Chapter 7 Lecture Notes

1 Equinumerous Sets (7.1)

We start with with some definitions formalizing the idea of two sets having the same size without counting how many elements a set has.

Definition 1.1. *Let A, B be sets. Say that A is equinumerous to B, written $A \sim B$, if there is a bijection $f : A \to B$.*

We also want to distinguish between sizes of sets.

Definition 1.2. *For $n \in \mathbb{N}$, let $I_n = \{i \in \mathbb{N} : 1 \leq i \leq n\} = \{1, \ldots, n\}$ (Note that $I_0 = \emptyset$). Say a set A is finite if there is an $n \in \mathbb{N}$ such that $A \sim I_n$. Say a set is infinite if it is not finite.*

Now we'll provide several examples of sets which are equinumerous.

1. $\{1,3,5,7\} \sim \{1,2,3,4\} = I_4$. This can be seen by writing down a bijection like $\{(1,1),(3,2),(5,3),(7,4)\}$. Hence the set $\{1,3,5,7\}$ is finite.

2. Let $E = \{2n : n \in \mathbb{Z}\}$. Then $E \sim \mathbb{Z} \setminus E = \{2n+1 : n \in \mathbb{Z}\}$. To show this define $f : E \to \mathbb{Z} \setminus E$ by $f(2n) = 2n+1$. We prove it's a bijection. Onto: For $2n+1 \in \mathbb{Z} \setminus E$, $2n+1 = f(2n)$ so $2n+1$ is in the range of f. 1-1: Suppose $2n+1 = f(2n) = f(2m) = 2m+1$. Then $2n = 2m$.

3. $E \sim \mathbb{Z}$. Define $f : \mathbb{Z} \to E$ by $f(n) = 2n$ and we show it is a bijection. Onto: For $2n \in E$, $2n = f(n)$. 1-1: Suppose $2n = f(n) = f(m) = 2m$. Then $n = m$.

4. $\mathbb{Z} \sim \mathbb{N}$. Define $f : \mathbb{Z} \to \mathbb{N}$ by

$$f(n) = \begin{cases} 2n-1 & n > 0 \\ -2n & n \leq 0 \end{cases}$$

   Now show this is a bijection. Onto: Let $n \in \mathbb{N}$. If $n = 2k$ for $k \geq 0$. Then $f(-k) = -2(-k) = 2k = n$. If $n = 2k-1$ for $k > 0$, then $f(k) = 2k-1 = n$. 1-1: Let $f(n) = f(m)$. If $f(n) = f(m)$ is even, then $n, m \leq 0$ so $-2n = f(n) = f(m) = -2m$ and thus $n = m$. If $f(n) = f(m)$ is odd, then $n, m > 0$ so $2n-1 = f(n) = f(m) = 2m-1$ and thus $n = m$.

5. $(0,1) \sim (1,2)$. Define $f : (0,1) \to (1,2)$ by $f(x) = x+1$. Note that this is a function into $(1,2)$ since if $0 < x < 1$, then $1 < x+1 < 2$. It is 1-1 since $x+1 = y+1 \to x = y$, and it is onto since for $y \in (1,2)$, $y-1 \in (0,1)$ and $f(y-1) = y$.

6. $(0,1) \sim (0,2)$. Define $f : (0,1) \to (0,2)$ by $f(x) = 2x$. This can be shown to be a bijection in a way similar to the last example.

7. For $a, b \in \mathbb{R}$, $(0,1) \sim (a,b)$, with a specific bijection being $f(x) = (b-a)x + a$. This is a function into (a,b) since if $0 < x < 1$, then $0 < (b-a)x < b-a$ and $a < (b-a)x + a < b$.

8. $(-\pi/2, \pi/2) \sim \mathbb{R}$ with a bijection being $\tan(x)$.

9. $\mathbb{R} \sim (0, \infty)$ with a bijection being e^x.

We also want a result that lets us combine these results.

Theorem 1.3. *Let A, B, C be sets.*

a) $A \sim A$.

b) If $A \sim B$, then $B \sim A$.

c) If $A \sim B$ and $B \sim C$, then $A \sim C$.

Proof. a) The identity map $i_A : A \to A$ is a bijection.

b) Suppose $f : A \to B$ is a bijection. Then $f^{-1} : B \to A$ is a bijection.

c) Suppose $f : A \to B$ and $g : B \to C$ are bijections. Then $g \circ f : A \to C$ is a bijection. □

This result allows us to show that every finite interval (a, b) is equinumerous to $\mathbb{R}$ and $(0, \infty)$. We also see that many sets are equinumerous to $\mathbb{N}$, and this suggests the following definitions.

Definition 1.4. *Say a set is denumerable (or countably infinite) if it is equinumerous to $\mathbb{N}$. A set is countable if it is finite or denumerable. A set is uncountable if it is not countable.*

We prove two more theorems about how we can combine bijections.

Theorem 1.5. *If $A \sim B$ and $C \sim D$, then $A \times C \sim B \times D$.*

Proof. Let $f : A \to B$ and $g : C \to D$ be bijections. Define $h : A \times C \to B \times D$ by $h(x, y) = (f(x), g(y)) \in B \times D$. We show this is a bijection. Onto: Let $(b, d) \in B \times D$. Find $a \in A$ so $f(a) = b$ and find $c \in C$ so $g(c) = d$. Then $h(a, c) = (f(a), g(c)) = (b, d)$. 1-1: Suppose $(x_1, y_1), (x_2, y_2) \in A \times C$ and $h(x_1, y_1) = h(x_2, y_2)$. So $(f(x_1), g(y_1)) = (f(x_2), g(y_2))$. Then $f(x_1) = f(x_2)$ and $g(y_1) = g(y_2)$. Then $x_1 = x_2$ and $y_1 = y_2$ so $(x_1, y_1) = (x_2, y_2)$. □

Theorem 1.6. *Suppose $A \sim B$ and $C \sim D$, and suppose that $A \cap C = \emptyset = B \cap D$. Then $A \cup C \sim B \cup D$.*

Proof. Let $f : A \to B$ and $g : C \to D$ be bijections. Define $h : A \cup C \to B \cup D$ by

$$h(x) = \begin{cases} f(x) & x \in A \\ g(x) & x \in C \end{cases}$$

Since $A \cap C = \emptyset$, h assigns a unique element of $B \cup D$ to each $x \in A \cup C$. So h is a function, and we will show it is a bijection. Onto: Let $z \in B \cup D$. If $z \in B$, there is an $x \in A$ so $h(x) = f(x) = z$. If $z \in D$, there is a $y \in C$ so $h(y) = g(y) = z$. Either way $z \in Ran(h)$. 1-1: Let $x, y \in A \cup C$ and suppose $h(x) = h(y)$. There are two cases. If $h(x) = h(y) \in B$, then since $B \cap D = \emptyset$, it must be that $x, y \in A$. Then $h(x) = h(y)$ implies that $f(x) = f(y)$, so $x = y$. If $h(x) = h(y) \in D$, then $x, y \in C$. That implies $g(x) = g(y)$, so $x = y$. So in either case $x = y$, and h is injective. □

2 Finite Sets

Recall that a set is finite if it is equinumerous to I_n for some $n \in \mathbb{N}$. However, we would like to refer to *the* size of a finite set and the definition doesn't guarantee that a set can be equinumerous to at most one I_n. To this end, we begin by showing that if a set A is finite, there is a unique $n \in \mathbb{N}$ such that $A \sim I_n$.

Lemma 2.1. *For a set A, $A \sim \emptyset$ iff $A = \emptyset$.*

Proof. One direction is clear since $\emptyset \sim \emptyset$. For the other direction, let $f : \emptyset \to A$ be a bijection. Since $f \subseteq \emptyset \times A = \emptyset$, $f = \emptyset$. But since f is a bijection, $A \subseteq Ran(f) = \emptyset$. So $A = \emptyset$. □

Lemma 2.2. *For a set A, $A \sim I_1$ iff $A = \{a\}$ for some a.*

Proof. For one direction, if $A = \{a\}$, then $f : A \to I_1$ defined by $f(a) = 1$ is a bijection.

For the other direction, let $f : I_1 \to A$ be a bijection. Let $a = f(1)$. We will show that $A = \{a\}$. Since $f(1) = a \in A$, $\{a\} \subseteq A$. Also, since f is a bijection, $A \subseteq Ran(f) = \{a\}$ and so $A = \{a\}$. □

Lemma 2.3. *Let $n \geq 1$. Suppose $A \sim I_n$ and let $x \in A$. Then $A \setminus \{x\} \sim I_{n-1}$.*

Proof. If $n = 1$, then $A = \{x\}$, so $A \setminus \{x\} = \emptyset = I_0$. So we may assume that $n > 1$. Let $f : A \to I_n$ be a bijection, and let $f(x) = i$. Use this to define a function $g : A \setminus \{x\} \to I_{n-1}$ by

$$g(a) = \begin{cases} f(a) & f(a) < i \\ f(a) - 1 & f(a) > i \end{cases}$$

This is defined for every element of $A \setminus \{x\}$ since x is the only element of A so $f(x) = i$ by the injectivity of f. And $g(a)$ is always an element of I_{n-1}, since values always remain at least 1, but some may be decreased by 1 to be at most $n - 1$. So g is in fact a function, and we then have to show that g is a bijection. Onto: Let $j \in I_{n-1}$. If $j < i$, then find an $a \in A \setminus \{x\}$ so $f(a) = j$ then also $g(a) = j$. If $i \leq j$, find an $a \in A \setminus \{x\}$ so $f(a) = j + 1$ then $g(a) = f(a) - 1 = j + 1 - 1 = j$. In either case we can find an $a \neq x$ since $f(x) = i$ and f is injective. 1-1: Let $y, z \in A \setminus \{x\}$ and assume $g(y) = g(z)$. If $g(y) = g(z) < i$, then $f(y) = g(y) = g(z) = f(z)$, so $y = z$. If $g(y) = g(z) \geq i$, then $f(y) - 1 = g(y) = g(z) = f(y) - 1$ so $f(y) = f(z)$ and $y = z$. So in either case $y = z$ and f is 1-1. □

We are now in a position to prove our main theorem. The proof proceeds by induction, with the previous lemma being a key fact used in the inductive step.

Theorem 2.4. *For all $n, m \in \mathbb{N}$, $I_m \sim I_n$ iff $m = n$.*

Proof. [$\Leftarrow$] This is clear since $I_n \sim I_n$.

[$\Rightarrow$] By the first lemma, if $I_m \sim I_0$, then $I_m = \emptyset$ and the only way for this to happen is if $m = 0$. So we will restrict ourselves to $n, m \geq 1$. In this case, we prove the following somewhat stronger statement which implies the contrapositive (the contrapositive being $m \neq n \to I_m \not\sim I_n$):

Let $m, n \geq 1$. Suppose that $m < n$ and $f : I_n \to I_m$. Then f is not injective.

We prove this statement by induction on m. Specifically, we prove $\forall m \geq 1\, S(m)$ where $S(m)$ is the statement

$$\forall n > m\,(\text{ If } f : I_n \to I_m \text{ then } f \text{ is not 1-1})$$

Base case of $m = 1$: Let $n > 1$. So $I_1 = \{1\}$ and $I_n = \{1, 2, \ldots, n\}$. Then for $f : I_n \to I_1$, $f(1) = f(2) = 1$ (indeed f sends every number to 1). Thus f isn't injective.

Inductive step: Let $m > 1$. Assume $S(m)$ is true, let $n > m + 1$, and let $f : I_n \to I_{m+1}$. To prove $S(m + 1)$, we must show f isn't 1-1. We have $n \in I_n$, so let $i = f(n) \in I_{m+1}$. If there is a $k < n$ so $f(k) = i$, then we know that f is not injective. So assume there is no $k < n$ with $f(k) = i$. Then if we restrict f to I_{n-1}, we see that $f \restriction I_{n-1} : I_{n-1} \to I_{m+1} \setminus \{i\}$. Towards a contradiction, assume this function is injective. From Lemma 2.3 we know that $I_{m+1} \setminus \{i\} \sim I_m$, so by composing functions there must be an injective function from I_{n-1} to I_m. But $n > m + 1$, so $n - 1 > m$, which contradicts our inductive assumption of $S(m)$. Thus $f \restriction I_{n-1}$ isn't injective. Therefore, because $f \restriction I_{n-1}$ agrees with f on I_{n-1}, there are $x, y \in I_{n-1}$ so $x \neq y$ but $f(x) = f(y)$. This proves that f is not injective, and hence $S(m + 1)$ is true.

□

Given this theorem, we can talk about *the* size of a finite set.

Definition 2.5. *Let A be finite. The cardinality of A, written $|A|$, is the unique $n \in \mathbb{N}$ such that $I_n \sim A$.*

So $|I_n| = n$ and $|\{\emptyset, \{\emptyset\}\}| = 2$. Being able to talk about the cardinality of a finite set allows us to rephrase theorems we had previously proved for I_n.

Proposition 2.6. *Let A be finite and nonempty with $x \in A$. Then $|A \setminus \{x\}| = |A| - 1$.*

Proof. Suppose $|A| = n$ for $n \geq 1$. So $A \sim I_n$. We proved that $A \setminus \{x\} \sim I_{n-1}$. Thus $|A \setminus \{x\}| = n - 1$. □

We can also prove theorems about finite sets using induction on the size of the set.

Theorem 2.7. *If A is finite and $B \subseteq A$, then B is finite. More specifically, if $|A| = n$, then $|B| \leq n$ and if $B \neq A$ then in fact $|B| < n$.*

Proof. Use induction on $n \in \mathbb{N}$ to prove $\forall n \in \mathbb{N}\, S(n)$ where $S(n)$ is the statement: If $|A| = n$ and $B \subseteq A$, then B is finite and $|B| \leq n$.

Base case ($n = 0$): If $|A| = 0$, then $A = \emptyset$. So $B = \emptyset$ also. Thus B is finite and $|Bl = 0$.

Induction step: Let $n \geq 0$ and assume $S(n)$. Suppose $|A| = n + 1$ and $B \subseteq A$. If $B = A$, then B is finite and $|B| = n + 1$. If $B \neq A$, choose $x \in A \setminus B$. Then $B \subseteq A \setminus \{x\}$. Since $|A \setminus \{x\}| = n$, we may use our inductive assumption to assert that B is finite and $|B| \leq n$. This proves $S(n + 1)$. Note that in the case where $B \neq A$ we see $|B| < n + 1$, proving the claim at the end of the theorem. □

We have several standard set-theoretic operations, union and product. We want to prove theorems telling us the cardinality changes when we apply these operations to finite sets.

Theorem 2.8. *If A, B are disjoint finite sets, then $A \cup B$ is finite and $|A \cup B| = |A| + |B|$.*

Proof. Suppose $|A| = m$ and $|B| = n$. Then $A \sim I_m$ and $B \sim I_n \sim \{m + 1, \ldots, m + n\}$, with this last part witnessed by the bijection $f : I_n \to \{m + 1, \ldots, m + n\}$ defined by $f(x) = x + m$. Since $I_m \cap \{m + 1, \ldots, m + n\} = \emptyset$, we can apply Theorem 1.6 to see that $A \cup B \sim I_m \cup \{m + 1, \ldots, m + n\} = I_{m+n}$. Thus $A \cup B$ is finite and has cardinality $m + n = |A| + |B|$. □

What about sets that aren't disjoint? We employ a standard method: we first prove what happens for disjoint case and then we reduce the non-disjoint case to the disjoint case.

Theorem 2.9. *(Inclusion-Exclusion Principle) Let A, B be finite sets. Then $|A \cup B| = |A| + |B| - |A \cap B|$.*

Proof. First write $A \cup B = A \cup (B \setminus A)$. Since $B \setminus A \subseteq B$, $B \setminus A$ is finite by Theorem 2.7. And since A, $B \setminus A$ are disjoint we can apply Theorem 2.8 to see that $A \cup B$ is finite and $|A \cup B| = |A| + B \setminus A|$. But we can also write $B = (B \setminus A) \cup (B \cap A)$, and since these sets are finite and disjoint, $|B| = |B \setminus A| + |A \cap B|$. Combining these two equations, we get that $|A \cup B| = |A| + |B| - |A \cap B|$. □

This formula can be understood in the following way. How do you count the elements of $A \cup B$? First count the elements of A and B separately. But if there are any elements in both A and B, you have counted them twice. So subtract off the size of $A \cap B$. There is a more general version of the Inclusion-Exclusion Principle that allows you to determine $|A_1 \cup \cdots \cup A_n|$ for finite sets $A_1, \ldots, A_n$. As an example, the version for $n = 3$ looks like

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

We now turn to products, where the formula for the cardinality of a product is exactly what you think it should be.

Theorem 2.10. *If A, B are finite, then $A \times B$ is finite and $|A \times B| = |A| \cdot |B|$.*

Proof. By induction on n, prove $\forall n \in \mathbb{N} S(n)$ where $S(n)$ is the statement: If $|A| = n$ and B is finite, then $A \times B$ is finite and $|A \times B| = |A| \cdot |B|$.

Base case (n=0): If $|A| = 0$, then $A = \emptyset$ so $A \times B = \emptyset$. Thus $A \times B$ is finite and $|A \times B| = 0 = 0 \cdot |B|$.

Base case (n=1): If $|A| = 1$, then $A = \{a_0\}$. So $A \times B = \{(a_0, b) : b \in B\}$. Define $f : B \to A \times B$ by $f(b) = (a_0, b)$. This is a bijection, so since B is finite $A \times B$ is also finite, and $|A \times B| = |B| = 1 \cdot |B|$.

Induction step: Let $n \geq 1$ and assume $S(n)$. Let A have cardinality $n + 1$ and let B be finite. Take $a \in A$. Then $|A \setminus \{a\}| = n$ so $|A \setminus \{a\} \times B| = n \cdot |B|$ by our inductive assumption of $S(n)$. To use this fact, notice that we can write $A \times B = \{(a, b) : b \in B\} \cup (A \setminus \{a\} \times B)$. These sets are disjoint and finite (the first set is finite by the $n = 1$ case we already prove), so $A \times B$ is finite and

$$|A \times B| = |\{(a, b) : b \in B\}| + |A \setminus \{a\} \times B| = |B| + n \cdot |B| = (n + 1) \cdot |B| = |A| \cdot |B|.$$

This proves $S(n + 1)$ and hence the theorem. □

Our last topic concerning finite sets is the following combinatorial principle:

Theorem 2.11. *(Pigeonhole Principle) Suppose $|A| = m$ and $|B| = n$ with $m > n$. If $f : A \to B$, then f isn't injective.*

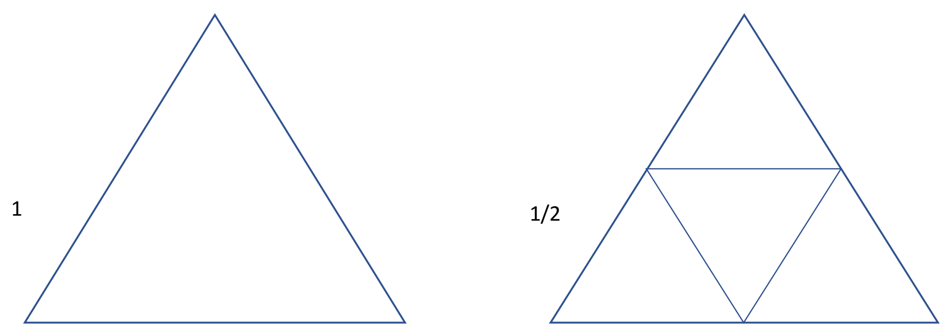
Proof. This follows from the fact, proved in Theorem 2.4, that if $m > n$ and $f : I_m \to I_n$, then f isn't 1-1. □

A statement of the Pigeonhole Principle in english is 'If you are putting things into containers and you have more things than containers, then two things must go in the same container.'

Example 1. *In a class with 17 people, two people must be born in the same month. To see this, since there are more people than months, the Pigeonhole Principle says that if we sort people by the month they were born, two people must be assigned the same month. More formally, if we define* $f : \{students\} \to \{months\}$ *by* $f(s) =$ *the month* s *was born, then* f *isn't injective so two students are assigned the same birth month.*

We also provide a more mathematical example.

Example 2. *Choose 5 points on or within an equilateral triangle of side length 1. Prove there must exist two points whose distance is at most* $\frac{1}{2}$*. To see this, split the triangle into 4 smaller equilateral triangles with sides of length* $\frac{1}{2}$*. By the Pigeonhole Principle, given 5 points, two must be in the same triangle, and two points in the same subtriangle have distance at most* $\frac{1}{2}$*. More formally, let* P *be the set of 5 points and let* T *be the set of 4 subtriangles. Define* $f : P \to T$ *by sending a point to the triangle it's in (breaking ties somehow if a point is on the boundary of two triangles). Since* $|P| > |T|$*,* f *isn't injective so two points must be sent to the same triangle.*



3 Denumerable Sets

Recall the following definitions.

Definition 3.1. *A set A is denumerable if $A \sim \mathbb{N}$. A set is countable if it is denumerable or finite.*

We have seen that the following sets are denumerable: $\mathbb{N}, \mathbb{Z}, \{2n : n \in \mathbb{Z}\}, \{n^2 : n \in \mathbb{N}\}, \mathbb{N}^+ = \{n \in \mathbb{N} : n \geq 1\}$. We haven't yet proven that these sets are infinite, but we are in a position to do so now.

Proposition 3.2. *For a set A, if there is $B \subseteq A$ such that $B \neq A$ and $B \sim A$, then A is infinite.*

Proof. Take such a $B \subseteq A$, so $B \neq A$ but $B \sim A$. Assume that A is finite, say $|A| = n$. In Theorem 2.7, we showed that in this situation $|B| < n$. This means that $B \not\sim A$, a contradiction. So A must be infinite. □

Since $\mathbb{N} \sim \mathbb{N}^+$, $\mathbb{N}$ is infinite, and so every denumerable set is infinite.

Although we won't prove it, the converse of this theorem holds. An important step in the proof, which we also won't prove, if the fact that every infinite set contains a denumerable subset. This fact along the the next theorem indicate that the denumerable sets are in some sense the smallest kind of infinite sets.

Theorem 3.3.

1. *If A is denumerable and $B \subseteq A$ is infinite, then B is denumerable.*
2. *If A is countable and $B \subseteq A$, then B is countable.*

Proof. We first prove part 1 for $A = \mathbb{N}$. Let $B \subseteq \mathbb{N}$ be infinite. We will define $f : \mathbb{N} \to B$ recursively. Let b_0 be the least element of B. This must exist by the Well-ordering Principle: if $S \subseteq \mathbb{N}$ is nonempty, then S has a least element. Define $f(0) = b_0$. Next, let b_1 be the least element of $B \setminus \{b_0\}$ and define $f(1) = b_1$. In general, let b_n be the least element of $B \setminus \{b_0, \ldots, b_{n-1}\}$ and define $f(n) = b_n$. This is always defined since B is infinite, so $B \setminus \{b_0, \ldots, b_{n-1}\}$ is always nonempty and thus has a least element. So we have a function $f : \mathbb{N} \to B$ and we must show that it is a bijection.

1-1: Let $n, m \in \mathbb{N}$ and assume that $n < m$. Then $b_m \in B \setminus \{b_0, \ldots, b_n, \ldots, b_{m-1}\}$, so $f(m) = b_m \neq b_n = f(n)$.

Onto: Let $b \in B$. Since there are only $b - 1$ numbers below b in $\mathbb{N}$, we can find an integer k so b is the least element of $B \setminus \{b_0, \ldots, b_k\}$. Then $f(k+1) = b$.

This finishes the proof if $A = \mathbb{N}$. If A is an arbitrary denumerable set, let $g : A \to \mathbb{N}$ be a bijection. Then $B \sim g(B)$ and $g(B)$ is an infinite subset of $\mathbb{N}$. Hence $G(B)$ is denumerable, and so B must also be denumerable.

For part 2, let A be countable and let $B \subseteq A$. If A is finite, then B is finite. If A is denumerable then either B is finite, or B is infinite, and then by part 1 B is denumerable. So in any case, B is countable.

□

Our next theorem provides another, more flexible, way of showing that a set is finite.

Theorem 3.4. *For a set A, TFAE (the following are equivalent):*

1. *A is countable.*

2. *$A = \emptyset$ or there is a surjection $\mathbb{N} \to A$.*

3. *There is an injection $f : A \to \mathbb{N}$.*

Proof. ($1 \Rightarrow 2$) Suppose $A \neq \emptyset$ is countable. If A is denumerable we can take f to be a bijection. If $|A| = n$ for $n \geq 1$, let $h : I_n \to A$ be a bijection. Define $g : \mathbb{N} \to I_n$ by

$$g(i) = \begin{cases} i & i \leq n \\ n & i > n \end{cases}$$

Then since g is onto, $f = h \circ g : \mathbb{N} \to A$ is onto.

($2 \Rightarrow 3$) If $A = \emptyset$, then $\emptyset$ is (vacuously) an injection from $\emptyset$ to $\mathbb{N}$. So assume $A \neq \emptyset$ and let $f : \mathbb{N} \to A$ be onto. Since f is onto, $f^{-1}(\{a\}) = \{n \in \mathbb{N} : f(n) = a\}$ is nonempty for each $a \in A$. Define a function $g : A \to \mathbb{N}$ by letting $g(a)$ be the least element of $f^{-1}(\{a\})$. To see that g is 1-1, let $a, b \in A$. So $g(a) \in f^{-1}(\{a\})$ and $g(b) \inf^{-1}(\{b\})$. This means $f(g(a)) = a$ and $f(g(b)) = b$. So if $g(a) = g(b)$, then $a = b$ since f is a function.

($3 \Rightarrow 1$) If $f : A \to \mathbb{N}$ is 1-1, then $f : A \to f(A)$ is a bijection. Since $f(A) \subseteq \mathbb{N}$, $f(A)$ is countable and so A is countable. □

When this theorem is used to show a set is countable, we are allowed to replace the 'ℕ' in parts 2 and 3 with any other set known to be countable. We will demonstrate this with some new examples of countable sets.

Example 3. *$\mathbb{N} \times \mathbb{N}$ is denumerable. $\mathbb{N} \times \mathbb{N}$ is infinite since $\mathbb{N} \times \{0\}$ is a subset equinumerous to $\mathbb{N}$. To see that $\mathbb{N} \times \mathbb{N}$ is countable, define a function $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $g(n, m) = 2^n 3^m$. This function is injective: if $2^{n_1} 3^{m_1} = 2^{n_2} 3^{m_2}$ with $n_1 \leq n_2$, we have $3^{m_1} = 2^{n_2 - n_1} 3^{m_2}$. But a power of 3 is odd, so $n_2 - n_1 = 0$ i.e. $n_2 = n_1$. Similarly $m_1 = m_2$ and so $(n_1, m_1) = (n_2, m_2)$.*

This, along with Theorem 1.5, implies a more general fact about products.

Corollary 3.5. *If A, B are denumerable, then $A \times B$ is denumerable.*

Example 4. *$\mathbb{Q}$ is denumerable. It is infinite since $\mathbb{N} \subseteq \mathbb{Q}$. Then we show $\mathbb{Q}$ is countable by applying Theorem 3.4 to the surjective function $f : \mathbb{Z} \times \mathbb{N}^+ \to \mathbb{Q}$ defined by $f(m, n) = \frac{m}{n}$. To get a more concrete idea of why $\mathbb{Q}$ is countable, we can list out all positive elements of $\mathbb{Q}$ based on the maximum of their numerator and denominator:*

$$\frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \frac{3}{2}, \frac{3}{3}, \frac{2}{3}, \frac{1}{3}, \frac{4}{1}, \ldots$$

We have yet to discuss the union of countable sets, and this will be the last topic of this section.

Theorem 3.6. 1. *If A, B are denumerable, then $A \cup B$ is denumerable.*

2. *If A, B are countable, then $A \cup B$ is countable.*

Proof. 1) First assume that $A \cap B = \emptyset$. Then since A, B are denumerable, $A \sim \mathbb{N} \sim \{2n : n \in \mathbb{N}\}$ and $B \sim \mathbb{N} \sim \{2n + 1 : n \in \mathbb{N}\}$. Then by Theorem 1.6, $A \cup B \sim \{2n : n \in \mathbb{N}\} \cup \{2n + 1 : n \in \mathbb{N}\} = \mathbb{N}$, so $A \cup B$ is denumerable. Now take A, B which are not necessarily disjoint. Then $A \cup B = A \cup (B \setminus A)$. These sets are disjoint, and there are two cases.

a) If $B \setminus A$ is infinite, then it is denumerable and we can use the first part of this proof.

b) If $B \setminus A$ is finite, say of cardinality n, then $B \setminus A \sim I_n$ and $A \sim \mathbb{N} \sim \{n+1, n+2, \ldots\}$ so $A \cup B \sim I_n \cup \{n+1, n+2, \ldots\} = \mathbb{N}^+$ and hence is denumerable.

2) Given countable sets A, B, consider A and $B \setminus A$. There are a few cases. If both are finite, then the union is finite. If both are denumerable, part 1 says the union is denumerable. If one is finite and the other is denumerable, proceed as in case 1b) from the first part of this theorem. □

We can extend this to finite unions. The proof is a standard proof by induction, with the base case being the previous theorem and the key part of the inductive step writing $A_1 \cup \cdots \cup A_n \cup A_{n+1}$ as $(A_1 \cup \cdots \cup A_n) \cup A_{n+1}$.

Theorem 3.7. *If $A_1, \ldots, A_n$ are denumerable (resp. countable) then $A_1 \cup \cdots \cup A_n$ is denumerable (countable).*

The last question is what happens when we take the union of a countably infinite collection of countable sets. It is possible for the union of countably many finite sets to be infinite. For example, if $A_n = \{n\}$, then each A_n is finite but $\bigcup_{n \in \mathbb{N}} A_n = \mathbb{N}$. Nevertheless, we have the following theorem.

Theorem 3.8. *If $\{A_n : n \in \mathbb{N}\}$ is a family of countable sets, then $\bigcup_{n \in \mathbb{N}} A_n = \mathbb{N}$ is countable.*

Proof. Let $A = \bigcup_{n \in \mathbb{N}} A_n = \mathbb{N}$. Since each A_n is countable, let $f_n : \mathbb{N} \to A_n$ be a surjection (using Theorem 3.4). Now define $f : \mathbb{N} \times \mathbb{N} \to A$ by $f(n, m) = f_n(m)$. Intuitively, f takes in a pair (n, m), uses the first coordinate n to determine which set it is looking at, i.e. A_n, and uses the second coordinate m to pick out the mth element of A_n. To complete the proof, we must show that f is onto. So let $x \in A$. Then for some $n \in \mathbb{N}$, $x \in A_n$. Since f_n maps onto A_n, find $m \in \mathbb{N}$ so $f_n(m) = x$. But then $f(n, m) = f_n(m) = x$. □

4 Uncountable Sets

We start investigating uncountable sets by rephrasing several theorems about denumerable sets.

Theorem 4.1. *1. If $B \subseteq A$ and B is uncountable, then A is uncountable.*

2. If A is uncountable and $B \subseteq A$ is countable, then $A \setminus B$ is uncountable.

3. If B is uncountable and $f : B \to A$ is 1-1, then A is uncountable.

4. If A is uncountable and $f : B \to A$ is onto, then B is uncountable.

Proof. For 1) use Theorem 3.3, for 2) use Theorem 3.6, and for 3) and 4) use Theorem 3.4. □

We have yet to produce any examples of uncountable sets. The operations of union and product don't allow us to obtain an uncountable set, but we have one remaining operation which works : the power set.

Theorem 4.2. *For any set A, $\mathcal{P}(A) \not\sim A$.*

Proof. Suppose $f : A \to \mathcal{P}(A)$ is surjective. We will obtain a contradiction, so in particular there can be no bijection from A to $\mathcal{P}(A)$.

For each $a \in A$, $f(a) \subseteq A$. For an element a, we can ask whether it is in $f(a)$ or not. Define the set $B = \{a \in A : a \notin f(a)\}$. So $B \subset A$. (We provide a couple of examples of how to deal with this set. Since $\emptyset \in \mathcal{P}(A)$ and f is onto, there is $a_0 \in A$ so $f(a_0) = \emptyset$. Then $a_0 \notin f(a_0)$ so $a_0 \in B$. Also since $A \in \mathcal{P}(A)$ and f is onto, there is $a_1 \in A$ so $f(a_1) = A$. Then $a_1 \in f(a_1)$ so $a_1 \notin B$.)

Now, since $B \in \mathcal{P}(A)$ and f is onto, there is $b \in A$ so $f(b) = B$. Now ask if $b \in B$ or not:

- If $b \in B$, then $b \in f(b)$, so $b \notin B$.
- If $b \notin B$ then $b \notin f(b)$, so $b \in B$.

One of these cases must occur, and both lead to a contradiction. So there can be no surjective function f.

□

Corollary 4.3. *$\mathcal{P}(\mathbb{N})$ is uncountable.*

Proof. There is an injection $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$, namely $f(n) = \{n\}$, so $\mathcal{P}(\mathbb{N})$ is infinite. But the theorem says $\mathcal{P}(\mathbb{N})$ is not denumerable, so it must be uncountable. □

Example 5. *Let $2^{\mathbb{N}}$ be the collection of infinite binary sequences. So elements of $2^{\mathbb{N}}$ are functions $f : \mathbb{N} \to \{0,1\}$ and can be thought of as $(x_0, x_1, x_2, \ldots)$ where each $x_i \in \{0,1\}$. This set is uncountable, and in fact $2^{\mathbb{N}} \sim \mathcal{P}(\mathbb{N})$. Define $g : \mathcal{P}(\mathbb{N}) \to 2^{\mathbb{N}}$ by $g(A) = \chi_A$ where χ_A is the characteristic function of A defined by*

$$\chi_A(n) = \begin{cases} 1 & n \in A \\ 0 & n \notin A \end{cases}$$

We show g is a bijection. 1-1: Suppose $A, B \subseteq \mathbb{N}$ and $\chi_A = \chi_B$. So $n \in A$ iff $\chi_A(n) = 1$ iff $\chi_B(n) = 1$ iff $n \in B$, and hence $A = B$. Onto: Given $f : \mathbb{N} \to \{0,1\}$, let $A = \{n \in \mathbb{N} : f(n) = 1\}$ and then $\chi_A = f$.

Our next result provides a more interesting example of an uncountable set. The method of proof is called *diagonalization*.

Theorem 4.4. *The interval* $(0,1)$ *in uncountable.*

For the proof we will be using the decimal representation of real numbers. For $x \in (0,1)$, $x = .a_1a_2a_3\ldots$ where each $a_i \in \{0,1,\ldots,9\}$. This means that $x = \sum_{i=1}^{\infty} \frac{a_i}{10^i} = \frac{a_1}{10} + \frac{a_2}{100} + \cdots$. This decimal expansion is unique *except* for when $x = .a_1a_2\ldots a_n\overline{9}$ with $a_n \neq 9$, and in this case x also equals $.a_1\ldots a_{n-1}(a_n+1)\overline{0}$. So for example, $.1\overline{9} = .2$ since

$$.1\overline{9} = \frac{1}{10} + \sum_{n=2}^{\infty} \frac{9}{10^i} = \frac{1}{10} + \frac{9/10^2}{1-1/10} = \frac{1}{10} + \frac{1}{10} = \frac{1}{5} = .2.$$

Proof. Assume that $(0,1)$ is countable. Then we can list $(0,1)$ as $\{a_1, a_2, \ldots\}$. Writing each a_n with its decimal expansion (choosing the expansion ending all zeros if its expansion isn't unique), we get the array

$$\begin{array}{ccllll} a_1 & = & .a_{11} & a_{12} & a_{13} & \ldots \\ a_2 & = & .a_{21} & a_{22} & a_{23} & \ldots \\ a_3 & = & .a_{31} & a_{32} & a_{33} & \ldots \\ \vdots & & & & & \ddots \end{array}$$

where each $a_{ij} \in \{0,\ldots,9\}$.

To get a contradiction, we will define a real number x so $x \in (0,1)$ but $x \neq a_n$ for any n. We define x by giving its decimal expansion, and we make $x \neq a_n$ by making sure x, a_n differ in at least one position.

Now define $x = .b_1b_2\ldots$ where $b_n = \begin{cases} 2 & a_{nn} \neq 2 \\ 3 & a_{nn} = 2 \end{cases}$. By construction $x \in (0,1)$. Since the decimal expansion of x contains only 2's and 3's, it must be unique. And for each $n \in \mathbb{N}$, $b_n \neq a_{nn}$, so x and a_n have different decimal representations, so $x \neq a_n$. This contradicts the fact that we assume we had a complete listing of $(0,1)$.

□

Since $(0,1) \sim \mathbb{R}$, we immediately have the following consequence.

Corollary 4.5. $\mathbb{R}$ *is uncountable.*

As another example, since $\mathbb{R}$ is uncountable and $\mathbb{Q} \subseteq \mathbb{R}$ is countable, the set of irrational numbers $\mathbb{R} \setminus \mathbb{Q}$ is uncountable.

5 The Cantor-Bernstein Theorem

We have seen that $(0,1) \sim (a,b) \sim (0,\infty) \sim \mathbb{R}$. We also know that $[0,1)$ is uncountable since it has an uncountable subset, but is it equinumerous to $(0,1)$? It is, but constructing an explicit bijection is difficult (what do you do with the point 0?). Instead, we prove the following important theorem which allows us to often forego finding a bijection.

Theorem 5.1. *(Cantor-Bernstein) Let A, B be sets and $f : A \to B$, $g : B \to A$ be injections. Then $A \sim B$.*

An equivalent formulation is: For sets A, B, if $A \sim B'$ where $B' \subseteq B$ and $B \sim A'$ where $A' \subseteq A$, then $A \sim B$.

Proof. Use the second statement. So let $f : A \to B'$ and $g : B \to A'$ be bijections, and $f^{-1} : B' \to A$ and $g^{-1} : A' \to B$ their inverses which are also bijections. We want to use these to construct a bijection $h : A \to B$. Both f and g^{-1} are functions taking elements of A to elements of B, so our bijection h will sometimes send a to $f(a)$, and sometimes send a to $g^{-1}(a)$. The problem is to figure out when to use f and when to use g^{-1}.

To this end, notice that for $x \in A$ we can apply f and g repeatedly to obtain a sequence $x, f(x), g(f(x)), f(g(f(x))), \ldots$. We can also ask how far *backwards* this sequence can go, i.e. how long of a sequence can we get by applying f^{-1} and g^{-1}?

- If $x \in A \setminus A'$, there is nothing in B which g maps to x. We will say that x has zero ancestors.
- If $x \in A'$, then $g^{-1}(x) \in B$. Call this the first ancestor of x. If $g^{-1}(x) \in B \setminus B'$ we can't go back any further, so x has only one ancestor.
- If $g^{-1}(x) \in B'$, then $f^{-1}(g^{-1}(x)) \in A$. Call this the second ancestor of x. If $f^{-1}(g^{-1}(x)) \in A \setminus A'$ we can't go back any further, so x has only two ancestors.
- If $f^{-1}(g^{-1}(x)) \in A'$, then $g^{-1}(f^{-1}(g^{-1}(x))) \in B$. Call this the third ancestor of x. If $g^{-1}(f^{-1}(g^{-1}(x))) \in B \setminus B'$ we can't go back any more so x has just 3 ancestors.
- And so on...

We will partition A into 3 sets, depending on how many ancestors they have:

- $A_0 = \{x \in A : x \text{ has an even number of ancestors}\}$ (The last ancestor is in $A \setminus A'$.)
- $A_1 = \{x \in A : x \text{ has an odd number of ancestors}\}$ (The last ancestor is in $B \setminus B'$.)
- $A_\infty = \{x \in A : x \text{ has an infinite number of ancestors}\}$

These sets form a partition of A, so they are pairwise disjoint and their union is all of A. We can similarly partition B into three sets B_0, B_1, B_∞. Note that $A \setminus A' \subseteq A_0$ and $B \setminus B' \subseteq B_0$.

What do elements in these sets look like? Given an element x with a last ancestor y, then y is obtained from x by going backwards using f^{-1} and g^{-1}, but it is also true that x can be obtained from y by going *forwards* using f and g.

- If $x \in A_0$, then its last ancestor is some $y \in A \setminus A'$ and $x = (g \circ f)^n(y)$, where $(g \circ f)^n$ means applying $g \circ f$ n times.
- If $x \in A_1$, then its last ancestor is some $y \in B \setminus B'$ and $x = g((f \circ g)^n(y))$.
- If $x \in B_0$, then its last ancestor is some $y \in B \setminus B'$ and $x = (f \circ g)^n(y)$.
- If $x \in B_1$, then its last ancestor is some $y \in A \setminus A'$ and $x = f((g \circ f)^n(y))$.

Now that we have an idea of what the elements of these sets look like, we can see what happens when we apply f or g^{-1} to elements of different types. If $x \in A_0$, then $f(x) = f((f \circ g)^n(y))$ for some $y \in A \setminus A'$. So $f(x) \in B_1$. If $x \in A_1$, then $f(x) = f(g((f \circ g)^n(y))) = (f \circ g)^{n+1}$ for some $y \in B \setminus B'$. So $f(x) \in B_0$. But also $f(x)$ must be in B'. However, it is also true that $g^{-1}(x) = (f \circ g)^n(y)$ for some $y \in B \setminus B'$ so $g^{-1}(x) \in B_0$. Finally, if $x \in A_\infty$, both $f(x)$ and $g^{-1}(x)$ are in B_∞.

With all of this preparation, we can finally define the bijection between A and B. Let $h : A \to B$ be given by

$$h(x) = \begin{cases} f(x) & x \in A_0 \cup A_\infty \\ g^{-1}(x) & x \in A_1 \end{cases}$$

First of all, h is a function since A_0, A_1, A_∞ partition A.

To see that h is 1-1, suppose $h(x) = h(y)$ for $x, y \in A$. This common value $h(x)$ must be in exactly one of B_0, B_1, B_∞, since they form a partition of B. If $h(x) \in B_0$, then as we have seen, x, y must both come from A_1. But on A_1, h is simply g^{-1} so then $g^{-1}(x) = g^{-1}(y)$, and thus $x = y$. Similarly if $h(x) = h(y) \in B_1$, then both $x, y \in A_0$ so it must be that $f(x) = f(y)$ which implies $x = y$. If $h(x) = h(y) \in B_\infty$, then $x, y \in A_\infty$ and the same argument shows $x = y$.

To see that h is onto, suppose $y \in B$. This y must be in exactly one of B_0, B_1, B_∞. If $y \in B_\infty$, then $f^{-1}(y)$ is defined and is in A_∞. Then $h(f^{-1}(y)) = f(f^{-1}(y)) = y$. If $y \in B_1$, then y has an odd number of ancestors, so it has at least one ancestor and so $f^{-1}(y)$ is defined and is in A_0. Then $h(f^{-1}(y)) = f(f^{-1}(y)) = y$. If $y \in B_0$, then $g(y)$ has one more ancestor so $g(y) \in A_1$. Then $h(g(y)) = g^{-1}(g(y)) = y$.

□

Corollary 5.2. $[0, 1) \sim (0, 1)$.

Proof. We have $(0, 1) \subseteq [0, 1)$. But also $[0, 1) \sim [\frac{1}{2}, 1) \subseteq (0, 1)$ where the bijection $f : [0, 1) \to [\frac{1}{2}, 1)$ is given by $f(x) = \frac{1}{2}x + \frac{1}{2}$. So by Cantor-Bernstein, $[0, 1) \sim (0, 1)$. □

As another example, we can show that $\mathbb{R} \times \mathbb{Q} \sim \mathbb{R}$ using Cantor-Bernstein. One injection is easy: $f : \mathbb{R} \to \mathbb{R} \times \mathbb{Q}$ defined by $f(x) = (x, 0)$ is clearly 1-1. For the other injection, use that $\mathbb{R} \times \mathbb{Q} \sim (0, 1) \times \mathbb{N}$ by Theorem 1.5. Now define a function $g : (0, 1) \times \mathbb{N} \to \mathbb{R}$ by $g(x, n) = n + x$. To see this is an injection, if $n + x = m + y$, then n, m are the integer parts of this number and x, y are the decimal parts (like splitting 17.19 into 17+.19) and so $n = m$ and $x = y$, which means $(n, x) = (m, y)$.