Contents

Cardinality and Countability

Countable Sets

Definition (Denumerable Set)**.** A set S is denumerable if there exists a function $f : S \to \mathbb{N}$ 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 $f : S \to \{1, 2, \dots, n\}$ 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 $f : A \to \mathbb{N}$ (since A is denumerable), and a bijection $g : B \to \{1, 2, \dots, n\}$ for some $n \in \mathbb{N}$ (since B is finite).

We create a new bijection $h : A \cup B \to \mathbb{N}$ 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 $f(x) + n \geqslant n$ and $0 \leqslant g(y) - 1 \leqslant n - 1$. Thus, we get that $0 \leqslant n \leqslant n - 1$, 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

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

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

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

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

We can also find a bijection $P : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, 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 $f : \mathbb{Z} \to \mathbb{N}$ be defined by

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

□

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

Theorem (Finite Subset Cardinality)**:** If $m, n \in \mathbb{N}$ and $m \neq n$, then $\{1, 2, \ldots, m\}$ and $\{1, 2, \ldots, n\}$ 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.

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 $f : \mathbb{N} \to \mathbb{R}$. 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

$$\begin{array}{c|l} f(0) & *.\cancel{a_1}\overset{\neq}{a_2}a_3\ldots \\ f(1) & *.b_1\cancel{b_2}\overset{\neq}{b_3}\ldots \\ f(2) & *.c_1c_2\cancel{c_3}\overset{\neq}{\ldots} \\ \vdots & \quad\vdots \end{array}$$

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, $3.999\cdots = 4.000\ldots$.

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 $f : S \to P(S)$. 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 $\text{card}(A) \leqslant \text{card}(B)$ 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,

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

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

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

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

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 $0 \leqslant n_i \leqslant 9$ for $i \geqslant 1$.

However, we can also write any real number as

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

with $0 \leqslant n_i \leqslant 2$ for all $i \geqslant 1$.

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

Proof 1: We define $f : S \to \mathbb{N}$ 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

$$f(x) = \prod_{i}^{\infty} p_i^{n_i},$$

where p_i denotes the ith 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 $q : f(S) \to \mathbb{N}$. Therefore, we have $q \circ f : S \to \mathbb{N}$ 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
$\vdots$	$\vdots$

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

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 $S_i \cap S_j = \varnothing$ (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.

Cantor–Schröder–Bernstein Theorem

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

This is because the $\leqslant$ 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, $|C| = |D|$.

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 $h : C \to D$ 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 $|A| \leqslant |B|$ or $|B| \leqslant |A|$.

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

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

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

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

To show that $|S| = |P(\mathbb{N})|$, define a subset of $\mathbb{N}$ by the support[II] of some element of S. This is a bijection between $P(\mathbb{N})$ 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 $f : (0, 1) \to \mathbb{R}$ to be $\cot(\pi x)$ — or $\tan(\pi x - \pi/2)$. These are bijections from $(0, 1)$ to $\mathbb{R}$. □

Definition (Continuum Hypothesis)**.** We are aware that

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

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]

[II] The elements that f does not map to 0 for some $f \in S$.

[III] Zermelo–Fraenkel Axioms with the Axiom of Choice.

Exercise (Challenge Problem)**:** Let $T = \left\{(a_0, a_1, a_2, \dots) \mid a_i \in \mathbb{N};\ \text{finitely many nonzero } a_i\right\}$. 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:

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

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.

[IV] In computers, the only gate that is necessary is the NAND gate.

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.

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

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

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

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

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

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

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

Notation: For some statement φ,

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

is shorthand for

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

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

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 $F : A \to B$ is onto (or surjective).

Example. We wish to show that if $f : A \xrightarrow{\text{onto}} B$, then there exists a function $g : B \to A$ 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 $\varnothing = \{\} = 0$. We set $1 = \{0\}$, $2 = \{0, 1\}$, etc. We have $n = \{0, \ldots, n-1\}$.

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

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

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

$$\exists s\ \left(\varnothing \in s \wedge \forall x\, (x \in s \Rightarrow x \cup \{x\} \in s) \wedge \forall y\, (y \in s \Rightarrow y = \varnothing \vee \exists x\, (x \cup \{x\} = y))\right)$$

[v] Hey, one of the topics for my Honors thesis is on this.

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 $0 \in 1 \in 2 \in \cdots$, and $n \subseteq n+1$, meaning $0 \subseteq 1 \subseteq 2 \subseteq \cdots$.

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

Recall: The infinity axiom states that

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

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

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

Definition (Natural Numbers)**.** For ω defined by

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

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.

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

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

Answer: No.

Consider the set $\left\{q \mid q > \sqrt{2}\right\}$. 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 $\omega = \{1, 2, \ldots\}$, $R_1 = R_2 =<$, then if $A = \{0, 2, 4, \ldots\}$, $\omega \cong A$.

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

[VI] I am not proving this here.

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

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

Question: Is $\in$ a total ordering on Y?

Answer: Yes.

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

Answer: Yes.

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

Answer: If there exists $f : \omega \to \omega^+$, 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.

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

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

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

while

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

We can also see that

$$\begin{aligned}\{a_0 < a_1 < a_2 < \cdots < b_0 < b_1 < b_3 < \cdots\} &= \omega + \omega \\ &= \omega 2\end{aligned}$$

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

We place the ordering

$$2^0 \prec 2^1 \prec \cdots 3^1 \prec 3^2 \prec \cdots \prec 5^1 \prec 5^2 \prec \cdots$$

In other words,

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

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

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

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

$$(x, y) \prec (x', y')$$

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

Example.

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

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

$$(a,b)\prec(a',b')$$

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 $\alpha\neq0$ 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.

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

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?

$$\phi(0) \wedge \forall \alpha \in \omega 2\,(\phi(\alpha) \Rightarrow \varphi\,(\alpha \cup \{\alpha\})).$$

[VII] All nonempty sets contain a well-ordering, which is another statement of the Axiom of Choice

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 $\omega 2$ 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:

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

Question: Which of the following are valid recursive definitions?

(a) $f : \mathbb{N} \to \mathbb{N}$, with

$$f(n) = \begin{cases} n^2 & n \text{ odd} \\ f(n/2) & n \text{ even, and} n > 0 \\ 1 & n = 0 \end{cases}.$$

(b) Let $f : [0, \infty) \to [0, \infty)$ defined by $f(0) = 1$, $f(x) = 2f(x/2)$.

(c) Let $f : \mathbb{N} \to \mathbb{N}$, $f(0) = 1$, $f(1) = 1$, and $f(n) = 2f(n-2)$ for all $n \geqslant 2$.

(d) Let $f : \mathbb{Z} \to \mathbb{Z}$, $f(0) = 1$, and

$$f(n) = \begin{cases} 2f(n-1) & n > 0 \\ 3f(n+1) & n < 0 \end{cases}.$$

(e) Let $A : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be defined by

$$A(m, n) = \begin{cases} n + 1 & m = 0 \\ A(m-1, 1) & m > 0 \\ A(m-1, A(m, n-1)) & m > 0 \,\&\, n > 0 \end{cases}$$

We can also write $A(m, n)$ as $A_m(n)$, with $A_0(n) = n + 1$, $A_{m+1}(n) = \underbrace{A_m \circ \cdots \circ A_m}_{n+1 \text{ times}}(1)$

(f) Let

$$C(n) = \begin{cases} n/2 & n \text{ even} \\ 3n + 1 & n \text{ odd}, n \neq 1 \\ 1 & n = 1 \end{cases}.$$

We define $f : \mathbb{N} \to \mathbb{N}$ by $f(0) = f(1) = 0$, and

$$f(n) = \begin{cases} f(n/2) & n \text{ even} \\ f(3n+1)+ & n \text{ odd} \end{cases}.$$

Answer:

(a) Since f is defined for either odd elements or some smaller element, and there is a base case of $n = 0$, this should be a valid definition.

(b) This isn't a valid definition, since a recursive definition needs to reach some "stopping point."

(c) This is a valid definition, since we ultimately reach some stopping point with $n = 0$ or $n = 1$.

(d) This is a valid definition.

(e) This is a valid definition — notice that the function is always defined in terms of some value "less than" the input, and it always has a minimum value. If we know $A(a, b)$ for all $(a, b) < (m, n)$,[VIII] then we can find (m, n). The function $A(m, n)$ is known as the Ackermann function.

(f) If you prove the Collatz conjecture, then this is a valid definition.

Example (Using Induction to show Validity of Recursion Formula)**.** Show there exists a unique $F : \mathbb{N} \to \mathbb{N}$ such that $F(0) = 0$, $F(1) = 1$, and $F(n) = F(n-1) + F(n-2)$.

Let G be the set of all $n \in \mathbb{N}$ such that there exists a unique $g : \{0, \dots, n\} \to \mathbb{N}$ defined by $g(0) = 0$, $g(1) = 1$, and $g(k) = g(k-1) + g(k-2)$ for all $2 \leqslant k \leqslant n$.

We will show that $G = \mathbb{N}$.

Let $n_0 = \min(\mathbb{N} \setminus G)$. It must be the case $n_0 \neq 0$ and $n_0 \neq 1$. Then, there exists a unique function $g' : \{0, \dots, n_0 - 1\} \to \mathbb{N}$ such that $g'(0) = 0$, $g'(1) = 1$, and $g'(k) = g'(k-1) + g'(k-2)$ for all $2 \leqslant k \leqslant n_0 - 1$. Define $g : \{0, \dots, n_0\} \to \mathbb{N}$ by $g(n_0) = g'(n_0 - 1) + g'(n_0 - 2)$ and $g(k) = g'(k)$ for $2 \leqslant k \leqslant n_0 - 1$.

Thus, we have shown existence. Suppose $\exists f : \{0, \dots, n_0\} \to \mathbb{N}$ such that $f(0) = 0$, $f(1) = 1$, and $f(k) = f(k-1) + f(k-2)$. However, $f|_{\{0,\dots,n_0-1\}} = g'$, by uniqueness meaning for all $k < n_0$, $f(k) = g'(k)$. Thus, $f(n_0) = f(n_0 - 1) + f(n_0 - 2) = g'(n_0 - 1) + g'(n_0 - 2) = g(n_0)$.

Thus, for each $n \in \mathbb{N}$, there exists a unique g_n that satisfies the given conditions. Let $F = \bigcup_{n \in \mathbb{N}} g_n$.

Cardinal Numbers

Define a relation $\sim$ on sets by $A \sim B \Leftrightarrow |A| = |B|$.

Question: Is this an equivalence relation?

Answer: Yes. Since bijections are invertible, the identity map is a bijection, and composing bijections yields another bijection, this is an equivalence relation.

Example.

$$\{3, 5\} \sim \{\emptyset, \omega\} \sim \{\{\omega\}, \mathbb{R}\} \sim 2 = \{0, 1\}.$$

From this, we intuitively select 2 to be the representative of this equivalence class.

Example.

$$\omega \sim \omega 2 \sim \omega 3 \sim \cdots \sim \omega^2 \sim \cdots \sim \omega^{\omega^{\omega}}$$

Similarly, we select ω to be the representative of $|\omega|$.

Definition (Cardinality of a Set)**.** Let A be a set. The cardinality of A is the least ordinal α such that there exists a bijection $f : A \to \alpha$. This ordinal α is denoted $|A|$.

Remark: Before today, $|A|$ had no definition. We did write $|A| = |B|$, but that was shorthand for $\exists f : A \xrightarrow{\text{bijection}} B$.

Question: What is $\left|\omega^2\right|$?

[VIII] Lexicographically, meaning $(a, b) < (c, d)$ if $a < b$ or if $a = c$ and $b < d$.

Answer: ω

What is $|\omega|$?

Answer: ω

What is $|3|$?

Answer: 3

What is $|\mathbb{R} \times \mathbb{R}|$ and its relation to $|\mathbb{R}|$ or $|P(\omega)|$.

Answer: $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}| = |P(\omega)| = \omega_1$ (assuming the continuum hypothesis)

Definition (Cardinal Number)**.** Let α be an ordinal. If $|\alpha| = \alpha$, we say α is a cardinal number.

Every natural number is an ordinal and a cardinal.

Notation: When dealing with cardinals, it is customary to write $\aleph_0$ to denote ω.

We wrote $|A| = |B|$ to be shorthand for $\exists f : A \xrightarrow{\text{bijection}} B$. However, now there is a new meaning, since $|A|$ is actually a set. This means that when we write $|A| = |B|$, then the ordinals referring to $|A|$ and $|B|$ are equal to each other.

We need to derive the "old meaning."

Theorem: $|A| = |B|$ if and only if there exists a bijection $f : A \to B$.

Proof. Let $\alpha = |A|$. Then, $\alpha = |B|$. By definition, there exist bijections $f : A \to \alpha$ and $g : B \to \alpha$. Composing $f \circ g^{-1} : A \to B$, we get a bijection.

Suppose there exists a bijection $f : A \to B$. Let $\alpha = |A|$. Thus, there exists a bijection $g : A \to \alpha$. So, taking $g \circ f^{-1}$, we get a bijection from B to α. We have α is a cardinal as $\alpha = |A|$, meaning $\alpha = |B|$. Thus, $|A| = |B|$. □

Question: What does $|A| < |B|$ mean?

Answer: Before today, $|A| < |B|$ meant there exists $f : A \hookrightarrow B$ and no bijection $g : A \to B$.

However, now, we mean $|A| < |B|$ means $|A| \in |B|$

Theorem: $|A| \in |B| \Leftrightarrow \exists f : A \hookrightarrow B$ and there is no bijection $g : A \to B$

Proof. Homework problem. □

Definition (Cardinal Arithmetic)**.** Let κ, λ be cardinals. Then,

$$\kappa +_{\text{card}} \lambda := |(\kappa \times \{0\}) \cup (\lambda \times \{1\})|$$
$$\kappa \cdot_{\text{card}} \lambda := |\kappa \times \lambda|$$

Question: Is $\kappa \cdot_{\text{card}} \lambda = \kappa \cdot_{\text{ord}} \lambda$?

Remark: If we use κ and λ, then we are referring to cardinal operations, while if we use α and β, we are referring to ordinal operations.

Theorem: Let κ, λ, and μ be cardinals.

(i) $\kappa + \lambda = \lambda + \kappa$ and $\kappa \cdot \lambda = \lambda \cdot \kappa$;

(ii) if $\kappa \leqslant \lambda$, then $\kappa + \mu \leqslant \lambda + \mu$ and $\kappa \cdot \mu \leqslant \lambda \times \mu$.

Proof. Homework problem. □

Theorem: If λ is an infinite cardinal, then $\lambda \cdot \lambda = \lambda$.

Example. In particular $\left|\mathbb{R}^2\right| = |\mathbb{R}|$, since

$$\begin{aligned}\left|\mathbb{R}^2\right| &= |\mathbb{R}\times\mathbb{R}|\\ &= |\mathbb{R}|\cdot|\mathbb{R}|\\ &= |\mathbb{R}|.\end{aligned}$$

Question: Is $|\omega| + |\mathbb{R}| \geqslant |\mathbb{R}|$?

Answer: No.

Corollary: If λ is an infinite cardinal, and $0 \neq \kappa \leqslant \lambda$, then $\kappa + \lambda = \lambda$, and $\kappa \cdot \lambda = \lambda$.

Proof.

$$\begin{aligned}\lambda &= 1\cdot\lambda && \text{Needs proof.}\\ &\leqslant \kappa\lambda\lambda\\ &\leqslant \lambda\cdot\lambda\\ &= \lambda.\end{aligned}$$

Thus, all the inequalities are equalities, meaning $\lambda = \kappa\cdot\lambda$.

$$\begin{aligned}\lambda &= 0+\lambda\\ &\leqslant \kappa+\lambda\\ &\leqslant \lambda+\lambda\\ &= |\lambda +_{\text{ord}} \lambda|\\ &= |\lambda \cdot_{\text{ord}} 2|\\ &= \lambda\cdot 2\\ &= 2\cdot\lambda\\ &\leqslant \lambda\cdot\lambda\\ &= \lambda.\end{aligned}$$

□

Example. Let $S = \{f \mid f : 3 \to 2\}$, or $S = \{f \mid f : \{0,1,2\} \to \{0,1\}\}$. Then, $S = 2\times2\times2 = 2^3$.

In general, if A and B are finite sets, we define $|\{f \mid f : A \to B\}| = |B|^{|A|}$.

Definition. Let A and B be arbitrary sets. Then,

$$|A|^{|B|} = |\{f \mid f : B \to A\}|$$

Example.

$$\begin{aligned}2^{\aleph_0} &= |\{f \mid f : \omega \to \{0,1\}\}|\\ &= |P(\omega)|\\ &= |\mathbb{R}|\\ &= \omega_1\end{aligned}$$

Theorem:

$$\left(\kappa^{\lambda}\right)^{\mu} = \kappa^{\lambda\cdot\mu}$$

Theorem: If κ is an infinite cardinal, then

$$\kappa^{\kappa} = 2^{\kappa}.$$

Proof.

$$\begin{aligned}\kappa^\kappa &= (2^\kappa)^\kappa \\ &= 2^{\kappa\cdot\kappa} \\ &= 2^\kappa \\ &\leqslant \kappa^\kappa.\end{aligned}$$

□

Equivalent Versions of the Axiom of Choice

Theorem (Traditional Statement of the Axiom of Choice)**:** If S is a set, and $\forall x \in S$, $x \notin \emptyset$, then

$$\exists f : S \to \bigcup S$$

such that $\forall x \in S$, $f(x) \in x$.

We say f is a choice function.

Theorem (Well-Ordering Theorem)**:** Every nonempty set admits a well-ordering.

Theorem (Zorn's Lemma)**:** In every partially ordered set S, if every chain has an upper bound in S, then S contains a maximal element.

The common joke is that the axiom of choice is obviously true, the well-ordering theorem is obviously false, and Zorn's lemma is unclear.

Definition (Partially Ordered Set)**.** A relation $\preceq$ is known as a partial order if

- $\forall x \in S\,(x \preceq x)$;
- $\forall x, y \in S\,(x \preceq y \land y \preceq x \Rightarrow x = y)$;
- $\forall x, y, z \in S\,(x \preceq y \land y \preceq z \Rightarrow x \preceq z)$.

A partial order may or may not be total. A total ordering includes a fourth condition:

- $\forall x, y \in S\,(x \preceq y \lor y \preceq x)$.

A set equipped with a partial ordering is known as a partially ordered set.

Definition (Chain)**.** A chain in S is a subset of S that is totally ordered by $\preceq$.

Definition (Upper Bound)**.** An upper bound of a subset of S is an element $u \in S$ such that $\forall x \in T\,(x \preceq u)$.

Definition (Maximal Element)**.** An element $m \in S$ is maximal if $\forall x \in S\,(x \succeq m \Rightarrow x = m)$.

Example (Using Zorn's Lemma)**.** We want to know if there exists an uncountable set T such that

(1) $\forall A \in T$, $A \subseteq \mathbb{R}$ and A is countable;

(2) $(T, \subseteq)$ is totally ordered.

The answer is yes.

Proof of Zorn's Lemma. Suppose S does not have a maximal element. Then, every chain C in S has a strict upper bound; i.e., for any upper bound b of C, $b \notin C$.

The Axiom of Choice implies that there exists $f : H = \{C \mid C \text{ is a chain in } S\} \to S$ such that $f(C)$ is a strict upper bound for c.

Let Γ be an arbitrary ordinal, $\alpha \in \Gamma$. Define $g : \Gamma \to H$ recursively by

$$g(\alpha) = \begin{cases} \varnothing & \alpha = \varnothing \\ g(\beta) \cup \{f(g(\beta))\} & \alpha = \beta + 1 \\ \bigcup_{\beta \in \alpha} g(\beta) & \alpha \text{ is a limit ordinal} \end{cases}.$$

We must show that g is injective.

If g is injective, then we have $|\Gamma| \leqslant |H|$. However, since Γ is arbitrary, we can find κ that is a cardinal for $|H|$, but this implies that $|H| \geqslant \kappa$. □

Theorem: Every vector space has a basis.

Proof. Let V be a vector space. Let $L = \left\{S \subseteq V \mid S \text{ is linearly independent}\right\}$. Then, $(L, \subseteq)$ is a partially ordered set.

Every chain C in L has an upper bound:

$$U = \bigcup_{A \in C} A.$$

Then, C is necessarily linearly independent, as otherwise, we would have $a_1v_1 + \cdots a_nv_n = 0$ with $a_1, \dots, a_n \neq 0$, implying $v_1, \dots, v_n \in A$ for some $A \in C$, implying A is linearly dependent.

Thus, by Zorn's lemma, L has a maximal element, $S_{\max}$. Then, $S_{\max} \in L$, so $S_{\max}$ is linearly independent.

Additionally, $S_{\max}$ spans V, because if there were some $w \in V$ with $w \notin \operatorname{span}(S_{\max})$, then we could take $S_{\max} \cup \{w\}$, which would still be linearly independent, contradicting the maximality of S. □

Example. Let $\Gamma = \{f : \mathbb{R} \to \mathbb{R}\}$, and let $\Gamma_C \left\{f : \mathbb{R} \xrightarrow{\text{continuous}} \mathbb{R}\right\}$. We want to prove that $|\Gamma_C| < |\Gamma|$.

Lemma: If $f, g \in \Gamma_C$ are continuous, and for every $x \in \mathbb{Q}$, $f(x) = g(x)$, then $f = g$.

Proof. Suppose toward contradiction that $\exists x$ with $f(x) \neq g(x)$. Then, $(f - g)(x) \neq 0$. Since $f - g$ is continuous, there is some δ such that on $(x - \delta, x + \delta)$, $f - g$ is never zero. However, since $\exists r \in \mathbb{Q}$ such that $r \in (x - \delta, x + \delta)$, this implies that $(f - g)(r) \neq 0$. □

Let $\gamma_{\mathbb{Q}} = \left\{f \big|_{\mathbb{Q}} \mid f \in \Gamma_C\right\}$. Let $\varphi : \Gamma_C \to \Gamma_{\mathbb{Q}}$ defined by $\varphi(f) = f|_{\mathbb{Q}}$. Then, φ is injective. Thus, $|\Gamma_C| \leqslant \left|\Gamma_{\mathbb{Q}}\right| \leqslant |\mathbb{R}|^{|\mathbb{Q}|} < |\mathbb{R}|^{|\mathbb{R}|}$ since $|\mathbb{Q}| < |\mathbb{R}|$, so $|\Gamma_C| < |\Gamma|$.

Computability and Provability

Turing Machines

We have currently seen many algorithms — however, it's very hard to explain what exactly an algorithm is. Informally, algorithms are computable procedures to solve a problem.

Example (An Algorithm to find Prime Numbers)**.** In short, given $n \in \mathbb{N}$, for each $k =\in \{2, 3, 4, \dots, n - 1\}$, we check if $k | n$.

This is not an efficient algorithm. However, it is an algorithm. In a more specific form, we can see that this algorithm is specified below.

(1) Let $k = 2$.

(2) If $k = n$, output yes and stop.

(3) If $k|n$, output `no` and stop.

(4) Increment k: `k <- k+1`.

(5) Go back to step 2.

Definition (Informal Definition for Computability)**.** A function $f : \mathbb{N} \to \mathbb{N}$ is computable if there exists an algorithm α such that for each $n \in \mathbb{N}$, α outputs $f(n)$ given input n.

Question: Is there an algorithm to decide if an arbitrary equation has solutions in the positive integers?

Answer: The answer is **no**. This is known as Hilbert's Tenth Problem.

Question: Is there an algorithm to verify the validity of a proof in mathematics?

Answer: The answer is **yes**. This is the basis of the programming language Lean.

Question: Let

$$p(n) = \begin{cases} 1 & n \text{ is prime} \\ 0 & \text{else} \end{cases}.$$

Answer: The answer is **yes**. We showed an algorithm for p earlier.

Question: Let $F(n)$ be the nth Fibonacci number. Is F computable?

Answer: **Yes**.

Question: Let $f(n)$ be the nth digit of π. Is f computable?

Answer: **Yes**.

Question: Let P be the set of all computer programs in C.

Let P be ordered lexicographically. Define a function $f(n)$ by

$$f(n) = \begin{cases} 1 & n\text{th program stops for every input.} \\ 0 & \text{else} \end{cases}.$$

Is f computable?

Answer: The answer is **no**. This is known as the halting problem, and it is provable.

In order to understand all these results, we need a precise definition of *computable*.

There are several approaches to computability:

- Turing machines;
- recursive functions;
- λ calculus;
- unlimited register machines (URMs);
- computable by (quantum) computers.

All of these have been proven equivalent. For the purposes of this course, we will look at Turing machines.

Definition (Turing Machine)**.** A Turing machine consists of the following:

- an infinite tape divided into discrete segments;
- each segment can contain one symbol (such as 1) or can be left blank;
- the Turing machine is given as much space and time as necessary to compute;

- the machine has a "head" that can read and write the tape, and can move left and right;
- the machine has a finite number of internal states that;
- instructions for the Turing machine are 4-tuples, (a, b, c, d): if in state a, reading symbol b, then do c, then enter state d.

Example. Let

$$\begin{aligned} I_1 &= q_1 1 R q_1 \\ I_2 &= q_1 B 1 q_2 \\ I_3 &= q_2 1 1 q_3. \end{aligned}$$

Here, I_1 essentially says "if current state is q_1, and reading symbol 1, move right, then enter state q_1."

Similarly, I_2 says "if current state is q_1, and reading symbol blank, *write* 1, and enter state q_3."

Consider a tape that reads $\ldots B111B \ldots$. The head starts at the left-most non-blank element, and starts with state q_1.

- The machine performs I_1, moving the head to the middle 1, and remains at state q_1.
- The machine performs I_1, moving the head to the right-most 1, and remains at state q_1.
- The machine performs I_1, moving the head to the blank element to the right of the right-most 1, and remains at state q_1.
- The machine now performs I_2, and writes 1 over the blank element, and enters state q_2.
- The machine now performs I_3, and enters state q_3.
- Since there are no instructions that start with state q_3, the machine halts.

Note that at the start of the Turing machine, there are always finitely many non-blank squares.

Notation: For input, each $n \in \mathbb{N}$ is represented by $n + 1$ consecutive 1s on the tape.

For output, the total number of 1s is the output.

Definition (Computable)**.** A function f is computable if there exists a Turing machine that computes f.

Definition (Partial/Total Function)**.** A partial function is a function $f : A \to \mathbb{N}$ where $A \subseteq \mathbb{N}$. If $A = \mathbb{N}$, then f is also a total function.

This is nice and all, but we need to be able to use multiple inputs too. For instance, we may want to calculate $f(m, n) = m + n$.

Notation (Multiple Inputs)**:** The convention is

$$f(x, y)$$

by taking

$$\underbrace{1, \ldots, 1}_{x+1}, B, \underbrace{1, \ldots, 1}_{y+1}$$

With this definition of multiple inputs, we can define a function $f : A \subseteq \mathbb{N}^n \to \mathbb{N}$ to be computable if it can be represented by a Turing machine.

If $f : \mathbb{Q} \to \mathbb{Q}$, we can represent $x \in \mathbb{Q}$ by (s, m, n), where s denotes the sign.

We can even represent Turing machines with natural numbers. We do this by ordering all the Turing machines lexicographically. Then, we have $T_0, T_1, T_2, \ldots$ via this process.

Question: Is there a Turing machine U such that $U(n, x)$ gives the same output as $T_n(x)$.

Answer: Yes. We call $U(n, x)$ a *universal* Turing machine.

An alternative way we can specify the state of a Turing machine, instead of using the tuple (a, b, c, d) with $a, d = q_i$, $b = B, 1$, and $c = B, 1, L, R$, we let the instruction be in the form $(n_1, n_2, n_3, n_4) \in \mathbb{N}^4$, where n_1, n_4 denote the initial and final states, $n_2 = 0, 1$ depending on whether the read instruction is blank or 1, and n_3 is $0, 1, 2, 3$ depending on if the instruction is B, 1, R, or L respectively.

Question: Is there a Turing machine that can tell whether or not a different Turing machine will halt for a given input.

We want a Turing machine, $T_H(n, x)$, where we ask if $T_n(x)$ halts.

Answer: No.

Theorem (Halting Problem)**:** Let

$$H(n, x) = \begin{cases} 1 & \text{if } T_n(x) \text{ halts} \\ 0 & \text{if } T_n(x) \text{ does not halt} \end{cases}.$$

Then, H is not computable.

Proof. Suppose H is computable. Define

$$G(n) = \begin{cases} 0 & \text{if } H(n, n) = 0 \\ \text{undefined} & \text{if } H(n, n) = 1 \end{cases}.$$

We start by showing that G is computable. Suppose H is computed by some Turing machine T_H. Then, $T_H(x) = H(n, x)$. Suppose $q_1, \dots, q_k$ are the only states T_H. Without loss of generality, we assume T_H halts if and only if T_H enters state q_k. We can also modify T_H such that if the output is 1, then the head ends up at the square with 1. We add an instruction, $q_k 1 1 q_k$ to construct T_G. The new Turing machine, T_G, does not halt. If T_G sees $n + 1$ 1s, we make T_G duplicate this input into $1, \dots, 1, B, 1, \dots, 1$, then run T_H

Now that we have shown that G is computable, there is some $n \in \mathbb{N}$ such that T_n computes G. Thus, $T_n(x)$ halts if and only if $G(x) = 0$. So, $T_n(n)$ halts if and only if $G(n) = 0$, which halts if and only if $H(n, n) = 0$, which is true if and only if $T_n(n)$ doesn't halt. $\perp$ $\square$

Recursive Functions, Decidable Sets, and Enumerable Sets

Now, we can look at the class of functions that "ought" to be computable. For instance, the following functions are computable.

- $C_0(n) = 0$ for all $n \in \mathbb{N}$;
- $S(n) = n + 1$ for all $n \in \mathbb{N}$;
- $P_i^{(k)}(n_1, \dots, n_k) = n_i$ for all $n_1, \dots, n_k \in \mathbb{N}$;
- all compositions of these functions: if $f(t_1, \dots, t_m)$ and $g_1, \dots, g_m$ are computable, then
$$h(x_1, \dots, x_n) = f(g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n)).$$

Example. The function $f(x, y) = y + 1$ is equal to

$$f(x, y) = S\left(P_2^{(2)}(x, y)\right).$$

Similarly, the function

$$g(x, y, z) = P_1^{(2)}\left(S\left(S\left(P_3^{(3)}(x, y, z)\right)\right), P_1^{(3)}(x, y, z)\right)$$

is computable.

Some primitive recursive functions are as follows.

Example.

- $h(n+1) = g(h(n))$ with $h(0)$ equal to some constant;
- $h(m, n+1) = g(m, n, h(m, n))$.

Definition (General Format of Primitive Recursion)**.**

$$h(m_1, \dots, m_k, n+1) = g(m_1, \dots, m_k, n, h(m_1, \dots, m_k, n)),$$

where $h(m_1, \dots, m_k, 0) = f(m_1, \dots, m_k)$. Here, $f(m_1, \dots, m_k)$ is written in terms of $C_0, S, P_i^{(k)}$. We say h is obtained from f and g by primitive recursion.

Definition (Primitive Recursive Function)**.** Any function obtained from $C_0, S, P_i^{(k)}$, composition, and primitive recursion, is called a primitive recursive function.

Theorem: Primitive recursive functions are able to be computed by Turing machines. The converse is not true.

Example (Addition is Primitive Recursive)**.** Show that

$$A(m, n) = m + n$$

is primitive recursive.

Proof. We can see that

$$A(m, n+1) = S(A(m, n)),$$

since $m + n + 1 = (m + n) + 1$. Additionally,

$$A(m, 0) = f(m)$$

with

$$f(m) = P_1^{(1)}(m).$$

Thus,

$$A(m, n+1) = g(m, n, A(m, n)),$$

with $g(x, y, z) = S\left(P_3^{(3)}(m, n, A(m, n))\right)$. Thus, A is computable by Turing machines. □

Example (Multiplication is Primitive Recursive)**.** Show that

$$M(m, n) = mn$$

is primitive recursive.

Proof. We can see that

$$\begin{aligned} M(m, n+1) &= M(m, n) + m \\ &= A(M(m, n), m). \end{aligned}$$

We also have $M(m, 0) = C_0(m)$. □

Example (Predecessor Function)**.** We have the predecessor function

$$\text{pred}(x) = \begin{cases} x - 1 & x \geqslant 1 \\ 0 & x = 0 \end{cases}.$$

is primitive recursive.

Proof. Note that

$$\text{pred}\,(n+1) = n.$$

Thus,

$$\text{pred}\,(n+1) = g\left(n, \text{pred}(n)\right)$$

where $g\,(x, y) = P_1^{(2)}(x, y)$. □

Example (Subtraction Function)**.** Show that

$$\text{sub}\,(x, y) = \begin{cases} x - y & x \geqslant y \\ 0 & \text{else} \end{cases}$$

is primitive recursive.

Proof. Note that we have

$$\begin{aligned} \text{sub}\,(x, y+1) &= \text{pred}\,(\text{sub}\,(x, y)) \\ \text{sub}\,(x, 0) &= x. \end{aligned}$$

□

Example (Characteristic Function for Equality)**.** Let

$$E\,(x, y) = \begin{cases} 1 & x = y \\ 0 & x \neq y. \end{cases}$$

We will show that $E\,(x, y)$ is primitive recursive.

Proof. Let $x \dot{-} y$ denote $\text{sub}\,(x, y)$.

$$E\,(x, y) = (1 \dot{-} (x \dot{-} y)) \dot{-} (x \dot{-} y)\,.$$

Written in the form of proven primitive recursive functions, we have

$$E\,(x, y) = \text{sub}\left(\text{sub}\left(S\left(C_0\left(P_1^{(2)}\,(x, y)\right)\right), \text{sub}\,(x, y)\right), \text{sub}\,(y, x)\right)$$

□

Example (Computable Functions that is not Primitive Recursive)**.** Not every computable function is primitive recursive. For instance, the Ackermann function,

$$A\,(m, n) = \begin{cases} n + 1 & m = 0 \\ A\,(m-1, 1) & m > 0, n = 0 \\ A\,(m-1, A\,(m, n-1)) & m > 0, n > 0 \end{cases},$$

is computable, but not primitive recursive. We will show this.

In the sequence of function growth, we have

$$\begin{aligned}
f_0(n) &= n + 2\\
f_1(n) &= n(2)\\
&= \underbrace{f_0 \circ \cdots \circ f_0}_{n \text{ times}}(0)\\
&= f_0^n(0)\\
f_2 &= 2^n\\
&= \underbrace{f_1 \circ \cdots \circ f_1}_{n \text{ times}}(1)\\
&= f_1^n(1)
\end{aligned}$$

$$f_{k+1}(n) = f_k^n(1). \tag{$*$}$$

These are examples of hyperoperations (beyond exponentiation). Note that if $n = 0$, then $f_{k+1}(0) = f_k^0(1) = 1$.

We define

$$H(k, n) = f_k(n). \tag{$**$}$$

Then,

$$\begin{aligned}
H(k+1, n+1) &= f_{k+1}(n+1) && \text{by } (**)\\
&= f_k^{n+1}(1) && \text{by } (*)\\
&= f_k\left(f_k^n(1)\right) && \text{by definition of } f_k^{n+1}\\
&= f_k\left(f_{k+1}(n)\right) && \text{by } (*)\\
&= f_k\left(H(k+1, n)\right)\\
&= H(k, H(k+1, n)). && \text{by } (**)
\end{aligned}$$

Thus, we have

$$H(k+1, n+1) = H(k, H(k+1, n))$$

Note that the input on H is always reducing via the lexicographical order. If we want $H(0, n)$ and $H(k, 0)$, we have

$$\begin{aligned}
H(0, n) &= n + 2\\
H(k, 0) &= \begin{cases} 2 & k = 0\\ 0 & k = 1\\ 1 & k > 1 \end{cases}.
\end{aligned}$$

Note that we ended up changing the initial conditions.

Since we can write the Ackermann function in any programming language, we can see that it is computable.

To see that the Ackermann function is not primitive recursive, we will show that for any $f : \mathbb{N}^2 \to \mathbb{N}$, there exists k and n such that $H(k, n) > f(k, n)$.

To show this, we show that $C_0, S, P_i^{(k)}$ satisfy this condition by "induction." Then, we show that, for any function that is dominated by the Ackermann function, primitive recursion still yields the function being dominated by the Ackermann function.

Note that the Ackermann function is total, but not primitive recursive. However, we may ask the opposite question.

Question: Is every primitive recursive function total?

Answer: Yes. Since composition, primitive recursion, and the primitive recursive functions all respect totality, all primitive recursive functions are total.

Thus, we necessarily have to conclude that non-total functions are not primitive recursive.

Example. The function $q(n, d)$ defined by

$$q(n, d) = \begin{cases} \frac{n}{d} & d \mid n \\ \text{undef} & \text{else} \end{cases}$$

is not primitive recursive as it is not total.

However, q is computable. We can write an algorithm as follows.

Input: (n, d)
Step 1: Let $k = 0$.
Step 2: If $kd = n$, then output k, and stop.
Step 3: Increment k.
Step 4: Return to Step 2.

We can write

$$q(n, d) = \min\{k \in \mathbb{N} \mid kd = n\},$$

with the convention $\min \emptyset = \text{undef}$.

Remark: The Church–Turing thesis states that any "reasonable" method of defining computability is equivalent to Turing-computability.

Definition. Let $f : \mathbb{N}^{m+1} \to \mathbb{N}$. Define $h : \mathbb{N}^m \to \mathbb{N}$ by

$$h(x_1, \dots, x_m) = \min\{z \in \mathbb{N} \mid f(x_1, \dots, x_m, z) = 0\},$$

with the convention that $\min \emptyset = \text{undef}$. We say h is obtained from f by minimalization.

We write

$$\begin{aligned} h(x_1, \dots, x_m) &= \min_z (f(x_1, \dots, x_m, z) = 0) \\ &= \mu z (f(x_1, \dots, x_m, z) = 0). \end{aligned}$$

Example. Returning to our function q, we can write

$$\begin{aligned} q(n, d) &= \min_z (f(n, d, z) = 0) \\ f(n, d, z) &= |n - dz|. \end{aligned}$$

Definition. A function f is (generally) recursive if f can obtained from S, C_0, and $P_i^{(k)}$ by composition, primitive recursion, and minimalization.

Theorem: Every recursive function is computable.

Theorem: Every computable function is recursive.

Example. Let

$$s_q(n) = \begin{cases} \sqrt{n} & \text{if } n \text{ is perfect square} \\ \text{undef} & \text{else} \end{cases}.$$

We will show s_q is recursive.

$$s_q(n) = \min_z \left(\left| z^2 - n \right| = 0 \right).$$

Note that $\left|z^2 - n\right| = \left(z^2 \dot{-} n\right) + \left(n \dot{-} z^2\right)$.

Definition. The range of f is

$$\text{Ran}(f) = \{ b \mid (a, b) \in f \}.$$

Definition (Recursively Enumerable Set)**.** A set $S \subseteq \mathbb{N}$ is recursively enumerable if there exists a computable function (i.e., Turing-computable or recursive) f such that

$$S = \text{Ran}(f).$$

Question: Is $\varnothing$ a function?

Answer: Yes.

Is $\varnothing$ recursively enumerable?

Answer: Yes (vacuous truth).

Example. Let $S = \left\{ n \in \mathbb{N} \,\middle|\, n \text{ is prime} \right\}$. Is S recursively enumerable?

We can imagine a function f written in our favorite programming language[IX] that yields this set, so it is the case that S is recursively enumerable.

We can show this by having

$$\pi(n) = \begin{cases} 1 & n \text{ is prime} \\ 0 & \text{else} \end{cases},$$

which we then show is recursive.

Afterward, we define a function P by

$$P(n) = p_n,$$

where $p_0 = 2$.

Then, $S = \text{Ran}(P)$.

We define

$$P(n+1) = \min_z \left((z > p(n)) \wedge (\pi(z) = 1) \right).$$

It now remains to be shown that the relation $z > p(n)$ is recursive.

[IX] I'm fond of LaTeX.

Goodstein Sequences

Consider the number written as sums of powers of 2:

$$7 = 2^2 + 2^1 + 2^0.$$

We replace every instance of 2 with 3, and subtract 1 yielding

$$\to 3^3 + 3^1.$$

We replace 3 with 4, and delete 1, and get

$$\to 4^4 + 3 \cdot 4^0.$$

At first glance, this sequence seems to be growing without bound. However, it is actually possible to prove that this sequence, known as the Goodstein sequence, converges to 0 as n grows without bound.

Note that the way we write our original number is using *hereditary* base notation. In other words

$$2^5 + 2^2 + 1 = 2^{2^2+1} + 2^2 + 1,$$

and continue this replacing sequence.