CS1231 Chapter 8

Cardinality

8.1 Pigeonhole principles

Proposition 8.1.1. Let $f: A \to B$ and $g: B \to C$.

(1) If f and g are surjective, then so is $g \circ f$.

(2) If f and g are injective, then so is $g \circ f$.

(3) If f and g are bijective, then so is $g \circ f$, and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof. (1) Suppose f and g are surjective. Let $z \in C$. Use the surjectivity of g to find $y \in B$ such that $z = g(y)$. Then use the surjectivity of f to find $x \in A$ such that $y = f(x)$. Now $z = g(y) = g(f(x)) = (g \circ f)(x)$ by Proposition 7.3.1, as required.

(2) Suppose f and g are injective. Let $x_1, x_2 \in A$ such that $(g \circ f)(x_1) = (g \circ f)(x_2)$. Then $g(f(x_1)) = g(f(x_2))$ by Proposition 7.3.1. The injectivity of g then implies $f(x_1) = f(x_2)$. So the injectivity of f tells us $x_1 = x_2$, as required.

(3) This follows from (1), (2), and Proposition 5.2.7. □

First Principle of Mathematical Induction (1PI, recall)**.** Let $b \in \mathbb{Z}$, and $P(n)$ be a statement for each integer $n \geqslant b$. Here are the steps to prove that $P(n)$ is true for all integers $n \geqslant b$ by 1PI.

Establish the **Basis:** Prove that $P(b)$ is true.

Make the **Induction Hypothesis:** Suppose $k \in \mathbb{Z}_{\geqslant b}$ such that $P(k)$ is true.

Complete the **Induction Step:** Use the Induction Hypothesis to prove that $P(k+1)$ is true.

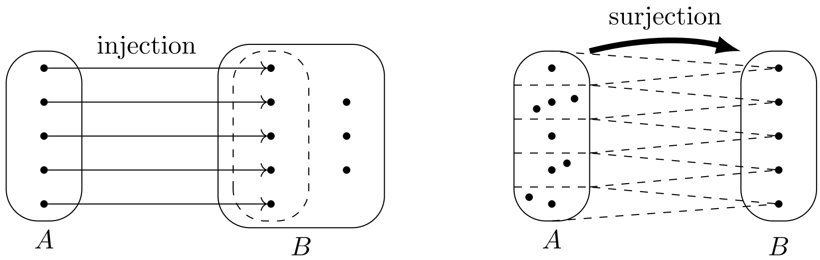

Figure 8.1: Injections, surjections, and the number of elements in the domain and the codomain

Theorem 8.1.2 (Pigeonhole Principle)**.** Let $A = \{x_1, x_2, \ldots, x_n\}$ and $B = \{y_1, y_2, \ldots, y_m\}$, where $n, m \in \mathbb{Z}_{\geqslant 0}$, the x's are different, and the y's are different. If there is an injection $A \to B$, then $n \leqslant m$.

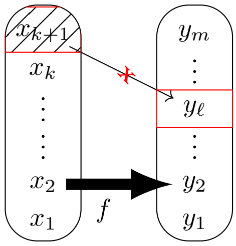

Figure 8.2: Induction proofs for the Pigeonhole Principles

Proof. We prove this by 1PI on n.

Basis: If $n = 0$ and $m \in \mathbb{Z}_{\geqslant 0}$, then $m \geqslant 0 = n$.

Induction Hypothesis: Suppose $k \in \mathbb{Z}_{\geqslant 0}$ such that the theorem is true when $n = k$.

Induction Step: Let $A = \{x_1, x_2, \ldots, x_{k+1}\}$ and $B = \{y_1, y_2, \ldots, y_m\}$, where $m \in \mathbb{Z}_{\geqslant 0}$, such that the x's are different, and the y's are different. Suppose we have an injection $f \colon A \to B$. Suppose $f(x_{k+1}) = y_\ell$. By the injectivity of f, as the x's are all different, no $i \in \{1, 2, \ldots, k\}$ can make $f(x_i) = f(x_{k+1}) = y_\ell$. All such $f(x_i)$'s must appear in the list

$$y_1, y_2, \ldots, y_{\ell-1}, y_{\ell+1}, \ldots, y_m.$$

Let $y_1^*, y_2^*, \ldots, y_{m-1}^*$ denote the elements of this list. Define $f^* \colon \{x_1, x_2, \ldots, x_k\} \to \{y_1^*, y_2^*, \ldots, y_{m-1}^*\}$ by setting $f^*(x_i) = f(x_i)$ for each $i \in \{1, 2, \ldots, k\}$. Then f^* is injective because if $i, j \in \{1, 2, \ldots, k\}$ such that $f^*(x_i) = f^*(x_j)$, then $f(x_i) = f(x_j)$ by the definition of f^*, and so the injectivity of f implies $x_i = x_j$. As the x's are all different and the y^*'s are all different, the induction hypothesis tells us $k \leqslant m - 1$. Hence $k + 1 \leqslant m$. □

Theorem 8.1.3 (Dual Pigeonhole Principle)**.** Let $A = \{x_1, x_2, \ldots, x_n\}$ and $B = \{y_1, y_2, \ldots, y_m\}$, where $n, m \in \mathbb{Z}_{\geqslant 0}$, the x's are different, and the y's are different. If there is a surjection $A \to B$, then $n \geqslant m$.

Proof. We prove this by 1PI on n.

Basis: Let $n = 0$ and f be a surjection $\{\} \to \{y_1, y_2, \ldots, y_m\}$, where $m \in \mathbb{Z}_{\geqslant 0}$, such that the y's are different. Suppose $m \geqslant 1$. Consider y_1. The surjectivity of f gives $x \in \{\}$ such that $f(x) = y$. However, no x can be in $\{\}$. This is a contradiction. So $m = 0 = n$.

Induction Hypothesis: Suppose $k \in \mathbb{Z}_{\geqslant 0}$ such that the theorem is true when $n = k$.

Induction Step: Let $A = \{x_1, x_2, \ldots, x_{k+1}\}$ and $B = \{y_1, y_2, \ldots, y_m\}$, where $m \in \mathbb{Z}_{\geqslant 0}$, such that the x's are different, and the y's are different. Suppose we have a surjection $f \colon A \to B$. Suppose $f(x_{k+1}) = y_\ell$. We split into two cases.

(1) Assume no $i \in \{1, 2, \ldots, k\}$ makes $f(x_i) = y_\ell$. Then all such $f(x_i)$'s must appear in the list

$$y_1, y_2, \ldots, y_{\ell-1}, y_{\ell+1}, \ldots, y_m.$$

Let $y_1^*, y_2^*, \ldots, y_{m-1}^*$ denote the elements of this list. Define $f^* \colon \{x_1, x_2, \ldots, x_k\} \to \{y_1^*, y_2^*, \ldots, y_{m-1}^*\}$ by setting $f^*(x_i) = f(x_i)$ for each $i \in \{1, 2, \ldots, k\}$.

We claim that f^* is surjective. To prove this, consider any y^*. It must equal y_h where $h \in \{1, 2, \ldots, m\} \setminus \{\ell\}$. By the surjectivity of f, we have $i \in \{1, 2, \ldots, k+1\}$ such that $y_h = f(x_i)$. As $\ell \neq h$ and the y's are all different, we know $y_\ell \neq y_h = f(x_i)$. Since $y_\ell = f(x_{k+1})$, we deduce that $i \neq k+1$. Hence $y_h = f(x_i) = f^*(x_i)$. As the x's are all different and the y^*'s are all different, the induction hypothesis tells us $k \geqslant m-1$. So $k+1 \geqslant m$.

(2) Assume some $i \in \{1, 2, \ldots, k\}$ makes $f(x_i) = y_\ell$. Define $f^* \colon \{x_1, x_2, \ldots, x_k\} \to \{y_1, y_2, \ldots, y_m\}$ by setting $f^*(x_i) = f(x_i)$ for each $i \in \{1, 2, \ldots, k\}$. Then f^* is surjective because, for each y_h, the surjectivity of f gives some x_i such that $y_h = f(x_i)$, and we can require this $i \neq k+1$ by our assumption; so $y_h = f(x_i) = f^*(x_i)$. As the x's are all different and the y's are all different, the induction hypothesis tells us $k \geqslant m$. So $k+1 \geqslant m+1 \geqslant m$. □

Theorem 8.1.4. Let $A = \{x_1, x_2, \ldots, x_n\}$ and $B = \{y_1, y_2, \ldots, y_m\}$, where $n, m \in \mathbb{Z}_{\geqslant 0}$, the x's are different, and the y's are different. Then $n = m$ if and only if there is a bijection $A \to B$.

Proof. ($\Rightarrow$) Suppose $n = m$. Define $f \colon A \to B$ by setting $f(x_i) = y_i$ for each $i \in \{1, 2, \ldots, n\}$. This definition is unambiguous because the x's are different.

To show injectivity, suppose $i, j \in \{1, 2, \ldots, n\}$ such that $f(x_i) = f(x_j)$. The definition of f tells us $f(x_i) = y_i$ and $f(x_j) = y_j$. Then $y_i = f(x_i) = f(x_j) = y_j$. So $i = j$ because the y's are different. This implies $x_i = x_j$.

Surjectivity follows from the observation that for every $y_i \in B$, we have $x_i \in A$ such that $f(x_i) = y_i$.

($\Leftarrow$) This follows directly from Theorem 8.1.2 and Theorem 8.1.3. □

Exercise 8.1.5. Prove the converse to Theorem 8.1.2 and the converse to Theorem 8.1.3. ✎ 8a

8.2 Same cardinality

Definition 8.2.1 (Cantor)**.** A set A is said to have the *same cardinality* as a set B if there is a bijection $A \to B$.

Note 8.2.2. We defined it means for a set to have the same cardinality as another set without defining what the cardinality of a set is.

Proposition 8.2.3. Let A, B, C be sets.

(1) A has the same cardinality as A. (reflexivity)

(2) If A has the same cardinality as B, then B has the same cardinality as A. (symmetry)

(3) If A has the same cardinality as B, and B has the same cardinality as C, then A has the same cardinality as C. (transitivity)

Proof. (Reflexivity.) It suffices to show that id_A is a bijection $A \to A$. For surjectivity, given any $x \in A$, we have $\mathrm{id}_A(x) = x$. For injectivity, if $x_1, x_2 \in A$ such that $\mathrm{id}_A(x_1) = \mathrm{id}_A(x_2)$, then $x_1 = x_2$.

(Symmetry.) If f is a bijection $A \to B$, then Proposition 7.4.3 tells us f^{-1} is a bijection $B \to A$.

(Transitivity.) If f is a bijection $A \to B$ and g is a bijection $B \to C$, then $g \circ f$ is a bijection $A \to C$ by Proposition 8.1.1(3). □

Definition 8.2.4. A set A is *finite* if it has the same cardinality as $\{1, 2, \ldots, n\}$ for some $n \in \mathbb{Z}_{\geqslant 0}$. In this case, we call n the *cardinality* or the *size* of A, and we denote it by $|A|$. A set is *infinite* if it is not finite.

8.3 Countability

Definition 8.3.1 (Cantor)**.** A set is *countable* if it is finite or it has the same cardinality as $\mathbb{Z}^+$. A set is *uncountable* if it is not countable.

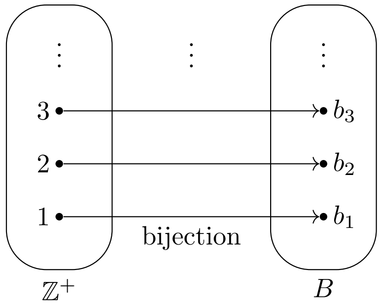

Figure 8.3: A countable infinite set B

Note 8.3.2. Some authors allow only infinite sets to be countable.

Example 8.3.3. (1) $\mathbb{Z}^+$ has the same cardinality as $\mathbb{Z}^+ \setminus \{1\}$ because the function $f : \mathbb{Z}^+ \to \mathbb{Z}^+ \setminus \{1\}$ satisfying $f(x) = x + 1$ for all $x \in \mathbb{Z}^+$ is a bijection. So $\mathbb{Z}^+ \setminus \{1\} = \{2, 3, 4, \dots\}$ is countable.

(2) $\mathbb{Z}^+$ has the same cardinality as $\mathbb{Z}^+ \setminus \{1, 3, 5, \dots\}$ because the function $g : \mathbb{Z}^+ \to \mathbb{Z}^+ \setminus \{1, 3, 5, \dots\}$ satisfying $g(x) = 2x$ for all $x \in \mathbb{Z}^+$ is a bijection. So $\mathbb{Z}^+ \setminus \{1, 3, 5, \dots\} = \{2, 4, 6, \dots\}$ is countable.

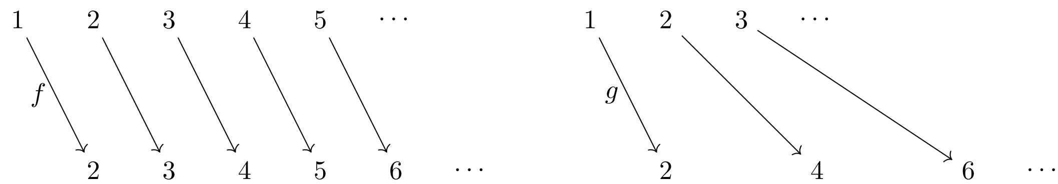

Figure 8.4: Removing 1 or half of the elements from $\mathbb{Z}^+$

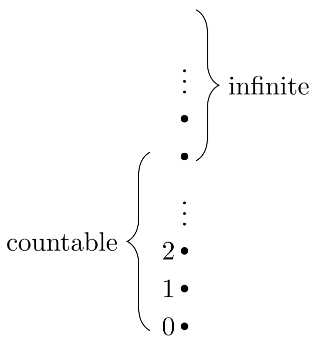

Figure 8.5: The smallest cardinalities

Proposition 8.3.4. 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 $B \setminus \{g_1, g_2, \ldots, g_i\} \neq \varnothing$ do:
   2.1. Pick any $g_{i+1} \in B \setminus \{g_1, g_2, \ldots, g_i\}$.
   2.2. Increment i to $i + 1$.

Suppose this procedure stops. Then a run results in $g_1, g_2, \ldots, g_\ell$, where $\ell \in \mathbb{Z}_{\geqslant 0}$. Define $g\colon \{1, 2, \ldots, \ell\} \to B$ by setting $g(i) = g_i$ for all $i \in \{1, 2, \ldots, \ell\}$. Notice $B \setminus \{g_1, g_2, \ldots, g_\ell\} = \varnothing$ 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 $g_{i+1} \notin \{g_1, g_2, \ldots, g_i\}$ by line 2.1. As g is a bijection $\{1, 2, \ldots, \ell\} \to B$, 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 $g\colon \mathbb{Z}^+ \to A$ by setting $g(i) = g_i$ for each $i \in \mathbb{Z}^+$. Then g is surjective by construction. It is injective because each $g_{i+1} \notin \{g_1, g_2, \ldots, g_i\}$ by line 2.1. As g is a bijection $\mathbb{Z}^+ \to A$, we deduce that A is countable.

Next, we verify that A is infinite. In view of the definition of infinite sets, it suffices to show that no function $f\colon \{1, 2, \ldots, n\} \to A$ where $n \in \mathbb{Z}_{\geqslant 0}$ can be surjective. Take any function $f\colon \{1, 2, \ldots, n\} \to A$, where $n \in \mathbb{Z}_{\geqslant 0}$. Now $f(1), f(2), \ldots, f(n)$ are all elements of A. Each of these is g_i for some $i \in \mathbb{Z}^+$ by the definition of A. Say $f(1), f(2), \ldots, f(n)$ are $g_{i_1}, g_{i_2}, \ldots, g_{i_n}$ respectively, where $i_1, i_2, \ldots, i_n \in \mathbb{Z}^+$. Let i be the largest element of the nonempty set $\{1, i_1, i_2, \ldots, i_n\}$. Then $g_{i+1} \in A$ and

$$g_{i+1} \notin \{g_1, g_2, \ldots, g_i\} \supseteq \{g_{i_1}, g_{i_2}, \ldots, g_{i_n}\} = \{f(1), f(2), \ldots, f(n)\}.$$

This shows f is not surjective. □

Proposition 8.3.5. Any subset A of a countable set B is countable.

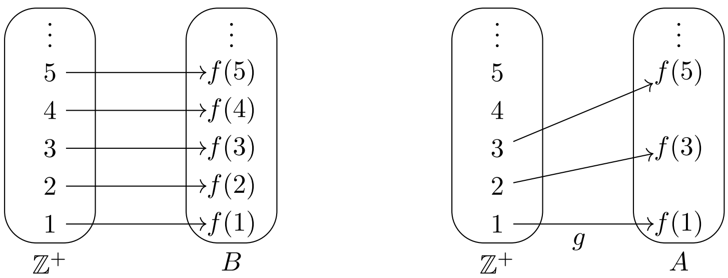

Figure 8.6: Countability of any subset A of a countable set B

Proof. If B is finite, then let f be a bijection $\{1, 2, \ldots, |B|\} \to B$, else let f be a bijection $\mathbb{Z}^+ \to B$. Run the following procedure.

1. Initialize $i = 0$.
2. While $A \setminus \{g_1, g_2, \ldots, g_i\} \neq \varnothing$ do:
   2.1. Note that $A \setminus \{g_1, g_2, \ldots, g_i\} \neq \varnothing$ when this line is reached. If $a_i \in A \setminus \{g_1, g_2, \ldots, g_i\}$, then $a_i = f(m)$ for some $m \in \mathbb{Z}^+$ because f is a surjection $\mathbb{Z}^+ \to A$. This says $\{m \in \mathbb{Z}^+ : f(m) \in A \setminus \{g_1, g_2, \ldots, g_i\}\} \neq \varnothing$, and so it must have a smallest element by the Well-Ordering Principle. Call this smallest element m_{i+1}.
   2.2. Set $g_{i+1} = f(m_{i+1})$. Note that $g_{i+1} \in A \setminus \{g_1, g_2, \ldots, g_i\}$ by the choice of m_{i+1}.
   2.3. Increment i to $i + 1$.

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

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

where $\ell \in \mathbb{Z}_{\geqslant 0}$. Define $g\colon \{1, 2, \ldots, \ell\} \to A$ by setting $g(i) = g_i$ for all $i \in \{1, 2, \ldots, \ell\}$.

Notice $A \setminus \{g_1, g_2, \ldots, g_\ell\} = \varnothing$ 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 because each $g_{i+1} \notin \{g_1, g_2, \ldots, g_i\}$ by line 2.2.

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

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

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

Define $g\colon \mathbb{Z}^+ \to A$ by setting $g(i) = g_i$ for all $i \in \mathbb{Z}^+$.

We claim that $m_{i+1} < m_{i+2}$ for all $i \in \mathbb{Z}_{\geqslant 0}$. Suppose not. Let $i \in \mathbb{Z}_{\geqslant 0}$ such that $m_{i+1} \geqslant m_{i+2}$. Line 2.2 tells us $g_{i+1} = f(m_{i+1})$ and $g_{i+2} = f(m_{i+2})$, but $g_{i+2} \neq g_{i+1}$. So $m_{i+1} \neq m_{i+2}$. This implies $m_{i+1} > m_{i+2}$. Note that $f(m_{i+2}) = g_{i+2} \in A \setminus \{g_1, g_2, \ldots, g_i\} \subseteq A \setminus \{g_1, g_2, \ldots, g_i\}$. So $m_{i+2} \in \{m \in \mathbb{Z}^+ : f(m) \in A \setminus \{g_1, g_2, \ldots, g_i\}\}$. However, we chose m_{i+1} to be the smallest element of this set, and $m_{i+2} < m_{i+1}$. This contradiction shows the claim.

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

We know g is injective because each $g_{i+1} \notin \{g_1, g_2, \ldots, g_i\}$ by line 2.2.

As g is a bijection $\mathbb{Z}^+ \to A$, we deduce that A is countable. □

8.4 More countable sets

Definition 8.4.1 (recall)**.** An integer is *even* if it is $2x$ for some $x \in \mathbb{Z}$. An integer is *odd* if it is $2x + 1$ for some $x \in \mathbb{Z}$.

Fact 8.4.2. Any integer is either even or odd, but not both.

Proof. We prove by induction on n that every $n \in \mathbb{Z}_{\geqslant 0}$ is either even or odd. For the basis, we know 0 is even because $0 = 2 \times 0$. For the induction step, assume $k \in \mathbb{Z}_{\geqslant 0}$ that is either even or odd. If k is even, say $k = 2x$ where $x \in \mathbb{Z}$, then $k + 1 = 2x + 1$, which is odd. If k is odd, say $k = 2x + 1$ where $x \in \mathbb{Z}$, then $k + 1 = 2x + 2 = 2(x + 2)$, which is even. So $k + 1$ is either even or odd in either case. This completes the induction.

Consider $n \in \mathbb{Z}^-$. We know $-n \in \mathbb{Z}^+$ and so it must be even or odd by the previous paragraph. If $-n$ is even, say $-n = 2x$ where $x \in \mathbb{Z}$, then $n = 2(-x)$, which is even. If $-n$ is odd, say $-n = 2x + 1$ where $x \in \mathbb{Z}$, then $n = -2x - 1 = 2(-x - 1) + 1$, which is odd. So $-n$ is either even or odd in either case.

Finally, suppose $n \in \mathbb{Z}$ that is both even and odd, say $2x = n = 2y + 1$ where $x, y \in \mathbb{Z}$. Then $x - y \in \mathbb{Z}$ but $x - y = 1/2 \notin \mathbb{Z}$. This is a contradiction. So no $n \in \mathbb{Z}$ can be both even and odd. □

Proposition 8.4.3. $\mathbb{Z}$ is countable.

Proof. Define $f\colon \mathbb{Z} \to \mathbb{Z}^+$ by setting, for each $x \in \mathbb{Z}$,

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

This f is well defined because if $x > 0$, then $2x > 0$ as well; and if $x \leqslant 0$, then $-2x + 1 \geqslant -2 \times 0 + 1 = 1$. In view of Proposition 8.2.3 (2), it suffices to show that f is a bijection.

To show surjectivity, pick any $y \in \mathbb{Z}^+$. Then Fact 8.4.2 tells us that y is either even or odd. If y is even, say $y = 2n$ where $n \in \mathbb{Z}$, then $n = y/2 > 0$, and so $f(n) = 2n = y$. If y is odd, say $y = 2n + 1$ where $n \in \mathbb{Z}$, then $n = (y - 1)/2 \geqslant (1 - 1)/2 = 0$, and so $f(-n) = -2(-n) + 1 = 2n + 1 = y$. Thus some $n \in \mathbb{Z}$ makes $f(n) = y$ in either case.

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 Fact 8.4.2, and so $x_1 = x_2$. If $f(x_1)$ is odd, then $f(x_1) = -2x_1 + 1$ and $f(x_2) = -2x_2 + 1$ by Fact 8.4.2, and so $x_1 = x_2$. Thus $x_1 = x_2$ in either case. □

Theorem 8.4.4 (Cantor 1877)**.** $\mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0}$ is countable.

Proof sketch.

$$
\begin{array}{cccccc}
\vdots & \vdots & \vdots & \vdots & \vdots & \iddots \\
(0,4) & (1,4) & (2,4) & (3,4) & (4,4) & \cdots \\
(0,3) & (1,3) & (2,3) & (3,3) & (4,3) & \cdots \\
(0,2) & (1,2) & (2,2) & (3,2) & (4,2) & \cdots \\
(0,1) & (1,1) & (2,1) & (3,1) & (4,1) & \cdots \\
(0,0) & (1,0) & (2,0) & (3,0) & (4,0) & \cdots
\end{array}
$$

The function $f \colon \mathbb{Z}^+ \to \mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0}$ such that $f(1), f(2), f(3), \ldots$ are respectively

$$(0,0), (1,0), (0,1), (2,0), (1,1), (0,2), (3,0), (2,1), (1,2), (0,3), (4,0), (3,1), (2,2), (1,3), (0,4), \ldots$$

following the arrows in the diagram above is a bijection. This shows $\mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0}$ is countable. □

Proposition 8.4.5. $\{0,1\}^*$ is countable.

Proof sketch. Let $f \colon \mathbb{Z}^+ \to \{0,1\}^*$ such that $f(1), f(2), f(3), \ldots$ are respectively

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

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

Corollary 8.4.6. The set of all computer programs is countable.

Proof sketch. Each program has a unique representation by a string over $\{0,1\}$ within a computer. So we can consider the set of all computer programs as a subset of $\{0,1\}^*$. As the latter set is countable by Proposition 8.4.5, so is the former, by Proposition 8.3.4. □