The union of \( A \) and \( B \), \( A \cup B \), is the set containing elements from \( A \) or \( B \).
\[
A \cup B = \{x : x \in A \lor x \in B\}
\]

Definition 11. Let \( A \) and \( B \) be sets. The intersection of \( A \) and \( B \), \( A \cap B \), is the set containing elements in both \( A \) and \( B \).
\[
A \cap B = \{x : x \in A \land x \in B\}
\]
<table>
<thead>
<tr>
<th>Identity</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A \cup \emptyset = A)</td>
<td>Identity laws</td>
</tr>
<tr>
<td>(A \cap U = A)</td>
<td></td>
</tr>
<tr>
<td>(A \cup U = U)</td>
<td>Domination laws</td>
</tr>
<tr>
<td>(A \cap \emptyset = \emptyset)</td>
<td></td>
</tr>
<tr>
<td>(A \cup A = A)</td>
<td>Idempotent laws</td>
</tr>
<tr>
<td>(A \cap A = A)</td>
<td></td>
</tr>
<tr>
<td>(A = A)</td>
<td>Complementation law</td>
</tr>
<tr>
<td>(A \cup B = B \cup A)</td>
<td>Commutative laws</td>
</tr>
<tr>
<td>(A \cap B = B \cap A)</td>
<td></td>
</tr>
<tr>
<td>(A \cup (B \cup C) = (A \cup B) \cup C)</td>
<td>Associative laws</td>
</tr>
<tr>
<td>(A \cap (B \cap C) = (A \cap B) \cap C)</td>
<td></td>
</tr>
<tr>
<td>(A \cap (B \cup C) = (A \cap B) \cup (A \cap C))</td>
<td>Distributive laws</td>
</tr>
<tr>
<td>(A \cup (B \cap C) = (A \cup B) \cap (A \cup C))</td>
<td></td>
</tr>
<tr>
<td>(A \cup B = A \cup B)</td>
<td>De Morgan’s laws</td>
</tr>
<tr>
<td>(A \cap B = A \cap B)</td>
<td></td>
</tr>
<tr>
<td>(A \cup (A \cap B) = A)</td>
<td>Absorption laws</td>
</tr>
<tr>
<td>(A \cap (A \cup B) = A)</td>
<td></td>
</tr>
<tr>
<td>(A \cup A = U)</td>
<td>Complement laws</td>
</tr>
<tr>
<td>(A \cap A = \emptyset)</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 1.** Set Identities

As usual, we can generalize union and intersection as follows.

**Definition 12.** Let \(A_0, A_1, \ldots, A_n\) be sets. Define

\[
\bigcup_{i=0}^{n} A_i = A_0 \cup A_1 \cup \cdots \cup A_n
\]

and

\[
\bigcap_{i=0}^{n} A_i = A_0 \cap A_1 \cap \cdots \cap A_n.
\]

**Remark.** In fact, we can do a little better. Let \(I\) be a set (not necessarily finite). Suppose we have a set \(A_i\) for each \(i \in I\). Then

\[
\bigcup_{i \in I} A_i = \{x : x \in A_i \text{ for some } i \in I\}
\]

and

\[
\bigcap_{i \in I} A_i = \{x : x \in A_i \text{ for all } i \in I\}.
\]

**Definition 13.** Two sets are **disjoint** if their intersection is the empty set.

**Definition 14.** Let \(A\) and \(B\) be sets. The **difference** of \(A\) and \(B\), \(A - B\), is the set contains elements in \(A\) but not in \(B\).

\[
A - B = \{x : x \in A \land x \notin B\}
\]

**Definition 15.** Let \(U\) be the universal set. The **complement** of the set \(A\), \(\bar{A}\) or \(A'\), is the complement of \(A\) with respect to \(U\).

\[
\bar{A} = U - A
\]

Figure 1 shows some useful set identities.

**Example 3.** Let \(A\), \(B\) and \(C\) be sets. Show \(\bar{A} \cup (B \cap C) = (\bar{C} \cup B) \cap \bar{A}\).

**Solution.**

\[
\bar{A} \cup (B \cap C) = \bar{A} \cap (B \cup C) = (\bar{B} \cup C) \cap \bar{A} = (\bar{C} \cup B) \cap \bar{A}.
\]
(1a) $\lfloor x \rfloor = n$ if and only if $n \leq x < n + 1$
(1b) $\lfloor x \rfloor = n$ if and only if $-1 < x < n$
(1c) $\lfloor x \rfloor = n$ if and only if $-1 < x \leq n$
(1d) $\lfloor x \rfloor = n$ if and only if $x < n < x + 1$

\[
x - 1 < \lfloor x \rfloor \leq x < x + 1
\]

\[
(\text{a}) \quad \lfloor x \rfloor = \lfloor y \rfloor
\]

\[
(\text{b}) \quad \lfloor x + y \rfloor = \lfloor x \rfloor + y
\]

\[
(\text{c}) \quad \lfloor x + n \rfloor = \lfloor x \rfloor + n
\]

where $x \in \mathbb{R}$ and $n \in \mathbb{Z}$

\[\text{Figure 2. Properties of Floor and Ceiling Functions}\]

3. Functions

Definition 16. Let $A$ and $B$ be sets. A function $f$ from $A$ to $B$, $f : A \to B$, is an assignment of exactly one element of $B$ to each element of $A$. Sometimes, we say $f$ maps $A$ to $B$ as well.

Definition 17. Let $A$ and $B$ be sets and $f : A \to B$. We say $A$ is the domain of $f$ and $B$ is the codomain of $f$. If $f(a) = b$, we say $b$ is the image of $a$ and $a$ is a preimage of $b$. The range of $f$ is the set of all images of elements of $A$.

Definition 18. Let $f$ and $g$ be functions from $A$ to $\mathbb{R}$. Then
\[
(f + g)(x) = f(x) + g(x) \\
(fg)(x) = f(x)g(x) \\
(f \circ g)(x) = f(g(x))
\]

Definition 19. Let $f$ be a function from $A$ to $B$ and $S \subseteq A$. The image of $S$, $f(S)$, is defined by
\[
f(S) = \{ f(s) : s \in S \}.
\]

Definition 20. A function $f : A \to B$ is said to be one-to-one, or injective, if and only if $f(x) = f(y)$ implies $x = y$.

A function $f : A \to B$ is said to be onto, or surjective, if and only if for any $b \in B$ there is an $a \in A$ such that $f(a) = b$.

A function $f$ is a one-to-one correspondence, or a bijection, if it is both injective and surjective.

Definition 21. A function $f$ whose domain and codomain are subsets of $\mathbb{R}$ is called strictly increasing if $f(x) < f(y)$ whenever $x < y$. $f$ is called strictly decreasing if $f(x) > f(y)$ whenever $x < y$.

Definition 22. Let $f : A \to B$ be a bijection. The inverse function of $f$, $f^{-1}$, is a function from $B$ to $A$ such that $f^{-1}(b) = a$ when $f(a) = b$.

Remark. Is $f^{-1}$ well-defined? That is, is it a function?

Definition 23. Let $g : A \to B$ and $f : B \to C$. The composition of $f$ and $g$, denoted by $f \circ g : A \to C$, is defined by
\[
(f \circ g)(a) = f(g(a)).
\]

Definition 24. Let $f : A \to B$. The graph of $f$ is the set
\[
\{(a, b) : a \in A \text{ and } f(a) = b\}.
\]

Definition 25. The floor function $\lfloor x \rfloor$ assigns the largest integer that is less than or equal to $x$. The ceiling function $\lceil x \rceil$ assigns the smallest integer that is greater than or equal to $x$.

Figure 2 shows some properties of floor and ceiling functions.

Example 4. Let $x \in \mathbb{R}$. Show $2\lfloor x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.

Solution. Let $x = n + \epsilon$ where $n \in \mathbb{Z}$ and $0 \leq \epsilon < 1$. Then $n = \lfloor x \rfloor$. Consider the following two cases:
<table>
<thead>
<tr>
<th>Sum</th>
<th>Closed form</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sum_{k=0}^{n} ar^k(r \neq 0)$</td>
<td>$\frac{a(r^{n+1}-a)}{r-1}, r \neq 1$</td>
</tr>
<tr>
<td>$\sum_{k=1}^{n} k$</td>
<td>$\frac{n(n+1)}{2}$</td>
</tr>
<tr>
<td>$\sum_{k=1}^{n} k^2$</td>
<td>$\frac{n(n+1)(2n+1)}{6}$</td>
</tr>
<tr>
<td>$\sum_{k=1}^{n} k^3,</td>
<td>x</td>
</tr>
<tr>
<td>$\sum_{k=0}^{\infty} k^x,</td>
<td>x</td>
</tr>
</tbody>
</table>

**Figure 3. Useful Summation Formulae**

- $0 \leq \epsilon < \frac{1}{2}$. $|x + \frac{1}{2}| = |x|$. Hence $|x| + |x + \frac{1}{2}| = 2n$. On the other hand, $|2x| = |2n + 2\epsilon| = 2n$ for $\epsilon < \frac{1}{2}$.
- $\frac{1}{2} \leq \epsilon < 1$. $|x + \frac{1}{2}| = |x| + 1$. Hence $|x| + |x + \frac{1}{2}| = 2n + 1$. On the other hand, $|2x| = |2n + 2\epsilon| = 2n + 1$ for $\epsilon \geq \frac{1}{2}$.

**Definition 26.** The factorial function $n!$ is defined by

$$n! = 1 \cdot 2 \cdots (n - 1) \cdot n.$$  

**4. SEQUENCES AND SUMMATIONS**

**Definition 27.** A sequence is a function from $\mathbb{Z}$ to a set $S$. We use $a_n$ to denote the image of the integer $n$ and call $a_n$ a term of the sequence.

**Definition 28.** A geometric progression is a sequence of the form

$$a, ar, ar^2, \ldots, ar^n,$$

where the initial term $a$ and the common ratio $r$ are in $\mathbb{R}$.

**Definition 29.** An arithmetic progression is a sequence of the form

$$a, a + d, a + 2d, \ldots, a + nd,$$

where the initial term $a$ and the common difference $d$ are in $\mathbb{R}$.

**Definition 30.** Consider the following summation notation

$$\sum_{j=m}^{n} a_j$$

where $j$ is called the index of summation, $m$ its lower limit, and $n$ its upper limit.

**5. SUPPLEMENTS**

5.1. **Russell’s paradox.** Consider the following statement: “The Serbian barber only shaves those who do not shave themselves.” Now ask yourself: does the barber shave himself or not? There are only two cases: either he shaves himself, or he doesn’t. Suppose he shaves himself. We are told that he does not shave those who shave themselves. Hence he does not shave himself. Now suppose he does not shave himself. We are told that he shaves those who do not shave themselves. Hence he does shave himself. Both cases lead to contradiction. What’s going on here?

The barber paradox is an intriguing question raised by philosophers. It seems like a tricky game of words. And nobody expects it would have anything to do with mathematics. However, Russell is able to exploit the idea and create a similar paradox in mathematics in 1903.

Consider the set

$$A = \{x : x \not\in x\}.$$  

Since $\emptyset \not\in \emptyset$, we have $\emptyset \in A$. $A$ does seem to make sense. Now, can you tell me whether $A \in A$?
Again, there are only two possibilities: either $A \in A$ or $A \notin A$. Suppose $A \in A$. Since any element $x$ of $A$ has the property that $x \notin x$, in particular $A \notin A$. A contradiction. On the other hand, suppose $A \notin A$. Then by the definition of $A$, $A \in A$. Another contradiction.

We can see the arguments of Russell’s paradox are similar to those in barber’s paradox. In both cases, we cannot tell the truth value of a proposition. In philosophy, it may be a game of language. But it is a serious matter in the foundation of mathematics.

Mathematicians now distinguish small from large sets. Mathematics is still good if we pay close attention to the collection of all sets (thus the name large set). In fact, Russell’s paradox can be avoided if we do not allow the collection of all sets as the universe.

In computer science, you can also find similar argument. It is often used in proving negative results. Consider the question: what can’t computers do? Of course, we know they can’t do poetry, write novels, nor compose a sheet of music. What about a mathematical function? Is it always possible to write programs for arbitrary mathematical functions? The following example shows a mathematical problem (called the halting problem) which cannot be solved by computers.

Example 5. Write a program $T(P)$ which accepts program text $P$ as input and returns 1 if $P$ will terminate, 0 if not.

Solution. Suppose there is such a program $T$. Let us consider the following program $M$:

1. program $M$
2. if $T(M) = 1$ then
3. while true do od
4. else $T(M) = 0$
5. exit

What is $T(M)$? Suppose $T(M) = 1$, $M$ terminates. Therefore $T(M) = 0$, or it would end in an infinite loop. On the other hand, suppose $T(M) = 0$, $M$ does not terminate. Hence $T(M) = 1$ because this is the only case where $M$ does not terminate. Both cases are contradiction. We conclude our assumption is incorrect. Hence $T$ does not exist. □

5.2. Cardinality of Infinite Sets. In Section §1, we define the cardinality of a finite set $A$ to be the number of its distinct members. In this section, we’ll briefly discuss the cardinalities of infinite sets.

For finite sets, we see that cardinality intuitively corresponds to the size of sets. If $A$ and $B$ are of the same size, we have $|A| = |B|$. For infinite sets, if there is a way to compare their sizes, we may define their cardinalities accordingly. The following definition provides a hint for comparing two infinite sets:

Definition 31. A set $A$ is countably infinite if there is a bijection $f : \mathbb{N} \rightarrow A$. In this case, define the cardinality of $A$, $|A|$, to be $\aleph_0$. A set $A$ is countable if it is finite or countably infinite.

In other words, if there is a bijection from $\mathbb{N}$ to $A$, we think $\mathbb{N}$ and $A$ are of the same size. For finite sets $A$ and $B$, if there is a bijection from $A$ to $B$, $|A| = |B|$. This corresponds to our intuition of cardinality for finite sets as well.

Example 6. Show the following sets are countably infinite: $\mathbb{N}, \mathbb{Z}^+, \mathbb{Z}, \mathbb{N} \times \mathbb{N}$.

Solution.

$f(n) = n$ is a bijection from $\mathbb{N}$ to $\mathbb{N}$. Thus $\mathbb{N}$ is countable. Similarly, $g(n) = n + 1$ is a bijection from $\mathbb{N}$ to $\mathbb{Z}^+$. $|\mathbb{Z}^+| = \aleph_0$.

Now consider the infinite sequence $0, 1, -1, 2, -2, 3, -3, \ldots$. It is easy to see all integers appear in the sequence exactly once. One can define a bijection accordingly.

Similarly, consider the infinite sequence

$(0, 0), (1, 0), (0, 1), (2, 0), (1, 1), (0, 2), (3, 0), (2, 1), (1, 2), (0, 3), \ldots$

Each element of $\mathbb{N} \times \mathbb{N}$ appears in the sequence exactly once. The desired bijection can be constructed as well. □

Surprisingly, $|\mathbb{N}| = |\mathbb{Z}| = \aleph_0$, although it looks like $\mathbb{Z}$ has twice as many elements in $\mathbb{N}$. Here is an even more surprising theorem:

Theorem 2. $\mathbb{Q}$ is countable.

In fact, we can construct a countable set out of several countable sets.

Theorem 3. A finite product of countable sets is countable.
Proof. (sketch) Let $A_0, A_1, \ldots, A_n$ be countable sets and $A = A_0 \times A_1 \times \cdots \times A_n$. Then $A = (\cdots ((A_0 \times A_1) \times A_2) \times \cdots \times A_n)$. □

Theorem 4. A countable union of countable sets is countable.

Example 7. The following sets are countable:

- $\bigodot_i \mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N}$ for any finite $i > 0$;
- $\bigcup_{i=1}^n \mathbb{N} \times \mathbb{N} \times \cdots \mathbb{N}$ for any finite $n > 0$;
- $\bigcup_{i=1}^\infty \mathbb{N} \times \mathbb{N} \times \cdots \mathbb{N}$;
- The set of all C programs.

We have seen many infinite sets so far. And they are all of the same cardinality of $\mathbb{N}$. Is there any set “larger” than $\mathbb{N}$? Let us first define the following term:

Definition 32. A set which is not countable is said to be uncountable.

Theorem 5. Let $\mathbb{B} = \{F, T\}$. Then $A = \mathbb{B} \times \mathbb{B} \times \cdots \times \mathbb{B} \times \cdots$ is uncountable.

Proof. Suppose there is a bijection $f : \mathbb{N} \to A$. Let

$$f(i) = b_{i0}b_{i1} \cdots b_{ij} \cdots$$

Define

$$c_i = \begin{cases} F & \text{if } b_{ii} = T \\ T & \text{if } b_{ii} = F \end{cases}$$

Then $c \neq f(i)$ for all $i$. But $c \in A$, a contradiction. □

This technique is first used by Cantor to prove that $\mathbb{R}$ is uncountable. It is called diagonalization.

Theorem 6. $\mathbb{R}$ is uncountable.

Surprisingly, we can construct not only infinite sets “larger” than $\mathbb{N}$, but also much more “larger” sets.

Theorem 7. Let $A$ be a set. $|\wp(A)| > |A|$.

Therefore, $|\wp(\mathbb{R})| > |\mathbb{R}|$, $|\wp(\wp(\mathbb{R}))| > |\wp(\mathbb{R})|$, etc.