

# CS1231 Chapter 9

## Countability

### 9.1 Countable sets

**Definition 9.1.1** (Cantor). A set is *countable* if it is finite or it has the same cardinality as  $\mathbb{N}$ . A set is *uncountable* if it is not countable.

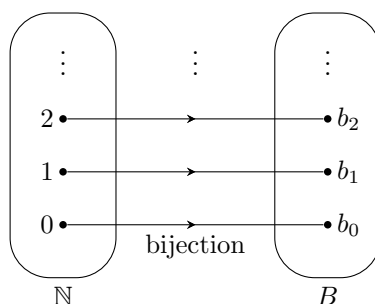


Figure 9.1: A countable infinite set  $B$

**Note 9.1.2.** Some authors allow only infinite sets to be countable.

**Example 9.1.3.** (1)  $\mathbb{N}$  is countable by Proposition 8.2.4(1).

(2) As shown in Example 8.2.3, both  $\mathbb{N} \setminus \{0\}$  and  $\mathbb{N} \setminus \{1, 3, 5, \dots\}$  are countable.

**Proposition 9.1.4.**  $\mathbb{Z}$  is countable.

**Proof.** Define  $f: \mathbb{Z} \rightarrow \mathbb{N}$  by setting, for each  $x \in \mathbb{Z}$ ,

$$f(x) = \begin{cases} 2x, & \text{if } x \geq 0; \\ 2(-x - 1) + 1, & \text{if } x < 0. \end{cases}$$

This definition indeed assigns to each element  $x \in \mathbb{Z}$  an element  $f(x) \in \mathbb{N}$  because if  $x \geq 0$ , then  $2x \geq 0$  as well; and if  $x < 0$ , then  $x \leq -1$  as  $x \in \mathbb{Z}$ , and so  $2(-x - 1) + 1 \geq 2(-(-1) - 1) + 1 = 1 > 0$ . It suffices to show that  $f$  is bijective.

To show surjectivity, pick any  $y \in \mathbb{N}$ . Then Proposition 3.2.21 tells us that  $y$  is either even or odd. If  $y$  is even, say  $y = 2x$  where  $x \in \mathbb{Z}$ , then  $x = y/2 \geq 0$ , and so  $f(x) = 2x = y$ . If  $y$  is odd, say  $y = 2x + 1$  where  $x \in \mathbb{Z}$ , then

$$x + 1 = \frac{y - 1}{2} + 1 \geq \frac{0 - 1}{2} + 1 = \frac{1}{2} > 0,$$

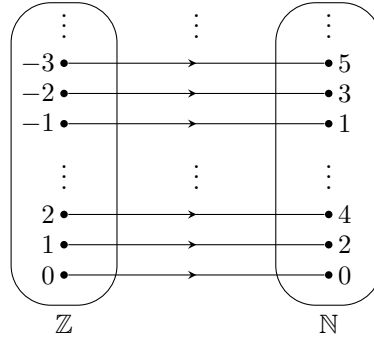


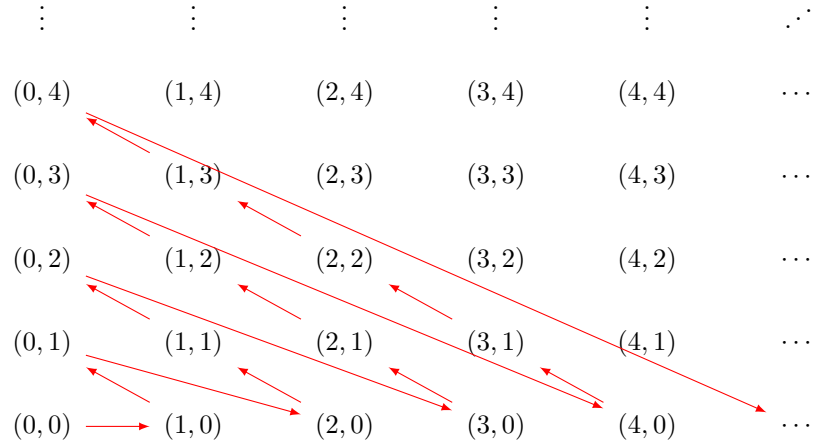
Figure 9.2: The countability of  $\mathbb{Z}$

and so  $f(-x-1) = 2(-(-x-1)-1) + 1 = 2x+1 = y$ . Thus some  $x \in \mathbb{Z}$  makes  $f(x) = y$  in all cases.

To show **injectivity**, pick  $x_1, x_2 \in \mathbb{Z}$  such that  $f(x_1) = f(x_2)$ . If  $f(x_1)$  is even, then  $f(x_1) = 2x_1$  and  $f(x_2) = 2x_2$  by Proposition 3.2.17, and so  $x_1 = x_2$ . If  $f(x_1)$  is odd, then  $f(x_1) = 2(-x_1-1) + 1$  and  $f(x_2) = 2(-x_2-1) + 1$  by Proposition 3.2.17, and so  $x_1 = x_2$ . Thus  $x_1 = x_2$  in all cases.  $\square$

**Theorem 9.1.5** (Cantor 1877).  $\mathbb{N} \times \mathbb{N}$  is countable.

**Proof sketch.**



The function  $f: \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$  such that  $f(0), f(1), f(2), \dots$  are respectively

$$(0,0), \underbrace{(1,0), (0,1)}_{\text{sum} = 1}, \underbrace{(2,0), (1,1), (0,2)}_{\text{sum} = 2}, \underbrace{(3,0), (2,1), (1,2), (0,3)}_{\text{sum} = 3}, (4,0), (3,1), (2,2), (1,3), \dots$$

is a **bijection**. This shows  $\mathbb{N} \times \mathbb{N}$  is countable.  $\square$

**Proposition 9.1.6.**  $\{0, 1\}^*$  is countable.

**Proof sketch.** Let  $f: \mathbb{N} \rightarrow \{0, 1\}^*$  such that  $f(0), f(1), f(2), \dots$  are respectively

$$\varepsilon, \underbrace{0, 1}_{\text{length } 1}, \underbrace{00, 01, 10, 11}_{\text{length } 2}, \underbrace{000, 001, 010, 011, 100, 101, 110, 111, \dots}_{\text{length } 3}, \dots,$$

where  $\varepsilon$  denotes the empty string. Then  $f$  is a **bijection**. This shows  $\{0, 1\}^*$  is **countable**.  $\square$

## 9.2 Countability

**Lemma 9.2.1.** Let  $A$  and  $B$  be sets of the same cardinality. Then  $A$  is **countable** if and only if  $B$  is **countable**.

**Exercise 9.2.2.** Prove Lemma 9.2.1. (Hint: imitate the proof of Lemma 8.2.8.)

 9a

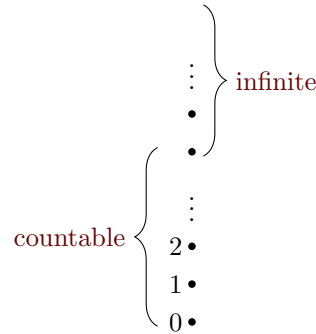


Figure 9.3: The smallest cardinalities

**Technique 9.2.3.** To prove  $\exists x P(x)$ , where  $P(x)$  is a sentence, produce an algorithmic procedure that outputs an object  $z$  for which  $P(z)$  is true.

**Justification.** This is based on Note 2.2.5(4).  $\square$

**Proposition 9.2.4.** Every **infinite set**  $B$  has a **countable infinite subset**.

**Proof.** Let  $B$  be an **infinite** set. Run the following procedure.

1. Initialize  $i = 0$ .
2. While  $B \setminus \{g_1, g_2, \dots, g_i\} \neq \emptyset$  do:
  - 2.1. Pick any  $g_{i+1} \in B \setminus \{g_1, g_2, \dots, g_i\}$ .
  - 2.2. Increment  $i$  to  $i + 1$ .

Suppose this procedure stops. Then a run results in  $g_1, g_2, \dots, g_\ell$ , where  $\ell \in \mathbb{N}$ . Define  $g: \{1, 2, \dots, \ell\} \rightarrow B$  by setting  $g(i) = g_i$  for all  $i \in \{1, 2, \dots, \ell\}$ . Notice  $B \setminus \{g_1, g_2, \dots, g_\ell\} = \emptyset$  as the stopping condition is reached. This says any element of  $B$  is equal to some  $g_i$ , thus some  $g(i)$ . So  $g$  is **surjective**. We know  $g$  is **injective** because each  $g_{i+1} \notin \{g_1, g_2, \dots, g_i\}$  by line 2.1. As  $g$  is a **bijection**  $\{1, 2, \dots, \ell\} \rightarrow B$ , we deduce that  $B$  is **finite**. This contradicts the condition that  $B$  is **infinite**.

**So this procedure does not stop.** Define  $A = \{g_i : i \in \mathbb{Z}^+\}$ , and  $g: \mathbb{N} \rightarrow A$  by setting  $g(i) = g_{i+1}$  for each  $i \in \mathbb{N}$ . Then  $g$  is **surjective** by construction. It is **injective** because each  $g_{i+1} \notin \{g_1, g_2, \dots, g_i\}$  by line 2.1. As  $g$  is a **bijection**  $\mathbb{N} \rightarrow A$ , we deduce that  $A$  is **countable**.

With  $g$ , we know  $A$  has the same cardinality as  $\mathbb{N}$ . So  $A$  is **infinite** by Lemma 8.2.8 and Exercise 8.2.7.  $\square$

**Example 9.2.5.** Knowing that  $\mathbb{R} \setminus \mathbb{Q}$  is infinite tells us  $\mathbb{R} \setminus \mathbb{Q}$  has a countable infinite subset by Proposition 9.2.4.

**Proposition 9.2.6.** Let  $A, B$  be sets such that  $A \subseteq B$ .

- (1) If  $B$  is **finite**, then  $A$  is **finite**.
- (2) If  $B$  is **countable**, then  $A$  is **countable**.

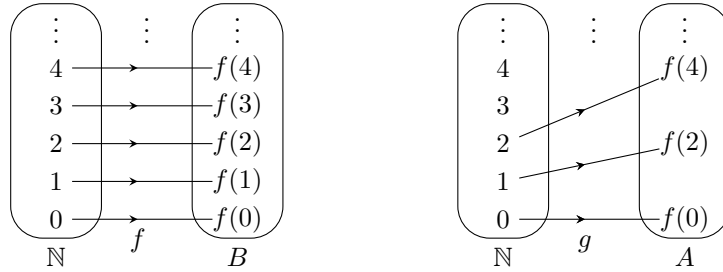


Figure 9.4: **Countability** of any subset  $A$  of a **countable** set  $B$

**Proof sketch.** One can prove part (1) in a way similar to how we handle part (2) below. So we leave the proof of (1) as an exercise and concentrate on (2). Suppose  $B$  is **countable**. If  $B$  is finite, then (1) tells us that  $A$  must also be finite and thus **countable**. So let us suppose  $B$  is **infinite**. As  $B$  is **countable** and **infinite**, there is a **bijection**  $\mathbb{N} \rightarrow B$ , say  $f$ . Run the following procedure. 9b

1. Initialize  $i = 0$ .
2. While  $A \setminus \{g_1, g_2, \dots, g_i\} \neq \emptyset$  do:
  - 2.1. Let  $m_{i+1}$  be the smallest element in  $\{m \in \mathbb{N} : f(m) \in A \setminus \{g_1, g_2, \dots, g_i\}\}$ .
  - 2.2. Set  $g_{i+1} = f(m_{i+1})$ .
  - 2.3. Increment  $i$  to  $i + 1$ .

On the one hand, suppose we are at line 2.2 when this procedure is run. Then the **loop condition** tells us  $A \setminus \{g_1, g_2, \dots, g_i\} \neq \emptyset$ . If  $a_i \in A \setminus \{g_1, g_2, \dots, g_i\}$ , then  $a_i = f(m)$  for some  $m \in \mathbb{N}$  because  $f$  is a **surjection**  $\mathbb{N} \rightarrow B$  and  $A \subseteq B$ . This says  $\{m \in \mathbb{N} : f(m) \in A \setminus \{g_1, g_2, \dots, g_i\}\} \neq \emptyset$ . So  $m_{i+1}$  must exist by the **Well-Ordering Principle**.

On the other hand, by the choices of  $m_{i+1}$  and  $g_{i+1}$  on lines 2.2 and 2.1,

$$\text{each } g_{i+1} \in A \setminus \{g_1, g_2, \dots, g_i\}. \quad (*)$$

**Case 1: this procedure stops after finitely many steps.** Then a run results in

$$m_1, m_2, \dots, m_\ell \quad \text{and} \quad g_1, g_2, \dots, g_\ell$$

where  $\ell \in \mathbb{N}$ . Define  $g: \{1, 2, \dots, \ell\} \rightarrow A$  by setting  $g(i) = g_i$  for all  $i \in \{1, 2, \dots, \ell\}$ .

Notice  $A \setminus \{g_1, g_2, \dots, g_\ell\} = \emptyset$  as the stopping condition is reached. This says any element of  $A$  is equal to some  $g_i$ , thus some  $g(i)$ . So  $g$  is **surjective**. We know  $g$  is **injective** by (\*).

As  $g$  is a **bijection**  $\{1, 2, \dots, \ell\} \rightarrow A$ , we deduce that  $A$  is **finite** and hence **countable**.

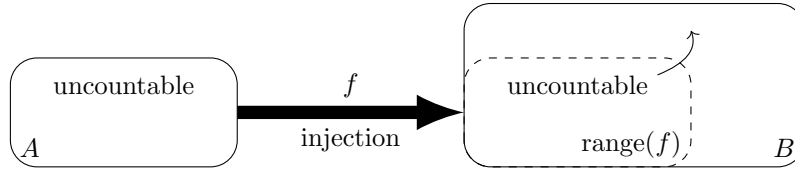


Figure 9.5: Injecting an uncountable set into another set

**Case 2: this procedure does not stop.** Then a run results in

$$m_1, m_2, m_3, \dots \quad \text{and} \quad g_1, g_2, g_3, \dots$$

Define  $g: \mathbb{N} \rightarrow A$  by setting  $g(i) = g_{i+1}$  for all  $i \in \mathbb{N}$ . As one can verify, this  $g$  is a **bijection**  $\mathbb{N} \rightarrow A$ . So  $A$  is **countable**.  $\square$

**Explanation of why  $g$  is bijective in the proof above (extra material).** We claim that  $m_{i+1} < m_{i+2}$  for all  $i \in \mathbb{N}$ . Let  $i \in \mathbb{N}$ . Line 2.2 tells us  $g_{i+1} = f(m_{i+1})$  and  $g_{i+2} = f(m_{i+2})$ , but  $g_{i+1} \neq g_{i+2}$  by (\*). So  $m_{i+1} \neq m_{i+2}$ . Note that  $f(m_{i+2}) = g_{i+2} \in A \setminus \{g_1, g_2, \dots, g_{i+1}\} \subseteq A \setminus \{g_1, g_2, \dots, g_i\}$ . Thus  $m_{i+2} \in \{m \in \mathbb{N} : f(m) \in A \setminus \{g_1, g_2, \dots, g_i\}\}$ . Since we **chose**  $m_{i+1}$  to be the smallest element of this set and  $m_{i+1} \neq m_{i+2}$ , we deduce that  $m_{i+1} < m_{i+2}$ , as claimed.

To show the **surjectivity** of  $g$ , assume we have  $y \in A$  such that  $g(i) \neq y$  for any  $i \in \mathbb{N}$ . As  $f$  is a **surjection**  $\mathbb{N} \rightarrow B$  and  $A \subseteq B$ , we get  $n \in \mathbb{N}$  making  $f(n) = y$ . The claim in the previous paragraph tells us that  $0 \leq m_1 < m_2 < \dots < m_{n+2}$ . So  $m_{n+2} \geq n+1 > n$ . Also, our assumption on  $y$  implies  $f(n) = y \in A \setminus \{g(0), g(1), \dots, g(n)\} = A \setminus \{g_1, g_2, \dots, g_{n+1}\}$ . However, we **chose**  $m_{n+2}$  to be the smallest  $m \in \mathbb{N}$  such that  $f(m) \in A \setminus \{g_1, g_2, \dots, g_{n+1}\}$ . This contradiction shows the **surjectivity** of  $g$ .

We know  $g$  is **injective** by (\*).  $\blacksquare$

**Corollary 9.2.7.** (1) **A set  $B$  is infinite if there is an injection  $f$  from some infinite set  $A$  to  $B$ .**

(2) **A set  $B$  is uncountable if there is an injection  $f$  from some uncountable set  $A$  to  $B$ .**

**Proof.** The proofs of the two parts are similar. So we concentrate on (2) and leave the proof of (1) as an exercise.  9c

As  $f$  is an injection  $A \rightarrow B$ , Exercise 8.2.5 implies that  $A$  has the same cardinality as  $\text{range}(f)$ . Since  $A$  is uncountable, Lemma 9.2.1 tells us  $\text{range}(f)$  is also uncountable. Recall from Remark 7.2.3(2) that  $\text{range}(f) \subseteq B$ . Hence  $B$  is uncountable too by Proposition 9.2.6(2).  $\square$

**Example 9.2.8.** The set of all programs is **countable**.

**Proof.** Every program is stored in a computer as a string over  $\{0,1\}$ . So the set of all programs is a subset of the set  $\{0,1\}^*$  of all strings over  $\{0,1\}$ , which we know is countable from Proposition 9.1.6. So Proposition 9.2.6(2) tells us that the set of all programs is countable.  $\square$

## 9.3 Uncountable sets

**Theorem 9.3.1** (Cantor 1891). No set  $A$  has the same cardinality as  $\mathcal{P}(A)$ .

	0	1	2	3	4	...
$f(0)$	$\boxed{\notin}$	$\in$	$\notin$	$\notin$	$\notin$	...
$f(1)$	$\in$	$\boxed{\notin}$	$\in$	$\notin$	$\in$	...
$f(2)$	$\notin$	$\in$	$\boxed{\in}$	$\notin$	$\in$	...
$f(3)$	$\notin$	$\notin$	$\in$	$\boxed{\notin}$	$\notin$	...
$f(4)$	$\in$	$\notin$	$\in$	$\in$	$\boxed{\notin}$	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
$R$	$\in$	$\in$	$\notin$	$\in$	$\in$	...

$x \in f(x) \Rightarrow x \notin R$   
 $x \notin f(x) \Rightarrow x \in R$

Figure 9.6: Illustration of Cantor's diagonal argument

**Proof.** We consider here only the particular case when  $A = \mathbb{N}$ . The general case is very similar, and is left as an exercise. ✎ 9d

Given any function  $f: \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N})$ , we will produce an element of  $\mathcal{P}(\mathbb{N})$  that is not equal to  $f(x)$  for any  $x \in \mathbb{N}$ . This will show that there is no **surjection**  $f: \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N})$ , and thus  $\mathbb{N}$  cannot have the **same cardinality** as  $\mathcal{P}(\mathbb{N})$ .

Let  $f: \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N})$ . Define  $R = \{x \in \mathbb{N} : x \notin f(x)\}$ . Then  $R \in \mathcal{P}(\mathbb{N})$  by the definition of power sets. We claim that  $R \neq f(x)$  for any  $x \in \mathbb{N}$ . We prove this by contradiction. Suppose we have  $a \in \mathbb{N}$  such that  $R = f(a)$ . From the definition of  $R$ ,

$$\forall x \in \mathbb{N} \quad (x \in R \Leftrightarrow x \notin f(x)). \quad (\dagger)$$

As  $R = f(a)$ , applying  $(\dagger)$  to  $x = a$  gives

$$a \in f(a) \Leftrightarrow a \notin f(a). \quad (\ddagger)$$

Split into two cases.

- Case 1: assume  $a \in f(a)$ . Then  $a \notin f(a)$  by the  $\Rightarrow$  part of  $(\ddagger)$ . This contradicts our assumption that  $a \in f(a)$ .
- Case 2: assume  $a \notin f(a)$ . Then  $a \in f(a)$  by the  $\Leftarrow$  part of  $(\ddagger)$ . This contradicts our assumption that  $a \notin f(a)$ .

In either case, we get a contradiction. This completes the proof of the claim and thus of the theorem. □

**Corollary 9.3.2.** Let  $A$  be a **countable infinite** set. Then  $\mathcal{P}(A)$  is **uncountable**. Hence  $\mathcal{P}(\mathbb{N})$  is **uncountable**.

**Proof.** We consider here only the particular case when  $A = \mathbb{N}$ . The general case is very similar, and is left as an exercise. ✎ 9e

According to the **definition of countability**, we need to show that  $\mathcal{P}(\mathbb{N})$  is infinite, and that  $\mathcal{P}(\mathbb{N})$  does not have the same cardinality as  $\mathbb{N}$ . We already have the latter from Theorem 9.3.1.

For the former, let  $f: \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N})$  defined by setting  $f(n) = \{n\}$  for each  $n \in \mathbb{N}$ . Then  $f$  is **injective** because if  $n_1, n_2 \in \mathbb{N}$  such that  $f(n_1) = f(n_2)$ , then  $\{n_1\} = \{n_2\}$ , and thus  $n_1 = n_2$  by the **definition of set equality**. Recall that  $\mathbb{N}$  is infinite from Exercise 8.2.7. So Corollary 9.2.7(1) tells us  $\mathcal{P}(\mathbb{N})$  is infinite too, as required. □

## 9.4 Non-computability

**Assumption 9.4.1.** Our programs have no time and memory limitation.

**Corollary 9.4.2.** There is a subset  $S$  of  $\mathbb{N}$  that is not computed by any program, i.e., no program can, when given any input  $n \in \mathbb{N}$ ,

- output T if  $n \in S$ ; and
- output F if  $n \notin S$ .

**Proof.** Suppose that every subset  $S \subseteq \mathbb{N}$  is computed by a program. For each  $S \in \mathcal{P}(\mathbb{N})$ , let  $f(S)$  be the smallest program that computes  $S$ . This defines a function  $f: \mathcal{P}(\mathbb{N}) \rightarrow \{0, 1\}^*$ , because each program has a unique representation by an element of  $\{0, 1\}^*$  within a computer. This function  $f$  is **injective** because if  $S_1, S_2 \in \mathcal{P}(\mathbb{N})$  such that  $f(S_1) = f(S_2)$ , then  $S_1$  and  $S_2$  are computed by the same program, and thus  $S_1 = S_2$  by the **definition of set equality**. Recall from Corollary 9.3.2 that  $\mathcal{P}(\mathbb{N})$  is uncountable. So Corollary 9.2.7(2) implies  $\{0, 1\}^*$  is uncountable as well. This contradicts the countability of  $\{0, 1\}^*$  from Proposition 9.1.6.  $\square$

**Theorem 9.4.3** (Turing 1936, extra material). The set

$$H = \{\sigma \in \{0, 1\}^* : \sigma \text{ is a program that does not stop on the empty input}\}$$

is not computed by any program, i.e., no program can, when given any input  $\sigma \in \{0, 1\}^*$ ,

- output T if  $\sigma \in H$ ; and
- output F if  $\sigma \notin H$ .

**Proof.** Suppose not. Use a program that computes  $H$  to devise a program  $R$  satisfying

$$\forall \sigma \in \{0, 1\}^* \left( R \text{ stops on input } \sigma \iff \begin{array}{l} \sigma \text{ is a program that does} \\ \text{not stop on input } \sigma \end{array} \right). \quad (\S)$$

Applying (§) to  $\sigma = R$  gives

$$R \text{ stops on input } R \iff \begin{array}{l} R \text{ is a program that does} \\ \text{not stop on input } R \end{array} \quad (\P)$$

Split into two cases.

- Case 1: assume  $R$  stops on input  $R$ . Then  $R$  does not stop on input  $R$  by the  $\Rightarrow$  part of ( $\P$ ). This contradicts our assumption that  $R$  stops on input  $R$ .
- Case 2: assume  $R$  does not stop on input  $R$ . Then  $R$  stops on input  $R$  by the  $\Leftarrow$  part of ( $\P$ ). This contradicts our assumption that  $R$  does not stop on input  $R$ .

In either case, we get a contradiction, as required.  $\square$

## Tutorial exercises

An asterisk (\*) indicates a more challenging exercise.

- 9.1. It is often desirable for small sets to be closed under (binary) unions, i.e., the union of two small sets should also be small. (Can you guess why?) The aim of this exercise is to show that finite sets are a kind of small sets with this desirable property.

Let  $A$  and  $B$  be sets. Prove that, if  $A$  and  $B$  are finite, then  $A \cup B$  is finite.

(Hint: start with the special case when  $A \cap B = \emptyset$ . Then use Extra Exercise 4.9 to generalize to all cases.)

- 9.2. The aim of this exercise is to show that **countable** sets are another kind of small sets with the desirable property put forward in Exercise 9.1.

Let  $A$  and  $B$  be sets. Prove that, if  $A$  and  $B$  are countable, then  $A \cup B$  is countable.

(Hint: as in Exercise 9.1, start with the special case when  $A \cap B = \emptyset$ . Then use Extra Exercise 4.9 to generalize to all cases.)

- 9.3. Recall the definition of  $\bigcup_{i=0}^n A_i$  from Extra Exercise 4.11.

(Induction corner) Let  $A_0, A_1, A_2, \dots$  be countable sets. Prove by induction on  $n$  that  $\bigcup_{i=0}^n A_i$  is countable for every  $n \in \mathbb{N}$ .

- 9.4\* Recall the definition of  $\bigcup_{i=0}^{\infty} A_i$  from Extra Exercise 4.11.

(a) Someone claims that one can deduce directly from what we established in Exercise 9.3 that, if  $A_0, A_1, A_2, \dots$  are countable sets, then  $\bigcup_{i=0}^{\infty} A_i$  is countable. What is wrong with this claim?

(b) Prove that, if  $A_0, A_1, A_2, \dots$  are countable sets, then  $\bigcup_{i=0}^{\infty} A_i$  is countable.  
(Hint: find an injection  $\bigcup_{i=0}^{\infty} A_i \rightarrow \mathbb{N} \times \mathbb{N}$ .)

- 9.5. For each of the following propositions, determine whether it is true. Prove that your answers are correct.

(a) If a set  $B$  has an uncountable subset  $A$ , then  $B$  is uncountable.

(b) If  $A$  is an uncountable set and  $B$  is a countable set, then  $A \setminus B$  is uncountable.

- 9.6. Corollary 9.3.2 states that the power set of a countable infinite set is uncountable. The aim of this exercise is to show that this corollary remains true even when one omits the word “countable” there.

Prove that the power set  $\mathcal{P}(A)$  of any infinite set  $A$  is uncountable.

## Extra exercises

- 9.7. According to **our definition**, there are two kinds of countable sets: finite sets, and sets that have the same cardinality as  $\mathbb{N}$ . Conceivably, this may lead to painful case-splittings in proofs about countable sets. Fortunately, in many circumstances, one can ignore the finite case via what we establish in this exercise.

Prove that, for every countable set  $A$ , there is a countable infinite set  $A^*$  such that  $A \subseteq A^*$ .

- 9.8. We defined **countability** using (the **notion of same-cardinality** and thus) **bijections**. We show in this exercise how one could have defined countability using **injections** instead.

Prove that a set  $A$  is countable if and only if there is an injection  $A \rightarrow \mathbb{N}$ .

- 9.9. We saw in Theorem 9.1.5 that  $\mathbb{N} \times \mathbb{N}$  is countable. In this exercise, we generalize this to the Cartesian product of any two countable sets, not only  $\mathbb{N}$ .

Let  $A, B$  be countable sets. Use Theorem 9.1.5 to prove that  $A \times B$  is countable.