

Contents

Cardinality and Countability	1
Section 1.1: Countable Sets	1
Theorem: Countability of Unions	1
Theorem: Countability of Subsets	1
Theorem: Union of Finite Sets	1
Theorem: Disjoint Union of Countable Sets	2
Theorem: Cartesian Product of Natural Numbers	2
Theorem: Countability of the Rationals	3
Theorem: Countability of the Integers	3
Theorem: Finite Subset Cardinality	3
Theorem: Infinitude of the Natural Numbers	3
Section 1.2: Uncountable Sets	3
Theorem: Uncountability of \mathbb{R}	3
Theorem: Power Set Surjection	4
Section 1.3: Cantor–Schröder–Bernstein Theorem	5
Theorem: Cantor–Schröder–Bernstein	5
Axiomatic Set Theory	7
Axioms of Set Theory	7
Axiom: Existence	7
Axiom: Empty Set	8
Axiom: Pairing	8
Axiom: Extensionality	8
Axiom: Union	8
Axiom: Power Set	8
Axiom: Comprehension schema	9
Axiom: Union	9
Axiom: Infinity	9
Axiom: Regularity	10
Axiom: Replacement Schema	10
Axiom: Choice	10
Ordinal Numbers and Well-Orderings	11
Induction and Recursion	15

Cardinality and Countability

Section 1.1: Countable Sets

Definition (Denumerable Set). A set S is denumerable if there exists a function $f : S \rightarrow \mathbb{N}$ with f a bijection. We also say S is countably infinite.

Definition (Countable Set). We say S is countable if S is either finite or denumerable.

Theorem (Countability of Unions): If A and B are countable sets, then $A \cup B$ is countable.

Theorem (Countability of Subsets): If $A \subseteq B$, then if B is countable, then A is countable.

Theorem (Union of Finite Sets): If A and B are finite, then $A \cup B$ is finite.

Proof. If A is finite and B has one element, then we show that $A \cup B$ is finite (with two cases).

Afterward, for $|B| > 1$, we use induction on $|B|$. □

Definition (Finite Set). A set A is finite if there exists a bijection $f : S \rightarrow \{1, 2, \dots, n\}$ for some $n \in \mathbb{N} = \{0, 1, \dots\}$.

We write $|A| = n$.

Theorem (Disjoint Union of Countable Sets): If A is denumerable, B is finite, and $A \cap B = \emptyset$, then $A \cup B$ is denumerable.

Proof. There exists a bijection $f : A \rightarrow \mathbb{N}$ (since A is denumerable), and a bijection $g : B \rightarrow \{1, 2, \dots, n\}$ for some $n \in \mathbb{N}$ (since B is finite).

We create a new bijection $h : A \cup B \rightarrow \mathbb{N}$ by:

$$h(x) = \begin{cases} g(x) - 1 & x \in B \\ f(x) + n & x \in A \end{cases}.$$

Since $A \cap B = \emptyset$, we know that h is well-defined.

Now, we must show that h is a bijection.

Suppose $h(x) = h(y)$.

Case 1: If $x, y \in B$, then $h(x) = g(x) - 1$, and $h(y) = g(y) - 1$, meaning $g(x) - 1 = g(y) - 1$, meaning $g(x) = g(y)$. Since g is a bijection, $x = y$.

Case 2: If $x, y \in A$, a similar argument yields that $x = y$.

Case 3: Without loss of generality, let $x \in A$ and $y \in B$. If $x \in A$, then $h(x) = f(x) + n$ and $h(y) = g(y) - 1$. Thus, $f(x) + n = g(y) - 1$. However, since $f(x) + n \geq n$ and $0 \leq g(y) - 1 \leq n - 1$. Thus, we get that $0 \leq n \leq n - 1$, which is a contradiction.

Thus, we have shown that h is injective. □

Theorem (Cartesian Product of Natural Numbers): $\mathbb{N} \times \mathbb{N}$ is denumerable.

Proof. We consider $\mathbb{N} \times \mathbb{N}$ as

$$\mathbb{N} \times \mathbb{N} = \mathbb{N} \times \{0\} \cup \mathbb{N} \times \{1\} \cup \dots,$$

$$\begin{array}{llllll} \mathbb{N} \times \{0\} : & (0, 0) & (1, 0) & (2, 0) & (3, 0) & \dots \\ \mathbb{N} \times \{1\} : & (0, 1) & (1, 1) & (2, 1) & (3, 1) & \dots \\ \mathbb{N} \times \{2\} : & (0, 2) & (1, 2) & (2, 2) & (3, 2) & \dots \\ \mathbb{N} \times \{3\} : & (0, 3) & (1, 3) & (2, 3) & (3, 3) & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Then, we can find an (informal) bijection as follows:

$$\begin{array}{llllll} \mathbb{N} \times \{0\} : & \cancel{(0, 0)}^0 & \cancel{(1, 0)}^2 & \cancel{(2, 0)}^5 & \cancel{(3, 0)}^9 & \dots \\ \mathbb{N} \times \{1\} : & \cancel{(0, 1)}^1 & \cancel{(1, 1)}^4 & \cancel{(2, 1)}^8 & (3, 1) & \dots \\ \mathbb{N} \times \{2\} : & \cancel{(0, 2)}^3 & \cancel{(1, 2)}^7 & (2, 2) & (3, 2) & \dots \\ \mathbb{N} \times \{3\} : & \cancel{(0, 3)}^6 & (1, 3) & (2, 3) & (3, 3) & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

We can also find a bijection $P : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, with

$$P(x, y) = \frac{(x+y)(x+y+1)}{2} + x$$

A fun challenge is to prove that P is a bijection. □

Theorem (Countability of the Rationals): \mathbb{Q} is denumerable.

Theorem (Countability of the Integers): The set \mathbb{Z} is denumerable.

Proof. Let $f : \mathbb{Z} \rightarrow \mathbb{N}$ be defined by

$$f(x) = \begin{cases} 2x & x \geq 0 \\ -2x - 1 & x < 0 \end{cases}$$

□

Definition (Cardinality). We say two sets, A and B , have the same cardinality if there exists a bijection $f : A \rightarrow B$.

Theorem (Finite Subset Cardinality): If $m, n \in \mathbb{N}$ and $m \neq n$, then $\{1, 2, \dots, m\}$ and $\{1, 2, \dots, n\}$ do not have the same cardinality.

Theorem (Infinitude of the Natural Numbers): \mathbb{N} is not finite.

Example. If $A \subsetneq B$ and $|A| = |B|$, then both A and B are infinite.

In order to prove this, we need to show that every injection from a finite set to itself is a bijection.

Section 1.2: Uncountable Sets

Definition (Uncountable Set). A set is uncountable if it is not countable.

Theorem (Uncountability of \mathbb{R}): \mathbb{R} is uncountable.

Proof. For all $x \in \mathbb{R}$, and for all $j \in \mathbb{N}$, we define $[x]_j$ to denote the $j + 1$ -th digit after the decimal point in the decimal expansion of x .

For example, $[\pi]_0 = 1$, $[\pi]_1 = 4$, etc.

Let $f : \mathbb{N} \rightarrow \mathbb{R}$. We will show that f is not surjective.

Let $y \in [0, 1) \subseteq \mathbb{R}$ defined by $\forall j \in \mathbb{N}$,

$$[y]_j = \begin{cases} 0 & [f(j)]_j = 1 \\ 1 & [f(j)]_j \neq 1 \end{cases}.$$

We claim that $y \notin f(\mathbb{N})$. We will show that $\forall j \in \mathbb{N}$, $f(j) \neq y$.

We can see that if $[f(j)]_j = 1$, then $[y]_j = 0$. Similarly, if $[f(j)]_j \neq 1$, then $[y]_j = 1$. Either way, $[f(j)]_j \neq [y]_j$ for all $j \in \mathbb{N}$. □

Remark: The above proof is an example of a diagonalization proof. It can be imagined as

$f(0)$	$*, \cancel{a_1}^{\neq} a_2 a_3 \dots$
$f(1)$	$*, b_1 \cancel{b_2}^{\neq} b_3 \dots$
$f(2)$	$*, c_1 c_2 \cancel{c_3}^{\neq} \dots$
\vdots	\vdots

Note: A substantial problem that we might need to deal with is that a real number does not necessarily have a unique decimal representation. For instance, $3.999\ldots = 4.000\ldots$.

In order to resolve this issue, we can default to the option with trailing 0 over trailing 9.

Definition (Power Set). The power set of a set S is

$$P(S) = \{A \mid A \subseteq S\}.$$

Theorem (Power Set Surjection): Let $f : S \rightarrow P(S)$. Then, f is not surjective.

Proof. Let $T = \{x \in S \mid x \notin f(x)\}$. Then, $T \notin f(S)$.

Let $y \in S$. We want to show that $f(y) \neq T$. Suppose toward contradiction that $f(y) = T$. Then, if $y \in T$, then $y \in f(y)$, which implies that $y \notin T$.

If $y \notin T$, then $y \notin f(y)$, which implies that $y \in T$.

Thus, it cannot be the case that $f(y) = T$. □

Definition (Cardinality Comparison). Let A and B be sets. Then, we write $\text{card}(A) \leq \text{card}(B)$ if there exists an injective map $f : A \hookrightarrow B$.

We write $\text{card}(A) < \text{card}(B)$ if there exists an injection $f : A \hookrightarrow B$ but no bijection.

Example (Cardinality of the Power Set). For every set,

$$\text{card}(S) < \text{card}(P(S)).$$

- (1) We know that $\text{card}(S) \leq \text{card}(P(S))$, defining $f : S \hookrightarrow P(S)$, $f(a) = \{a\}$, since if $f(x) = f(y)$, then $\{x\} = \{y\}$, meaning $x \in \{y\}$, so $x = y$.

In the case of $f : \emptyset \rightarrow \{\emptyset\}$, we define $\emptyset = f \subseteq \emptyset \times \{\emptyset\}$.

- (2) Since there exists no bijection $f : S \rightarrow P(S)$, it is the case that $\text{card}(S) \neq \text{card}(P(S))$.

Example (Decimal Expansion). We know that for some decimal expansion

$$\begin{aligned} 3.14159\ldots &= 3 + \frac{1}{10} + \frac{4}{100} + \cdots \\ &= \sum_{i=0}^{\infty} \frac{n_i}{10^i}, \end{aligned}$$

with $0 \leq n_i \leq 9$ for $i \geq 1$.

However, we can also write any real number as

$$\sum_{i=0}^{\infty} \frac{n_i}{3^i}$$

with $0 \leq n_i \leq 2$ for all $i \geq 1$.

Example (Finite Strings). Let S be the set of all finite strings of 0 and 1. S is countable.

Proof 1: We define $f : S \rightarrow \mathbb{N}$ by, for a string $x \in S$, x starts with n_1 zeroes, then has n_2 ones, then n_3 zeroes, etc. We define $f(x) := 2^{n_1} \times 3^{n_2} \times 5^{n_3} \times 7^{n_4} \times 11^{n_5} \cdots$, or

$$f(x) = \prod_i p_i^{n_i},$$

where p_i denotes the i th prime number. We can see that f is an injection.

Since S is infinite (proof omitted), we can see that $f(S)$ is also infinite.¹ Since $f(S)$ is an infinite subset of \mathbb{N} , $f(S)$ is denumerable, meaning there exists a bijection $q : f(S) \rightarrow \mathbb{N}$. Therefore, we have $q \circ f : S \rightarrow \mathbb{N}$ is a bijection, meaning S is denumerable.

Proof 2: List the elements of S by length and lexicographic order: short strings come before long strings, and 0s come before 1s.

Rank	String
0	0
1	1
2	00
3	01
4	10
5	11
\vdots	\vdots

This pattern yields a systematic way to map S to the natural numbers.

Proof 3: We can see that

$$S = \bigcup_{i=1}^{\infty} S_i,$$

where S_i is the set of all strings of length i , each of which contains 2^i elements.

Since each S_i is finite, and $S_i \cap S_j = \emptyset$ (by definition). Thus, S is a countable union of pairwise disjoint countable sets, so S is countable.

Example (All Possible Writings). Let W be the set of all possible writings in English. We let W_n denote the writing with n characters. Then,

$$W = \bigcup_{n=1}^{\infty} W_n,$$

which is a countable union of disjoint finite sets, which is countable.

Similarly, we can list all the writings by length and lexicographic order.

This result implies that “almost all” real numbers, in a sense, are unable to be described.

Section 1.3: Cantor–Schröder–Bernstein Theorem

Example. If we have $|A| \leq |B|$ and $|B| \leq |A|$, it does not necessarily imply $|A| = |B|$.

This is because the \leq in the cardinality comparison implies there exist injections $f : A \hookrightarrow B$ and $g : B \hookrightarrow A$, not that the cardinalities are necessarily “less than or equal to” each other.

However, at the same time, this fact is true — this is what is known as the Cantor–Schröder–Bernstein Theorem.

Theorem (Cantor–Schröder–Bernstein): Let $f : C \hookrightarrow D$ and $g : D \hookrightarrow C$ be injective maps. Then, $|C| = |D|$.

¹If $f(S)$ is finite, then there exists a bijection $g : f(S) \rightarrow \{1, \dots, n\}$. Composing g and f , we find S is finite as $g \circ f|_S$ is a bijection.

An Informal Proof Sketch. Consider C to be a set of cats and D to be a set of dogs. Every cat chases a dog, and every dog chases a cat, with different cats chasing different dogs and vice versa.

There are four potential arrangements:

- (1) A set of cats and dogs are chasing each other in a circle.
- (2) A chain of dogs chasing cats that starts with a dog.
- (3) A chain of cats chasing dogs that starts with a cat.
- (4) An endless chain of cats chasing dogs with no discernible start or end point.

These four cases create a bijection from C to D :

- (1) Pair each cat with the dog that it is chasing.
- (2) Pair each cat with the dog that it is chasing.
- (3) Pair each cat with the dog that *is chasing it*.
- (4) Pair each cat with the dog that it is chasing.

□

A More Formal Proof Sketch. For $C = \{c_i\}_{i \in I}$ and $D = \{d_i\}_i$, we have four types of sequences.

- (i) Circular sequence: for some $m \in \mathbb{N}$, there exist c_1, \dots, c_m and d_1, \dots, d_m such that $f(c_i) = d_i$ and $g(d_i) = c_{i+1}$, where $c_{m+1} = c_1$.
- (ii) Cat sequence: there is c_1, c_2, \dots and d_1, d_2, \dots such that $f(c_i) = d_i$ and $g(d_i) = c_{i+1}$.
- (iii) Dog sequence: there is c_1, c_2, \dots and d_1, d_2, \dots such that $f(c_i) = d_{i+1}$ and $g(d_i) = c_i$.
- (iv) Bi-infinite sequence: $\{c_i\}_{i \in \mathbb{Z}}$ and $\{d_i\}_{i \in \mathbb{Z}}$ such that $f(c_i) = d_i$ and $g(d_i) = c_{i+1}$.

Claim 1: For every $c \in C$, c is in exactly one sequence that is either a circular sequence, a cat sequence, a dog sequence, or a bi-infinite sequence.

We define our bijection $h : C \rightarrow D$ by

$$h(c) = \begin{cases} g^{-1}(c) & c \text{ in a dog sequence} \\ f(c) & \text{else} \end{cases}.$$

Claim 2: h is well-defined.

Claim 3: h is a bijection.

□

Theorem: For every set A, B , either $|A| \leq |B|$ or $|B| \leq |A|$.

In order to prove this, we need the axiom of choice.

Example (Cardinality of the Reals). Recall that $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$ and $|\mathbb{N}| < |\mathbb{R}|$. According to the previous theorem, it is the case that either $|\mathcal{P}(\mathbb{N})| \leq |\mathbb{R}|$ or $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{N})|$.

In particular, $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$.

An Informal Proof. Let S be the set of all functions $f : \mathbb{N} \rightarrow \{0, 1\}$. We will show that $|S| = |\mathcal{P}(\mathbb{N})|$ and $|S| = |\mathbb{R}|$. This will show that $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$ (by composing bijections).

To show that $|S| = |\mathcal{P}(\mathbb{N})|$, define a subset of \mathbb{N} by the supportⁱⁱ of some element of S . This is a bijection between $\mathcal{P}(\mathbb{N})$ and S .

To show $|S| = |\mathbb{R}|$, we place a decimal point in front of the string, and consider it as a real number in base 2, which yields a bijection between S and $[0, 1]$.

Next, we show that $|[0, 1]| = |(0, 1)|$.

Finally, we show that $|(0, 1)| = |\mathbb{R}|$. Take $f : (0, 1) \rightarrow \mathbb{R}$ to be $\cot(\pi x)$ — or $\tan(\pi x - \pi/2)$. These are bijections from $(0, 1)$ to \mathbb{R} . \square

Definition (Continuum Hypothesis). We are aware that

$$|\mathbb{N}| < |\mathbb{R}| = |\mathcal{P}(\mathbb{N})|.$$

The continuum hypothesis states that there exists no set S such that

$$|\mathbb{N}| < |S| < |\mathbb{R}|.$$

The continuum hypothesis is independent of the ZFC axioms.ⁱⁱⁱ

Exercise (Challenge Problem): Let $T = \{(a_0, a_1, a_2, \dots) \mid a_i \in \mathbb{N}; \text{finitely many nonzero } a_i\}$. Is T countable? We also write

$$T = \bigoplus_{i=0}^{\infty} \mathbb{N}.$$

Axiomatic Set Theory

Question: Is there a set A such that $A \in A$?

Answer. Yes.

There is the set $\{\cdots\{\}\cdots\}$, which contains infinitely many sets in itself. Additionally, there is the set $A = \{x \mid x \text{ is a set}\}$.

Example (Russell's Paradox). Consider the set

$$R = \{x \mid x \notin x\}.$$

The question is if $R \in R$. However, this cannot be true, because if $R \in R$, then $R \notin R$ and vice versa.

Axioms of Set Theory

We cannot just say

$$S = \{x \mid x \text{ is blah}\},$$

as evidenced by Russell's paradox. We need to carefully construct rules to create a rigorous description of formal set theory.

Axiom (Existence): The existence axiom states that there exists a set:

$$\exists a (a = a).$$

ⁱⁱThe elements that f does not map to 0 for some $f \in S$.

ⁱⁱⁱZermelo–Fraenkel Axioms with the Axiom of Choice.

Axiom (Empty Set): The empty set axiom states that there exists a set with no elements:

$$\exists a \forall x (x \notin a).$$

Axiom (Pairing): The pairing axiom states that, given any sets a and b , there is a set c such that the only elements of c are a and b :

$$\forall a \forall b \exists c \forall x (x \in c \Leftrightarrow x = a \vee x = b)$$

Axiom (Extensionality): The axiom of extensionality states that if two sets have the same elements, they are the same sets:

$$\forall a \forall b (\forall x (x \in a \Leftrightarrow x \in b) \Rightarrow a = b)$$

Question: What is a set?

Answer. The unsatisfying answer is that “set” and “element” have no meaning *per se*. The main reason we define these axioms is to define relationships between objects (rather than objects themselves).

Example. We want to prove that for every set b , there exists a set $\{b\}$.

Symbolically, we want to show

$$\forall b \exists c \forall x (x \in c \Leftrightarrow x = b).$$

In particular, we can see that, in the pairing axiom, there is no requirement that a and b be distinct. Therefore, we can use the pairing axiom of $a = b$ and $b = b$. Therefore, the pairing axiom becomes

$$\forall b \forall b \exists c \forall x (x \in c \Leftrightarrow x = b \vee x = b),$$

which reduces to

$$\forall b \exists c \forall x (x \in c \Leftrightarrow x = b).$$

In particular, if $b = \{\}$ in the previous example, then the pairing axiom implies the uniqueness of the empty set. We will denote $\{\} = \emptyset$. We can create a tower

$$\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}, \dots,$$

entirely consisting of the empty set.

Axiom (Union): The axiom of union states that for any set a , there exists a set consisting of all the elements of a

$$\forall a \exists u \forall x \forall y ((x \in y \wedge y \in a) \Rightarrow x \in u)$$

Definition. The string $a \subseteq b$ is shorthand for

$$\forall x (x \in a \Rightarrow x \in b).$$

Axiom (Power Set): The power set axiom states that for all a , there is a set b such that all elements of b are subsets of a and all subsets of a are contained in b :

$$\forall a \exists b \forall y (y \in b \Leftrightarrow y \subseteq a).$$

Definition. We let (a, b) be shorthand for the set

$$\{a, \{a, b\}\}.$$

Exercise: If $\{a, \{a, b\}\} = \{c, \{c, d\}\}$, it is the case that $a = c$ and $b = d$.

Recall that

$$c = \{x \mid x \text{ is blah}\}$$

is a problematic definition of a set. However, if a is a set, we can define

$$c = \{x \mid x \in a \wedge x \text{ is blah}\},$$

which does not cause any contradictions. The following axiom schema formalizes this fact.

Axiom (Comprehension schema): The comprehension schema says that, given any formula $\varphi(x)$, in which x is a free variable, there exists a set c whose elements are those in a that satisfy φ :

$$\forall a \exists c \forall x (x \in c \Leftrightarrow x \in a \wedge \varphi(x)).$$

Remark: There are infinitely many axioms in the comprehension schema, one for each formula φ . This is why it is known as a schema rather than an axiom.

Remark: Since we can specify a formula $\varphi(x) : x \neq x$, the comprehension schema obviates the empty set axiom.

Example (Some Logic). An example of a formula is $\forall p \exists q (p \Rightarrow q)$.

In the formula $\exists q (p \Rightarrow q)$, we say p is a free variable.

The main symbols in logic are $\wedge, \vee, \neg, \Rightarrow, \Leftrightarrow, ()$ (the symbols that make up propositional logic), as well as \forall, \exists (which form the basis of first-order logic).

In propositional logic, the only two symbols that are needed are \wedge and \neg (or \vee and \neg).^{IV}

When we get to set theory, the last symbol we need is \in .

We can build larger formulae by substituting formulae into other formulae.

Example (Using the Comprehension Schema). Let $\phi(x) : \exists y (y \in x)$. This is an axiom:

$$\forall a \exists b \forall x (x \in b \Leftrightarrow x \in a \wedge \exists y (y \in x))$$

In particular, this axiom is equivalent to saying

$$\forall a \exists b \text{ s.t. } b = \{x \in a \mid x \neq \emptyset\}.$$

Axiom (Union): The union axiom states that for a collection of sets T , there is a union of the sets, $a = \bigcup T$.

$$\forall t \exists a \forall x (x \in a \Leftrightarrow \exists y (y \in t \wedge x \in y)).$$

Alternatively, we can say

$$\forall t a = \{x \mid x \in \text{some element of } t\}$$

is a set.

Axiom (Infinity): There exists an infinite set.

$$\exists a (\emptyset \in a \wedge \forall x (x \in a \Rightarrow x \cup \{x\} \in a))$$

Remark: To see that this set, a has an element, \emptyset . Thus,

$$a = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset, \{\emptyset\}\}\}, \dots\}$$

We define $0 = \emptyset$, $1 = \{\emptyset, \{\emptyset\}\}$, etc. Thus, the axiom of infinity defines the natural numbers.

^{IV}In computers, the only gate that is necessary is the NAND gate.

Axiom (Regularity): There is no infinite chain of the form

$$\cdots \in d \in c \in b \in a.$$

$$\forall s \exists x (s = \emptyset \vee s \neq \emptyset \Rightarrow (x \in s \wedge x \cap s = \emptyset))$$

Remark: The existence of this axiom is meant to obviate the case where we imagined a set a with $a \in a$.

Definition (Function-like Formula). Let $\psi(x, y)$ be a formula with x, y free variables such that $\forall x, y, z, \psi(x, y) \wedge \psi(x, z) \Rightarrow y = z$.

Axiom (Replacement Schema):

$$\forall a \exists b \forall x (x \in b \Leftrightarrow \exists y (y \in a \wedge \psi(x, y)))$$

Remark: It is possible to prove the comprehension schema from the replacement schema.

The axioms that we have discussed so far are known as the Zermelo–Fraenkel axioms.

Question: If A and B are nonempty, is it the case that $A \times B \neq \emptyset$

Answer. Yes.

There exists $a \in A$ and $b \in B$ such that $(a, b) \in A \times B$. This can be proven using the ZF axioms.

Question: If $A_1, A_2, \dots, \neq \emptyset$, then is $A_1 \times A_2 \times \cdots \neq \emptyset$?

Answer. This requires the axiom of choice.

Axiom (Choice): If T is a collection of sets, $\exists b$ such that $\forall a \in T, a \cap b \neq \emptyset$.

$$\forall t \exists b (\forall a (a \in t \Rightarrow \exists x (x \in a \wedge x \in b)))$$

Remark: We define $x \in (a \cap b)$ as shorthand for $x \in a \wedge x \in b$.

Remark: The axiom of choice is controversial.

Remark: The axiom of choice entails certain counterintuitive results, such as the Banach–Tarski paradox^v and the existence of non-measurable sets.

The Banach–Tarski paradox states that for any two bounded subsets of \mathbb{R}^3 with nonempty interior, one of the sets can be partitioned into finitely many subsets, with certain isometries applied to said partition, and reconstituted into the second set.

Recall:

$$A \times B = \{(x, y) \mid x \in A \wedge y \in B\}$$

Definition. For any sets A and B , each subset of $A \times B$ is a relation from A to B .

Definition. A relation $R \subseteq A \times B$ is a function if

$$\forall x \forall y \forall z ((x, y) \in R \wedge (x, z) \in R \Rightarrow y = z).$$

Definition. A function $F \subseteq A \times B$ is injective if

$$\forall x \forall x' \forall y ((x, y) \in F \wedge (x', y) \in F \Rightarrow x = x')$$

Notation: For some statement φ ,

$$\forall x \in A (\varphi)$$

is shorthand for

$$\forall x (x \in A \Rightarrow \varphi)$$

^vHey, one of the topics for my Honors thesis is on this.

Notation: If $F \subseteq A \times B$ and $\forall x \in A, (x, y) \in F$, then we write $F : A \rightarrow B$.

Also, $\forall (x, y) \in F$, we write $F(x) = y$.

Definition. A function F is onto B if

$$\forall y \in B \exists x (x, y) \in F.$$

Remark: Do not say “onto” without mentioning B . It is okay to say $F : A \rightarrow B$ is onto (or surjective).

Example. We wish to show that if $f : A \xrightarrow{\text{onto}} B$, then there exists a function $g : B \rightarrow A$ such that g is an injection.

Since f is onto B , for every $b \in B$, there exists $a \in A$ such that $f(a) = b$. We define $g(b)$ to be a particular choice function on the set of all a such that $f(a) = b$.

Remark: The above statement (that every surjective function has a right-inverse, which is necessarily injective) is an equivalent statement to the axiom of choice.

Example (Natural Numbers). Since the empty set exists, we can define $\emptyset = \{\} = 0$. We set $1 = \{0\}$, $2 = \{0, 1\}$, etc. We have $n = \{0, \dots, n-1\}$.

If we take $n \cup \{n\}$, we have

$$\begin{aligned} \{0, \dots, n-1\} \cup \{n\} &= \{0, \dots, n\} \\ &= n+1. \end{aligned}$$

In other words, we define addition by taking $n \cup \{n\}$.

Question: Is $n \in n+1$? Is $n \subseteq n+1$?

Answer. Yes. and yes.

Definition. We say $m < n$ if $m \in n$, or $m \subseteq n$.

Example. We will use the ZF axioms to show that there exists a set whose elements are all the natural numbers.

Defining using the axiom of infinity, we get

$$\exists s (\emptyset \in s \wedge \forall x (x \in s \Rightarrow x \cup \{x\} \in s) \wedge \forall y (y \in s \Rightarrow y = \emptyset \vee \exists x (x \cup \{x\} = y)))$$

Ordinal Numbers and Well-Orderings

Recall: Recall that we define $\emptyset = 0$, $1 = 0 \cup \{0\}$, and $n+1 = n \cup \{n\}$.

Notice that $n \in n+1$, meaning $0 \in 1 \in 2 \in \dots$, and $n \subseteq n+1$, meaning $0 \subseteq 1 \subseteq 2 \subseteq \dots$.

Notation: For any set x , $x^+ = x \cup \{x\}$. We call x^+ the successor of x .

Recall: The infinity axiom states that

$$\exists A (\emptyset \in A \wedge \forall x (x \in A \Rightarrow x \cup \{x\} \in A)).$$

One of our previous homework problems showed that there exists a set that contains all natural numbers and only natural numbers.

$$\exists \omega \forall x (x \in \omega \Leftrightarrow x \in A \wedge (x = \emptyset \vee \exists y (y \in \omega \wedge x = y^+)))$$

Definition (Natural Numbers). For ω defined by

$$\exists \omega \forall x (x \in \omega \Leftrightarrow x \in A \wedge (x = \emptyset \vee \exists y (y \in \omega \wedge x = y^+))),$$

we say ω is the set of all natural numbers.

Remark: Given a relation R , we write $(x, y) \in R$ if xRy .

Definition (Total/Linear Order). Given a set A , a (strict) total/linear order is a relation R such that $\forall x, y \in A$, then exactly one of the following holds:

$$xRy \vee yRx \vee x = y.$$

Additionally, $\forall x, y, z \in A, xRy \wedge yRz \Rightarrow xRz$, meaning R is transitive.

Remark: This is a strict inequality.

Notation: For a total ordering R , we use the symbol $<$. This does not imply that a given ordering is a “less than” type of ordering.

Example. The relation $x < y$ is a total ordering on \mathbb{Q} (or \mathbb{R}).

Definition (Well-Ordering). A well-ordering on A is a total ordering R on A such that every nonempty subset of A has a least element.

$$\forall S (S \subseteq A \wedge S \neq \emptyset \Rightarrow \exists x \in S \forall y \in S (x < y \vee x = y))$$

Question: Is \mathbb{Q} well-ordered by $<$?

Answer. No.

Consider the set $\{q \mid q > \sqrt{2}\}$. Since $\sqrt{2} \notin \mathbb{Q}$ ^{VI}, this set has no least element, meaning \mathbb{Q} is not well-ordered.

Definition. Let R_1 be a relation on A_1 , and R_2 a relation on A_2 .

We say (A_1, R_1) is order-isomorphic to (A_2, R_2) if

$$\exists f : A_1 \xrightarrow{\text{bijection}} A_2$$

and $\forall x, y \in A_1, xR_1y \Leftrightarrow f(x)R_2f(y)$.

Remark: If R_1 and R_2 are understood, we say A_1 is order-isomorphic to A_2 , and we write $A_1 \cong A_2$.

Example. If $\omega = \{1, 2, \dots\}$, $R_1 = R_2 = <$, then if $A = \{0, 2, 4, \dots\}$, $\omega \cong A$.

Question: Is \in a total order on $\omega^+ = \omega \cup \{\omega\}$?

Answer. Yes.

Notice that

$$\begin{aligned} \omega^+ &= \{0, 1, 2, \dots, \omega\} \\ &= \{0, 1, 2, \dots, \{0, 1, 2, \dots\}\}. \end{aligned}$$

This is also a well-ordering.

Example. Consider, now

$$\begin{aligned} Y &= (\omega^+)^+ \\ &= \omega^+ \cup \{\omega^+\} \\ &= \{0, 1, \dots, \omega, \omega^+\}. \end{aligned}$$

Question: Is \in a total ordering on Y ?

Answer. Yes.

Question: Is \in a well-ordering on Y ?

^{VI}I am not proving this here.

Answer. Yes.

Question: Is $(\omega, \in) \cong (\omega^+, \in)$.

Answer. If there exists $f : \omega \rightarrow \omega^+$, then $f(n) = \omega$ for some n . Since $f(n+1) \in \omega^+$, and $f(n) \in f(n+1)$, it is the case that $\omega \in f(n+1)$.

However, $f(n+1) \in \omega^+ \setminus \{\omega\}$, meaning $f(n+1) \in \omega = \omega$.

Thus, we have $\omega \in f(n+1) \in \omega$, which violates the axiom of regularity.

Question: Suppose A, B, C are well-ordered by R_A, R_B, R_C .

True/False: $A \cong A$.

True/False: If $A \cong B$, then $B \cong A$.

True/False: If $A \cong B$ and $B \cong C$, then $A \cong C$.

Answer. True for all three.

Therefore, we can talk about \cong as an equivalence relation on the set class of well-ordered sets.

Example. The following are representatives of separate equivalence classes in the class of well-ordered sets with respect to order-isomorphism.

$$\begin{aligned} \omega &= \{0, 1, 2, \dots\} \\ \underbrace{\omega^+}_{\omega+1} &= \{0, 1, 2, \dots, \omega\} \\ \omega + 2 &= \{0, 1, 2, \dots, \omega, \omega + 1\}, \quad \vdots \end{aligned}$$

Notice that these sets are all denumerable, but they are not order-isomorphic.

Theorem: Every such equivalence class has exactly one element that is well-ordered by \in and is \in -transitive.

This element is called an ordinal.

Definition. A set A is \in -transitive if $a \in b$ and $b \in A$ implies $a \in A$. Alternatively, every element of a is a subset of A .

Example. We can see that ω is \in -transitive, since for any $a \in b$ and $b \in \omega$, then $a \in \omega$ (by definition of ω).

Question: Is 3 \in -transitive?

Answer. Yes.

Theorem: For any two ordinals α, β , either $\alpha \in \beta$, $\beta \in \alpha$, or $\beta = \alpha$.

Recall: An ordinal is a set that is \in -transitive and well-ordered by \in .

A set t is \in -transitive if $a \in b$ and $b \in t$ implies $a \in t$. Equivalently, $b \in t \Rightarrow b \subseteq t$.

Example. The set

$$\{a < b < c\} \cong 3 = \{0, 1, 2\},$$

since $0 < 1 < 2$.

The set

$$\{a_0 < a_1 < \dots\} \cong \omega,$$

while

$$\{a_0 < a_1 < \dots < b_0\} \cong \omega^+ := \omega + 1 = \omega \cup \{\omega\}.$$

We can also see that

$$\begin{aligned} \{a_0 < a_1 < a_2 < \dots < b_0 < b_1 < b_2 < \dots\} &= \omega + \omega \\ &= \omega 2 \end{aligned}$$

Example. Let $S = \{p^n \mid p \text{ prime}, n \in \omega\}$.

We place the ordering

$$2^0 < 2^1 < \dots < 3^1 < 3^2 < \dots < 5^1 < 5^2 < \dots$$

In other words,

$$\begin{aligned} p_k^m &< p_{k+1}^n \\ p_k^m &< p_k^{m+1}. \end{aligned}$$

We can see that this ordering must be isomorphic to $\omega\omega$, since it must be greater than ωk for all $k \in \omega$.

Example. We define

$$\begin{aligned} 1 + \omega &\cong \{b_0 < a_0 < a_1 < a_2 < \dots\} \\ &\cong \omega. \end{aligned}$$

This means $1 + \omega = \omega$, while $\omega + 1 \neq \omega$.

This is because $\omega + 1$ has a greatest element, while ω does not.

Definition (Addition). For any ordinals α and β , $\alpha + \beta$ is the ordinal that is order isomorphic to the following well-ordered set.

$$S = \{0\} \times \alpha \cup \{1\} \times \beta.$$

The ordering for this set is the lexicographical ordering. We declare

$$(x, y) < (x', y')$$

$x \in x'$ or $x = x'$ and $y \in y'$.

Example.

$$\begin{aligned} 2 + 3 &= \{0, 1\} + \{0, 1, 2\} \\ S &= \{0\} \times \{0, 1\} \cup \{1\} \times \{0, 1, 2\} \\ &= \{(0, 0), (0, 1), (1, 0), (1, 1), (1, 2)\} \\ &= \{(0, 0) < (0, 1) < (1, 0) < (1, 1) < (1, 2)\} \\ &\cong \{0, 1, 2, 3, 4\} \\ &= 5 \end{aligned}$$

Definition (Multiplication). For any ordinals α and β , $\alpha\beta$ is the ordinal that is order-isomorphic to the following well-ordered set

$$S = \alpha \times \beta,$$

ordered by

$$(a, b) < (a', b')$$

if $a \in a'$ or $a = a'$ and $b \in b'$

Remark: For general ordinals, addition and multiplication are *not* commutative.

For instance, $1 + \omega \neq \omega + 1$, since $1 + \omega = \omega$. However, addition and multiplication of ordinals is associative.

Theorem:

$$\begin{aligned}(\alpha + \beta) + \gamma &= \alpha + (\beta + \gamma) \\ (\alpha\beta)\gamma &= \alpha(\beta\gamma).\end{aligned}$$

Remark: We define

$$\begin{aligned}\omega^2 &:= \omega\omega, \\ \omega^3 &:= \omega\omega\omega.\end{aligned}$$

However, we may ask how to define

$$\omega^\omega.$$

Definition (Exponentiation). For any ordinals α and β , we define

$$\alpha^\beta = \begin{cases} 1 & \text{if } \beta = 0 \\ \alpha^\gamma \alpha & \text{if } \beta = \gamma^+ \text{ for some } \gamma \\ \bigcup_{\gamma < \beta} \alpha^\gamma & \text{else} \end{cases}$$

Remark: If an ordinal $\alpha \neq 0$ and α has no predecessor, then α is known as a limit ordinal. For instance, ω is a limit ordinal.

Example. From this definition,

$$\omega^\omega = \bigcup_{n \in \omega} \omega^n.$$

Remark: Notice that ω^ω is countable, since it is the countable union of countable sets.

Definition.

$$\begin{aligned}\omega^{\omega^\omega} &:= \omega^{(\omega^\omega)} \\ \omega^{\omega^{\omega^{\dots}}} &:= \bigcup_{n \in \omega} \omega^{\omega^{\dots^{\omega}}} \\ &= \epsilon_0.\end{aligned}$$

Definition. We define

$$\omega_1 := \{\alpha \mid \alpha \text{ is an ordinal and } \alpha \text{ is countable}\}.$$

Remark: It can be proven that ω_1 is indeed an ordinal.

Every subset of ω_1 is well-ordered (or else we would violate the Axiom of Regularity).

Theorem: It is not the case that ω_1 is countable.

Induction and Recursion

Definition (Principle of Mathematical Induction). Let ϕ be a formula such that

$$\phi(0) \wedge \forall n \in \omega (\phi(n) \Rightarrow \phi(n+1))$$

Then, $\forall n \in \omega, \phi(n)$.

Equivalently, let S be a set such that

$$0 \in S \wedge \forall n \in \omega (n \in S \Rightarrow n+1 \in S).$$

Then, $\omega \subseteq S$.

Definition (Strong Principle of Mathematical Induction). Let S be a set such that

$$0 \in S \wedge \forall n \in \omega (n \subseteq S \Rightarrow n \in S).$$

Then, $\omega \subseteq S$.

Remark: Strong induction implies weak induction, since the antecedent in strong induction is more restrictive than the antecedent in weak induction.

Proof. Suppose toward contradiction that $\omega \not\subseteq S$. Then, since $\omega \setminus S \subseteq \omega$ must be nonempty, and ω is well-ordered, there exists n_0 such that $n_0 \in \omega \setminus S$. Thus, for every $m < n_0$, $m \in S$.

Thus, $\forall m \in n_0$, $m \in S$, meaning $n_0 \subseteq S$. Thus, $n_0 \in S$, meaning $n_0 \in S \wedge n_0 \notin S$. \perp □

Remark: The above proof shows that everything you can prove by induction, you can prove by contradiction (since induction follows from contradiction).

Example. Suppose $<$ is a well-ordering on \mathbb{R} .^{vii} Define $x \in \mathbb{R}$ to be “good” if a certain condition is satisfied. We wish to show that $x \in \mathbb{R}$ — in particular, we cannot use either weak or strong induction.

Proof Idea. Suppose there exists some real number x that fails the condition. Let x_0 the least element that fails the condition. Then, $\forall y < x_0$, y is good. Then, we need to use some inductive step to show that such a condition implies that x_0 is good. □

Example. Suppose that for all $m, n \in \mathbb{N}$, Then, $G_{m,n}$ is some graph, group, etc.

We want to show that every $G_{m,n}$ satisfies some condition.

Suppose there is a bad $G_{a,b}$. Take the smallest such $G_{a,b}$ (via the lexicographical order), and we can use strong induction to show that such a $G_{a,b}$ also satisfies the condition.

Example (Transfinite Induction). Suppose we want to show that for all $\alpha \in \omega_2$, $\phi(\alpha)$.

Question: Is the following enough?

$$\phi(0) \wedge \forall \alpha \in \omega_2 (\phi(\alpha) \Rightarrow \phi(\alpha \cup \{\alpha\})).$$

Answer. No.

The reason why the above cannot work (as a statement of induction) is because ω is a limit ordinal (i.e., ω is not a successor to any particular ordinal).

We can use contradiction.

Proof by Contradiction. Suppose toward contradiction that $\phi(\alpha)$ is not true for all $\alpha \in \omega_2$. Let α_0 be the smallest ordinal in ω_2 such that $\phi(\alpha_0)$ is false.

Then, for every $\alpha \in \alpha_0$, $\phi(\alpha)$. Then, we would have to conclude $\phi(\alpha_0)$, implying a contradiction. □

The above is an example of transfinite induction.

Example (Recursion). Recall the Fibonacci numbers:

$$0, 1, 1, 2, 3, 5, 8, \dots$$

We define the Fibonacci numbers recursively:

$$\begin{aligned} F(0) &= 0 \\ F(1) &= 1 \\ F(n+2) &= F(n+1) + F(n). \end{aligned}$$

^{vii}All nonempty sets contain a well-ordering, which is another statement of the Axiom of Choice