

## 9 Uncountable Sets and Power Sets

### 9.1 Uncountable Sets

**Definition 9.1.** A set  $X$  is called **uncountable** if it is infinite but not countable.

We want to show that  $\mathbb{R}$  is uncountable. To do this we will show that the interval  $(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$  is uncountable. As an exercise, one can then show that there exists a bijection between the interval  $(0, 1)$  and  $\mathbb{R}$ .

Now, assume that every real number between 0 and 1 has a decimal expansion of the form

$$0.a_1a_2a_3 \cdots = \sum_{k \in \mathbb{N}} a_k 10^{-k}$$

where  $a_k$  is an integer such that  $0 \leq a_k \leq 9$  for each  $k \in \mathbb{N}$ . Note that

$$\begin{aligned} 0.999 \cdots &= \sum_{k \in \mathbb{N}} 9 \cdot 10^{-k} \\ &= 9 \left( \frac{1/10}{1 - 1/10} \right) \\ &= 1 \end{aligned}$$

since  $\sum_{k \in \mathbb{N}} 10^{-k}$  is a convergent geometric series. Consequently, if there exists some  $N \in \mathbb{N}$  such that  $a_N \neq 9$  and  $a_n = 9$  for all  $n \in \mathbb{N}$  with  $n > N$ , we have that

$$0.a_1a_2a_3 \cdots = 0.a_1a_2 \cdots a_{N-1}b_N$$

where  $b_N = a_N + 1$ . We will assume the result that for every  $\alpha \in \mathbb{R}$  with  $0 < \alpha < 1$ , there is a unique way to write  $\alpha$  as  $0.a_1a_2a_3 \cdots$  where  $a_k$  is an integer such that  $0 \leq a_k \leq 9$  for each  $k \in \mathbb{N}$  and for all  $N \in \mathbb{N}$ , there exists  $n \in \mathbb{N}$  such that  $n \geq N$  and  $a_n \neq 9$ .

We have the following theorem.

**Theorem 9.2.** The interval  $(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$  is uncountable.

*Proof.* (Cantor's diagonalisation argument). We know that the interval  $(0, 1)$  is infinite, since  $f : \mathbb{N} \rightarrow (0, 1)$  defined by  $f(k) = 10^{-k}$ , for all  $k \in \mathbb{N}$ , is easily shown to be injective.

To the contrary, suppose that  $(0, 1)$  is countable. Hence, we can enumerate the elements of  $(0, 1)$  as  $\alpha_1, \alpha_2, \alpha_3, \dots$ . We write each  $\alpha_k$  as a decimal expansion as described above, that is

$$\alpha_k = 0.a_{k1}a_{k2}a_{k3} \cdots$$

where  $a_{ki}$  is an integer such that  $0 \leq a_{ki} \leq 9$  for each  $k \in \mathbb{N}$ . Further, we assume that, for all  $N \in \mathbb{N}$ , there exists an  $n \in \mathbb{N}$  such that  $n > N$  and  $a_n \neq 9$ . Now, for each  $k \in \mathbb{N}$ , set

$$b_k = \begin{cases} 1, & \text{if } a_{kk} \neq 1; \\ 2, & \text{if } a_{kk} = 1, \end{cases}$$

and set  $\beta = 0.b_1b_2b_3 \cdots$ . Then  $\beta \in \mathbb{R}$  with  $0 < \beta < 1$  and for all  $N \in \mathbb{N}$ , there exists an  $n \in \mathbb{N}$  such that  $n > N$  and  $b_n \neq 9$ . Hence by assumption,  $\beta = \alpha_m$  for some  $m \in \mathbb{N}$ . But  $b_m \neq a_{mm}$ , which contradicts the uniqueness of the representation of  $\beta$  as a decimal expansion not ending in an infinite sequence of 9s. Hence, we must have that  $(0, 1)$  is uncountable.  $\square$

**Remark.** Suppose that we have  $m \in \mathbb{N}$  where  $a_m$  is an integer such that  $0 \leq a_m \leq 9$  (not all 0) for each  $m$ , and

$$\alpha = 0.a_1a_2 \cdots a_m a_1 a_2 \cdots a_m a_1 a_2 \cdots a_m \cdots = 0.\overline{a_1 a_2 \cdots a_m}.$$

Then  $\alpha$  is a rational number. This follows since if  $b = \sum_{k=1}^m a_k \cdot 10^{m-k}$ , then  $b \in \mathbb{N}$  and

$$\begin{aligned} \alpha &= \sum_{n \in \mathbb{N}} b \cdot 10^{-mn} \\ &= b \left( \frac{10^{-m}}{1 - 10^{-m}} \right) \\ &= \frac{b}{10^m - 1}. \end{aligned}$$

Note that the map  $g : (0, 1) \rightarrow \mathbb{R}$  given by  $g(x) = x$ , for all  $x \in (0, 1)$  is injective, so  $|(0, 1)| \leq |\mathbb{R}|$ . Since  $|\mathbb{N}| < |(0, 1)|$ , we have that  $|\mathbb{N}| < |\mathbb{R}|$ , that is  $\mathbb{R}$  is uncountable. The following corollary, whose proof is left as an exercise, shows that  $|(0, 1)| = |\mathbb{R}|$ . This is another way to argue that  $\mathbb{R}$  is uncountable.

**Corollary 9.3.** *There exists a bijection between the interval  $(0, 1)$  and  $\mathbb{R}$ .*

*Proof.* Exercise 6.4. □

## 9.2 Power Sets

**Definition 9.4.** Let  $A$  be a set and define  $\mathcal{P}(A) = \{C : C \subseteq A\}$ . Then  $\mathcal{P}(A)$  is called the *power set* of  $A$ .

**Example.** We have  $\mathcal{P}(\emptyset) = \{\emptyset\}$ , so  $|\mathcal{P}(\emptyset)| = 1$ .

**Example.** We have that  $\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$ , so  $|\mathcal{P}(\{1, 2\})| = 4 = 2^2$ .

**Example.** We have that  $\mathcal{P}(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$ . So  $|\mathcal{P}(\{1, 2, 3\})| = 8 = 2^3$ .

Note that, for any nonempty set  $X$ , we know that  $\emptyset, X$  are distinct subsets of  $X$ . Hence, we have that  $|\mathcal{P}(X)| \geq 2$ . We have the following results, whose proofs are left as an exercise.

**Theorem 9.5.** Suppose that  $A$  is a finite set with  $|A| = n$  for some  $n \in \mathbb{N}_0$ . Then  $|\mathcal{P}(A)| = 2^n$ .

*Proof.* Exercise 6.5. □

**Proposition 9.6.** Let  $A, B$  be sets. Then

- (i)  $A \subseteq B$  if and only if  $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ .
- (ii)  $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$ .
- (iii)  $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$ .

*Proof.* Exercise 6.6. □

We have the following theorem.

**Theorem 9.7** (Cantor's Theorem). *Let  $X$  be a set. Then  $|X| < |\mathcal{P}(X)|$ .*

*Proof.* Suppose  $X = \emptyset$ . Then  $|X| = 0 < 1 = |\mathcal{P}(X)|$ . So suppose  $X$  is nonempty, and define  $f : X \rightarrow \mathcal{P}(X)$  by  $f(x) = \{x\}$ , for all  $x \in X$ . We will show that  $f$  is injective. So suppose that  $x, x' \in X$  are such that  $f(x) = f(x')$ . Then  $\{x\} = \{x'\}$ . Hence, we have that  $x_1 = x_2$ . Therefore,  $f$  is injective, so  $|X| \leq |\mathcal{P}(X)|$ .

Now, we want to show that there exists no bijection between  $X$  and  $\mathcal{P}(X)$ . To the contrary, suppose there exists such a bijection  $g : X \rightarrow \mathcal{P}(X)$ . Define

$$A = \{x \in X : x \notin g(x)\}.$$

Then  $A$  is a subset of  $X$ , so  $A \in \mathcal{P}(X)$ . Further, since  $g$  is bijective, there exists some  $z \in X$  such that  $g(z) = A$ . By the definition of  $g$ ,  $z \in A$  if and only if  $z \notin g(z) = A$ , which is a contradiction since  $z \in A$  if and only if  $z \notin A$ . Therefore, there does not exist a bijective function  $g : X \rightarrow \mathcal{P}(X)$ . It follows that  $|X| < |\mathcal{P}(X)|$ .  $\square$