Part I

Naïve Set Theory

The material in this part is an introduction to basic naive set theory. With the inclusion of Tim Button's Open Set Theory, this also covers the construction of number systems, and discussion of infinity, which are not required for the logical parts of the OLP.

Chapter 1

Sets

1.1 Extensionality

sfr:set:bas:sec

A *set* is a collection of objects, considered as a single object. The objects making up the set are called *elements* or *members* of the set. If x is an element of a set a, we write $x \in a$; if not, we write $x \notin a$. The set which has no elements is called the *empty* set and denoted "$\emptyset$".

It does not matter how we *specify* the set, or how we *order* its elements, or indeed how *many times* we count its elements. All that matters are what its elements are. We codify this in the following principle. explanation

Definition 1.1 (Extensionality). If A and B are sets, then $A = B$ iff every element of A is also an element of B, and vice versa.

Extensionality licenses some notation. In general, when we have some objects $a_1, \ldots, a_n$, then $\{a_1, \ldots, a_n\}$ is *the* set whose elements are $a_1, \ldots, a_n$. We emphasise the word "*the*", since extensionality tells us that there can be only *one* such set. Indeed, extensionality also licenses the following:

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

This delivers on the point that, when we consider sets, we don't care about the order of their elements, or how many times they are specified.

Example 1.2. Whenever you have a bunch of objects, you can collect them together in a set. The set of Richard's siblings, for instance, is a set that contains one person, and we could write it as $S = \{\text{Ruth}\}$. The set of positive integers less than 4 is $\{1, 2, 3\}$, but it can also be written as $\{3, 2, 1\}$ or even as $\{1, 2, 1, 2, 3\}$. These are all the same set, by extensionality. For every element of $\{1, 2, 3\}$ is also an element of $\{3, 2, 1\}$ (and of $\{1, 2, 1, 2, 3\}$), and vice versa.

Frequently we'll specify a set by some property that its elements share. We'll use the following shorthand notation for that: $\{x : \varphi(x)\}$, where the $\varphi(x)$ stands for the property that x has to have in order to be counted among the elements of the set.

Example 1.3. In our example, we could have specified S also as

$$S = \{x : x \text{ is a sibling of Richard}\}.$$

Example 1.4. A number is called *perfect* iff it is equal to the sum of its proper divisors (i.e., numbers that evenly divide it but aren't identical to the number). For instance, 6 is perfect because its proper divisors are 1, 2, and 3, and $6 = 1 + 2 + 3$. In fact, 6 is the only positive integer less than 10 that is perfect. So, using extensionality, we can say:

$$\{6\} = \{x : x \text{ is perfect and } 0 \leq x \leq 10\}$$

We read the notation on the right as "the set of x's such that x is perfect and $0 \leq x \leq 10$". The identity here confirms that, when we consider sets, we don't care about how they are specified. And, more generally, extensionality guarantees that there is always only one set of x's such that $\varphi(x)$. So, extensionality justifies calling $\{x : \varphi(x)\}$ *the* set of x's such that $\varphi(x)$.

Extensionality gives us a way for showing that sets are identical: to show that $A = B$, show that whenever $x \in A$ then also $x \in B$, and whenever $y \in B$ then also $y \in A$.

Problem 1.1. Prove that there is at most one empty set, i.e., show that if A and B are sets without elements, then $A = B$.

1.2 Subsets and Power Sets

explanation We will often want to compare sets. And one obvious kind of comparison one might make is as follows: *everything in one set is in the other too*. This situation is sufficiently important for us to introduce some new notation. sfr:set:sub:sec

Definition 1.5 (Subset). If every element of a set A is also an element of B, then we say that A is a *subset* of B, and write $A \subseteq B$. If A is not a subset of B we write $A \nsubseteq B$. If $A \subseteq B$ but $A \neq B$, we write $A \subsetneq B$ and say that A is a *proper subset* of B.

Example 1.6. Every set is a subset of itself, and $\emptyset$ is a subset of every set. The set of even numbers is a subset of the set of natural numbers. Also, $\{a, b\} \subseteq \{a, b, c\}$. But $\{a, b, e\}$ is not a subset of $\{a, b, c\}$.

Example 1.7. The number 2 is an element of the set of integers, whereas the set of even numbers is a subset of the set of integers. However, a set may happen to *both* be an element and a subset of some other set, e.g., $\{0\} \in \{0, \{0\}\}$ and also $\{0\} \subseteq \{0, \{0\}\}$.

Extensionality gives a criterion of identity for sets: $A = B$ iff every element of A is also an element of B and vice versa. The definition of "subset" defines $A \subseteq B$ precisely as the first half of this criterion: every element of A is also

an element of B. Of course the definition also applies if we switch A and B: that is, $B \subseteq A$ iff every element of B is also an element of A. And that, in turn, is exactly the "vice versa" part of extensionality. In other words, extensionality entails that sets are equal iff they are subsets of one another.

Proposition 1.8. *$A = B$ iff both $A \subseteq B$ and $B \subseteq A$.*

Now is also a good opportunity to introduce some further bits of helpful notation. In defining when A is a subset of B we said that "every element of A is . . . ," and filled the ". . . " with "an element of B". But this is such a common *shape* of expression that it will be helpful to introduce some formal notation for it.

sfr:set:sub:forallxina

Definition 1.9. $(\forall x \in A)\varphi$ abbreviates $\forall x(x \in A \to \varphi)$. Similarly, $(\exists x \in A)\varphi$ abbreviates $\exists x(x \in A \wedge \varphi)$.

Using this notation, we can say that $A \subseteq B$ iff $(\forall x \in A)x \in B$.

Now we move on to considering a certain kind of set: the set of all subsets of a given set.

Definition 1.10 (Power Set). The set consisting of all subsets of a set A is called the *power set of* A, written $\wp(A)$.

$$\wp(A) = \{B : B \subseteq A\}$$

Example 1.11. What are all the possible subsets of $\{a, b, c\}$? They are: $\emptyset$, $\{a\}$, $\{b\}$, $\{c\}$, $\{a, b\}$, $\{a, c\}$, $\{b, c\}$, $\{a, b, c\}$. The set of all these subsets is $\wp(\{a, b, c\})$:

$$\wp(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$$

Problem 1.2. List all subsets of $\{a, b, c, d\}$.

Problem 1.3. Show that if A has n elements, then $\wp(A)$ has 2^n elements.

1.3 Some Important Sets

sfr:set:imp:sec

Example 1.12. We will mostly be dealing with sets whose elements are mathematical objects. Four such sets are important enough to have specific names:

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$
the set of natural numbers

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$
the set of integers

$$\mathbb{Q} = \{m/n : m, n \in \mathbb{Z} \text{ and } n \neq 0\}$$
the set of rationals

$$\mathbb{R} = (-\infty, \infty)$$
the set of real numbers (the continuum)

These are all *infinite* sets, that is, they each have infinitely many elements.

As we move through these sets, we are adding *more* numbers to our stock. Indeed, it should be clear that $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$: after all, every natural number is an integer; every integer is a rational; and every rational is a real. Equally, it should be clear that $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q}$, since -1 is an integer but not a natural number, and $1/2$ is rational but not integer. It is less obvious that $\mathbb{Q} \subsetneq \mathbb{R}$, i.e., that there are some real numbers which are not rational.

We'll sometimes also use the set of positive integers $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ and the set containing just the first two natural numbers $\mathbb{B} = \{0, 1\}$.

Example 1.13 (Strings). Another interesting example is the set A^* of *finite strings* over an alphabet A: any finite sequence of elements of A is a string over A. We include the *empty string* Λ among the strings over A, for every alphabet A. For instance,

$$\mathbb{B}^* = \{\Lambda, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111, 0000, \ldots\}.$$

If $x = x_1 \ldots x_n \in A^*$is a string consisting of n "letters" from A, then we say *length* of the string is n and write $\text{len}(x) = n$.

Example 1.14 (Infinite sequences). For any set A we may also consider the set A^ω of infinite sequences of elements of A. An infinite sequence $a_1 a_2 a_3 a_4 \ldots$ consists of a one-way infinite list of objects, each one of which is an element of A.

1.4 Unions and Intersections

explanation

In section 1.1, we introduced definitions of sets by abstraction, i.e., definitions of the form $\{x : \varphi(x)\}$. Here, we invoke some property φ, and this property can mention sets we've already defined. So for instance, if A and B are sets, the set $\{x : x \in A \vee x \in B\}$ consists of all those objects which are elements

sfr:set:uni:sec

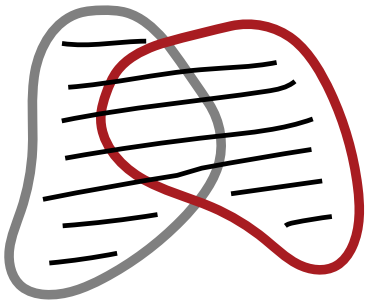


Figure 1.1: The union $A \cup B$ of two sets is set of elements of A together with those of B.

sfr:set:uni:
fig:union

of either A or B, i.e., it's the set that combines the elements of A and B. We can visualize this as in Figure 1.1, where the highlighted area indicates the elements of the two sets A and B together.

This operation on sets—combining them—is very useful and common, and so we give it a formal name and a symbol.

Definition 1.15 (Union). The *union* of two sets A and B, written $A \cup B$, is the set of all things which are elements of A, B, or both.

$$A \cup B = \{x : x \in A \vee x \in B\}$$

Example 1.16. Since the multiplicity of elements doesn't matter, the union of two sets which have an element in common contains that element only once, e.g., $\{a, b, c\} \cup \{a, 0, 1\} = \{a, b, c, 0, 1\}$.

The union of a set and one of its subsets is just the bigger set: $\{a, b, c\} \cup \{a\} = \{a, b, c\}$.

The union of a set with the empty set is identical to the set: $\{a, b, c\} \cup \emptyset = \{a, b, c\}$.

Problem 1.4. Prove that if $A \subseteq B$, then $A \cup B = B$.

We can also consider a "dual" operation to union. This is the operation that forms the set of all elements that are elements of A and are also elements of B. This operation is called *intersection*, and can be depicted as in Figure 1.2.

explanation

Definition 1.17 (Intersection). The *intersection* of two sets A and B, written $A \cap B$, is the set of all things which are elements of both A and B.

$$A \cap B = \{x : x \in A \wedge x \in B\}$$

Two sets are called *disjoint* if their intersection is empty. This means they have no elements in common.

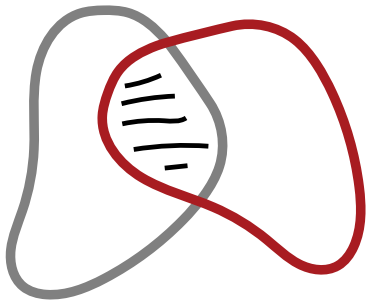


Figure 1.2: The intersection $A \cap B$ of two sets is the set of elements they have in common.

sfr:set:uni: fig:intersection

Example 1.18. If two sets have no elements in common, their intersection is empty: $\{a, b, c\} \cap \{0, 1\} = \emptyset$.

If two sets do have elements in common, their intersection is the set of all those: $\{a, b, c\} \cap \{a, b, d\} = \{a, b\}$.

The intersection of a set with one of its subsets is just the smaller set: $\{a, b, c\} \cap \{a, b\} = \{a, b\}$.

The intersection of any set with the empty set is empty: $\{a, b, c\} \cap \emptyset = \emptyset$.

Problem 1.5. Prove rigorously that if $A \subseteq B$, then $A \cap B = A$.

explanation

We can also form the union or intersection of more than two sets. An elegant way of dealing with this in general is the following: suppose you collect all the sets you want to form the union (or intersection) of into a single set. Then we can define the union of all our original sets as the set of all objects which belong to at least one element of the set, and the intersection as the set of all objects which belong to every element of the set.

Definition 1.19. If A is a set of sets, then $\bigcup A$ is the set of elements of elements of A:

$$\begin{aligned} \bigcup A &= \{x : x \text{ belongs to an element of } A\}, \text{ i.e.,} \\ &= \{x : \text{there is a } B \in A \text{ so that } x \in B\} \end{aligned}$$

Definition 1.20. If A is a set of sets, then $\bigcap A$ is the set of objects which all elements of A have in common:

$$\begin{aligned} \bigcap A &= \{x : x \text{ belongs to every element of } A\}, \text{ i.e.,} \\ &= \{x : \text{for all } B \in A, x \in B\} \end{aligned}$$

Example 1.21. Suppose $A = \{\{a, b\}, \{a, d, e\}, \{a, d\}\}$. Then $\bigcup A = \{a, b, d, e\}$ and $\bigcap A = \{a\}$.

Problem 1.6. Show that if A is a set and $A \in B$, then $A \subseteq \bigcup B$.

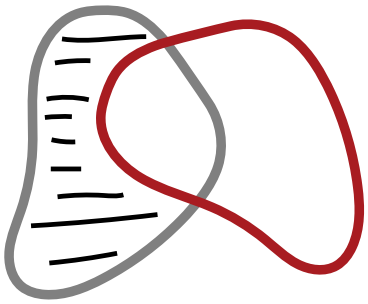


Figure 1.3: The difference $A \setminus B$ of two sets is the set of those elements of A which are not also elements of B.

sfr:set:uni:difference

We could also do the same for a sequence of sets A_1, A_2, ...

$$\bigcup_i A_i = \{x : x \text{ belongs to one of the } A_i\}$$
$$\bigcap_i A_i = \{x : x \text{ belongs to every } A_i\}.$$

When we have an *index* of sets, i.e., some set I such that we are considering A_i for each $i \in I$, we may also use these abbreviations:

$$\bigcup_{i \in I} A_i = \bigcup \{A_i : i \in I\}$$
$$\bigcap_{i \in I} A_i = \bigcap \{A_i : i \in I\}$$

Finally, we may want to think about the set of all elements in A which are not in B. We can depict this as in Figure 1.3.

Definition 1.22 (Difference). The *set difference* $A \setminus B$ is the set of all elements of A which are not also elements of B, i.e.,

$$A \setminus B = \{x : x \in A \text{ and } x \notin B\}.$$

Problem 1.7. Prove that if $A \subsetneq B$, then $B \setminus A \neq \emptyset$.

1.5 Pairs, Tuples, Cartesian Products

sfr:set:pai:sec

It follows from extensionality that sets have no order to their elements. So if we want to represent order, we use *ordered pairs* $\langle x, y \rangle$. In an unordered pair $\{x, y\}$, the order does not matter: $\{x, y\} = \{y, x\}$. In an ordered pair, it does: if $x \neq y$, then $\langle x, y \rangle \neq \langle y, x \rangle$.

explanation

How should we think about ordered pairs in set theory? Crucially, we want to preserve the idea that ordered pairs are identical iff they share the same first element and share the same second element, i.e.:

$$\langle a, b\rangle = \langle c, d\rangle \text{ iff both } a = c \text{ and } b = d.$$

We can define ordered pairs in set theory using the Wiener-Kuratowski definition.

Definition 1.23 (Ordered pair). $\langle a, b\rangle = \{\{a\}, \{a, b\}\}$. sfr:set:pai: wienerkuratowski

Problem 1.8. Using Definition 1.23, prove that $\langle a, b\rangle = \langle c, d\rangle$ iff both $a = c$ and $b = d$.

explanation Having fixed a definition of an ordered pair, we can use it to define further sets. For example, sometimes we also want ordered sequences of more than two objects, e.g., *triples* $\langle x, y, z\rangle$, *quadruples* $\langle x, y, z, u\rangle$, and so on. We can think of triples as special ordered pairs, where the first element is itself an ordered pair: $\langle x, y, z\rangle$ is $\langle\langle x, y\rangle, z\rangle$. The same is true for quadruples: $\langle x, y, z, u\rangle$ is $\langle\langle\langle x, y\rangle, z\rangle, u\rangle$, and so on. In general, we talk of *ordered n-tuples* $\langle x_1, \ldots, x_n\rangle$.

Certain sets of ordered pairs, or other ordered n-tuples, will be useful.

Definition 1.24 (Cartesian product). Given sets A and B, their *Cartesian product* $A \times B$ is defined by

$$A \times B = \{\langle x, y\rangle : x \in A \text{ and } y \in B\}.$$

Example 1.25. If $A = \{0, 1\}$, and $B = \{1, a, b\}$, then their product is

$$A \times B = \{\langle 0, 1\rangle, \langle 0, a\rangle, \langle 0, b\rangle, \langle 1, 1\rangle, \langle 1, a\rangle, \langle 1, b\rangle\}.$$

Example 1.26. If A is a set, the product of A with itself, $A \times A$, is also written A^2. It is the set of *all* pairs $\langle x, y\rangle$ with $x, y \in A$. The set of all triples $\langle x, y, z\rangle$ is A^3, and so on. We can give a recursive definition:

$$A^1 = A$$
$$A^{k+1} = A^k \times A$$

Problem 1.9. List all elements of $\{1, 2, 3\}^3$.

Proposition 1.27. *If A has n elements and B has m elements, then $A \times B$ has $n \cdot m$ elements.* *sfr:set:pai: cardnmprod*

Proof. For every element x in A, there are m elements of the form $\langle x, y\rangle \in A \times B$. Let $B_x = \{\langle x, y\rangle : y \in B\}$. Since whenever $x_1 \neq x_2$, $\langle x_1, y\rangle \neq \langle x_2, y\rangle$, $B_{x_1} \cap B_{x_2} = \emptyset$. But if $A = \{x_1, \ldots, x_n\}$, then $A \times B = B_{x_1} \cup \cdots \cup B_{x_n}$, and so has $n \cdot m$ elements.

To visualize this, arrange the elements of $A \times B$ in a grid:

$$\begin{array}{rcccc} B_{x_1} = & \{\langle x_1, y_1\rangle & \langle x_1, y_2\rangle & \dots & \langle x_1, y_m\rangle\} \\ B_{x_2} = & \{\langle x_2, y_1\rangle & \langle x_2, y_2\rangle & \dots & \langle x_2, y_m\rangle\} \\ \vdots & & \vdots & & \\ B_{x_n} = & \{\langle x_n, y_1\rangle & \langle x_n, y_2\rangle & \dots & \langle x_n, y_m\rangle\} \end{array}$$

Since the x_i are all different, and the y_j are all different, no two of the pairs in this grid are the same, and there are $n \cdot m$ of them. □

Problem 1.10. Show, by induction on k, that for all $k \geq 1$, if A has n elements, then A^k has n^k elements.

Example 1.28. If A is a set, a *word* over A is any sequence of elements of A. A sequence can be thought of as an n-tuple of elements of A. For instance, if $A = \{a, b, c\}$, then the sequence "*bac*" can be thought of as the triple $\langle b, a, c\rangle$. Words, i.e., sequences of symbols, are of crucial importance in computer science. By convention, we count elements of A as sequences of length 1, and $\emptyset$ as the sequence of length 0. The set of *all* words over A then is

$$A^* = \{\emptyset\} \cup A \cup A^2 \cup A^3 \cup \dots$$

1.6 Russell's Paradox

sfr:set:rus: sec

Extensionality licenses the notation $\{x : \varphi(x)\}$, for *the* set of x's such that $\varphi(x)$. However, all that extensionality *really* licenses is the following thought. *If* there is a set whose members are all and only the φ's, *then* there is only one such set. Otherwise put: having fixed some φ, the set $\{x : \varphi(x)\}$ is unique, *if it exists*.

But this conditional is important! Crucially, not every property lends itself to *comprehension*. That is, some properties do *not* define sets. If they all did, then we would run into outright contradictions. The most famous example of this is Russell's Paradox.

Sets may be elements of other sets—for instance, the power set of a set A is made up of sets. And so it makes sense to ask or investigate whether a set is an element of another set. Can a set be a member of itself? Nothing about the idea of a set seems to rule this out. For instance, if *all* sets form a collection of objects, one might think that they can be collected into a single set—the set of all sets. And it, being a set, would be an element of the set of all sets.

Russell's Paradox arises when we consider the property of not having itself as an element, of being *non-self-membered*. What if we suppose that there is a set of all sets that do not have themselves as an element? Does

$$R = \{x : x \notin x\}$$

exist? It turns out that we can prove that it does not.

sfr:set:rus: thm:russells-paradox

Theorem 1.29 (Russell's Paradox). *There is no set* $R = \{x : x \notin x\}$.

Proof. For reductio, suppose that $R = \{x : x \notin x\}$ exists. Then $R \in R$ iff $R \notin R$, since sets are extensional. But this is a contradicion. □

explanation

Let's run through the proof that no set R of non-self-membered sets can exist more slowly. If R exists, it makes sense to ask if $R \in R$ or not—it must be either $\in R$ or $\notin R$. Suppose the former is true, i.e., $R \in R$. R was defined as the set of all sets that are not elements of themselves, and so if $R \in R$, then R does not have this defining property of R. But only sets that have this property are in R, hence, R cannot be an element of R, i.e., $R \notin R$. But R can't both be and not be an element of R, so we have a contradiction.

Since the assumption that $R \in R$ leads to a contradiction, we have $R \notin R$. But this also leads to a contradiction! For if $R \notin R$, it does have the defining property of R, and so would be an element of R just like all the other non-self-membered sets. And again, it can't both not be and be an element of R.

digression

How do we set up a set theory which avoids falling into Russell's Paradox, i.e., which avoids making the *inconsistent* claim that $R = \{x : x \notin x\}$ exists? Well, we would need to lay down axioms which give us very precise conditions for stating when sets exist (and when they don't).

The set theory sketched in this chapter doesn't do this. It's *genuinely naïve*. It tells you only that sets obey extensionality and that, if you have some sets, you can form their union, intersection, etc. It is possible to develop set theory more rigorously than this.

Chapter 2

Relations

2.1 Relations as Sets

sfr:rel:set:sec

In section 1.3, we mentioned some important sets: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. You will no doubt remember some interesting relations between the elements of some of these sets. For instance, each of these sets has a completely standard *order relation* on it. There is also the relation *is identical with* that every object bears to itself and to no other thing. There are many more interesting relations that we'll encounter, and even more possible relations. Before we review them, though, we will start by pointing out that we can look at relations as a special sort of set.

explanation

For this, recall two things from section 1.5. First, recall the notion of a *ordered pair*: given a and b, we can form $\langle a, b\rangle$. Importantly, the order of elements *does* matter here. So if $a \neq b$ then $\langle a, b\rangle \neq \langle b, a\rangle$. (Contrast this with unordered pairs, i.e., 2-element sets, where $\{a, b\} = \{b, a\}$.) Second, recall the notion of a *Cartesian product*: if A and B are sets, then we can form $A \times B$, the set of all pairs $\langle x, y\rangle$ with $x \in A$ and $y \in B$. In particular, $A^2 = A \times A$ is the set of all ordered pairs from A.

Now we will consider a particular relation on a set: the $<$-relation on the set $\mathbb{N}$ of natural numbers. Consider the set of all pairs of numbers $\langle n, m\rangle$ where $n < m$, i.e.,

$$R = \{\langle n, m\rangle : n, m \in \mathbb{N} \text{ and } n < m\}.$$

There is a close connection between n being less than m, and the pair $\langle n, m\rangle$ being a member of R, namely:

$$n < m \text{ iff } \langle n, m\rangle \in R.$$

Indeed, without any loss of information, we can consider the set R to *be* the $<$-relation on $\mathbb{N}$.

In the same way we can construct a subset of $\mathbb{N}^2$ for any relation between numbers. Conversely, given any set of pairs of numbers $S \subseteq \mathbb{N}^2$, there is a corresponding relation between numbers, namely, the relationship n bears to m if and only if $\langle n, m\rangle \in S$. This justifies the following definition:

Definition 2.1 (Binary relation). A *binary relation* on a set A is a subset of A^2. If $R \subseteq A^2$ is a binary relation on A and $x, y \in A$, we sometimes write Rxy (or xRy) for $\langle x, y\rangle \in R$.

Example 2.2. The set $\mathbb{N}^2$ of pairs of natural numbers can be listed in a 2-dimensional matrix like this: sfr:rel:set: relations

$$\begin{array}{cccccc}
\langle \mathbf{0},\mathbf{0}\rangle & \langle 0,1\rangle & \langle 0,2\rangle & \langle 0,3\rangle & \dots \\
\langle 1,0\rangle & \langle \mathbf{1},\mathbf{1}\rangle & \langle 1,2\rangle & \langle 1,3\rangle & \dots \\
\langle 2,0\rangle & \langle 2,1\rangle & \langle \mathbf{2},\mathbf{2}\rangle & \langle 2,3\rangle & \dots \\
\langle 3,0\rangle & \langle 3,1\rangle & \langle 3,2\rangle & \langle \mathbf{3},\mathbf{3}\rangle & \dots \\
\vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

We have put the diagonal, here, in bold, since the subset of $\mathbb{N}^2$ consisting of the pairs lying on the diagonal, i.e.,

$$\{\langle 0,0\rangle, \langle 1,1\rangle, \langle 2,2\rangle, \dots\},$$

is the *identity relation on* $\mathbb{N}$. (Since the identity relation is popular, let's define $\mathrm{Id}_A = \{\langle x, x\rangle : x \in X\}$ for any set A.) The subset of all pairs lying above the diagonal, i.e.,

$$L = \{\langle 0,1\rangle, \langle 0,2\rangle, \dots, \langle 1,2\rangle, \langle 1,3\rangle, \dots, \langle 2,3\rangle, \langle 2,4\rangle, \dots\},$$

is the *less than* relation, i.e., Lnm iff $n < m$. The subset of pairs below the diagonal, i.e.,

$$G = \{\langle 1,0\rangle, \langle 2,0\rangle, \langle 2,1\rangle, \langle 3,0\rangle, \langle 3,1\rangle, \langle 3,2\rangle, \dots\},$$

is the *greater than* relation, i.e., Gnm iff $n > m$. The union of L with I, which we might call $K = L \cup I$, is the *less than or equal to* relation: Knm iff $n \leq m$. Similarly, $H = G \cup I$ is the *greater than or equal to relation.* These relations L, G, K, and H are special kinds of relations called *orders.* L and G have the property that no number bears L or G to itself (i.e., for all n, neither Lnn nor Gnn). Relations with this property are called *irreflexive*, and, if they also happen to be orders, they are called *strict orders.*

explanation

Although orders and identity are important and natural relations, it should be emphasized that according to our definition *any* subset of A^2 is a relation on A, regardless of how unnatural or contrived it seems. In particular, $\emptyset$ is a relation on any set (the *empty relation*, which no pair of elements bears), and A^2 itself is a relation on A as well (one which every pair bears), called the *universal relation.* But also something like $E = \{\langle n, m\rangle : n > 5 \text{ or } m \times n \geq 34\}$ counts as a relation.

Problem 2.1. List the elements of the relation $\subseteq$ on the set $\wp(\{a, b, c\})$.

2.2 Philosophical Reflections

sfr:rel:ref:sec

In section 2.1, we defined relations as certain sets. We should pause and ask a quick philosophical question: what is such a definition *doing*? It is extremely doubtful that we should want to say that we have *discovered* some metaphysical identity facts; that, for example, the order relation on $\mathbb{N}$ *turned out* to be the set $R = \{\langle n, m\rangle : n, m \in \mathbb{N} \text{ and } n < m\}$ we defined in section 2.1. Here are three reasons why.

First: in Definition 1.23, we defined $\langle a, b\rangle = \{\{a\}, \{a, b\}\}$. Consider instead the definition $\|a, b\| = \{\{b\}, \{a, b\}\} = \langle b, a\rangle$. When $a \neq b$, we have that $\langle a, b\rangle \neq \|a, b\|$. But we could equally have regarded $\|a, b\|$ as our definition of an ordered pair, rather than $\langle a, b\rangle$. Both definitions would have worked equally well. So now we have two equally good candidates to "be" the order relation on the natural numbers, namely:

$$R = \{\langle n, m\rangle : n, m \in \mathbb{N} \text{ and } n < m\}$$
$$S = \{\|n, m\| : n, m \in \mathbb{N} \text{ and } n < m\}.$$

Since $R \neq S$, by extensionality, it is clear that they cannot *both* be identical to the order relation on $\mathbb{N}$. But it would just be arbitrary, and hence a bit embarrassing, to claim that R rather than S (or vice versa) *is* the ordering relation, as a matter of fact. (This is a very simple instance of an argument against set-theoretic reductionism which Benacerraf made famous in 1965. We will revisit it several times.)

Second: if we think that *every* relation should be identified with a set, then the relation of set-membership itself, $\in$, should be a particular set. Indeed, it would have to be the set $\{\langle x, y\rangle : x \in y\}$. But does this set exist? Given Russell's Paradox, it is a non-trivial claim that such a set exists. In fact, it is possible to develop set theory in a rigorous way as an axiomatic theory. In this theory, it will be provable that there is no set of all sets. So, even if some relations can be treated as sets, the relation of set-membership will have to be a special case.

Third: when we "identify" relations with sets, we said that we would allow ourselves to write Rxy for $\langle x, y\rangle \in R$. This is fine, provided that the membership relation, "$\in$", is treated *as* a predicate. But if we think that "$\in$" stands for a certain kind of set, then the expression "$\langle x, y\rangle \in R$" just consists of three singular terms which stand for sets: "$\langle x, y\rangle$", "$\in$", and "R". And such a list of names is no more capable of expressing a proposition than the nonsense string: "the cup penholder the table". Again, even if some relations can be treated as sets, the relation of set-membership must be a special case. (This rolls together a simple version of Frege's concept *horse* paradox, and a famous objection that Wittgenstein once raised against Russell.)

So where does this leave us? Well, there is nothing *wrong* with our saying that the relations on the numbers are sets. We just have to understand the spirit in which that remark is made. We are not stating a metaphysical identity fact. We are simply noting that, in certain contexts, we can (and will) *treat* (certain) relations as certain sets.

2.3 Special Properties of Relations

intro

Some kinds of relations turn out to be so common that they have been given special names. For instance, $\leq$ and $\subseteq$ both relate their respective domains (say, $\mathbb{N}$ in the case of $\leq$ and $\wp(A)$ in the case of $\subseteq$) in similar ways. To get at exactly how these relations are similar, and how they differ, we categorize them according to some special properties that relations can have. It turns out that (combinations of) some of these special properties are especially important: orders and equivalence relations.

sfr:rel:prp:sec

Definition 2.3 (Reflexivity). A relation $R \subseteq A^2$ is *reflexive* iff, for every $x \in A$, Rxx.

Definition 2.4 (Transitivity). A relation $R \subseteq A^2$ is *transitive* iff, whenever Rxy and Ryz, then also Rxz.

Definition 2.5 (Symmetry). A relation $R \subseteq A^2$ is *symmetric* iff, whenever Rxy, then also Ryx.

Definition 2.6 (Anti-symmetry). A relation $R \subseteq A^2$ is *anti-symmetric* iff, whenever both Rxy and Ryx, then $x = y$ (or, in other words: if $x \neq y$ then either $\neg Rxy$ or $\neg Ryx$).

explanation

In a symmetric relation, Rxy and Ryx always hold together, or neither holds. In an anti-symmetric relation, the only way for Rxy and Ryx to hold together is if $x = y$. Note that this does not *require* that Rxy and Ryx holds when $x = y$, only that it isn't ruled out. So an anti-symmetric relation can be reflexive, but it is not the case that every anti-symmetric relation is reflexive. Also note that being anti-symmetric and merely not being symmetric are different conditions. In fact, a relation can be both symmetric and anti-symmetric at the same time (e.g., the identity relation is).

Definition 2.7 (Connectivity). A relation $R \subseteq A^2$ is *connected* if for all $x, y \in A$, if $x \neq y$, then either Rxy or Ryx.

Problem 2.2. Give examples of relations that are (a) reflexive and symmetric but not transitive, (b) reflexive and anti-symmetric, (c) anti-symmetric, transitive, but not reflexive, and (d) reflexive, symmetric, and transitive. Do not use relations on numbers or sets.

Definition 2.8 (Irreflexivity). A relation $R \subseteq A^2$ is called *irreflexive* if, for all $x \in A$, not Rxx.

Definition 2.9 (Asymmetry). A relation $R \subseteq A^2$ is called *asymmetric* if for no pair $x, y \in A$ we have both Rxy and Ryx.

Note that if $A \neq \emptyset$, then no irreflexive relation on A is reflexive and every asymmetric relation on A is also anti-symmetric. However, there are $R \subseteq A^2$ that are not reflexive and also not irreflexive, and there are anti-symmetric relations that are not asymmetric.

2.4 Equivalence Relations

sfr:rel:eqv:sec

The identity relation on a set is reflexive, symmetric, and transitive. Relations R that have all three of these properties are very common.

Definition 2.10 (Equivalence relation). A relation $R \subseteq A^2$ that is reflexive, symmetric, and transitive is called an *equivalence relation*. Elements x and y of A are said to be *R-equivalent* if Rxy.

Equivalence relations give rise to the notion of an *equivalence class*. An equivalence relation "chunks up" the domain into different partitions. Within each partition, all the objects are related to one another; and no objects from different partitions relate to one another. Sometimes, it's helpful just to talk about these partitions *directly*. To that end, we introduce a definition:

sfr:rel:eqv:def:equivalenceclass

Definition 2.11. Let $R \subseteq A^2$ be an equivalence relation. For each $x \in A$, the *equivalence class* of x in A is the set $[x]_R = \{y \in A : Rxy\}$. The *quotient* of A under R is $A/_R = \{[x]_R : x \in A\}$, i.e., the set of these equivalence classes.

The next result vindicates the definition of an equivalence class, in proving that the equivalence classes are indeed the partitions of A:

Proposition 2.12. *If $R \subseteq A^2$ is an equivalence relation, then Rxy iff $[x]_R = [y]_R$.*

Proof. For the left-to-right direction, suppose Rxy, and let $z \in [x]_R$. By definition, then, Rxz. Since R is an equivalence relation, Ryz. (Spelling this out: as Rxy and R is symmetric we have Ryx, and as Rxz and R is transitive we have Ryz.) So $z \in [y]_R$. Generalising, $[x]_R \subseteq [y]_R$. But exactly similarly, $[y]_R \subseteq [x]_R$. So $[x]_R = [y]_R$, by extensionality.

For the right-to-left direction, suppose $[x]_R = [y]_R$. Since R is reflexive, Ryy, so $y \in [y]_R$. Thus also $y \in [x]_R$ by the assumption that $[x]_R = [y]_R$. So Rxy. □

Example 2.13. A nice example of equivalence relations comes from modular arithmetic. For any a, b, and $n \in \mathbb{N}$, say that $a \equiv_n b$ iff dividing a by n gives remainder b. (Somewhat more symbolically: $a \equiv_n b$ iff $(\exists k \in \mathbb{N})a - b = kn$.) Now, $\equiv_n$ is an equivalence relation, for any n. And there are exactly n distinct equivalence classes generated by $\equiv_n$; that is, $\mathbb{N}/_{\equiv_n}$ has n elements. These are: the set of numbers divisible by n without remainder, i.e., $[0]_{\equiv_n}$; the set of numbers divisible by n with remainder 1, i.e., $[1]_{\equiv_n}$; ...; and the set of numbers divisible by n with remainder $n-1$, i.e., $[n-1]_{\equiv_n}$.

Problem 2.3. Show that $\equiv_n$ is an equivalence relation, for any $n \in \mathbb{N}$, and that $\mathbb{N}/_{\equiv_n}$ has exactly n members.

2.5 Orders

explanation

Many of our comparisons involve describing some objects as being "less than", "equal to", or "greater than" other objects, in a certain respect. These involve *order* relations. But there are different kinds of order relations. For instance, some require that any two objects be comparable, others don't. Some include identity (like $\leq$) and some exclude it (like $<$). It will help us to have a taxonomy here.

sfr:rel:ord:sec

Definition 2.14 (Preorder). A relation which is both reflexive and transitive is called a *preorder*.

Definition 2.15 (Partial order). A preorder which is also anti-symmetric is called a *partial order*.

Definition 2.16 (Linear order). A partial order which is also connected is called a *total order* or *linear order*.

Every linear order is also a partial order, and every partial order is also a preorder, but the converses don't hold.

Example 2.17. Every linear order is also a partial order, and every partial order is also a preorder, but the converses don't hold. The universal relation on A is a preorder, since it is reflexive and transitive. But, if A has more than one element, the universal relation is not anti-symmetric, and so not a partial order.

Example 2.18. Consider the *no longer than* relation $\preccurlyeq$ on $\mathbb{B}^*$: $x \preccurlyeq y$ iff $\mathrm{len}(x) \leq \mathrm{len}(y)$. This is a preorder (reflexive and transitive), and even connected, but not a partial order, since it is not anti-symmetric. For instance, $01 \preccurlyeq 10$ and $10 \preccurlyeq 01$, but $01 \neq 10$.

Example 2.19. An important partial order is the relation $\subseteq$ on a set of sets. This is not in general a linear order, since if $a \neq b$ and we consider $\wp(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$, we see that $\{a\} \not\subseteq \{b\}$ and $\{a\} \neq \{b\}$ and $\{b\} \not\subseteq \{a\}$.

Example 2.20. The relation of *divisibility without remainder* gives us a partial order which isn't a linear order. For integers n, m, we write $n \mid m$ to mean n (evenly) divides m, i.e., iff there is some integer k so that $m = kn$. On $\mathbb{N}$, this is a partial order, but not a linear order: for instance, $2 \nmid 3$ and also $3 \nmid 2$. Considered as a relation on $\mathbb{Z}$, divisibility is only a preorder since it is not anti-symmetric: $1 \mid -1$ and $-1 \mid 1$ but $1 \neq -1$.

Definition 2.21 (Strict order). A *strict order* is a relation which is irreflexive, asymmetric, and transitive.

Definition 2.22 (Strict linear order). A strict order which is also connected is called a *strict linear order*.

Example 2.23. $\leq$ is the linear order corresponding to the strict linear order $<$. $\subseteq$ is the partial order corresponding to the strict order $\subsetneq$.

sfr:rel:ord: def:strictlinearorder **Definition 2.24 (Total order).** A strict order which is also connected is called a *total order*. This is also sometimes called a *strict linear order*.

Any strict order R on A can be turned into a partial order by adding the diagonal Id_A, i.e., adding all the pairs $\langle x, x\rangle$. (This is called the *reflexive closure* of R.) Conversely, starting from a partial order, one can get a strict order by removing Id_A. These next two results make this precise.

sfr:rel:ord: prop:stricttopartial **Proposition 2.25.** *If R is a strict order on A, then $R^+ = R \cup \mathrm{Id}_A$ is a partial order. Moreover, if R is total, then R^+ is a linear order.*

Proof. Suppose R is a strict order, i.e., $R \subseteq A^2$ and R is irreflexive, asymmetric, and transitive. Let $R^+ = R \cup \mathrm{Id}_A$. We have to show that R^+ is reflexive, antisymmetric, and transitive.

R^+ is clearly reflexive, since $\langle x, x\rangle \in \mathrm{Id}_A \subseteq R^+$ for all $x \in A$.

To show R^+ is antisymmetric, suppose for reductio that R^+xy and R^+yx but $x \neq y$. Since $\langle x, y\rangle \in R \cup \mathrm{Id}_X$, but $\langle x, y\rangle \notin \mathrm{Id}_X$, we must have $\langle x, y\rangle \in R$, i.e., Rxy. Similarly, Ryx. But this contradicts the assumption that R is asymmetric.

To establish transitivity, suppose that R^+xy and R^+yz. If both $\langle x, y\rangle \in R$ and $\langle y, z\rangle \in R$, then $\langle x, z\rangle \in R$ since R is transitive. Otherwise, either $\langle x, y\rangle \in \mathrm{Id}_X$, i.e., $x = y$, or $\langle y, z\rangle \in \mathrm{Id}_X$, i.e., $y = z$. In the first case, we have that R^+yz by assumption, $x = y$, hence R^+xz. Similarly in the second case. In either case, R^+xz, thus, R^+ is also transitive.

Concerning the "moreover" clause, suppose R is a total order, i.e., that R is connected. So for all $x \neq y$, either Rxy or Ryx, i.e., either $\langle x, y\rangle \in R$ or $\langle y, x\rangle \in R$. Since $R \subseteq R^+$, this remains true of R^+, so R^+ is connected as well. □

sfr:rel:ord: prop:partialtostrict **Proposition 2.26.** *If R is a partial order on X, then $R^- = R \setminus \mathrm{Id}_X$ is a strict order. Moreover, if R is linear, then R^- is total.*

Proof. This is left as an exercise. □

Problem 2.4. Give a proof of Proposition 2.26.

Example 2.27. $\leq$ is the linear order corresponding to the total order $<$. $\subseteq$ is the partial order corresponding to the strict order $\subsetneq$.

The following simple result which establishes that total orders satisfy an extensionality-like property:

sfr:rel:ord: prop:extensionality-totalorders **Proposition 2.28.** *If $<$ totally orders A, then:*

$$(\forall a, b \in A)((\forall x \in A)(x < a \leftrightarrow x < b) \rightarrow a = b)$$

Proof. Suppose $(\forall x \in A)(x < a \leftrightarrow x < b)$. If $a < b$, then $a < a$, contradicting the fact that $<$ is irreflexive; so $a \not< b$. Exactly similarly, $b \not< a$. So $a = b$, as $<$ is connected. □

2.6 Graphs

sfr:rel:grp:sec

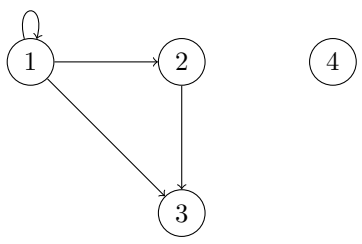
A *graph* is a diagram in which points—called "nodes" or "vertices" (plural of "vertex")—are connected by edges. Graphs are a ubiquitous tool in discrete mathematics and in computer science. They are incredibly useful for representing, and visualizing, relationships and structures, from concrete things like networks of various kinds to abstract structures such as the possible outcomes of decisions. There are many different kinds of graphs in the literature which differ, e.g., according to whether the edges are directed or not, have labels or not, whether there can be edges from a node to the same node, multiple edges between the same nodes, etc. *Directed graphs* have a special connection to relations.

Definition 2.29 (Directed graph). A *directed graph* $G = \langle V, E\rangle$ is a set of *vertices* V and a set of *edges* $E \subseteq V^2$.

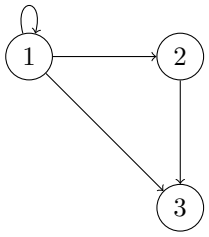
explanation

According to our definition, a graph just is a set together with a relation on that set. Of course, when talking about graphs, it's only natural to expect that they are graphically represented: we can draw a graph by connecting two vertices v_1 and v_2 by an arrow iff $\langle v_1, v_2\rangle \in E$. The only difference between a relation by itself and a graph is that a graph specifies the set of vertices, i.e., a graph may have isolated vertices. The important point, however, is that every relation R on a set X can be seen as a directed graph $\langle X, R\rangle$, and conversely, a directed graph $\langle V, E\rangle$ can be seen as a relation $E \subseteq V^2$ with the set V explicitly specified.

Example 2.30. The graph $\langle V, E\rangle$ with $V = \{1, 2, 3, 4\}$ and $E = \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 1, 3\rangle, \langle 2, 3\rangle\}$ looks like this:



This is a different graph than $\langle V', E\rangle$ with $V' = \{1, 2, 3\}$, which looks like this:



Problem 2.5. Consider the less-than-or-equal-to relation $\leq$ on the set $\{1, 2, 3, 4\}$ as a graph and draw the corresponding diagram.

2.7 Operations on Relations

sfr:rel:ops: sec

It is often useful to modify or combine relations. In Proposition 2.25, we considered the *union* of relations, which is just the union of two relations considered as sets of pairs. Similarly, in Proposition 2.26, we considered the relative difference of relations. Here are some other operations we can perform on relations.

sfr:rel:ops: relationoperations

Definition 2.31. Let R, S be relations, and A be any set.

The *inverse* of R is $R^{-1} = \{\langle y, x\rangle : \langle x, y\rangle \in R\}$.

The *relative product* of R and S is $(R \mid S) = \{\langle x, z\rangle : \exists y(Rxy \wedge Syz)\}$.

The *restriction* of R to A is $R{\restriction_A} = R \cap A^2$.

The *application* of R to A is $R[A] = \{y : (\exists x \in A)Rxy\}$

Example 2.32. Let $S \subseteq \mathbb{Z}^2$ be the successor relation on $\mathbb{Z}$, i.e., $S = \{\langle x, y\rangle \in \mathbb{Z}^2 : x + 1 = y\}$, so that Sxy iff $x + 1 = y$.

S^{-1} is the predecessor relation on $\mathbb{Z}$, i.e., $\{\langle x, y\rangle \in \mathbb{Z}^2 : x - 1 = y\}$.

$S \mid S$ is $\{\langle x, y\rangle \in \mathbb{Z}^2 : x + 2 = y\}$

$S{\restriction_{\mathbb{N}}}$ is the successor relation on $\mathbb{N}$.

$S[\{1, 2, 3\}]$ is $\{2, 3, 4\}$.

Definition 2.33 (Transitive closure). Let $R \subseteq A^2$ be a binary relation.

The *transitive closure* of R is $R^+ = \bigcup_{0<n\in\mathbb{N}} R^n$, where we recursively define $R^1 = R$ and $R^{n+1} = R^n \mid R$.

The *reflexive transitive closure* of R is $R^* = R^+ \cup \mathrm{Id}_X$.

Example 2.34. Take the successor relation $S \subseteq \mathbb{Z}^2$. S^2xy iff $x + 2 = y$, S^3xy iff $x + 3 = y$, etc. So S^+xy iff $x + n = y$ for some $n > 1$. In other words, S^+xy iff $x < y$, and S^*xy iff $x \leq y$.

Problem 2.6. Show that the transitive closure of R is in fact transitive.

Chapter 3

Functions

3.1 Basics

explanation

A *function* is a map which sends each element of a given set to a specific element in some (other) given set. For instance, the operation of adding 1 defines a function: each number n is mapped to a unique number $n + 1$.

sfr:fun:bas:sec

More generally, functions may take pairs, triples, etc., as inputs and returns some kind of output. Many functions are familiar to us from basic arithmetic. For instance, addition and multiplication are functions. They take in two numbers and return a third.

In this mathematical, abstract sense, a function is a *black box*: what matters is only what output is paired with what input, not the method for calculating the output.

Definition 3.1 (Function). A *function* $f\colon A \to B$ is a mapping of each element of A to an element of B.

We call A the *domain* of f and B the *codomain* of f. The elements of A are called inputs or *arguments* of f, and the element of B that is paired with an argument x by f is called the *value of* f for argument x, written $f(x)$.

The *range* $\operatorname{ran}(f)$ of f is the subset of the codomain consisting of the values of f for some argument; $\operatorname{ran}(f) = \{f(x) : x \in A\}$.

The diagram in Figure 3.1 may help to think about functions. The ellipse on the left represents the function's *domain*; the ellipse on the right represents the function's *codomain*; and an arrow points from an *argument* in the domain to the corresponding *value* in the codomain.

Example 3.2. Multiplication takes pairs of natural numbers as inputs and maps them to natural numbers as outputs, so goes from $\mathbb{N} \times \mathbb{N}$ (the domain) to $\mathbb{N}$ (the codomain). As it turns out, the range is also $\mathbb{N}$, since every $n \in \mathbb{N}$ is $n \times 1$.

Example 3.3. Multiplication is a function because it pairs each input—each pair of natural numbers—with a single output: $\times\colon \mathbb{N}^2 \to \mathbb{N}$. By contrast,

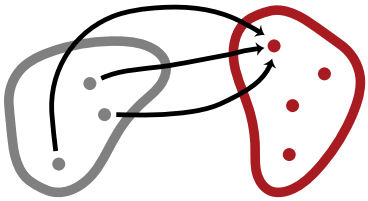


Figure 3.1: A function is a mapping of each element of one set to an element of another. An arrow points from an argument in the domain to the corresponding value in the codomain.

sfr:fun:bas: fig:function

the square root operation applied to the domain $\mathbb{N}$ is not functional, since each positive integer n has two square roots: $\sqrt{n}$ and $-\sqrt{n}$. We can make it functional by only returning the positive square root: $\sqrt{\ } : \mathbb{N} \to \mathbb{R}$.

Example 3.4. The relation that pairs each student in a class with their final grade is a function—no student can get two different final grades in the same class. The relation that pairs each student in a class with their parents is not a function: students can have zero, or two, or more parents.

We can define functions by specifying in some precise way what the value of the function is for every possible argment. Different ways of doing this are by giving a formula, describing a method for computing the value, or listing the values for each argument. However functions are defined, we must make sure that for each argment we specify one, and only one, value. explanation

Example 3.5. Let $f : \mathbb{N} \to \mathbb{N}$ be defined such that $f(x) = x + 1$. This is a definition that specifies f as a function which takes in natural numbers and outputs natural numbers. It tells us that, given a natural number x, f will output its successor $x + 1$. In this case, the codomain $\mathbb{N}$ is not the range of f, since the natural number 0 is not the successor of any natural number. The range of f is the set of all positive integers, $\mathbb{Z}^+$.

sfr:fun:bas: examplefunext

Example 3.6. Let $g : \mathbb{N} \to \mathbb{N}$ be defined such that $g(x) = x+2-1$. This tells us that g is a function which takes in natural numbers and outputs natural numbers. Given a natural number n, g will output the predecessor of the successor of the successor of x, i.e., $x + 1$.

We just considered two functions, f and g, with different *definitions*. However, these are the *same function*. After all, for any natural number n, we have that $f(n) = n + 1 = n + 2 - 1 = g(n)$. Otherwise put: our definitions for f and g specify the same mapping by means of different equations. Implicitly, then, we are relying upon a principle of extensionality for functions, explanation

$$\text{if } \forall x\, f(x) = g(x), \text{ then } f = g$$

provided that f and g share the same domain and codomain.

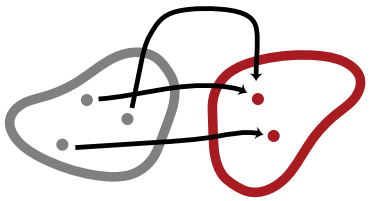


Figure 3.2: A surjective function has every element of the codomain as a value.

sfr:fun:kin:
fig:surjective

Example 3.7. We can also define functions by cases. For instance, we could define $h\colon \mathbb{N} \to \mathbb{N}$ by

$$h(x) = \begin{cases} \frac{x}{2} & \text{if } x \text{ is even} \\ \frac{x+1}{2} & \text{if } x \text{ is odd.} \end{cases}$$

Since every natural number is either even or odd, the output of this function will always be a natural number. Just remember that if you define a function by cases, every possible input must fall into exactly one case. In some cases, this will require a proof that the cases are exhaustive and exclusive.

3.2 Kinds of Functions

explanation

It will be useful to introduce a kind of taxonomy for some of the kinds of functions which we encounter most frequently.

sfr:fun:kin:
sec

To start, we might want to consider functions which have the property that every member of the codomain is a value of the function. Such functions are called surjective, and can be pictured as in Figure 3.2.

Definition 3.8 (Surjective function). A function $f\colon A \to B$ is *surjective* iff B is also the range of f, i.e., for every $y \in B$ there is at least one $x \in A$ such that $f(x) = y$, or in symbols:

$$(\forall y \in B)(\exists x \in A) f(x) = y.$$

We call such a function a surjection from A to B.

explanation

If you want to show that f is a surjection, then you need to show that every object in f's codomain is the value of $f(x)$ for some input x.

Note that any function *induces* a surjection. After all, given a function $f\colon A \to B$, let $f'\colon A \to \operatorname{ran}(f)$ be defined by $f'(x) = f(x)$. Since $\operatorname{ran}(f)$ is *defined* as $\{f(x) \in B : x \in A\}$, this function f' is guaranteed to be a surjection

explanation

Now, any function maps each possible input to a unique output. But there are also functions which never map different inputs to the same outputs. Such functions are called injective, and can be pictured as in Figure 3.3.

Definition 3.9 (Injective function). A function $f\colon A \to B$ is *injective* iff for each $y \in B$ there is at most one $x \in A$ such that $f(x) = y$. We call such a function an injection from A to B.

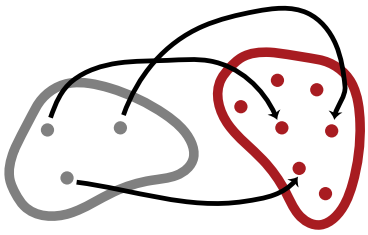


Figure 3.3: An injective function never maps two different arguments to the same value.

sfr:fun:kin:
fig:injective

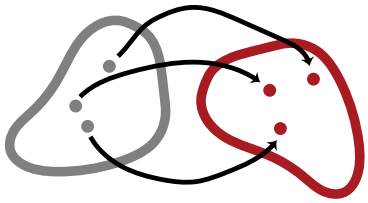


Figure 3.4: A bijective function uniquely pairs the elements of the codomain with those of the domain.

sfr:fun:kin:
fig:bijective

If you want to show that f is an injection, you need to show that for any elements x and y of f's domain, if $f(x) = f(y)$, then $x = y$. explanation

Example 3.10. The constant function $f\colon \mathbb{N} \to \mathbb{N}$ given by $f(x) = 1$ is neither injective, nor surjective.

The identity function $f\colon \mathbb{N} \to \mathbb{N}$ given by $f(x) = x$ is both injective and surjective.

The successor function $f\colon \mathbb{N} \to \mathbb{N}$ given by $f(x) = x + 1$ is injective but not surjective.

The function $f\colon \mathbb{N} \to \mathbb{N}$ defined by:

$$f(x) = \begin{cases} \frac{x}{2} & \text{if } x \text{ is even} \\ \frac{x+1}{2} & \text{if } x \text{ is odd.} \end{cases}$$

is surjective, but not injective.

Often enough, we want to consider functions which are both injective and surjective. We call such functions bijective. They look like the function pictured in Figure 3.4. Bijections are also sometimes called *one-to-one correspondences*, since they uniquely pair elements of the codomain with elements of the domain. explanation

Definition 3.11 (Bijection). A function $f\colon A \to B$ is *bijective* iff it is both surjective and injective. We call such a function a bijection from A to B (or between A and B).

3.3 Functions as Relations

explanation

A function which maps elements of A to elements of B obviously defines a relation between A and B, namely the relation which holds between x and y iff $f(x) = y$. In fact, we might even—if we are interested in reducing the building blocks of mathematics for instance—*identify* the function f with this relation, i.e., with a set of pairs. This then raises the question: which relations define functions in this way?

sfr:fun:rel: sec

Definition 3.12 (Graph of a function). Let $f\colon A \to B$ be a function. The *graph* of f is the relation $R_f \subseteq A \times B$ defined by

$$R_f = \{\langle x, y\rangle : f(x) = y\}.$$

explanation

The graph of a function is uniquely determined, by extensionality. Moreover, extensionality (on sets) will immediate vindicate the implicit principle of extensionality for functions, whereby if f and g share a domain and codomain then they are identical if they agree on all values.

Similarly, if a relation is "functional", then it is the graph of a function.

sfr:fun:rel: prop:graph-function

Proposition 3.13. *Let $R \subseteq A \times B$ be such that:*

1. *If Rxy and Rxz then $y = z$; and*
2. *for every $x \in A$ there is some $y \in B$ such that $\langle x, y\rangle \in R$.*

Then R is the graph of the function $f\colon A \to B$ defined by $f(x) = y$ iff Rxy.

Proof. Suppose there is a y such that Rxy. If there were another $z \neq y$ such that Rxz, the condition on R would be violated. Hence, if there is a y such that Rxy, this y is unique, and so f is well-defined. Obviously, $R_f = R$. □

explanation

Every function $f\colon A \to B$ has a graph, i.e., a relation on $A \times B$ defined by $f(x) = y$. On the other hand, every relation $R \subseteq A \times B$ with the properties given in Proposition 3.13 is the graph of a function $f\colon A \to B$. Because of this close connection between functions and their graphs, we can think of a function simply as its graph. In other words, functions can be identified with certain relations, i.e., with certain sets of tuples. Note, though, that the spirit of this "identification" is as in section 2.2: it is not a claim about the metaphysics of functions, but an observation that it is convenient to *treat* functions as certain sets. One reason that this is so convenient, is that we can now consider performing similar operations on functions as we performed on relations (see section 2.7). In particular:

sfr:fun:rel: defn:funimage

Definition 3.14. Let $f\colon A \to B$ be a function with $C \subseteq A$.

The *restriction* of f to C is the function $f{\restriction_C}\colon C \to B$ defined by $(f{\restriction_C})(x) = f(x)$ for all $x \in C$. In other words, $f{\restriction_C} = \{\langle x, y\rangle \in R_f : x \in C\}$.

The *application* of f to C is $f[C] = \{f(x) : x \in C\}$. We also call this the *image* of C under f.

It follows from these definition that $\operatorname{ran}(f) = f[\operatorname{dom}(f)]$, for any function f. These notions are exactly as one would expect, given the definitions in section 2.7 and our identification of functions with relations. But two other operations—inverses and relative products—require a little more detail. We will provide that in the section 3.4 and section 3.5. explanation

3.4 Inverses of Functions

sfr:fun:inv:sec

We think of functions as maps. An obvious question to ask about functions, then, is whether the mapping can be "reversed." For instance, the successor function $f(x) = x+1$ can be reversed, in the sense that the function $g(y) = y-1$ "undoes" what f does. explanation

But we must be careful. Although the definition of g defines a function $\mathbb{Z} \to \mathbb{Z}$, it does not define a *function* $\mathbb{N} \to \mathbb{N}$, since $g(0) \notin \mathbb{N}$. So even in simple cases, it is not quite obvious whether a function can be reversed; it may depend on the domain and codomain.

This is made more precise by the notion of an inverse of a function.

Definition 3.15. A function $g\colon B \to A$ is an *inverse* of a function $f\colon A \to B$ if $f(g(y)) = y$ and $g(f(x)) = x$ for all $x \in A$ and $y \in B$.

If f has an inverse g, we often write f^{-1} instead of g.

Now we will determine when functions have inverses. A good candidate for an inverse of $f\colon A \to B$ is $g\colon B \to A$ "defined by" explanation

$$g(y) = \text{"the" } x \text{ such that } f(x) = y.$$

But the scare quotes around "defined by" (and "the") suggest that this is not a definition. At least, it will not always work, with complete generality. For, in order for this definition to specify a function, there has to be one and only one x such that $f(x) = y$—the output of g has to be uniquely specified. Moreover, it has to be specified for every $y \in B$. If there are x_1 and $x_2 \in A$ with $x_1 \neq x_2$ but $f(x_1) = f(x_2)$, then $g(y)$ would not be uniquely specified for $y = f(x_1) = f(x_2)$. And if there is no x at all such that $f(x) = y$, then $g(y)$ is not specified at all. In other words, for g to be defined, f must be both injective and surjective.

sfr:fun:inv:prop:bijection-inverse

Proposition 3.16. *Every bijection has a unique inverse.*

Proof. Exercise. □

Problem 3.1. Prove Proposition 3.16. That is, show that if $f\colon A \to B$ is bijective, an inverse g of f exists. You have to define such a g, show that it is a function, and show that it is an inverse of f, i.e., $f(g(y)) = y$ and $g(f(x)) = x$ for all $x \in A$ and $y \in B$.

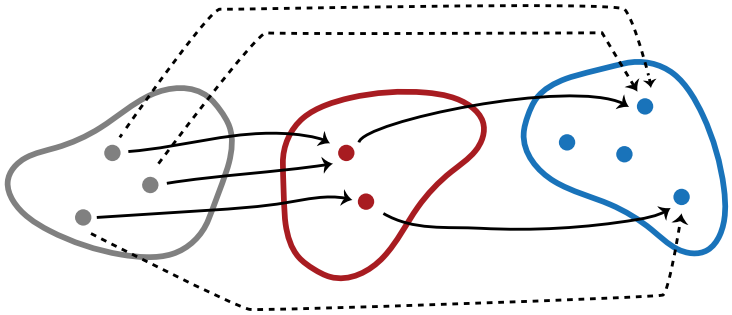


Figure 3.5: The composition $g \circ f$ of two functions f and g.

sfr:fun:cmp:
fig:composition

explanation

However, there is a slightly more general way to extract inverses. We saw in section 3.2 that every function f induces a surjection $f' \colon A \to \operatorname{ran}(f)$ by letting $f'(x) = f(x)$ for all $x \in A$. Clearly, if f is an injection, then f' is a bijection, so that it has a unique inverse by Proposition 3.16. By a very minor abuse of notation, we sometimes call the inverse of f' simply "the inverse of f."

Problem 3.2. Show that if $f \colon A \to B$ has an inverse g, then f is bijective.

Proposition 3.17. *Every function f has at most one inverse.*

sfr:fun:inv:
prop:inverse-unique

Proof. Exercise. □

Problem 3.3. Prove Proposition 3.17. That is, show that if $g \colon B \to A$ and $g' \colon B \to A$ are inverses of $f \colon A \to B$, then $g = g'$, i.e., for all $y \in B$, $g(y) = g'(y)$.

3.5 Composition of Functions

explanation

We saw in section 3.4 that the inverse f^{-1} of a bijection f is itself a function. Another operation on functions is composition: we can define a new function by composing two functions, f and g, i.e., by first applying f and then g. Of course, this is only possible if the ranges and domains match, i.e., the range of f must be a subset of the domain of g. This operation on functions is the analogue of the operation of relative product on relations from section 2.7.

sfr:fun:cmp:
sec

A diagram might help to explain the idea of composition. In Figure 3.5, we depict two functions $f \colon A \to B$ and $g \colon B \to C$ and their composition $(g \circ f)$. The function $(g \circ f) \colon A \to C$ pairs each element of A with an element of C. We specify which element of C an element of A is paired with as follows: given an input $x \in A$, first apply the function f to x, which will output some $f(x) = y \in B$, then apply the function g to y, which will output some $g(f(x)) = g(y) = z \in C$.

Definition 3.18 (Composition). Let $f \colon A \to B$ and $g \colon B \to C$ be functions. The *composition* of f with g is $g \circ f \colon A \to C$, where $(g \circ f)(x) = g(f(x))$.

Example 3.19. Consider the functions $f(x) = x + 1$, and $g(x) = 2x$. Since $(g \circ f)(x) = g(f(x))$, for each input x you must first take its successor, then multiply the result by two. So their composition is given by $(g \circ f)(x) = 2(x+1)$.

Problem 3.4. Show that if $f\colon A \to B$ and $g\colon B \to C$ are both injective, then $g \circ f\colon A \to C$ is injective.

Problem 3.5. Show that if $f\colon A \to B$ and $g\colon B \to C$ are both surjective, then $g \circ f\colon A \to C$ is surjective.

Problem 3.6. Suppose $f\colon A \to B$ and $g\colon B \to C$. Show that the graph of $g \circ f$ is $R_f \mid R_g$.

3.6 Partial Functions

sfr:fun:par:sec

It is sometimes useful to relax the definition of function so that it is not required that the output of the function is defined for all possible inputs. Such mappings are called *partial functions*. explanation

Definition 3.20. A *partial function* $f\colon A \nrightarrow B$ is a mapping which assigns to every element of A at most one element of B. If f assigns an element of B to $x \in A$, we say $f(x)$ is *defined*, and otherwise *undefined*. If $f(x)$ is defined, we write $f(x)\downarrow$, otherwise $f(x)\uparrow$. The *domain* of a partial function f is the subset of A where it is defined, i.e., $\mathrm{dom}(f) = \{x \in A : f(x)\downarrow\}$.

Example 3.21. Every function $f\colon A \to B$ is also a partial function. Partial functions that are defined everywhere on A—i.e., what we so far have simply called a function—are also called *total* functions.

Example 3.22. The partial function $f\colon \mathbb{R} \nrightarrow \mathbb{R}$ given by $f(x) = 1/x$ is undefined for $x = 0$, and defined everywhere else.

Problem 3.7. Given $f\colon A \nrightarrow B$, define the partial function $g\colon B \nrightarrow A$ by: for any $y \in B$, if there is a unique $x \in A$ such that $f(x) = y$, then $g(y) = x$; otherwise $g(y)\uparrow$. Show that if f is injective, then $g(f(x)) = x$ for all $x \in \mathrm{dom}(f)$, and $f(g(y)) = y$ for all $y \in \mathrm{ran}(f)$.

Definition 3.23 (Graph of a partial function). Let $f\colon A \nrightarrow B$ be a partial function. The *graph* of f is the relation $R_f \subseteq A \times B$ defined by

$$R_f = \{\langle x, y\rangle : f(x) = y\}.$$

Proposition 3.24. *Suppose $R \subseteq A \times B$ has the property that whenever Rxy and Rxy' then $y = y'$. Then R is the graph of the partial function $f\colon X \nrightarrow Y$ defined by: if there is a y such that Rxy, then $f(x) = y$, otherwise $f(x)\uparrow$. If R is also* serial*, i.e., for each $x \in X$ there is a $y \in Y$ such that Rxy, then f is total.*

Proof. Suppose there is a y such that Rxy. If there were another $y' \neq y$ such that Rxy', the condition on R would be violated. Hence, if there is a y such that Rxy, that y is unique, and so f is well-defined. Obviously, $R_f = R$ and f is total if R is serial. □

Chapter 4

The Size of Sets

This chapter discusses enumerations, countability and uncountability. Several sections come in two versions: a more elementary one, that takes enumerations to be lists, or surjections from $\mathbb{Z}^+$; and a more abstract one that defines enumerations as bijections with $\mathbb{N}$.

4.1 Introduction

sfr:siz:int:sec

When Georg Cantor developed set theory in the 1870s, one of his aims was to make palatable the idea of an infinite collection—an actual infinity, as the medievals would say. A key part of this was his treatment of the *size* of different sets. If a, b and c are all distinct, then the set $\{a, b, c\}$ is intuitively *larger* than $\{a, b\}$. But what about infinite sets? Are they all as large as each other? It turns out that they are not.

The first important idea here is that of an enumeration. We can list every finite set by listing all its elements. For some infinite sets, we can also list all their elements if we allow the list itself to be infinite. Such sets are called enumerable. Cantor's surprising result, which we will fully understand by the end of this chapter, was that some infinite sets are not enumerable.

4.2 Enumerations and Enumerable Sets

sfr:siz:enm:sec

This section discusses enumerations of sets, defining them as surjections from $\mathbb{Z}^+$. It does things slowly, for readers with little mathematical background. An alternative, terser version is given in section 4.11, which defines enumerations differently: as bijections with $\mathbb{N}$ (or an initial segment).

explanation We've already given examples of sets by listing their elements. Let's discuss in more general terms how and when we can list the elements of a set, even if that set is infinite.

Definition 4.1 (Enumeration, informally). Informally, an *enumeration* of a set A is a list (possibly infinite) of elements of A such that every element of A appears on the list at some finite position. If A has an enumeration, then A is said to be *enumerable*.

explanation A couple of points about enumerations:

1. We count as enumerations only lists which have a beginning and in which every element other than the first has a single element immediately preceding it. In other words, there are only finitely many elements between the first element of the list and any other element. In particular, this means that every element of an enumeration has a finite position: the first element has position 1, the second position 2, etc.

2. We can have different enumerations of the same set A which differ by the order in which the elements appear: 4, 1, 25, 16, 9 enumerates the (set of the) first five square numbers just as well as 1, 4, 9, 16, 25 does.

3. Redundant enumerations are still enumerations: 1, 1, 2, 2, 3, 3, ... enumerates the same set as 1, 2, 3, ... does.

4. Order and redundancy *do* matter when we specify an enumeration: we can enumerate the positive integers beginning with 1, 2, 3, 1, ..., but the pattern is easier to see when enumerated in the standard way as 1, 2, 3, 4, ...

5. Enumerations must have a beginning: ..., 3, 2, 1 is not an enumeration of the positive integers because it has no first element. To see how this follows from the informal definition, ask yourself, "at what position in the list does the number 76 appear?"

6. The following is not an enumeration of the positive integers: 1, 3, 5, ..., 2, 4, 6, ... The problem is that the even numbers occur at places $\infty + 1$, $\infty + 2$, $\infty + 3$, rather than at finite positions.

7. The empty set is enumerable: it is enumerated by the empty list!

Proposition 4.2. *If A has an enumeration, it has an enumeration without repetitions.*

Proof. Suppose A has an enumeration $x_1, x_2, \ldots$ in which each x_i is an element of A. We can remove repetitions from an enumeration by removing repeated elements. For instance, we can turn the enumeration into a new one in which we list x_i if it is an element of A that is not among $x_1, \ldots, x_{i-1}$ or remove x_i from the list if it already appears among $x_1, \ldots, x_{i-1}$. □

The last argument shows that in order to get a good handle on enumerations and enumerable sets and to prove things about them, we need a more precise definition. The following provides it.

Definition 4.3 (Enumeration, formally). An *enumeration* of a set $A \neq \emptyset$ is any surjective function $f\colon \mathbb{Z}^+ \to A$.

explanation

Let's convince ourselves that the formal definition and the informal definition using a possibly infinite list are equivalent. First, any surjective function from $\mathbb{Z}^+$ to a set A enumerates A. Such a function determines an enumeration as defined informally above: the list $f(1)$, $f(2)$, $f(3)$, ... Since f is surjective, every element of A is guaranteed to be the value of $f(n)$ for some $n \in \mathbb{Z}^+$. Hence, every element of A appears at some finite position in the list. Since the function may not be injective, the list may be redundant, but that is acceptable (as noted above).

On the other hand, given a list that enumerates all elements of A, we can define a surjective function $f\colon \mathbb{Z}^+ \to A$ by letting $f(n)$ be the nth element of the list, or the final element of the list if there is no nth element. The only case where this does not produce a surjective function is when A is empty, and hence the list is empty. So, every non-empty list determines a surjective function $f\colon \mathbb{Z}^+ \to A$.

sfr:siz:enm: defn:enumerable

Definition 4.4. A set A is enumerable iff it is empty or has an enumeration.

Example 4.5. A function enumerating the positive integers ($\mathbb{Z}^+$) is simply the identity function given by $f(n) = n$. A function enumerating the natural numbers $\mathbb{N}$ is the function $g(n) = n - 1$.

Example 4.6. The functions $f\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ and $g\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ given by

$$f(n) = 2n \text{ and}$$
$$g(n) = 2n + 1$$

enumerate the even positive integers and the odd positive integers, respectively. However, neither function is an enumeration of $\mathbb{Z}^+$, since neither is surjective.

Problem 4.1. Define an enumeration of the positive squares 1, 4, 9, 16, ...

Example 4.7. The function $f(n) = (-1)^n \lceil \frac{(n-1)}{2} \rceil$ (where $\lceil x \rceil$ denotes the *ceiling* function, which rounds x up to the nearest integer) enumerates the set of integers $\mathbb{Z}$. Notice how f generates the values of $\mathbb{Z}$ by "hopping" back and forth between positive and negative integers:

$f(1)$	$f(2)$	$f(3)$	$f(4)$	$f(5)$	$f(6)$	$f(7)$	...
$-\lceil \frac{0}{2} \rceil$	$\lceil \frac{1}{2} \rceil$	$-\lceil \frac{2}{2} \rceil$	$\lceil \frac{3}{2} \rceil$	$-\lceil \frac{4}{2} \rceil$	$\lceil \frac{5}{2} \rceil$	$-\lceil \frac{6}{2} \rceil$	...
0	1	-1	2	-2	3	...	

You can also think of f as defined by cases as follows:

$$f(n) = \begin{cases} 0 & \text{if } n = 1 \\ n/2 & \text{if } n \text{ is even} \\ -(n-1)/2 & \text{if } n \text{ is odd and } > 1 \end{cases}$$

Problem 4.2. Show that if A and B are enumerable, so is $A \cup B$. To do this, suppose there are surjective functions $f\colon \mathbb{Z}^+ \to A$ and $g\colon \mathbb{Z}^+ \to B$, and define a surjective function $h\colon \mathbb{Z}^+ \to A \cup B$ and prove that it is surjective. Also consider the cases where A or $B = \emptyset$.

Problem 4.3. Show that if $B \subseteq A$ and A is enumerable, so is B. To do this, suppose there is a surjective function $f\colon \mathbb{Z}^+ \to A$. Define a surjective function $g\colon \mathbb{Z}^+ \to B$ and prove that it is surjective. What happens if $B = \emptyset$?

Problem 4.4. Show by induction on n that if A_1, A_2, …, A_n are all enumerable, so is $A_1 \cup \cdots \cup A_n$. You may assume the fact that if two sets A and B are enumerable, so is $A \cup B$.

Although it is perhaps more natural when listing the elements of a set to start counting from the 1st element, mathematicians like to use the natural numbers $\mathbb{N}$ for counting things. They talk about the 0th, 1st, 2nd, and so on, elements of a list. Correspondingly, we can define an enumeration as a surjective function from $\mathbb{N}$ to A. Of course, the two definitions are equivalent.

Proposition 4.8. *There is a surjection $f\colon \mathbb{Z}^+ \to A$ iff there is a surjection $g\colon \mathbb{N} \to A$.* *sfr:siz:enm: prop:enum-shift*

Proof. Given a surjection $f\colon \mathbb{Z}^+ \to A$, we can define $g(n) = f(n+1)$ for all $n \in \mathbb{N}$. It is easy to see that $g\colon \mathbb{N} \to A$ is surjective. Conversely, given a surjection $g\colon \mathbb{N} \to A$, define $f(n) = g(n+1)$. □

This gives us the following result:

Corollary 4.9. *A set A is enumerable iff it is empty or there is a surjective function $f\colon \mathbb{N} \to A$.* *sfr:siz:enm: cor:enum-nat*

We discussed above than an list of elements of a set A can be turned into a list without repetitions. This is also true for enumerations, but a bit harder to formulate and prove rigorously. Any function $f\colon \mathbb{Z}^+ \to A$ must be defined for all $n \in \mathbb{Z}^+$. If there are only finitely many elements in A then we clearly cannot have a function defined on the infinitely many elements of $\mathbb{Z}^+$ that takes as values all the elements of A but never takes the same value twice. In that case, i.e., in the case where the list without repetitions is finite, we must choose a different domain for f, one with only finitely many elements. Not having repetitions means that f must be injective. Since it is also surjective, we are looking for a bijection between some finite set $\{1, \ldots, n\}$ or $\mathbb{Z}^+$ and A.

sfr:siz:enm: prop:enum-bij **Proposition 4.10.** *If $f\colon \mathbb{Z}^+ \to A$ is surjective (i.e., an enumeration of A), there is a bijection $g\colon Z \to A$ where Z is either $\mathbb{Z}^+$ or $\{1,\ldots,n\}$ for some $n \in \mathbb{Z}^+$.*

Proof. We define the function g recursively: Let $g(1) = f(1)$. If $g(i)$ has already been defined, let $g(i+1)$ be the first value of $f(1), f(2), \ldots$ not already among $g(1), \ldots, g(i)$, if there is one. If A has just n elements, then $g(1), \ldots, g(n)$ are all defined, and so we have defined a function $g\colon \{1,\ldots,n\} \to A$. If A has infinitely many elements, then for any i there must be an element of A in the enumeration $f(1), f(2), \ldots$, which is not already among $g(1), \ldots, g(i)$. In this case we have defined a funtion $g\colon \mathbb{Z}^+ \to A$.

The function g is surjective, since any element of A is among $f(1), f(2), \ldots$ (since f is surjective) and so will eventually be a value of $g(i)$ for some i. It is also injective, since if there were $j < i$ such that $g(j) = g(i)$, then $g(i)$ would already be among $g(1), \ldots, g(i-1)$, contrary to how we defined g. □

sfr:siz:enm: cor:enum-nat-bij **Corollary 4.11.** *A set A is enumerable iff it is empty or there is a bijection $f\colon N \to A$ where either $N = \mathbb{N}$ or $N = \{0,\ldots,n\}$ for some $n \in \mathbb{N}$.*

Proof. A is enumerable iff A is empty or there is a surjective $f\colon \mathbb{Z}^+ \to A$. By Proposition 4.10, the latter holds iff there is a bijective function $f\colon Z \to A$ where $Z = \mathbb{Z}^+$ or $Z = \{1,\ldots,n\}$ for some $n \in \mathbb{Z}^+$. By the same argument as in the proof of Proposition 4.8, that in turn is the case iff there is a bijection $g\colon N \to A$ where either $N = \mathbb{N}$ or $N = \{0,\ldots,n-1\}$. □

Problem 4.5. According to Definition 4.4, a set A is enumerable iff $A = \emptyset$ or there is a surjective $f\colon \mathbb{Z}^+ \to A$. It is also possible to define "enumerable set" precisely by: a set is enumerable iff there is an injective function $g\colon A \to \mathbb{Z}^+$. Show that the definitions are equivalent, i.e., show that there is an injective function $g\colon A \to \mathbb{Z}^+$ iff either $A = \emptyset$ or there is a surjective $f\colon \mathbb{Z}^+ \to A$.

4.3 Cantor's Zig-Zag Method

sfr:siz:zigzag: sec We've already considered some "easy" enumerations. Now we will consider something a bit harder. Consider the set of pairs of natural numbers, which we defined in section 1.5 thus: explanation

$$\mathbb{N} \times \mathbb{N} = \{\langle n, m\rangle : n, m \in \mathbb{N}\}$$

We can organize these ordered pairs into an *array*, like so:

	0	**1**	**2**	**3**	...
0	$\langle 0,0\rangle$	$\langle 0,1\rangle$	$\langle 0,2\rangle$	$\langle 0,3\rangle$	...
1	$\langle 1,0\rangle$	$\langle 1,1\rangle$	$\langle 1,2\rangle$	$\langle 1,3\rangle$	...
2	$\langle 2,0\rangle$	$\langle 2,1\rangle$	$\langle 2,2\rangle$	$\langle 2,3\rangle$	...
3	$\langle 3,0\rangle$	$\langle 3,1\rangle$	$\langle 3,2\rangle$	$\langle 3,3\rangle$	...
⋮	⋮	⋮	⋮	⋮	⋱

Clearly, every ordered pair in $\mathbb{N} \times \mathbb{N}$ will appear exactly once in the array. In particular, $\langle n, m \rangle$ will appear in the nth row and mth column. But how do we organize the elements of such an array into a "one-dimensional" list? The pattern in the array below demonstrates one way to do this (although of course there are many other options):

	0	**1**	**2**	**3**	**4**	...
0	0	1	3	6	10	...
1	2	4	7	11	...	...
2	5	8	12	...	...	...
3	9	13	...	...	...	...
4	14	...	...	...	...	...
⋮	⋮	⋮	⋮	⋮	...	⋱

This pattern is called *Cantor's zig-zag method*. It enumerates $\mathbb{N} \times \mathbb{N}$ as follows:

$$\langle 0,0\rangle, \langle 0,1\rangle, \langle 1,0\rangle, \langle 0,2\rangle, \langle 1,1\rangle, \langle 2,0\rangle, \langle 0,3\rangle, \langle 1,2\rangle, \langle 2,1\rangle, \langle 3,0\rangle, \ldots$$

And this establishes the following:

Proposition 4.12. *$\mathbb{N} \times \mathbb{N}$ is enumerable.*

sfr:siz:zigzag: natsquaredenumerable

Proof. Let $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ take each $k \in \mathbb{N}$ to the tuple $\langle n, m \rangle \in \mathbb{N} \times \mathbb{N}$ such that k is the value of the nth row and mth column in Cantor's zig-zag array. □

explanation

This technique also generalises rather nicely. For example, we can use it to enumerate the set of ordered triples of natural numbers, i.e.:

$$\mathbb{N} \times \mathbb{N} \times \mathbb{N} = \{\langle n, m, k\rangle : n, m, k \in \mathbb{N}\}$$

We think of $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ as the Cartesian product of $\mathbb{N} \times \mathbb{N}$ with $\mathbb{N}$, that is,

$$\mathbb{N}^3 = (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} = \{\langle \langle n, m\rangle, k\rangle : n, m, k \in \mathbb{N}\}$$

and thus we can enumerate $\mathbb{N}^3$ with an array by labelling one axis with the enumeration of $\mathbb{N}$, and the other axis with the enumeration of $\mathbb{N}^2$:

	0	**1**	**2**	**3**	...
$\langle \mathbf{0}, \mathbf{0}\rangle$	$\langle 0,0,0\rangle$	$\langle 0,0,1\rangle$	$\langle 0,0,2\rangle$	$\langle 0,0,3\rangle$	...
$\langle \mathbf{0}, \mathbf{1}\rangle$	$\langle 0,1,0\rangle$	$\langle 0,1,1\rangle$	$\langle 0,1,2\rangle$	$\langle 0,1,3\rangle$	...
$\langle \mathbf{1}, \mathbf{0}\rangle$	$\langle 1,0,0\rangle$	$\langle 1,0,1\rangle$	$\langle 1,0,2\rangle$	$\langle 1,0,3\rangle$	...
$\langle \mathbf{0}, \mathbf{2}\rangle$	$\langle 0,2,0\rangle$	$\langle 0,2,1\rangle$	$\langle 0,2,2\rangle$	$\langle 0,2,3\rangle$	...
⋮	⋮	⋮	⋮	⋮	⋱

Thus, by using a method like Cantor's zig-zag method, we may similarly obtain an enumeration of $\mathbb{N}^3$. And we can keep going, obtaining enumerations of $\mathbb{N}^n$ for any natural number n. So, we have:

Proposition 4.13. *$\mathbb{N}^n$ is enumerable, for every $n \in \mathbb{N}$.*

4.4 Pairing Functions and Codes

sfr:siz:pai:sec

Cantor's zig-zag method makes the enumerability of $\mathbb{N}^n$ visually evident. But let us focus on our array depicting $\mathbb{N}^2$. Following the zig-zag line in the array and counting the places, we can check that $\langle 1, 2\rangle$ is associated with the number 7. However, it would be nice if we could compute this more directly. That is, it would be nice to have to hand the *inverse* of the zig-zag enumeration, $g\colon \mathbb{N}^2 \to \mathbb{N}$, such that

explanation

$$g(\langle 0, 0\rangle) = 0,\ g(\langle 0, 1\rangle) = 1,\ g(\langle 1, 0\rangle) = 2,\ \ldots, g(\langle 1, 2\rangle) = 7,\ \ldots$$

This would enable to calculate exactly where $\langle n, m\rangle$ will occur in our enumeration.

In fact, we can define g directly by making two observations. First: if the nth row and mth column contains value v, then the $(n+1)$st row and $(m-1)$st column contains value $v+1$. Second: the first row of our enumeration consists of the triangular numbers, starting with 0, 1, 3, 5, etc. The kth triangular number is the sum of the natural numbers $< k$, which can be computed as $k(k+1)/2$. Putting these two observations together, consider this function:

$$g(n, m) = \frac{(n + m + 1)(n + m)}{2} + n$$

We often just write $g(n, m)$ rather that $g(\langle n, m\rangle)$, since it is easier on the eyes. This tells you first to determine the $(n+m)^{\text{th}}$ triangle number, and then subtract n from it. And it populates the array in exactly the way we would like. So in particular, the pair $\langle 1, 2\rangle$ is sent to $\frac{4\times 3}{2} + 1 = 7$.

This function g is the *inverse* of an enumeration of a set of pairs. Such functions are called *pairing functions*.

Definition 4.14 (Pairing function). A function $f\colon A \times B \to \mathbb{N}$ is an arithmetical *pairing function* if f is injective. We also say that f *encodes* $A \times B$, and that $f(x, y)$ is the *code* for $\langle x, y\rangle$.

We can use pairing functions encode, e.g., pairs of natural numbers; or, in other words, we can represent each *pair* of elements using a *single* number. Using the inverse of the pairing function, we can *decode* the number, i.e., find out which pair it represents.

explanation

Problem 4.6. Give an enumeration of the set of all non-negative rational numbers.

Problem 4.7. Show that $\mathbb{Q}$ is enumerable. Recall that any rational number can be written as a fraction z/m with $z \in \mathbb{Z}$, $m \in \mathbb{N}^+$.

Problem 4.8. Define an enumeration of $\mathbb{B}^*$.

Problem 4.9. Recall from your introductory logic course that each possible truth table expresses a truth function. In other words, the truth functions are all functions from $\mathbb{B}^k \to \mathbb{B}$ for some k. Prove that the set of all truth functions is enumerable.

Problem 4.10. Show that the set of all finite subsets of an arbitrary infinite enumerable set is enumerable.

Problem 4.11. A subset of $\mathbb{N}$ is said to be *cofinite* iff it is the complement of a finite set $\mathbb{N}$; that is, $A \subseteq \mathbb{N}$ is cofinite iff $\mathbb{N} \setminus A$ is finite. Let I be the set whose elements are exactly the finite and cofinite subsets of $\mathbb{N}$. Show that I is enumerable.

Problem 4.12. Show that the enumerable union of enumerable sets is enumerable. That is, whenever A_1, A_2, ... are sets, and each A_i is enumerable, then the union $\bigcup_{i=1}^{\infty} A_i$ of all of them is also enumerable. [NB: this is hard!]

Problem 4.13. Let $f\colon A \times B \to \mathbb{N}$ be an arbitrary pairing function. Show that the inverse of f is an enumeration of $A \times B$.

Problem 4.14. Specify a function that encodes $\mathbb{N}^3$.

4.5 An Alternative Pairing Function

explanation

There are other enumerations of $\mathbb{N}^2$ that make it easier to figure out what their inverses are. Here is one. Instead of visualizing the enumeration in an array, start with the list of positive integers associated with (initially) empty spaces. Imagine filling these spaces successively with pairs $\langle n, m\rangle$ as follow. Starting with the pairs that have 0 in the first place (i.e., pairs $\langle 0, m\rangle$), put the first (i.e., $\langle 0, 0\rangle$) in the first empty place, then skip an empty space, put the second (i.e., $\langle 0, 2\rangle$) in the next empty place, skip one again, and so forth. The (incomplete) beginning of our enumeration now looks like this

sfr:siz:pai-alt:sec

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	...
$\langle 0, 1\rangle$		$\langle 0, 2\rangle$		$\langle 0, 3\rangle$		$\langle 0, 4\rangle$		$\langle 0, 5\rangle$		...

Repeat this with pairs $\langle 1, m\rangle$ for the place that still remain empty, again skipping every other empty place:

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	...
$\langle 0, 0\rangle$	$\langle 1, 0\rangle$	$\langle 0, 1\rangle$		$\langle 0, 2\rangle$	$\langle 1, 1\rangle$	$\langle 0, 3\rangle$		$\langle 0, 4\rangle$	$\langle 1, 2\rangle$	...

Enter pairs $\langle 2, m\rangle$, $\langle 2, m\rangle$, etc., in the same way. Our completed enumeration thus starts like this:

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	...
$\langle 0, 0\rangle$	$\langle 1, 0\rangle$	$\langle 0, 1\rangle$	$\langle 2, 0\rangle$	$\langle 0, 2\rangle$	$\langle 1, 1\rangle$	$\langle 0, 3\rangle$	$\langle 3, 0\rangle$	$\langle 0, 4\rangle$	$\langle 1, 2\rangle$	...

If we number the cells in the array above according to this enumeration, we will not find a neat zig-zag line, but this arrangement:

	0	**1**	**2**	**3**	**4**	**5**	...
0	1	3	5	7	9	11	...
1	2	6	10	14	18	...	...
2	4	12	20	28	...	...	...
3	8	24	40	...	...	...	...
4	16	48	...	...	...	...	...
5	32	...	...	...	...	...	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

We can see that the pairs in row 0 are in the odd numbered places of our enumeration, i.e., pair $\langle 0, m\rangle$ is in place $2m + 1$; pairs in the second row, $\langle 1, m\rangle$, are in places whose number is the double of an odd number, specifically, $2 \cdot (2m + 1)$; pairs in the third row, $\langle 2, m\rangle$, are in places whose number is four times an odd number, $4 \cdot (2m + 1)$; and so on. The factors of $(2m + 1)$ for each row, 1, 2, 4, 8, ..., are exactly the powers of 2: $1 = 2^0$, $2 = 2^1$, $4 = 2^2$, $8 = 2^3$, ... In fact, the relevant exponent is always the first member of the pair in question. Thus, for pair $\langle n, m\rangle$ the factor is 2^n. This gives us the general formula: $2^n \cdot (2m+1)$. However, this is a mapping of pairs to *positive* integers, i.e., $\langle 0, 0\rangle$ has position 1. If we want to begin at position 0 we must subtract 1 from the result. This gives us:

Example 4.15. The function $h\colon \mathbb{N}^2 \to \mathbb{N}$ given by

$$h(n, m) = 2^n(2m + 1) - 1$$

is a pairing function for the set of pairs of natural numbers $\mathbb{N}^2$.

Accordingly, in our second enumeration of $\mathbb{N}^2$, the pair $\langle 0, 0\rangle$ has code $h(0, 0) = 2^0(2 \cdot 0 + 1) - 1 = 0$; $\langle 1, 2\rangle$ has code $2^1 \cdot (2 \cdot 2 + 1) - 1 = 2 \cdot 5 - 1 = 9$; $\langle 2, 6\rangle$ has code $2^2 \cdot (2 \cdot 6 + 1) - 1 = 51$. explanation

Sometimes it is enough to encode pairs of natural numbers $\mathbb{N}^2$ without requiring that the encoding is surjective. Such encodings have inverses that are only partial functions.

Example 4.16. The function $j\colon \mathbb{N}^2 \to \mathbb{N}^+$ given by

$$j(n, m) = 2^n 3^m$$

is an injective function $\mathbb{N}^2 \to \mathbb{N}$.

4.6 Non-enumerable Sets

sfr:siz:nen:sec

This section proves the non-enumerability of $\mathbb{B}^\omega$ and $\wp(\mathbb{Z}^+)$ using the definition in section 4.2. It is designed to be a little more elementary and a little more detailed than the version in section 4.11

Some sets, such as the set $\mathbb{Z}^+$ of positive integers, are infinite. So far we've seen examples of infinite sets which were all enumerable. However, there are also infinite sets which do not have this property. Such sets are called *non-enumerable*.

First of all, it is perhaps already surprising that there are non-enumerable sets. For any enumerable set A there is a surjective function $f\colon \mathbb{Z}^+ \to A$. If a set is non-enumerable there is no such function. That is, no function mapping the infinitely many elements of $\mathbb{Z}^+$ to A can exhaust all of A. So there are "more" elements of A than the infinitely many positive integers.

How would one prove that a set is non-enumerable? You have to show that no such surjective function can exist. Equivalently, you have to show that the elements of A cannot be enumerated in a one way infinite list. The best way to do this is to show that every list of elements of A must leave at least one element out; or that no function $f\colon \mathbb{Z}^+ \to A$ can be surjective. We can do this using Cantor's *diagonal method*. Given a list of elements of A, say, x_1, x_2, ..., we construct another element of A which, by its construction, cannot possibly be on that list.

Our first example is the set $\mathbb{B}^\omega$ of all infinite, non-gappy sequences of 0's and 1's.

Theorem 4.17. *$\mathbb{B}^\omega$ is non-enumerable.*

sfr:siz:nen: thm:nonenum-bin-omega

Proof. Suppose, by way of contradiction, that $\mathbb{B}^\omega$ is enumerable, i.e., suppose that there is a list s_1, s_2, s_3, s_4, ... of all elements of $\mathbb{B}^\omega$. Each of these s_i is itself an infinite sequence of 0's and 1's. Let's call the j-th element of the i-th sequence in this list $s_i(j)$. Then the i-th sequence s_i is

$$s_i(1), s_i(2), s_i(3), \ldots$$

We may arrange this list, and the elements of each sequence s_i in it, in an array:

	1	2	3	4	...
1	$\mathbf{s_1(1)}$	$s_1(2)$	$s_1(3)$	$s_1(4)$	...
2	$s_2(1)$	$\mathbf{s_2(2)}$	$s_2(3)$	$s_2(4)$	...
3	$s_3(1)$	$s_3(2)$	$\mathbf{s_3(3)}$	$s_3(4)$	...
4	$s_4(1)$	$s_4(2)$	$s_4(3)$	$\mathbf{s_4(4)}$	...
⋮	⋮	⋮	⋮	⋮	⋱

The labels down the side give the number of the sequence in the list s_1, s_2, ...; the numbers across the top label the elements of the individual sequences. For instance, $s_1(1)$ is a name for whatever number, a 0 or a 1, is the first element in the sequence s_1, and so on.

Now we construct an infinite sequence, $\overline{s}$, of 0's and 1's which cannot possibly be on this list. The definition of $\overline{s}$ will depend on the list s_1, s_2, ... Any infinite list of infinite sequences of 0's and 1's gives rise to an infinite sequence $\overline{s}$ which is guaranteed to not appear on the list.

To define $\overline{s}$, we specify what all its elements are, i.e., we specify $\overline{s}(n)$ for all $n \in \mathbb{Z}^+$. We do this by reading down the diagonal of the array above (hence the name "diagonal method") and then changing every 1 to a 0 and every 0 to a 1. More abstractly, we define $\overline{s}(n)$ to be 0 or 1 according to whether the n-th element of the diagonal, $s_n(n)$, is 1 or 0.

$$\overline{s}(n) = \begin{cases} 1 & \text{if } s_n(n) = 0 \\ 0 & \text{if } s_n(n) = 1. \end{cases}$$

If you like formulas better than definitions by cases, you could also define $\overline{s}(n) = 1 - s_n(n)$.

Clearly $\overline{s}$ is an infinite sequence of 0's and 1's, since it is just the mirror sequence to the sequence of 0's and 1's that appear on the diagonal of our array. So $\overline{s}$ is an element of $\mathbb{B}^\omega$. But it cannot be on the list s_1, s_2, ... Why not?

It can't be the first sequence in the list, s_1, because it differs from s_1 in the first element. Whatever $s_1(1)$ is, we defined $\overline{s}(1)$ to be the opposite. It can't be the second sequence in the list, because $\overline{s}$ differs from s_2 in the second element: if $s_2(2)$ is 0, $\overline{s}(2)$ is 1, and vice versa. And so on.

More precisely: if $\overline{s}$ were on the list, there would be some k so that $\overline{s} = s_k$. Two sequences are identical iff they agree at every place, i.e., for any n, $\overline{s}(n) = s_k(n)$. So in particular, taking $n = k$ as a special case, $\overline{s}(k) = s_k(k)$ would have to hold. $s_k(k)$ is either 0 or 1. If it is 0 then $\overline{s}(k)$ must be 1—that's how we defined $\overline{s}$. But if $s_k(k) = 1$ then, again because of the way we defined $\overline{s}$, $\overline{s}(k) = 0$. In either case $\overline{s}(k) \neq s_k(k)$.

We started by assuming that there is a list of elements of $\mathbb{B}^\omega$, s_1, s_2, ... From this list we constructed a sequence $\overline{s}$ which we proved cannot be on the list. But it definitely is a sequence of 0's and 1's if all the s_i are sequences of 0's and 1's, i.e., $\overline{s} \in \mathbb{B}^\omega$. This shows in particular that there can be no list of *all* elements of $\mathbb{B}^\omega$, since for any such list we could also construct a sequence $\overline{s}$ guaranteed to not be on the list, so the assumption that there is a list of all sequences in $\mathbb{B}^\omega$ leads to a contradiction. □

explanation

This proof method is called "diagonalization" because it uses the diagonal of the array to define $\overline{s}$. Diagonalization need not involve the presence of an array: we can show that sets are not enumerable by using a similar idea even when no array and no actual diagonal is involved.

sfr:siz:nen:thm:nonenum-pownat

Theorem 4.18. *$\wp(\mathbb{Z}^+)$ is not enumerable.*

Proof. We proceed in the same way, by showing that for every list of subsets of $\mathbb{Z}^+$ there is a subset of $\mathbb{Z}^+$ which cannot be on the list. Suppose the following

is a given list of subsets of $\mathbb{Z}^+$:

$$Z_1, Z_2, Z_3, \ldots$$

We now define a set $\overline{Z}$ such that for any $n \in \mathbb{Z}^+$, $n \in \overline{Z}$ iff $n \notin Z_n$:

$$\overline{Z} = \{n \in \mathbb{Z}^+ : n \notin Z_n\}$$ □

$\overline{Z}$ is clearly a set of positive integers, since by assumption each Z_n is, and thus $\overline{Z} \in \wp(\mathbb{Z}^+)$. But $\overline{Z}$ cannot be on the list. To show this, we'll establish that for each $k \in \mathbb{Z}^+$, $\overline{Z} \neq Z_k$.

So let $k \in \mathbb{Z}^+$ be arbitrary. We've defined $\overline{Z}$ so that for any $n \in \mathbb{Z}^+$, $n \in \overline{Z}$ iff $n \notin Z_n$. In particular, taking $n = k$, $k \in \overline{Z}$ iff $k \notin Z_k$. But this shows that $\overline{Z} \neq Z_k$, since k is an element of one but not the other, and so $\overline{Z}$ and Z_k have different elements. Since k was arbitrary, $\overline{Z}$ is not on the list Z_1, Z_2, ...

explanation

The preceding proof did not mention a diagonal, but you can think of it as involving a diagonal if you picture it this way: Imagine the sets Z_1, Z_2, ..., written in an array, where each element $j \in Z_i$ is listed in the j-th column. Say the first four sets on that list are $\{1, 2, 3, \ldots\}$, $\{2, 4, 6, \ldots\}$, $\{1, 2, 5\}$, and $\{3, 4, 5, \ldots\}$. Then the array would begin with

$$\begin{array}{lccccccc}
Z_1 = \{ & \mathbf{1}, & 2, & 3, & 4, & 5, & 6, & \ldots\} \\
Z_2 = \{ & & \mathbf{2}, & & 4, & & 6, & \ldots\} \\
Z_3 = \{ & 1, & 2, & & & 5 & & \} \\
Z_4 = \{ & & & 3, & \mathbf{4}, & 5, & 6, & \ldots\} \\
\vdots & & & & & \ddots & &
\end{array}$$

Then $\overline{Z}$ is the set obtained by going down the diagonal, leaving out any numbers that appear along the diagonal and include those j where the array has a gap in the j-th row/column. In the above case, we would leave out 1 and 2, include 3, leave out 4, etc.

Problem 4.15. Show that $\wp(\mathbb{N})$ is non-enumerable by a diagonal argument.

Problem 4.16. Show that the set of functions $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ is non-enumerable by an explicit diagonal argument. That is, show that if f_1, f_2, ..., is a list of functions and each $f_i : \mathbb{Z}^+ \to \mathbb{Z}^+$, then there is some $\overline{f} : \mathbb{Z}^+ \to \mathbb{Z}^+$ not on this list.

4.7 Reduction

sfr:siz:red:sec

This section proves non-enumerability by reduction, matching the results in section 4.6. An alternative, slightly more condensed version matching the results in section 4.12 is provided in section 4.13.

We showed $\wp(\mathbb{Z}^+)$ to be non-enumerable by a diagonalization argument. We already had a proof that $\mathbb{B}^\omega$, the set of all infinite sequences of 0s and 1s, is non-enumerable. Here's another way we can prove that $\wp(\mathbb{Z}^+)$ is non-enumerable: Show that *if* $\wp(\mathbb{Z}^+)$ *is enumerable then* $\mathbb{B}^\omega$ *is also enumerable*. Since we know $\mathbb{B}^\omega$ is not enumerable, $\wp(\mathbb{Z}^+)$ can't be either. This is called *reducing* one problem to another—in this case, we reduce the problem of enumerating $\mathbb{B}^\omega$ to the problem of enumerating $\wp(\mathbb{Z}^+)$. A solution to the latter—an enumeration of $\wp(\mathbb{Z}^+)$—would yield a solution to the former—an enumeration of $\mathbb{B}^\omega$.

How do we reduce the problem of enumerating a set B to that of enumerating a set A? We provide a way of turning an enumeration of A into an enumeration of B. The easiest way to do that is to define a surjective function $f\colon A \to B$. If $x_1, x_2, \ldots$ enumerates A, then $f(x_1), f(x_2), \ldots$ would enumerate B. In our case, we are looking for a surjective function $f\colon \wp(\mathbb{Z}^+) \to \mathbb{B}^\omega$.

Problem 4.17. Show that if there is an injective function $g\colon B \to A$, and B is non-enumerable, then so is A. Do this by showing how you can use g to turn an enumeration of A into one of B.

Proof of Theorem 4.18 by reduction. Suppose that $\wp(\mathbb{Z}^+)$ were enumerable, and thus that there is an enumeration of it, $Z_1, Z_2, Z_3, \ldots$

Define the function $f\colon \wp(\mathbb{Z}^+) \to \mathbb{B}^\omega$ by letting $f(Z)$ be the sequence s_k such that $s_k(n) = 1$ iff $n \in Z$, and $s_k(n) = 0$ otherwise. This clearly defines a function, since whenever $Z \subseteq \mathbb{Z}^+$, any $n \in \mathbb{Z}^+$ either is an element of Z or isn't. For instance, the set $2\mathbb{Z}^+ = \{2, 4, 6, \ldots\}$ of positive even numbers gets mapped to the sequence $010101\ldots$, the empty set gets mapped to $0000\ldots$ and the set $\mathbb{Z}^+$ itself to $1111\ldots$.

It also is surjective: Every sequence of 0s and 1s corresponds to some set of positive integers, namely the one which has as its members those integers corresponding to the places where the sequence has 1s. More precisely, suppose $s \in \mathbb{B}^\omega$. Define $Z \subseteq \mathbb{Z}^+$ by:

$$Z = \{n \in \mathbb{Z}^+ : s(n) = 1\}$$

Then $f(Z) = s$, as can be verified by consulting the definition of f.

Now consider the list

$$f(Z_1), f(Z_2), f(Z_3), \ldots$$

Since f is surjective, every member of $\mathbb{B}^\omega$ must appear as a value of f for some argument, and so must appear on the list. This list must therefore enumerate all of $\mathbb{B}^\omega$.

So if $\wp(\mathbb{Z}^+)$ were enumerable, $\mathbb{B}^\omega$ would be enumerable. But $\mathbb{B}^\omega$ is non-enumerable (Theorem 4.17). Hence $\wp(\mathbb{Z}^+)$ is non-enumerable. □

It is easy to be confused about the direction the reduction goes in. For instance, a surjective function $g\colon \mathbb{B}^\omega \to B$ does *not* establish that B is non-enumerable. (Consider $g\colon \mathbb{B}^\omega \to \mathbb{B}$ defined by $g(s) = s(1)$, the function that explanation

maps a sequence of 0's and 1's to its first element. It is surjective, because some sequences start with 0 and some start with 1. But $\mathbb{B}$ is finite.) Note also that the function f must be surjective, or otherwise the argument does not go through: $f(x_1)$, $f(x_2)$, ... would then not be guaranteed to include all the elements of B. For instance,

$$h(n) = \underbrace{000\ldots0}_{n \text{ 0's}}$$

defines a function $h\colon \mathbb{Z}^+ \to \mathbb{B}^\omega$, but $\mathbb{Z}^+$ is enumerable.

Problem 4.18. Show that the set of all *sets of* pairs of positive integers is non-enumerable by a reduction argument.

Problem 4.19. Show that $\mathbb{N}^\omega$, the set of infinite sequences of natural numbers, is non-enumerable by a reduction argument.

Problem 4.20. Let P be the set of functions from the set of positive integers to the set $\{0\}$, and let Q be the set of *partial* functions from the set of positive integers to the set $\{0\}$. Show that P is enumerable and Q is not. (Hint: reduce the problem of enumerating $\mathbb{B}^\omega$ to enumerating Q).

Problem 4.21. Let S be the set of all surjective functions from the set of positive integers to the set $\{0,1\}$, i.e., S consists of all surjective $f\colon \mathbb{Z}^+ \to \mathbb{B}$. Show that S is non-enumerable.

Problem 4.22. Show that the set $\mathbb{R}$ of all real numbers is non-enumerable.

4.8 Equinumerosity

sfr:siz:equ:sec

We have an intuitive notion of "size" of sets, which works fine for finite sets. But what about infinite sets? If we want to come up with a formal way of comparing the sizes of two sets of *any* size, it is a good idea to start by defining when sets are the same size. Here is Frege:

> If a waiter wants to be sure that he has laid exactly as many knives as plates on the table, he does not need to count either of them, if he simply lays a knife to the right of each plate, so that every knife on the table lies to the right of some plate. The plates and knives are thus uniquely correlated to each other, and indeed through that same spatial relationship. (Frege, 1884, §70)

The insight of this passage can be brought out through a formal definition:

sfr:siz:equ:comparisondef

Definition 4.19. A is *equinumerous* with B, written $A \approx B$, iff there is a bijection $f\colon A \to B$.

sfr:siz:equ:equinumerosityisequi

Proposition 4.20. *Equinumerosity is an equivalence relation.*

Proof. We must show that equinumerosity is reflexive, symmetric, and transitive. Let A, B, and C be sets.

Reflexivity. The identity map $\mathrm{Id}_A \colon A \to A$, where $\mathrm{Id}_A(x) = x$ for all $x \in A$, is a bijection. So $A \approx A$.

Symmetry. Suppose $A \approx B$, i.e., there is a bijection $f \colon A \to B$. Since f is bijective, its inverse f^{-1} exists and is also bijective. Hence, $f^{-1} \colon B \to A$ is a bijection, so $B \approx A$.

Transitivity. Suppose that $A \approx B$ and $B \approx C$, i.e., there are bijections $f \colon A \to B$ and $g \colon B \to C$. Then the composition $g \circ f \colon A \to C$ is bijective, so that $A \approx C$. □

Proposition 4.21. *If $A \approx B$, then A is enumerable if and only if B is.*

> The following proof uses Definition 4.4 if section 4.2 is included and Definition 4.27 otherwise.

Proof. Suppose $A \approx B$, so there is some bijection $f \colon A \to B$, and suppose that A is enumerable. Then either $A = \emptyset$ or there is a surjective function $g \colon \mathbb{Z}^+ \to A$. If $A = \emptyset$, then $B = \emptyset$ also (otherwise there would be an element $y \in B$ but no $x \in A$ with $g(x) = y$). If, on the other hand, $g \colon \mathbb{Z}^+ \to A$ is surjective, then $g \circ f \colon \mathbb{Z}^+ \to B$ is surjective. To see this, let $y \in B$. Since g is surjective, there is an $x \in A$ such that $g(x) = y$. Since f is surjective, there is an $n \in \mathbb{Z}^+$ such that $f(n) = x$. Hence,

$$(g \circ f)(n) = g(f(n)) = g(x) = y$$

and thus $g \circ f$ is surjective. We have that $g \circ f$ is an enumeration of B, and so B is enumerable.

If B is enumerable, we obtain that A is enumerable by repeating the argument with the bijection $f^{-1} \colon B \to A$ instead of f. □

Problem 4.23. Show that if $A \approx C$ and $B \approx D$, and $A \cap B = C \cap D = \emptyset$, then $A \cup B \approx C \cup D$.

Problem 4.24. Show that if A is infinite and enumerable, then $A \approx \mathbb{N}$.

4.9 Sets of Different Sizes, and Cantor's Theorem

sfr:siz:car: sec

We have offered a precise statement of the idea that two sets have the same size. explanation We can also offer a precise statement of the idea that one set is smaller than another. Our definition of "is smaller than (or equinumerous)" will require, instead of a bijection between the sets, an injection from the first set to the second. If such a function exists, the size of the first set is less than or equal to the size of the second. Intuitively, an injection from one set to another guarantees that the range of the function has at least as many elements as the domain, since no two elements of the domain map to the same element of the range.

Definition 4.22. A is *no larger than* B, written $A \preceq B$, iff there is an injection $f\colon A \to B$.

It is clear that this is a reflexive and transitive relation, but that it is not symmetric (this is left as an exercise). We can also introduce a notion, which states that one set is (strictly) smaller than another.

Definition 4.23. A is *smaller than* B, written $A \prec B$, iff there is an injection $f\colon A \to B$ but no bijection $g\colon A \to B$, i.e., $A \preceq B$ and $A \not\approx B$.

It is clear that this is relation is anti-reflexive and transitive. (This is left as an exercise.) Using this notation, we can say that a set A is enumerable iff $A \preceq \mathbb{N}$, and that A is non-enumerable iff $\mathbb{N} \prec A$. This allows us to restate Theorem 4.32 as the observation that $\mathbb{N} \prec \wp(\mathbb{N})$. In fact, Cantor (1892) proved that this last point is *perfectly general*:

Theorem 4.24 (Cantor). *$A \prec \wp(A)$, for any set A.* *sfr:siz:car: thm:cantor*

Proof. The map $f(x) = \{x\}$ is an injection $f\colon A \to \wp(A)$, since if $x \neq y$, then also $\{x\} \neq \{y\}$ by extensionality, and so $f(x) \neq f(y)$. So we have that $A \preceq \wp(A)$.

> We present the slow proof if section 4.6 is present, otherwise a faster proof matching section 4.12.

We show that there cannot be a surjective function $g\colon A \to \wp(A)$, let alone a bijective one, and hence that $A \not\approx \wp(A)$. For suppose that $g\colon A \to \wp(A)$. Since g is total, every $x \in A$ is mapped to a subset $g(x) \subseteq A$. We show that g cannot be surjective. To do this, we define a subset $\overline{A} \subseteq A$ which by definition cannot be in the range of g. Let

$$\overline{A} = \{x \in A : x \notin g(x)\}.$$

Since $g(x)$ is defined for all $x \in A$, $\overline{A}$ is clearly a well-defined subset of A. But, it cannot be in the range of g. Let $x \in A$ be arbitrary, we show that $\overline{A} \neq g(x)$. If $x \in g(x)$, then it does not satisfy $x \notin g(x)$, and so by the definition of $\overline{A}$, we have $x \notin \overline{A}$. If $x \in \overline{A}$, it must satisfy the defining property of $\overline{A}$, i.e., $x \in A$ and $x \notin g(x)$. Since x was arbitrary, this shows that for each $x \in \overline{A}$, $x \in g(x)$ iff $x \notin \overline{A}$, and so $g(x) \neq \overline{A}$. In other words, $\overline{A}$ cannot be in the range of g, contradicting the assumption that g is surjective. □

explanation

It's instructive to compare the proof of Theorem 4.24 to that of Theorem 4.18. There we showed that for any list Z_1, Z_2, ..., of subsets of $\mathbb{Z}^+$ one can construct a set $\overline{Z}$ of numbers guaranteed not to be on the list. It was guaranteed not to be on the list because, for every $n \in \mathbb{Z}^+$, $n \in Z_n$ iff $n \notin \overline{Z}$. This way, there is always some number that is an element of one of Z_n or $\overline{Z}$ but not

the other. We follow the same idea here, except the indices n are now elements of A instead of $\mathbb{Z}^+$. The set $\overline{B}$ is defined so that it is different from $g(x)$ for each $x \in A$, because $x \in g(x)$ iff $x \notin \overline{B}$. Again, there is always an element of A which is an element of one of $g(x)$ and $\overline{B}$ but not the other. And just as $\overline{Z}$ therefore cannot be on the list $Z_1, Z_2, \ldots$, $\overline{B}$ cannot be in the range of g.

It's instructive to compare the proof of Theorem 4.24 to that of Theorem 4.32. There we showed that for any list $N_0, N_1, N_2, \ldots$, of subsets of $\mathbb{N}$ we can construct a set D of numbers guaranteed not to be on the list. It was guaranteed not to be on the list because $n \in N_n$ iff $n \notin D$, for every $n \in \mathbb{N}$. We follow the same idea here, except the indices n are now elements of A rather than of $\mathbb{N}$. The set D is defined so that it is different from $g(x)$ for each $x \in A$, because $x \in g(x)$ iff $x \notin D$.

The proof is also worth comparing with the proof of Russell's Paradox, Theorem 1.29. Indeed, Cantor's Theorem was the inspiration for Russell's own paradox.

Problem 4.25. Show that there cannot be an injection $g\colon \wp(A) \to A$, for any set A. Hint: Suppose $g\colon \wp(A) \to A$ is injective. Consider $D = \{g(B) : B \subseteq A \text{ and } g(B) \notin B\}$. Let $x = g(D)$. Use the fact that g is injective to derive a contradiction.

4.10 The Notion of Size, and Schröder-Bernstein

sfr:siz:sb:sec

Here is an intuitive thought: if A is no larger than B and B is no larger than A, then A and B are equinumerous. To be honest, if this thought were *wrong*, then we could scarcely justify the thought that our defined notion of equinumerosity has anything to do with comparisons of "sizes" between sets! Fortunately, though, the intuitive thought is correct. This is justified by the Schröder-Bernstein Theorem. explanation

sfr:siz:sb:thm:schroder-bernstein

Theorem 4.25 (Schröder-Bernstein). *If $A \preceq B$ and $B \preceq A$, then $A \approx B$.*

In other words, if there is an injection from A to B, and an injection from B to A, then there is a bijection from A to B. explanation

This result, however, is really rather *difficult* to prove. Indeed, although Cantor stated the result, others proved it.[1] For now, you can (and must) take it on trust.

Fortunately, Schröder-Bernstein is *correct*, and it vindicates our thinking of the relations we defined, i.e., $A \approx B$ and $A \preceq B$, as having something to do with "size". Moreover, Schröder-Bernstein is very *useful*. It can be difficult to think of a bijection between two equinumerous sets. The Schröder-Bernstein Theorem allows us to break the comparison down into cases so we only have to think of an injection from the first to the second, and vice-versa.

[1] For more on the history, see e.g., Potter (2004, pp. 165–6).

The following section 4.11, section 4.12, section 4.13 are alternative versions of section 4.2, section 4.6, section 4.7 due to Tim Button for use in his Open Set Theory text. They are slightly more advanced and use a difference definition of enumerability more suitable in a set theory context (i.e., bijection with $\mathbb{N}$ or an initial segment, rather than being listable or being the range of a surjective function from $\mathbb{Z}^+$).

4.11 Enumerations and Enumerable Sets

sfr:siz:enm-alt:sec

This section defines enumerations as bijections with (initial segments) of $\mathbb{N}$, the way it's done in set theory. So it conflicts slightly with the definitions in section 4.2, and repeats all the examples there. It is also a bit more terse than that section.

We can specify finite set is by simply enumerating its elements. We do this when we define a set like so:

$$A = \{a_1, a_2, \ldots, a_n\}.$$

Assuming that the elements $a_1, \ldots, a_n$ are all distinct, this gives us a bijection between A and the first n natural numbers $0, \ldots, n-1$. Conversely, since every finite set has only finitely many elements, every finite set can be put into such a correspondence. In other words, if A is finite, there is a bijection between A and $\{0, \ldots, n-1\}$, where n is the number of elements of A.

If we allow for certain kinds of infinite sets, then we will also allow some infinite sets to be enumerated. We can make this precise by saying that an infinite set is enumerated by a bijection between it and all of $\mathbb{N}$.

Definition 4.26 (Enumeration, set-theoretic). An *enumeration* of a set A is a bijection whose range is A and whose domain is either an initial set of natural numbers $\{0, 1, \ldots, n\}$ or the entire set of natural numbers $\mathbb{N}$.

explanation

There is an intuitive underpinning to this use of the word *enumeration*. For to say that we have enumerated a set A is to say that there is a bijection f which allows us to count out the elements of the set A. The 0th element is $f(0)$, the 1st is $f(1)$, ...the nth is $f(n)$....[2] The rationale for this may be made even clearer by adding the following:

Definition 4.27. A set A is enumerable iff either $A = \emptyset$ or there is an enumeration of A. We say that A is non-enumerable iff A is not enumerable.

sfr:siz:enm-alt:defn:enumerable

[2] Yes, we count from 0. Of course we could also start with 1. This would make no big difference. We would just have to replace $\mathbb{N}$ by $\mathbb{Z}^+$.

So a set is enumerable iff it is empty or you can use an enumeration to count out its elements. explanation

Example 4.28. A function enumerating the natural numbers is simply the identity function $\mathrm{Id}_{\mathbb{N}} \colon \mathbb{N} \to \mathbb{N}$ given by $\mathrm{Id}_{\mathbb{N}}(n) = n$. A function enumerating the *positive* natural numbers, $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$, is the function $g(n) = n + 1$, i.e., the successor function.

Problem 4.26. Show that a set A is enumerable iff either $A = \emptyset$ or there is a surjection $f \colon \mathbb{N} \to A$. Show that A is enumerable iff there is an injection $g \colon A \to \mathbb{N}$.

Example 4.29. The functions $f \colon \mathbb{N} \to \mathbb{N}$ and $g \colon \mathbb{N} \to \mathbb{N}$ given by

$$f(n) = 2n \text{ and}$$
$$g(n) = 2n + 1$$

respectively enumerate the even natural numbers and the odd natural numbers. But neither is surjective, so neither is an enumeration of $\mathbb{N}$.

Problem 4.27. Define an enumeration of the square numbers 1, 4, 9, 16, ...

Example 4.30. Let $\lceil x \rceil$ be the *ceiling* function, which rounds x up to the nearest integer. Then the function $f \colon \mathbb{N} \to \mathbb{Z}$ given by:

$$f(n) = (-1)^n \left\lceil \tfrac{n}{2} \right\rceil$$

enumerates the set of integers $\mathbb{Z}$ as follows:

$f(0)$	$f(1)$	$f(2)$	$f(3)$	$f(4)$	$f(5)$	$f(6)$	...
$\left\lceil \frac{0}{2} \right\rceil$	$-\left\lceil \frac{1}{2} \right\rceil$	$\left\lceil \frac{2}{2} \right\rceil$	$-\left\lceil \frac{3}{2} \right\rceil$	$\left\lceil \frac{4}{2} \right\rceil$	$-\left\lceil \frac{5}{2} \right\rceil$	$\left\lceil \frac{6}{2} \right\rceil$	...
0	-1	1	-2	2	-3	3	...

Notice how f generates the values of $\mathbb{Z}$ by "hopping" back and forth between positive and negative integers. You can also think of f as defined by cases as follows:

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ -\frac{n+1}{2} & \text{if } n \text{ is odd} \end{cases}$$

Problem 4.28. Show that if A and B are enumerable, so is $A \cup B$.

Problem 4.29. Show by induction on n that if A_1, A_2, ..., A_n are all enumerable, so is $A_1 \cup \cdots \cup A_n$.

4.12 Non-enumerable Sets

sfr:siz:nen-alt:sec

This section proves the non-enumerability of $\mathbb{B}^\omega$ and $\wp(\mathbb{N})$ using the definitions in section 4.11, i.e., requiring a bijection with $\mathbb{N}$ instead of a surjection from $\mathbb{Z}^+$.

explanation

The set $\mathbb{N}$ of natural numbers is infinite. It is also trivially enumerable. But the remarkable fact is that there are *non-enumerable* sets, i.e., sets which are not enumerable (see Definition 4.27).

This might be surprising. After all, to say that A is non-enumerable is to say that there is *no* bijection $f\colon \mathbb{N} \to A$; that is, no function mapping the infinitely many elements of $\mathbb{N}$ to A exhausts all of A. So if A is non-enumerable, there are "more" elements of A than there are natural numbers.

To prove that a set is non-enumerable, you have to show that no appropriate bijection can exist. The best way to do this is to show that every attempt to enumerate elements of A must leave at least one element out; this shows that no function $f\colon \mathbb{N} \to A$ is surjective. And a general strategy for establishing this is to use Cantor's *diagonal method*. Given a list of elements of A, say, x_1, x_2, ..., we construct another element of A which, by its construction, cannot possibly be on that list.

But all of this is best understood by example. So, our first example is the set $\mathbb{B}^\omega$ of all infinite strings of 0's and 1's. (The '$\mathbb{B}$' stands for binary, and we can just think of it as the two-element set $\{0, 1\}$.)

Theorem 4.31. *$\mathbb{B}^\omega$ is non-enumerable.*

sfr:siz:nen-alt:thm:nonenum-bin-omega

Proof. Consider any enumeration of a subset of $\mathbb{B}^\omega$. So we have some list s_0, s_1, s_2, ... where every s_n is an infinite string of 0's and 1's. Let $s_n(m)$ be the nth digit of the mth string in this list. So we can now think of our list as an array, where $s_n(m)$ is placed at the nth row and mth column:

	0	1	2	3	...
0	$\mathbf{s_0(0)}$	$s_0(1)$	$s_0(2)$	$s_0(3)$	...
1	$s_1(0)$	$\mathbf{s_1(1)}$	$s_1(2)$	$s_1(3)$	...
2	$s_2(0)$	$s_2(1)$	$\mathbf{s_2(2)}$	$s_2(3)$	...
3	$s_3(0)$	$s_3(1)$	$s_3(2)$	$\mathbf{s_3(3)}$	...
⋮	⋮	⋮	⋮	⋮	⋱

We will now construct an infinite string, d, of 0's and 1's which is not on this list. We will do this by specifying each of its entries, i.e., we specify $d(n)$ for all $n \in \mathbb{N}$. Intuitively, we do this by reading down the diagonal of the array above (hence the name "diagonal method") and then changing every 1 to a 0

and every 1 to a 0. More abstractly, we define $d(n)$ to be 0 or 1 according to whether the n-th element of the diagonal, $s_n(n)$, is 1 or 0, that is:

$$d(n) = \begin{cases} 1 & \text{if } s_n(n) = 0 \\ 0 & \text{if } s_n(n) = 1 \end{cases}$$

Clearly $d \in \mathbb{B}^\omega$, since it is an infinite string of 0's and 1's. But we have constructed d so that $d(n) \neq s_n(n)$ for any $n \in \mathbb{N}$. That is, d differs from s_n in its nth entry. So $d \neq s_n$ for any $n \in \mathbb{N}$. So d cannot be on the list s_0, s_1, s_2, ...

We have shown, given an arbitrary enumeration of some subset of $\mathbb{B}^\omega$, that it will omit some element of $\mathbb{B}^\omega$. So there is no enumeration of the set $\mathbb{B}^\omega$, i.e., $\mathbb{B}^\omega$ is non-enumerable. □

This proof method is called "diagonalization" because it uses the diagonal of the array to define d. However, diagonalization need not involve the presence of an array. Indeed, we can show that some set is non-enumerable by using a similar idea, even when no array and no actual diagonal is involved. The following result illustrates how. explanation

sfr:siz:nen-alt: *thm:nonenum-pownat*

Theorem 4.32. *$\wp(\mathbb{N})$ is not enumerable.*

Proof. We proceed in the same way, by showing that every list of subsets of $\mathbb{N}$ omits some subset of $\mathbb{N}$. So, suppose that we have some list $N_0, N_1, N_2, \ldots$ of subsets of $\mathbb{N}$. We define a set D as follows: $n \in D$ iff $n \notin N_n$:

$$D = \{n \in \mathbb{N} : n \notin N_n\}$$

Clearly $D \subseteq \mathbb{N}$. But D cannot be on the list. After all, by construction $n \in D$ iff $n \notin N_n$, so that $D \neq N_n$ for any $n \in \mathbb{N}$. □

The preceding proof did not mention a diagonal. Still, you can think of it as involving a diagonal if you picture it this way: Imagine the sets N_0, N_1, ..., written in an array, where we write N_n on the nth row by writing m in the mth column iff if $m \in N_n$. For example, say the first four sets on that list are $\{0, 1, 2, \ldots\}$, $\{1, 3, 5, \ldots\}$, $\{0, 1, 4\}$, and $\{2, 3, 4, \ldots\}$; then our array would begin with explanation

$$\begin{array}{lccccccc}
N_0 = \{\mathbf{0}, & 1, & 2, & & & & & \ldots\} \\
N_1 = \{ & \mathbf{1}, & & 3, & & 5, & & \ldots\} \\
N_2 = \{0, & 1, & & & 4 & & & \} \\
N_3 = \{ & & 2, & \mathbf{3}, & 4, & & & \ldots\} \\
\vdots & & & & & & & \ddots
\end{array}$$

Then D is the set obtained by going down the diagonal, placing $n \in D$ iff n is *not* on the diagonal. So in the above case, we would leave out 0 and 1, we would include 2, we would leave out 3, etc.

Problem 4.30. Show that the set of all functions $f : \mathbb{N} \to \mathbb{N}$ is non-enumerable by an explicit diagonal argument. That is, show that if f_1, f_2, ..., is a list of functions and each $f_i : \mathbb{N} \to \mathbb{N}$, then there is some $g : \mathbb{N} \to \mathbb{N}$ not on this list.

4.13 Reduction

sfr:siz:red-alt:sec

This section proves non-enumerability by reduction, matching the results in section 4.12. An alternative, slightly more elaborate version matching the results in section 4.6 is provided in section 4.7.

We proved that $\mathbb{B}^\omega$ is non-enumerable by a diagonalization argument. We used a similar diagonalization argument to show that $\wp(\mathbb{N})$ is non-enumerable. But here's another way we can prove that $\wp(\mathbb{N})$ is non-enumerable: show that *if* $\wp(\mathbb{N})$ *is enumerable then* $\mathbb{B}^\omega$ *is also enumerable*. Since we know $\mathbb{B}^\omega$ is non-enumerable, it will follow that $\wp(\mathbb{N})$ is too.

This is called *reducing* one problem to another. In this case, we reduce the problem of enumerating $\mathbb{B}^\omega$ to the problem of enumerating $\wp(\mathbb{N})$. A solution to the latter—an enumeration of $\wp(\mathbb{N})$—would yield a solution to the former—an enumeration of $\mathbb{B}^\omega$.

To reduce the problem of enumerating a set B to that of enumerating a set A, we provide a way of turning an enumeration of A into an enumeration of B. The easiest way to do that is to define a surjection $f\colon A \to B$. If x_1, x_2, ... enumerates A, then $f(x_1)$, $f(x_2)$, ... would enumerate B. In our case, we are looking for a surjection $f\colon \wp(\mathbb{N}) \to \mathbb{B}^\omega$.

Problem 4.31. Show that if there is an injective function $g\colon B \to A$, and B is non-enumerable, then so is A. Do this by showing how you can use g to turn an enumeration of A into one of B.

Proof of Theorem 4.32 by reduction. For reductio, suppose that $\wp(\mathbb{N})$ is enumerable, and thus that there is an enumeration of it, N_1, N_2, N_3, ...

Define the function $f\colon \wp(\mathbb{N}) \to \mathbb{B}^\omega$ by letting $f(N)$ be the string s_k such that $s_k(n) = 1$ iff $n \in N$, and $s_k(n) = 0$ otherwise.

This clearly defines a function, since whenever $N \subseteq \mathbb{N}$, any $n \in \mathbb{N}$ either is an element of N or isn't. For instance, the set $2\mathbb{N} = \{2n : n \in \mathbb{N}\} = \{0, 2, 4, 6, \dots\}$ of even naturals gets mapped to the string $1010101\dots$; $\emptyset$ gets mapped to $0000\dots$; $\mathbb{N}$ gets mapped to $1111\dots$.

It is also surjective: every string of 0s and 1s corresponds to some set of natural numbers, namely the one which has as its members those natural numbers corresponding to the places where the string has 1s. More precisely, if $s \in \mathbb{B}^\omega$, then define $N \subseteq \mathbb{N}$ by:

$$N = \{n \in \mathbb{N} : s(n) = 1\}$$

Then $f(N) = s$, as can be verified by consulting the definition of f.

Now consider the list

$$f(N_1), f(N_2), f(N_3), \dots$$

Since f is surjective, every member of $\mathbb{B}^\omega$ must appear as a value of f for some argument, and so must appear on the list. This list must therefore enumerate all of $\mathbb{B}^\omega$.

So if $\wp(\mathbb{N})$ were enumerable, $\mathbb{B}^\omega$ would be enumerable. But $\mathbb{B}^\omega$ is non-enumerable (Theorem 4.31). Hence $\wp(\mathbb{N})$ is non-enumerable. □

Problem 4.32. Show that the set of all *sets of* pairs of natural numbers, i.e., $\wp(\mathbb{N} \times \mathbb{N})$, is non-enumerable by a reduction argument.

Problem 4.33. Show that $\mathbb{N}^\omega$, the set of infinite sequences of natural numbers, is non-enumerable by a reduction argument.

Problem 4.34. Let S be the set of all surjections from $\mathbb{N}$ to the set $\{0, 1\}$, i.e., S consists of all surjections $f : \mathbb{N} \to \mathbb{B}$. Show that S is non-enumerable.

Problem 4.35. Show that the set $\mathbb{R}$ of all real numbers is non-enumerable.

Chapter 5

Arithmetization

The material in this chapter presents the construction of the number systems in naïve set theory. It is taken from Tim Button's Open Set Theory text.

5.1 From $\mathbb{N}$ to $\mathbb{Z}$

sfr:arith:int:sec

Here are two basic realisations:

1. Every integer can be written in the form $n - m$, with $n, m \in \mathbb{N}$.
2. The information encoded in an expression $n - m$ can equally be encoded by an ordered pair $\langle n, m \rangle$.

We already know that the ordered pairs of natural numbers are the elements of $\mathbb{N}^2$. And we are assuming that we understand $\mathbb{N}$. So here is a naïve suggestion, based on the two realisations we have had: *let's treat integers as ordered pairs of natural numbers.*

In fact, this suggestion is too naïve. Obviously we want it to be the case that $0 - 2 = 4 - 6$. But evidently $\langle 0, 2 \rangle \neq \langle 4, 6 \rangle$. So we cannot simply say that $\mathbb{N}^2$ is the set of integers.

Generalising from the preceding problem, what we want is the following:

$$a - b = c - d \text{ iff } a + d = c + b$$

(It should be obvious that this is how integers are *meant* to behave: just add b and d to both sides.) And the easy way to guarantee this behaviour is just to define an equivalence relation between ordered pairs, $\sim$, as follows:

$$\langle a, b \rangle \sim \langle c, d \rangle \text{ iff } a + d = c + b$$

We now have to show that this is an equivalence relation.

Proposition 5.1. *$\sim$ is an equivalence relation.*

Proof. We must show that $\sim$ is reflexive, symmetric, and transitive.

Reflexivity: Evidently $\langle a, b\rangle \sim \langle a, b\rangle$, since $a + b = b + a$.

Symmetry: Suppose $\langle a, b\rangle \sim \langle c, d\rangle$, so $a + d = c + b$. Then $c + b = a + d$, so that $\langle c, d\rangle \sim \langle a, b\rangle$.

Transitivity: Suppose $\langle a, b\rangle \sim \langle c, d\rangle \sim \langle m, n\rangle$. So $a + d = c + b$ and $c + n = m + d$. So $a + d + c + n = c + b + m + d$, and so $a + n = m + b$. Hence $\langle a, b\rangle \sim \langle m, n\rangle$. □

Now we can use this equivalence relation to take equivalence classes:

Definition 5.2. The integers are the equivalence classes, under $\sim$, of ordered pairs of natural numbers; that is, $\mathbb{Z} = \mathbb{N}^2/_\sim$.

Now, one might have plenty of different *philosophical* reactions to this stipulative definition. Before we consider those reactions, though, it is worth continuing with some of the technicalities.

Having said what the integers are, we shall need to define basic functions and relations on them. Let's write $[m, n]_\sim$ for the equivalence class under $\sim$ with $\langle m, n\rangle$ as an element.[1] That is:

$$[m, n]_\sim = \{\langle a, b\rangle \in \mathbb{N}^2 : \langle a, b\rangle \sim \langle m, n\rangle\}$$

So now we offer some definitions:

$$\begin{aligned}
[a, b]_\sim + [c, d]_\sim &= [a + c, b + d]_\sim \\
[a, b]_\sim \times [c, d]_\sim &= [ac + bd, ad + bc]_\sim \\
[a, b]_\sim \leq [c, d]_\sim &\text{ iff } a + d \leq b + c
\end{aligned}$$

(As is common, I'm using 'ab' stand for '$(a \times b)$', just to make the axioms easier to read.) Now, we need to make sure that these definitions behave as they *ought* to. Spelling out what this means, and checking it through, is rather laborious; we relegate the details to section 5.6. But the short point is: everything works!

One final thing remains. We have constructed the integers using natural numbers. But this will mean that the natural numbers *are not themselves integers*. We will return to the philosophical significance of this in section 5.5. On a purely technical front, though, we will need some way to be able to treat natural numbers *as* integers. The idea is quite easy: for each $n \in \mathbb{N}$, we just stipulate that $n_\mathbb{Z} = [n, 0]_\sim$. We need to confirm that this definition is well-behaved, i.e., that for any $m, n \in \mathbb{N}$

$$\begin{aligned}
(m + n)_\mathbb{Z} &= m_\mathbb{Z} + n_\mathbb{Z} \\
(m \times n)_\mathbb{Z} &= m_\mathbb{Z} \times n_\mathbb{Z} \\
m \leq n &\leftrightarrow m_\mathbb{Z} \leq n_\mathbb{Z}
\end{aligned}$$

[1] Note: using the notation introduced in Definition 2.11, we would have written $[\langle m, n\rangle]_\sim$ for the same thing. But that's just a bit harder to read.

But this is all pretty straightforward. For example, to show that the second of these obtains, we can simply help ourselves to the behaviour of the natural numbers and reason as follows:

$$\begin{aligned}(m \times n)_{\mathbb{Z}} &= [m \times n, 0]_{\sim} \\ &= [m \times n + 0 \times 0, m \times 0 + 0 \times n]_{\sim} \\ &= [m, 0]_{\sim} \times [n, 0]_{\sim} \\ &= m_{\mathbb{Z}} \times n_{\mathbb{Z}}\end{aligned}$$

We leave it as an exercise to confirm that the other two conditions hold.

Problem 5.1. Show that $(m + n)_{\mathbb{Z}} = m_{\mathbb{Z}} + n_{\mathbb{Z}}$ and $m \leq n \leftrightarrow m_{\mathbb{Z}} \leq n_{\mathbb{Z}}$, for any $m, n \in \mathbb{N}$.

5.2 From $\mathbb{Z}$ to $\mathbb{Q}$

sfr:arith:rat:sec

We just saw how to construct the integers from the natural numbers, using some naïve set theory. We shall now see how to construct the rationals from the integers in a very similar way. Our initial realisations are:

1. Every rational can be written in the form i/j, where both i and j are integers but j is non-zero.

2. The information encoded in an expression i/j can equally be encoded in an ordered pair $\langle i, j\rangle$.

The obvious approach would be to think of the rationals *as* ordered pairs drawn from $\mathbb{Z} \times (\mathbb{Z} \setminus \{0_{\mathbb{Z}}\})$. As before, though, that would be a bit too naïve, since we want $3/2 = 6/4$, but $\langle 3, 2\rangle \neq \langle 6, 4\rangle$. More generally, we will want the following:

$$a/b = c/d \text{ iff } a \times d = b \times c$$

To get this, we define an equivalence relation on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0_{\mathbb{Z}}\})$ thus:

$$\langle a, b\rangle \backsim \langle c, d\rangle \text{ iff } a \times d = b \times c$$

We must check that this is an equivalence relation. This is very much like the case of $\sim$, and we will leave it as an exercise.

Problem 5.2. Show that $\backsim$ is an equivalence relation.

But this allows us to say:

Definition 5.3. The rationals are the equivalence classes, under $\backsim$, of pairs of integers (whose second element is non-zero): $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0_{\mathbb{Z}}\}))/_{\backsim}$.

As with the integers, we also want to define some basic operations. Where $[i, j]_\backsim$ is the equivalence class under $\backsim$ with $\langle i, j\rangle$ as an element, we say:

$$[a, b]_\backsim + [c, d]_\backsim = [ad + bc, bd]_\backsim$$
$$[a, b]_\backsim \times [c, d]_\backsim = [ac, bd]_\backsim$$
$$[a, b]_\backsim \leq [c, d]_\backsim \text{ iff } ad \leq bc$$

We then need to check that these definitions behave as they *ought* to; and we relegate this to section 5.6. But they indeed do! Finally, we want some way to treat integers *as* rationals; so for each $i \in \mathbb{Z}$, we stipulate that $i_\mathbb{Q} = [i, 1_\mathbb{Z}]_\backsim$. Again, we check that all of this behaves correctly in section 5.6.

Problem 5.3. Show that $(i + j)_\mathbb{Q} = i_\mathbb{Q} + j_\mathbb{Q}$ and $(i \times j)_\mathbb{Q} = i_\mathbb{Q} \times j_\mathbb{Q}$ and $i \leq j \leftrightarrow i_\mathbb{Q} \leq j_\mathbb{Q}$, for any $i, j \in \mathbb{Z}$.

5.3 The Real Line

sfr:arith:real: sec

The next step is to show how to construct the reals from the rationals. Before that, we need to understand what is *distinctive* about the reals.

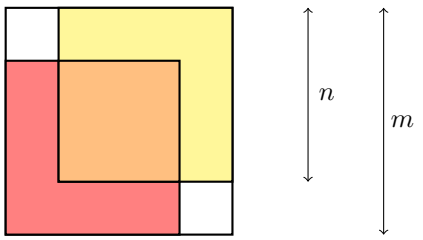
The reals behave very much like the rationals. (Technically, both are examples of *ordered fields*; for the definition of this, see Definition 5.9.) Now, if you worked through the exercises to chapter 4, you will know that there are strictly more reals than rationals, i.e., that $\mathbb{Q} \prec \mathbb{R}$. This was first proved by Cantor. But it's been known for about two and a half millennia that there are irrational numbers, i.e., reals which are not rational. Indeed:

sfr:arith:real: root2irrational

Theorem 5.4. *$\sqrt{2}$ is not rational, i.e., $\sqrt{2} \notin \mathbb{Q}$*

Proof. Suppose, for reductio, that $\sqrt{2}$ is rational. So $\sqrt{2} = {}^m/_n$ for some natural numbers m and n. Indeed, we can choose m and n so that the fraction cannot be reduced any further. Re-organising, $m^2 = 2n^2$. From here, we can complete the proof in two ways:

First, geometrically (following Tennenbaum).[2] Consider these squares:



□

Since $m^2 = 2n^2$, the region where the two squares of side n overlap has the same area as the region which neither of the two squares cover; i.e., the area of the orange square equals the sum of the area of the two unshaded squares.

[2] This proof is reported by Conway (2006).

So where the orange square has side p, and each unshaded square has side q, $p^2 = 2q^2$. But now $\sqrt{2} = {}^{p}/_{q}$, with $p < m$ and $q < n$ and $p, q \in \mathbb{N}$. This contradicts the fact that m and n were chosen to be as small as possible.

Second, formally. Since $m^2 = 2n^2$, it follows that m is even. (It is easy to show that, if x is odd, then x^2 is odd.) So $m = 2r$, for some $r \in \mathbb{N}$. Rearranging, $2r^2 = n^2$, so n is also even. So both m and n are even, and hence the fraction ${}^{m}/_{n}$ *can* be reduced further. Contradiction!

In passing, this diagrammatic proof allows us to revisit the material from **??**. Tennenbaum (1927–2006) was a thoroughly modern mathematician; but the proof is undeniably lovely, completely rigorous, and appeals to geometric intuition!

In any case: the reals are "more expansive" than the rationals. In some sense, there are "gaps" in the rationals, and these are filled by the reals. Weierstrass realised that this describes a single property of the real numbers, which distinguishes them from the rationals, namely the Completeness Property: *Every non-empty set of real numbers with an upper bound has a least upper bound.*

It is easy to see that the rationals do not have the Completeness Property. For example, consider the set of rationals less than or equal to $\sqrt{2}$, i.e.:

$$\{p \in \mathbb{Q} : p^2 < 2 \text{ or } p < 0\}$$

What is the greatest of these? You want to say '$\sqrt{2}$'; but we have just seen that $\sqrt{2}$ is not rational. And there is no *least* rational number less than $\sqrt{2}$.

By contrast, the continuum 'morally ought' to have the Completeness Property. We do not just want $\sqrt{2}$ to be a real number; we want to fill all the "gaps" in the rational line. Indeed, we want the continuum itself to have no "gaps" in it. That is just what we will get via Completeness.

5.4 From $\mathbb{Q}$ to $\mathbb{R}$

sfr:arith:cuts:sec

In essence, the Completeness Property shows that any point α of the real line divides that line into two halves perfectly: those for which α is the least upper bound, and those for which α is the greatest lower bound. To *construct* the real numbers from the rational numbers, Dedekind suggested that we simply think of the reals as the *cuts* that partition the rationals. That is, we identify $\sqrt{2}$ with the *cut* which separates the rationals $< \sqrt{2}$ from the rationals $\sqrt{2}$.

Let's tidy this up. If we cut the rational numbers into two halves, we can uniquely identify the partition we made just by considering its *bottom* half. So, getting precise, we offer the following definition:

Definition 5.5 (Cut). A *cut* α is any non-empty proper initial segment of the rationals with no greatest element. That is, α is a cut iff:

1. *non-empty, proper*: $\emptyset \neq \alpha \subsetneq \mathbb{Q}$
2. *initial*: for all $p, q \in \mathbb{Q}$: if $p < q \in \alpha$ then $p \in \alpha$

3. *no maximum*: for all $p \in \alpha$ there is a $q \in \alpha$ such that $p < q$

Then $\mathbb{R}$ is the set of cuts.

So now we can say that $\sqrt{2} = \{p \in \mathbb{Q} : p^2 < 2 \text{ or } p < 0\}$. Of course, we need to check that this *is* a cut, but we relegate that to section 5.6.

As before, having defined some entities, we next need to define basic functions and relations upon them. We begin with an easy one:

$$\alpha \leq \beta \text{ iff } \alpha \subseteq \beta$$

This definition of an order allows to *state* the central result, that the set of cuts has the Completeness Property. Spelled out fully, the statement has this shape. If S is a non-empty set of cuts with an upper bound, then S has a least upper bound; i.e., there is some cut λ such that $(\forall \alpha \in S)\alpha \subseteq \lambda$ and $(\forall \alpha \in \mathbb{R})(\alpha \subsetneq \lambda \to (\exists \kappa \in S)\kappa \nsubseteq \alpha)$. Now here is the proof of the result:

sfr:arith:cuts: realcompleteness

Theorem 5.6. *The set of cuts has the Completeness Property.*

Proof. Let S be any non-empty set of cuts with an upper bound. Let $\lambda = \bigcup S$. We first claim that λ is a cut:

1. Since S has an upper bound, at least one cut is in S, so $\emptyset \neq \alpha$. Since S is a set of cuts, $\lambda \subseteq \mathbb{Q}$. Since S has an upper bound, some $p \in \mathbb{Q}$ is absent from every cut $\alpha \in S$. So $p \notin \lambda$, and hence $\lambda \subsetneq \mathbb{Q}$.

2. Suppose $p < q \in \lambda$. So there is some $\alpha \in S$ such that $q \in \alpha$. Since α is a cut, $p \in \alpha$. So $p \in \lambda$.

3. Suppose $p \in \lambda$. So there is some $\alpha \in S$ such that $p \in \alpha$. Since α is a cut, there is some $q \in \alpha$ such that $p < q$. So $q \in \lambda$.

This proves the claim. Moreover, clearly $(\forall \alpha \in S)\alpha \subseteq \bigcup S = \lambda$. So now consider any cut $\kappa < \lambda$, i.e., $\kappa \subsetneq \lambda$. So there is some $p \in \lambda \setminus \kappa$. Since $p \in \lambda$, there is some $\alpha \in S$ such that $p \in \alpha$. So $\kappa \nsubseteq \alpha$, and hence κ is not an upper bound on S. So λ is the *least* upper bound on S. □

So we have a bunch of entities which satisfy the Completeness Property. And one way to put this is: there are no "gaps" in our cuts. (So: taking further "cuts" of reals, rather than rationals, would yield no interesting new objects.)

Next, we must define some operations on the reals. We start by embedding the rationals into the reals by stipulating that $p_{\mathbb{R}} = \{q \in \mathbb{Q} : q < p\}$ for each $p \in \mathbb{Q}$. We then define:

$$\alpha + \beta = \{p + q : p \in \alpha \wedge q \in \beta\}$$
$$\alpha \times \beta = \{p \times q : 0 \leq p \in \alpha \wedge 0 \leq q \in \beta\} \cup 0^{\mathbb{R}} \qquad \text{if } \alpha, \beta \geq 0_{\mathbb{R}}$$

To handle the other multiplication cases, first let:

$$-\alpha = \{p - q : p < 0 \wedge q \notin \alpha\}$$

and then stipulate:

$$\alpha \times \beta := \begin{cases} -\alpha \times -\beta & \text{if } \alpha < 0_{\mathbb{R}} \text{ and } \beta < 0_{\mathbb{R}} \\ -(-\alpha \times -\beta) & \text{if } \alpha < 0_{\mathbb{R}} \text{ and } \beta > 0_{\mathbb{R}} \\ -(-\alpha \times -\beta) & \text{if } \alpha > 0_{\mathbb{R}} \text{ and } \beta < 0_{\mathbb{R}} \end{cases}$$

We then need to check that each of these definitions always yields a cut. And finally, we need to go through an easy (but long-winded) demonstration that the cuts, so defined, behave exactly as they should. But we relegate all of this to section 5.6.

5.5 Some Philosophical Reflections

sfr:arith:ref:sec

So much for the technicalities. But what did they achieve?

Well, pretty uncontestably, some lovely pure mathematics. Moreover, there were some deep conceptual achievements. It was a profound insight, to see that the Completeness Property expresses the crucial difference between the reals and the rationals. Moreover, the explicit construction of reals, as Dedekind cuts, puts the subject matter of analysis on a firm footing. We know that the notion of a *complete ordered field* is coherent, for the cuts form just such a field.

For all that, we should air a few reservations about this achievement.

First, it is not clear that thinking of reals in terms of cuts is any *more* rigorous than thinking of reals in terms of their familiar (possibly infinite) decimal expansions. This latter "construction" of the reals has some resemblance to the construction of the reals via Cauchy sequence; but in fact, it was essentially known to mathematicians from the early seventeenth century onwards (see section 5.7). The real increase in rigour came from the realisation that the reals have the Completeness Property; the ability to construct real numbers as particular sets is perhaps not, by itself, so very interesting.

It is even less clear that the (much easier) arithmetisation of the integers, or of the rationals, increases rigour in those areas. Here, it is worth making a simple observation. Having *constructed* the integers as equivalence classes of ordered pairs of naturals, and then constructed the rationals as equivalence classes of ordered pairs of integers, and then constructed the reals as sets of rationals, we immediately *forget about* the constructions. In particular: no one would ever want to *invoke* these constructions during a mathematical proof (excepting, of course, a proof that the constructions behaved as they were supposed to). It's much easier to speak about a real, directly, than to speak about some set of sets of sets of sets of sets of sets of sets of naturals.

It is most doubtful of all that these definitions tell us what the integers, rationals, or reals *are*, *metaphysically speaking*. That is, it is doubtful that the

reals (say) *are* certain sets (of sets of sets...). The main barrier to such a view is that the construction could have been done in many different ways. In the case of the reals, there are some genuinely interestingly different constructions (see section 5.7). But here is a really trivial way to obtain some different constructions: as in section 2.2, we could have defined ordered pairs slightly differently; if we had used this alternative notion of an ordered pair, then our constructions would have worked precisely as well as they did, but we would have ended up with different objects. As such, there are many rival set-theoretic constructions of the integers, the rationals, and the reals. And now it would just be arbitrary (and embarrassing) to claim that the integers (say) are *these* sets, rather than *those*. (As in section 2.2, this is an instance of an argument made famous by Benacerraf 1965.)

A further point is worth raising: there is something quite *odd* about our constructions. We started with the natural numbers. We then construct the integers, and construct "the 0 of the integers", i.e., $[0,0]_\sim$. But $0 \neq [0,0]_\sim$. Indeed, given our constructions, *no* natural number is an integer. But that seems extremely counter-intuitive. Indeed, in section 1.3, we claimed without much argument that $\mathbb{N} \subseteq \mathbb{Q}$. If the constructions tell us exactly *what* the numbers are, this claim was trivially false.

Standing back, then, where do we get to? Working in a naïve set theory, and helping ourselves to the naturals, we are able to *treat* integers, rationals, and reals as certain sets. In that sense, we can *embed* the theories of these entities within a set theory. But the philosophical import of this embedding is just not that straightforward.

Of course, none of this is the last word! The point is only this. Showing that the arithmetisation of the reals *is* of deep philosophical significance would require some additional *philosophical* argument.

5.6 Ordered Rings and Fields

sfr:arith:check:sec

Throughout this chapter, we claimed that certain definitions behave "as they ought". In this technical appendix, we will spell out what we mean, and (sketch how to) show that the definitions do behave "correctly".

In section 5.1, we defined addition and multiplication on $\mathbb{Z}$. We want to show that, as defined, they endow $\mathbb{Z}$ with the structure we "would want" it to have. In particular, the structure in question is that of a commutative ring.

Definition 5.7. A *commutative ring* is a set S, equipped with specific ele-

ments 0 and 1 and operations + and ×, satisfying these eight formulas:[3]

Associativity	$a + (b + c) = (a + b) + c$	$(a \times b) \times c = a \times (b \times c)$
Commutativity	$a + b = b + a$	$a \times b = b \times a$
Identities	$a + 0 = a$	$a \times 1 = a$
Additive Inverse	$(\exists b \in S)0 = a + b$	
Distributivity	$a \times (b + c) = (a \times b) + (a \times c)$	

So, to check that the integers form a commutative ring, we just need to check that we meet these eight conditions. None of the conditions is difficult to establish, but this is a bit laborious. For example, here is how to prove *Associativity*, in the case of addition:

Proof. Fix $i, j, k \in \mathbb{Z}$. So there are $m_1, n_1, m_2, n_2, m_3, n_3 \in \mathbb{N}$ such that $i = [m_1, n_1]$ and $j = [m_2, n_2]$ and $k = [m_3, n_3]$. (For legibility, we write "$[x, y]$" rather than "$[x, y]_\sim$"; we'll do this throughout this section.) Now:

$$\begin{aligned} i + (j + k) &= [m_1, n_1] + ([m_2, n_2] + [m_3, n_3]) \\ &= [m_1, n_1] + [m_2 + m_3, n_2 + n_3] \\ &= [m_1 + (m_2 + m_3), n_1 + (n_2 + n_3)] \\ &= [(m_1 + m_2) + m_3, (n_1 + n_2) + n_3] \\ &= [m_1 + m_2, n_1 + n_2] + [m_3, n_3] \\ &= ([m_1, n_1] + [m_2, n_2]) + [m_3, n_3] \\ &= (i + j) + k \end{aligned}$$

helping ourselves freely to the behavior of addition on $\mathbb{N}$. □

Equally, here is how to prove *Additive Inverse*:

Proof. Fix $i \in \mathbb{Z}$, so that $i = [m, n]$ for some $m, n \in \mathbb{N}$. Let $j = [n, m] \in \mathbb{Z}$. Helping myself to the behaviour of the naturals, $(m+n)+0 = 0+(n+m)$, so that $\langle m + n, n + m\rangle \sim_\mathbb{Z} \langle 0, 0\rangle$ by definition, and hence $[m + n, n + m] = [0, 0] = 0_\mathbb{Z}$. So now $i + j = [m, n] + [n, m] = [m + n, n + m] = [0, 0] = 0_\mathbb{Z}$. □

And here is a proof of *Distributivity*:

[3] Implicitly, these are all bound with universal quantifiers restricted to S. Thus the first principle, more explicitly, is: $(\forall a, b, c \in S)a+(b+c) = (a+b)+c$. And note that the elements 0 and 1 here need not be the natural numbers with the same name.

Proof. As above, fix $i = [m_1, n_1]$ and $j = [m_2, n_2]$ and $k = [m_3, n_3]$. Now:

$$\begin{aligned}
i \times (j + k) &= [m_1, n_1] \times ([m_2, n_2] + [m_3, n_3]) \\
&= [m_1, n_1] \times [m_2 + m_3, n_2 + n_3] \\
&= [m_1(m_2 + m_3) + n_1(n_2 + n_3), m_1(n_2 + n_3) + n_1(m_2 + m_3)] \\
&= [m_1m_2 + m_1m_3 + n_1n_2 + n_1n_3, m_1n_2 + m_1n_3 + m_2n_1 + m_3n_1] \\
&= [m_1m_2 + n_1n_2, m_1n_2 + m_2n_1] + [m_1m_3 + n_1n_3, m_1n_3 + m_3n_1] \\
&= ([m_1, n_1] \times [m_2, n_2]) + ([m_1, n_1] \times [m_3, n_3]) \\
&= (i \times j) + (i \times k)
\end{aligned}$$

□

We leave it as an exercise to prove the remaining five conditions. Having done that, we have shown that $\mathbb{Z}$ constitutes a commutative ring, i.e., that addition and multiplication (as defined) behave as they should.

Problem 5.4. Prove that $\mathbb{Z}$ is a commutative ring.

But our task is not over. As well as defining addition and multiplication over $\mathbb{Z}$, we defined an ordering relation, $\leq$, and we must check that this behaves as it should. In more detail, we must show that $\mathbb{Z}$ constitutes an *ordered* ring.

Definition 5.8. An *ordered ring* is a commutative ring which is also equipped with a total ordering relation, $\leq$, such that:[4]

$$\begin{aligned}
a \leq b &\to a + c \leq b + c \\
(a \leq b \wedge 0 \leq c) &\to a \times c \leq b \times c
\end{aligned}$$

Problem 5.5. Prove that $\mathbb{Z}$ is an ordered ring.

As before, it is laborious but routine to show that $\mathbb{Z}$, as constructed, is an ordered ring. We will leave that to you.

This takes care of the integers. But now we need to show very similar things of the rationals. In particular, we now need to show that the rationals form an ordered *field*, under our given definitions of $+$, $\times$, and $\leq$:

sfr:arith:check: orderedfield

Definition 5.9. An *ordered field* is an ordered ring which also satisfies:

$$\textit{Multiplicative Inverse} \qquad (\forall a \in S \setminus \{0\})(\exists b \in S) a \times b = 1$$

Once you have shown that $\mathbb{Z}$ constitutes an ordered ring, it is easy but laborious to show that $\mathbb{Q}$ constitutes an ordered field.

Problem 5.6. Prove that $\mathbb{Q}$ is an ordered field.

[4] Recall from Definition 2.24 that a total ordering is a relation which is reflexive, transitive, and connected. In the context of order relations, connectedness is sometimes called *trichotomy*, since for any a and b we have $a \leq b \vee a = b \vee a \geq b$.

Having dealt with the integers and the rationals, it only remains to deal with the reals. In particular, we need to show that $\mathbb{R}$ constitutes a *complete* ordered field, i.e., an ordered field with the Completeness Property. Now, Theorem 5.6 established that $\mathbb{R}$ has the Completeness Property. However, it remains to run through the (tedious) of checking that $\mathbb{R}$ is an ordered field.

Before tearing off into *that* laborious exercise, we need to check some more "immediate" things. For example, we need a guarantee that $\alpha + \beta$, as defined, is indeed a *cut*, for any cuts α and β. Here is a proof of that fact:

Proof. Since α and β are both cuts, $\alpha + \beta = \{p + q : p \in \alpha \wedge q \in \beta\}$ is a non-empty proper subset of $\mathbb{Q}$. Now suppose $x < p + q$ for some $p < \alpha$ and $q < \beta$. Then $x - p < q$, so $x - p \in \beta$, and $x = p + (x - p) \in \alpha + \beta$. So $\alpha + \beta$ is an initial segment of $\mathbb{Q}$. Finally, for any $p + q \in \alpha + \beta$, since α and β are both cuts, there are $p_1 \in \alpha$ and $q_1 \in \beta$ such that $p < p_1$ and $q < q_1$; so $p + q < p_1 + q_1 \in \alpha + \beta$; so $\alpha + \beta$ has no maximum. □

Similar efforts will allow you to check that $\alpha - \beta$ and $\alpha \times \beta$ and $\alpha \div \beta$ are cuts (in the last case, ignoring the case where β is the zero-cut). Again, though, we will simply leave this to you.

Problem 5.7. Prove that $\mathbb{R}$ is an ordered field.

But here is a small loose end to tidy up. In section 5.4, we suggest that we can take $\sqrt{2} = \{p \in \mathbb{Q} : p < 0 \text{ or } p^2 < 2\}$. But we do need to show that this set is a *cut*. Here is a proof of that fact:

Proof. Clearly this is a nonempty proper initial segment of the rationals; so it suffices to show that it has no maximum. In particular, it suffices to show that, where p is a positive rational with $p^2 < 2$ and $q = \frac{2p+2}{p+2}$, both $p < q$ and $q^2 < 2$. To see that $p < q$, just note:

$$\begin{aligned} p^2 &< 2 \\ p^2 + 2p &< 2 + 2p \\ p(p+2) &< 2 + 2p \\ p &< \tfrac{2+2p}{p+2} = q \end{aligned}$$

To see that $q^2 < 2$, just note:

$$\begin{aligned} p^2 &< 2 \\ 2p^2 + 4p + 2 &< p^2 + 4p + 4 \\ 4p^2 + 8p + 4 &< 2(p^2 + 4p + 4) \\ (2p+2)^2 &< 2(p+2)^2 \\ \tfrac{(2p+2)^2}{(p+2)^2} &< 2 \\ q^2 &< 2 \end{aligned}$$

□

5.7 The Reals as Cauchy Sequences

sfr:arith:cauchy:sec

In section 5.4, we constructed the reals as Dedekind cuts. In this section, we explain an alternative construction. It builds on Cauchy's definition of (what we now call) a Cauchy sequence; but the use of this definition to *construct* the reals is due to other nineteenth-century authors, notably Weierstrass, Heine, Méray and Cantor. (For a nice history, see O'Connor and Robertson 2005.)

Before we get to the nineteenth century, it's worth considering Simon Stevin (1548–1620). In brief, Stevin realised that we can think of each real in terms of its decimal expansion. Thus even an irrational number, like $\sqrt{2}$, has a nice decimal expansion, beginning:

$$1.41421356237\ldots$$

It is very easy to model decimal expansions in set theory: simply consider them as functions $d\colon \mathbb{N} \to \mathbb{N}$, where $d(n)$ is the nth decimal place that we are interested in. We will then need a bit of tweak, to handle the bit of the real number that comes before the decimal point (here, just 1). We will also need a further tweak (an equivalence relation) to guarantee that, for example, $0.999\ldots = 1$. But it is not difficult to offer a perfectly rigorous construction of the real numbers, in the manner of Stevin, within set theory.

Stevin is not our focus. (For more on Stevin, see Katz and Katz 2012.) But here is a closely related thought. Instead of treating $\sqrt{2}$'s decimal expansion directly, we can instead consider a *sequence* of increasingly accurate rational approximations to $\sqrt{2}$, by considering the increasingly precise expansions:

$$1, 1.4, 1.414, 1.4142, 1.41421, \ldots$$

The idea that reals can be considered via "increasingly good approximations" provides us with the basis for another sequence of insights (akin to the realisations that we used when constructing $\mathbb{Q}$ from $\mathbb{Z}$, or $\mathbb{Z}$ from $\mathbb{N}$). The basic insights are these:

1. Every real can be written as a (perhaps infinite) decimal expansion.
2. The information encoded by a (perhaps infinite) decimal expansion can be equally be encoded by a sequence of rational numbers.
3. A sequence of rational numbers can be thought of as a function from $\mathbb{N}$ to $\mathbb{Q}$; just let $f(n)$ be the nth rational in the sequence.

Of course, not just *any* function from $\mathbb{N}$ to $\mathbb{Q}$ will give us a real number. For instance, consider this function:

$$f(n) = \begin{cases} 1 & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even} \end{cases}$$

Essentially the worry here is that the sequence $0, 1, 0, 1, 0, 1, 0, \ldots$ doesn't seem to "hone in" on any real. So: to ensure that we consider sequences which do

hone in on some real, we need to restrict our attention to sequences which have some *limit*.

We have already encountered the idea of a limit, in **??**. But we cannot use *quite* the same definition as we used there. The expression "$(\forall \varepsilon > 0)$" there tacitly involved quantification over the real numbers; and we were considering the limits of functions on the real numbers; so invoking that definition would be to help ourselves to the real numbers; and they are exactly what we were aiming to *construct*. Fortunately, we can work with a closely related idea of a limit.

sfr:arith:cauchy:
def:CauchySequence

Definition 5.10. A function $f : \mathbb{N} \to \mathbb{Q}$ is a *Cauchy sequence* iff for any positive $\varepsilon \in \mathbb{Q}$ we have that $(\exists \ell \in \mathbb{N})(\forall m, n > \ell)|f(m) - f(n)| < \varepsilon$.

The general idea of a limit is the same as before: if you want a certain level of precision (measured by ε), there is a "region" to look in (any input greater than ℓ). And it is easy to see that our sequence 1, 1.4, 1.414, 1.4142, 1.41421... has a limit: if you want to approximate $\sqrt{2}$ to within an error of $1/10^n$, then just look to any entry after the nth.

The obvious thought, then, would be to say that a real number just *is* any Cauchy sequence. But, as in the constructions of $\mathbb{Z}$ and $\mathbb{Q}$, this would be too naïve: for any given real number, multiple different Cauchy sequences indicate that real number. A simple way to see this as follows. Given a Cauchy sequence f, define g to be exactly the same function as f, except that $g(0) \neq f(0)$. Since the two sequences agree everywhere after the first number, we will (ultimately) want to say that they have the same limit, in the sense employed in Definition 5.10, and so should be thought of "defining" the same real. So, we should really think of these Cauchy sequences as the same real number.

Consequently, we again need to define an equivalence relation on the Cauchy sequences, and identify real numbers with equivalence relations. First we need the idea of a function which tends to 0 in the limit. For any function $h : \mathbb{N} \to \mathbb{Q}$, say that h *tends to* 0 iff for any positive $\varepsilon \in \mathbb{Q}$ we have that $(\exists \ell \in \mathbb{N})(\forall n > \ell)|f(n)| < \varepsilon$.[5] Further, where f and g are functions $\mathbb{N} \to \mathbb{Q}$, let $(f - g)(n) = f(n) - g(n)$. Now define:

$$f \eqsim g \text{ iff } (f - g) \text{ tends to } 0.$$

We need to check that $\eqsim$ is an equivalence relation; and it is. We can then, if we like, define the reals as the equivalence classes, under $\eqsim$, of all Cauchy sequences from $\mathbb{N} \to \mathbb{Q}$.

Problem 5.8. Let $f(n) = 0$ for every n. Let $g(n) = \frac{1}{(n+1)^2}$. Show that both are Cauchy sequences, and indeed that the limit of both functions is 0, so that also $f \sim_{\mathbb{R}} g$.

Having done this, we shall as usual write $[f]_{\eqsim}$ for the equivalence class with f as an element. However, to keep things readable, in what follows we will

[5] Compare this with the definition of $\lim_{x\to\infty} f(x) = 0$ in **??**.

drop the subscript and write just $[f]$. We also stipulate that, for each $q \in \mathbb{Q}$, we have $q_{\mathbb{R}} = [c_q]$, where c_q is the constant function $c_q(n) = q$ for all $n \in \mathbb{N}$. We then define basic relations and operations on the reals, e.g.:

$$[f] + [g] = [(f + g)]$$
$$[f] \times [g] = [(f \times g)]$$

where $(f+g)(n) = f(n)+g(n)$ and $(f \times g)(n) = f(n) \times g(n)$. Of course, we also need to check that each of $(f + g)$, $(f - g)$ and $(f \times g)$ are Cauchy sequences when f and g are; but they are, and we leave this to you.

Finally, we define we a notion of order. Say $[f]$ is *positive* iff both $[f] \neq 0_{\mathbb{Q}}$ and $(\exists \ell \in \mathbb{N})(\forall n > \ell) 0 < f(n)$. Then say $[f] < [g]$ iff $[(g - f)]$ is positive. We have to check that this is well-defined (i.e., that it does not depend upon choice of "representative" function from the equivalence class). But having done this, it is quite easy to show that these yield the right algebraic properties; that is:

sfr:arith:cauchy: thm:cauchyorderedfield

Theorem 5.11. *The Cauchy sequences constitute an* ordered field*.*

Proof. Exercise. □

Problem 5.9. Prove that the Cauchy sequences constitute an ordered field.

It is harder to prove that the reals, so constructed, have the Completeness Property, so we will give the proof.

Theorem 5.12. *Every non-empty set of Cauchy sequences with an upper bound has a least upper bound.*

Proof sketch. Let S be any non-empty set of Cauchy sequences with an upper bound. So there is some $p \in \mathbb{Q}$ such that $p_{\mathbb{R}}$ is an upper bound for S. Let $r \in S$; then there is some $q \in \mathbb{Q}$ such that $q_{\mathbb{R}} < r$. So if a least upper bound on S exists, it is between $q_{\mathbb{R}}$ and $p_{\mathbb{R}}$ (inclusive).

We will hone in on the l.u.b., by approaching it simultaneously from below and above. In particular, we define two functions, $f, g \colon \mathbb{N} \to \mathbb{Q}$, with the aim that f will hone in on the l.u.b. from above, and g will hone on in it from below. We start by defining:

$$f(0) = p$$
$$g(0) = q$$

Then, where $a_n = \frac{f(n)+g(n)}{2}$, let:[6]

$$f(n+1) = \begin{cases} a_n & \text{if } (a_n)_{\mathbb{R}} \text{ is an upper bound for } S \\ f(n) & \text{otherwise} \end{cases}$$

$$g(n+1) = \begin{cases} a_n & \text{if } (a_n)_{\mathbb{R}} \text{ is a lower bound for } S \\ g(n) & \text{otherwise} \end{cases}$$

[6] This is a recursive definition. But we have not *yet* given any reason to think that recursive definitions are ok.

Both f and g are Cauchy sequences. (This can be checked fairly easily; but we leave it as an exercise.) Note that the function $(f - g)$ tends to 0, since the difference between f and g halves at every step. Hence $[f] = [g]$.

To show that $[f]$ is an upper bound for S, we will invoke Theorem 5.11. Let $[h] \in S$ and suppose, for reductio, that $[f] < [h]$, so that $0_{\mathbb{R}} < [(h - f)]$. Since f is a monotonically decreasing Cauchy sequence, there is some $k \in \mathbb{N}$ such that $[(c_{f(k)} - f)] < [(h - f)]$. So:

$$(f(k))_{\mathbb{R}} = [c_{f(k)}] < [f] + [(h - f)] = [h],$$

contradicting the fact that $(f(k)_{\mathbb{R}})$ is, by construction, an upper bound for S.

In an exactly similar way, we can show that $[g]$ is a lower bound for S. So $[f] = [g]$ is the *least* upper bound for S. □

Chapter 6

Infinite Sets

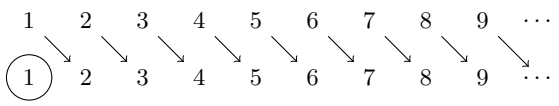
This chapter on infinite sets is taken from Tim Button's *Open Set Theory*.

6.1 Hilbert's Hotel

sfr:infinite:hilbert:sec

The set of the natural numbers is obviously infinite. So, if we do not want to *help ourselves* to the natural numbers, our first step must be characterize an infinite set in terms that do not require mentioning the natural numbers themselves. Here is a nice approach, presented by Hilbert in a lecture from 1924. He asks us to imagine

> [...] a hotel with a finite number of rooms. All of these rooms should be occupied by exactly one guest. If the guests now swap their rooms somehow, [but] so that each room still contains no more than one person, then no rooms will become free, and the hotel-owner cannot in this way create a new place for a newly arriving guest [...¶...]
>
> Now we stipulate that the hotel shall have infinitely many numbered rooms 1, 2, 3, 4, 5, ..., each of which is occupied by exactly one guest. As soon as a new guest comes along, the owner only needs to move each of the old guests into the room associated with the number one higher, and room 1 will be free for the newly-arriving guest.



(published in Hilbert 2013, 730; translation by Tim Button)

The crucial point is that Hilbert's Hotel has infinitely many rooms; and we can take his explanation to define what it means to say this. Indeed, this was Dedekind's approach (presented here, of course, with massive anachronism; Dedekind's definition is from 1888):

Definition 6.1. A set A is *Dedekind infinite* iff there is an injection from A to a proper subset of A. That is, there is some $o \in A$ and an injection $f : A \to A$ such that $o \notin \mathrm{ran}(f)$. sfr:infinite:hilbert:defn:DedekindInfinite

6.2 Dedekind Algebras

We not only want natural numbers to be infinite; we want them to have certain (algebraic) properties: they need to behave well under addition, multiplication, and so forth. sfr:infinite:dedekind:sec

Dedekind's idea was to take the idea of the *successor function* as basic, and then characterise the numbers as those with the following properties:

1. There is a number, 0, which is not the successor of any number
   i.e., $0 \notin \mathrm{ran}(s)$
   i.e., $\forall x\ s(x) \neq 0$

2. Distinct numbers have distinct successors
   i.e., s is an injection
   i.e., $\forall x \forall y (s(x) = s(y) \to x = y)$

3. Every number is obtained from 0 by repeated applications of the successor function. sfr:infinite:dedekind:repeatedapplication

The first two conditions are easy to deal with using first-order logic (see above). But we cannot deal with (3) just using first-order logic. Dedekind's breakthrough was to reformulate condition (3), set-theoretically, as follows:

3′. The natural numbers are the smallest set that is *closed under the successor function*: that is, if we apply s to any element of the set, we obtain another element of the set.

But we shall need to spell this out slowly.

Definition 6.2. For any function f, the set X is *f-closed* iff $(\forall x \in X) f(x) \in X$. Now define, for any o: sfr:infinite:dedekind:Closure

$$\mathrm{clo}_f(o) = \bigcap \{X : o \in X \text{ and } X \text{ is } f\text{-closed}\}$$

So $\mathrm{clo}_f(o)$ is the intersection of all the f-closed sets with o as an element. Intuitively, then, $\mathrm{clo}_f(o)$ is the *smallest* f-closed set with o as an element. This next result makes that intuitive thought precise;

Lemma 6.3. *For any function f and any $o \in A$:* *sfr:infinite:dedekind:closureproperties*

sfr:infinite:dedekind: closurehaselem
1. $o \in \mathrm{clo}_f(o)$; *and*

sfr:infinite:dedekind: closureclosed
2. $\mathrm{clo}_f(o)$ *is* f*-closed; and*

sfr:infinite:dedekind: closuresmallest
3. *if* X *is* f*-closed and* $o \in X$*, then* $\mathrm{clo}_f(o) \subseteq X$

Proof. Note that there is at least one f-closed set, namely $\mathrm{ran}(f) \cup \{o\}$. So $\mathrm{clo}_f(o)$, the intersection of *all* such sets, exists. We must now check (1)–(3).

(1). $o \in \mathrm{clo}_f(o)$ as it is an intersection of sets which all have o as an element.

(2). Let X be f-closed with $o \in X$. If $x \in \mathrm{clo}_f(o)$, then $x \in X$, and now $f(x) \in X$ as X is f-closed, so $f(x) \in \mathrm{clo}_f(o)$.

(3). This follows from the general fact that if $X \in C$ then $\bigcap C \subseteq X$. □

Using this, we can say:

Definition 6.4. A *Dedekind algebra* is a set A together with a function $f\colon A \to A$ and some $o \in A$ such that:

sfr:infinite:dedekind: ded:proper
1. $o \notin \mathrm{ran}(f)$

sfr:infinite:dedekind: ded:injection
2. f is an injection

sfr:infinite:dedekind: ded:closure
3. $A = \mathrm{clo}_f(o)$

Since $A = \mathrm{clo}_f(o)$, our earlier result tells us that A is the smallest f-closed set with o as an element. Clearly a Dedekind algebra is Dedekind infinite; just look at clauses (1) and (2) of the definition. But the more exciting fact is that any Dedekind infinite set can be turned into a Dedekind algebra.

sfr:infinite:dedekind: thm:DedekindInfiniteAlgebra
Theorem 6.5. *If there is a Dedekind infinite set, then there is a Dedekind algebra.*

Proof. Let D be Dedekind infinite. So there is an injection $g\colon D \to D$ and an element $o \in D \setminus \mathrm{ran}(g)$. Now let $A = \mathrm{clo}_g(o)$, and note that $o \in A$. Let $f = g\restriction_A$. We will show that this constitutes a Dedekind algebra.

Concerning (1): $o \notin \mathrm{ran}(g)$ and $\mathrm{ran}(f) \subseteq \mathrm{ran}(g)$ so $o \notin \mathrm{ran}(f)$.

Concerning (2): g is an injection on D; so $f \subseteq g$ must be an injection.

Concerning (3): Let $o \in B$. By Lemma 6.3, if $B \subsetneq A$, then B is not g-closed. So B is not f-closed either, as $f = g\restriction_A$. So A is the *smallest* f-closed set with o as an element, i.e., $A = \mathrm{clo}_f(o)$. □

6.3 Dedekind Algebras and Arithmetical Induction

sfr:infinite:induction: sec
Crucially, now, a Dedekind algebra—indeed, *any* Dedekind algebra—will serve as a surrogate for the natural numbers. This is thanks to the following trivial consequence:

sfr:infinite:induction: thm:dedinfiniteinduction
Theorem 6.6 (Arithmetical induction). *Let* N, s, o *yield a Dedekind algebra. Then for any set* X*:*

if $o \in X$ *and* $(\forall n \in N \cap X)s(n) \in X$*, then* $N \subseteq X$*.*

Proof. By the definition of a Dedekind algebra, $N = \mathrm{clo}_s(o)$. Now if both $o \in X$ and $(\forall n \in N)(n \in X \to s(n) \in X)$, then $N = \mathrm{clo}_s(o) \subseteq X$. □

Since induction is characteristic of the natural numbers, the point is this. Given any Dedekind infinite set, we can form a Dedekind algebra, and use that algebra as our surrogate for the natural numbers.

Admittedly, Theorem 6.6 formulates induction in *set-theoretic* terms. But we can easily put the principle in terms which might be more familiar:

Corollary 6.7. *Let* N, s, o *yield a Dedekind algebra. Then for any formula* $\varphi(x)$*, which may have parameters:* *sfr:infinite:induction:natinductionschema*

$$\text{if } \varphi(o) \text{ and } (\forall n \in N)(\varphi(n) \to \varphi(s(n))), \text{ then } (\forall n \in N)\varphi(n)$$

Proof. Let $X = \{n \in N : \varphi(n)\}$, and now use Theorem 6.6 □

In this result, we spoke of a formula "having parameters". What this means, roughly, is that for any objects $c_1, \ldots, c_n$, we can work with $\varphi(x, c_1, \ldots, c_k)$. More precisely, we can state the result without mentioning "parameters" as follows. For any formula $\varphi(x, v_1, \ldots, v_k)$, whose free variables are all displayed, we have:

$$\begin{aligned}\forall v_1 \ldots \forall v_k((&\varphi(o, v_1, \ldots, v_k) \wedge \\ &(\forall x \in N)(\varphi(x, v_1, \ldots, v_k) \to \varphi(s(x), v_1, \ldots, v_k))) \to \\ &(\forall x \in N)\varphi(x, v_1, \ldots, v_k))\end{aligned}$$

Evidently, speaking of "having parameters" can make things much easier to read. (In **??**, we will use this device rather frequently.)

Returning to Dedekind algebras: given any Dedekind algebra, we can also define the usual arithmetical functions of addition, multiplication and exponentiation. This is non-trivial, however, and it involves the technique of *recursive definition*. That is a technique which we shall introduce and justify much later, and in a much more general context. (Enthusiasts might want to revisit this after **??**, or perhaps read an alternative treatment, such as Potter 2004, pp. 95–8.) But, where N, s, o yield a Dedekind algebra, we will ultimately be able to stipulate the following:

$$\begin{array}{lll} m + o = m & m \times o = o & m^o = s(o) \\ m + s(n) = s(m + n) & m \times s(n) = (m \times n) + m & m^{s(n)} = m^n \times m \end{array}$$

and show that these behave as one would hope.

6.4 Dedekind's "Proof" of the Existence of an Infinite Set

sfr:infinite:dedekindsproof:sec

In this chapter, we have offered a set-theoretic treatment of the natural numbers, in terms of Dedekind algebras. In section 5.5, we reflected on the philosophical significance of the arithmetisation of analysis (among other things). Now we should reflect on the significance of what we have achieved here.

Throughout chapter 5, we took the natural numbers as given, and used them to construct the integers, rationals, and reals, explicitly. In this chapter, we have not given an explicit construction of the natural numbers. We have just shown that, *given any Dedekind infinite set*, we can define a set which will behave just like we want $\mathbb{N}$ to behave.

Obviously, then, we cannot claim to have answered a metaphysical question, such as *which objects are the natural numbers*. But that's a good thing. After all, in section 5.5, we emphasized that we would be wrong to think of the definition of $\mathbb{R}$ as the set of Dedekind cuts as a *discovery*, rather than a convenient stipulation. The crucial observation is that the Dedekind cuts exemplify the same key mathematical properties as the real numbers. So too here: the crucial observation is that *any* Dedekind algebra exemplifies the key mathematical properties as the natural numbers. (Indeed, Dedekind pushed this point home by proving that all Dedekind algebras are *isomorphic* (1888, Theorems 132–3). It is no surprise, then, that many contemporary "structuralists" cite Dedekind as a forerunner.)

Moreover, we have shown how to embed the theory of the natural numbers into a naïve simple set theory, which itself still remains rather informal, but which doesn't (apparently) assume the natural numbers as given. So, we may be on the way to realising Dedekind's own ambitious project, which he explained thus:

> In science nothing capable of proof ought to be believed without proof. Though this demand seems reasonable, I cannot regard it as having been met even in the most recent methods of laying the foundations of the simplest science; viz., that part of logic which deals with the theory of numbers. In speaking of arithmetic (algebra, analysis) as merely a part of logic I mean to imply that I consider the number-concept entirely independent of the notions or intuitions of space and time—that I rather consider it an immediate product of the pure laws of thought. (Dedekind, 1888, preface)

Dedekind's bold idea is this. We have just shown how to build the natural numbers using (naïve) set theory alone. In chapter 5, we saw how to construct the reals given the natural numbers and some set theory. So, perhaps, "arithmetic (algebra, analysis)" turn out to be "merely a part of logic" (in Dedekind's extended sense of the word "logic").

That's the idea. But hold on for a moment. Our construction of a Dedekind algebra (our surrogate for the natural numbers) is conditional on the existence

of a Dedekind infinite set. (Just look back to Theorem 6.5.) Unless the existence of a Dedekind infinite set can be established via "logic" or "the pure laws of thought", the project stalls.

So, *can* the existence of a Dedekind infinite set be established by "the pure laws of thought"? Here was Dedekind's effort:

> My own realm of thoughts, i.e., the totality S of all things which can be objects of my thought, is infinite. For if s signifies an element of S, then the thought s' that s can be an object of my thought, is itself an element of S. If we regard this as an image $\varphi(s)$ of the element s, then ... S is [Dedekind] infinite, which was to be proved. (Dedekind, 1888, §66)

This is quite an astonishing thing to find in the middle of a book which largely consists of highly rigorous mathematical proofs. Two remarks are worth making.

First: this "proof" scarcely has what we would now recognize as a "mathematical" character. It speaks of psychological objects (thoughts), and merely *possible* ones at that.

Second: at least as we have presented Dedekind algebras, this "proof" has a straightforward technical shortcoming. If Dedekind's argument is successful, it establishes only that there are infinitely many things (specifically, infinitely many thoughts). But Dedekind also needs to give us a reason to regard S as a single *set*, with infinitely many elements, rather than thinking of S as *some things* (in the plural).

The fact that Dedekind did not see a gap here might suggest that his use of the word "totality" does not precisely track *our* use of the word "set".[1] But this would not be too surprising. The project we have pursued in the last two chapters—a "construction" of the naturals, and from them a "construction" of the integers, reals and rationals—has all been carried out naïvely. We have helped ourselves to this set, or that set, as and when we have needed them, without laying down many general principles concerning exactly which sets exist, and when. But we know that we need *some* general principles, for otherwise we will fall into Russell's Paradox.

The time has come for us to outgrow our naïvety.

6.5 A Proof of Schröder-Bernstein

sfr:infinite:card-sb:sec

Before we depart from naïve set theory, we have one last naïve (but sophisticated!) proof to consider. This is a proof of Schröder-Bernstein (Theorem 4.25): if $A \preceq B$ and $B \preceq A$ then $A \approx B$; i.e., given injections $f\colon A \to B$ and $g\colon B \to A$ there is a bijection $h\colon A \to B$.

In this chapter, we followed Dedekind's notion of *closures*. In fact, Dedekind provided a lovely proof of using this notion, and we will present it here. The

[1] Indeed, we have other reasons to think it did not; see e.g., Potter (2004, p. 23).

proof closely follows Potter (2004, pp. 157–8), if you want a slightly different but essentially similar treatment. A little googling will also convince you that this is a theorem—rather like the irrationality of $\sqrt{2}$—for which *many* interesting and different proofs exist.

Using similar notation as Definition 6.2, let

$$\mathrm{Clo}_f(B) = \bigcap\{X : B \subseteq X \text{ and } X \text{ is } f\text{-closed}\}$$

for each set B and function f. Defined thus, $\mathrm{Clo}_f(B)$ is the smallest f-closed set containing B, in that:

sfr:infinite:card-sb: Closureprops

Proposition 6.8. *For any function f, and any B:*

sfr:infinite:card-sb: Closurehaselem

1. *$B \subseteq \mathrm{Clo}_f(B)$; and*

sfr:infinite:card-sb: Closureclosed

2. *$\mathrm{Clo}_f(B)$ is f-closed; and*

sfr:infinite:card-sb: Closuresmallest

3. *if X is f-closed and $B \subseteq X$, then $\mathrm{Clo}_f(B) \subseteq X$.*

Proof. Exactly as in Lemma 6.3. □

We need one last fact to get to Bernstein:

sfr:infinite:card-sb: sbhelper

Proposition 6.9. *If $A \subseteq B \subseteq C$ and $A \approx C$, then $A \approx B \approx C$.*

Proof. Given a bijection $f : C \to A$, let $F = \mathrm{Clo}_f(C \setminus B)$ and define a function g with domain C as follows:

$$g(x) = \begin{cases} f(x) & \text{if } x \in F \\ x & \text{otherwise} \end{cases}$$

We'll show that g is a bijection from $C \to B$, from which it will follow that $g \circ f^{-1} : A \to B$ is a bijection, completing the proof.

First we claim that if $x \in F$ but $y \notin F$ then $g(x) \neq g(y)$. For reductio suppose otherwise, so that $y = g(y) = g(x) = f(x)$. Since $x \in F$ and F is f-closed by Proposition 6.8, we have $y = f(x) \in F$, a contradiction.

Now suppose $g(x) = g(y)$. So, by the above, $x \in F$ iff $y \in F$. If $x, y \in F$, then $f(x) = g(x) = g(y) = f(y)$ so that $x = y$ since f is a bijection. If $x, y \notin F$, then $x = g(x) = g(y) = y$. So g is an injection.

It remains to show that $\mathrm{ran}(g) = B$. So fix $x \in B \subseteq C$. If $x \notin F$, then $g(x) = x$. If $x \in F$, then $x = f(y)$ for some $y \in F$, since $x \in B$ and F is the *smallest* f-closed set extending $C \setminus B$, so that $g(y) = f(y) = x$. □

Finally, here is the proof of the main result. Recall that given a function h and set D, we define $h[D] = \{h(x) : x \in D\}$.

Proof of Schröder-Berstein.. Let $f\colon A \to B$ and $g\colon B \to A$ be injections. Since $f[A] \subseteq B$ we have that $g[f[A]] \subseteq g[B] \subseteq A$. Also, $g \circ f\colon A \to g[f[A]]$ is an injection since both g and f are; and indeed $g \circ f$ is a bijection, just by the way we defined its codomain. So $A \approx g[f[A]]$, and hence by Proposition 6.9 there is a bijection $h\colon A \to g[B]$. Moreover, g^{-1} is a bijection $g[B] \to B$. So $g^{-1} \circ h\colon A \to B$ is a bijection. □

Photo Credits

Bibliography

Benacerraf, Paul. 1965. What numbers could not be. *The Philosophical Review* 74(1): 47–73.

Cantor, Georg. 1892. Über eine elementare Frage der Mannigfaltigkeitslehre. *Jahresbericht der deutschen Mathematiker-Vereinigung* 1: 75–8.

Conway, John. 2006. The power of mathematics. In *Power*, eds. Alan Blackwell and David MacKay, Darwin College Lectures. Cambridge: Cambridge University Press. URL `http://www.cs.toronto.edu/~mackay/conway.pdf`.

Dedekind, Richard. 1888. *Was sind und was sollen die Zahlen?* Braunschweig: Vieweg.

Frege, Gottlob. 1884. *Die Grundlagen der Arithmetik: Eine logisch mathematische Untersuchung über den Begriff der Zahl*. Breslau: Wilhelm Koebner. Translation in Frege (1953).

Frege, Gottlob. 1953. *Foundations of Arithmetic*, ed. J. L. Austin. Oxford: Basil Blackwell & Mott, 2nd ed.

Hilbert, David. 2013. *David Hilbert's Lectures on the Foundations of Arithmetic and Logic 1917–1933*, eds. William Bragg Ewald and Wilfried Sieg. Heidelberg: Springer.

Katz, Karin Usadi and Mikhail G. Katz. 2012. Stevin numbers and reality. *Foundations of Science* 17(2): 109–23.

O'Connor, John J. and Edmund F. Robertson. 2005. The real numbers: Stevin to Hilbert URL `http://www-history.mcs.st-and.ac.uk/HistTopics/Real_numbers_2.html`.

Potter, Michael. 2004. *Set Theory and its Philosophy*. Oxford: Oxford University Press.