Chapter udf

The Size of Sets

siz.1 Introduction

sfr:siz:int:sec

When Georg Cantor developed set theory in the 1870s, his interest was in part to make palatable the idea of an infinite collection—an actual infinity, as the medievals would say. Key to this rehabilitation of the notion of the infinite was a way to assign sizes—"cardinalities"—to sets. The cardinality of a finite set is just a natural number, e.g., $\emptyset$ has cardinality 0, and a set containing five things has cardinality 5. But what about infinite sets? Do they all have the same cardinality, ∞? It turns out, they do 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 was that some infinite sets are not enumerable.

siz.2 Enumerable Sets

sfr:siz:enm:sec

One way of specifying a finite set is by listing its elements. But conversely, since there are only finitely many elements in a set, every finite set can be enumerated. By this we mean: its elements can be put into a list (a list with a beginning, where each element of the list other than the first has a unique predecessor). Some infinite sets can also be enumerated, such as the set of positive integers.

Definition siz.1 (Enumeration)**.** Informally, an *enumeration* of a set X is a list (possibly infinite) of elements of X such that every element of X appears on the list at some finite position. If X has an enumeration, then X is said to be *enumerable*. If X is enumerable and infinite, we say X is denumerable.

A couple of points about enumerations: explanation

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 pre-

ceding 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 X 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. Lists may be gappy: 2, −, 4, −, 6, −, ... enumerates the even positive integers.

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

Proposition siz.2. *If X has an enumeration, it has an enumeration without gaps or repetitions.*

Proof. Suppose X has an enumeration $x_1, x_2, \ldots$ in which each x_i is an element of X or a gap. We can remove repetitions from an enumeration by replacing repeated elements by gaps. For instance, we can turn the enumeration into a new one in which x'_i is x_i if x_i is an element of X that is not among $x_1, \ldots, x_{i-1}$ or is $-$ if it is. We can remove gaps by closing up the elements in the list. To make precise what "closing up" amounts to is a bit difficult to describe. Roughly, it means that we can generate a new enumeration $x''_1, x''_2, \ldots$, where each x''_i is the first element in the enumeration $x'_1, x'_2, \ldots$ after x''_{i-1} (if there is one). □

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 siz.3 (Enumeration)**.** An *enumeration* of a set X is any surjective function $f\colon \mathbb{Z}^+ \to X$.

explanation

Let's convince ourselves that the formal definition and the informal definition using a possibly gappy, possibly infinite list are equivalent. A surjective function (partial or total) from $\mathbb{Z}^+$ to a set X enumerates X. 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 X is guaranteed to be the value of $f(n)$ for some $n \in \mathbb{Z}^+$. Hence, every element of X 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 X, we can define a surjective function $f\colon \mathbb{Z}^+ \to X$ by letting $f(n)$ be the nth element of the list that is not a gap, or the final element of the list if there is no nth element. There is one case in which this does not produce a surjective function: if X is empty, and hence the list is empty. So, every non-empty list determines a surjective function $f\colon \mathbb{Z}^+ \to X$.

sfr:siz:enm: defn:enumerable

Definition siz.4. A set X is enumerable iff it is empty or has an enumeration.

Example siz.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 $g(n) = n - 1$.

Problem siz.1. According to Definition siz.4, a set X is enumerable iff $X = \emptyset$ or there is a surjective $f\colon \mathbb{Z}^+ \to X$. It is also possible to define "enumerable set" precisely by: a set is enumerable iff there is an injective function $g\colon X \to \mathbb{Z}^+$. Show that the definitions are equivalent, i.e., show that there is an injective function $g\colon X \to \mathbb{Z}^+$ iff either $X = \emptyset$ or there is a surjective $f\colon \mathbb{Z}^+ \to X$.

Example siz.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 siz.2. Define an enumeration of the positive squares 4, 9, 16, ...

Example siz.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 siz.3. Show that if X and Y are enumerable, so is $X \cup Y$.

Problem siz.4. Show by induction on n that if X_1, X_2, ..., X_n are all enumerable, so is $X_1 \cup \cdots \cup X_n$.

explanation

That is fine for "easy" sets. What about the set of, say, pairs of positive integers?

$$\mathbb{Z}^+ \times \mathbb{Z}^+ = \{\langle n, m\rangle : n, m \in \mathbb{Z}^+\}$$

We can organize the pairs of positive integers in an *array*, such as the following:

	1	**2**	**3**	**4**	...
1	$\langle 1,1\rangle$	$\langle 1,2\rangle$	$\langle 1,3\rangle$	$\langle 1,4\rangle$	...
2	$\langle 2,1\rangle$	$\langle 2,2\rangle$	$\langle 2,3\rangle$	$\langle 2,4\rangle$	...
3	$\langle 3,1\rangle$	$\langle 3,2\rangle$	$\langle 3,3\rangle$	$\langle 3,4\rangle$	...
4	$\langle 4,1\rangle$	$\langle 4,2\rangle$	$\langle 4,3\rangle$	$\langle 4,4\rangle$	...
⋮	⋮	⋮	⋮	⋮	⋱

Clearly, every ordered pair in $\mathbb{Z}^+ \times \mathbb{Z}^+$ will appear exactly once in the array. In particular, $\langle n, m\rangle$ will appear in the nth column and mth row. But how do we organize the elements of such an array into a one-way list? The pattern in the array below demonstrates one way to do this:

	1	2	4	7	...
	3	5	8	...	...
	6	9	...	...	...
	10	...	...	...	...
	⋮	⋮	⋮	⋮	⋱

This pattern is called *Cantor's zig-zag method*. Other patterns are perfectly permissible, as long as they "zig-zag" through every cell of the array. By Cantor's zig-zag method, the enumeration for $\mathbb{Z}^+ \times \mathbb{Z}^+$ according to this scheme would be:

$$\langle 1,1\rangle, \langle 1,2\rangle, \langle 2,1\rangle, \langle 1,3\rangle, \langle 2,2\rangle, \langle 3,1\rangle, \langle 1,4\rangle, \langle 2,3\rangle, \langle 3,2\rangle, \langle 4,1\rangle, \ldots$$

What ought we do about enumerating, say, the set of ordered triples of positive integers?

$$\mathbb{Z}^+ \times \mathbb{Z}^+ \times \mathbb{Z}^+ = \{\langle n, m, k\rangle : n, m, k \in \mathbb{Z}^+\}$$

We can think of $\mathbb{Z}^+ \times \mathbb{Z}^+ \times \mathbb{Z}^+$ as the Cartesian product of $\mathbb{Z}^+ \times \mathbb{Z}^+$ and $\mathbb{Z}^+$, that is,

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

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

	1	**2**	**3**	**4**	...
$\langle \mathbf{1}, \mathbf{1}\rangle$	$\langle 1,1,1\rangle$	$\langle 1,1,2\rangle$	$\langle 1,1,3\rangle$	$\langle 1,1,4\rangle$	...
$\langle \mathbf{1}, \mathbf{2}\rangle$	$\langle 1,2,1\rangle$	$\langle 1,2,2\rangle$	$\langle 1,2,3\rangle$	$\langle 1,2,4\rangle$	...
$\langle \mathbf{2}, \mathbf{1}\rangle$	$\langle 2,1,1\rangle$	$\langle 2,1,2\rangle$	$\langle 2,1,3\rangle$	$\langle 2,1,4\rangle$	...
$\langle \mathbf{1}, \mathbf{3}\rangle$	$\langle 1,3,1\rangle$	$\langle 1,3,2\rangle$	$\langle 1,3,3\rangle$	$\langle 1,3,4\rangle$	...
⋮	⋮	⋮	⋮	⋮	⋱

Thus, by using a method like Cantor's zig-zag method, we may similarly obtain an enumeration of $(\mathbb{Z}^+)^3$.

Cantor's zig-zag method makes the enumerability of $(\mathbb{Z}^+)^2$ (and analogously, $(\mathbb{Z}^+)^3$, etc.) visually evident. Following the zig-zag line in the array and counting the places, we can tell that $\langle 2, 3\rangle$ is at place 8, but specifying the inverse $g\colon (\mathbb{Z}^+)^2 \to \mathbb{Z}^+$ of the zig-zag enumeration such that

$$g(\langle 1,1\rangle) = 1, \quad g(\langle 1,2\rangle) = 2, \quad g(\langle 2,1\rangle) = 3, \quad \ldots \quad g(\langle 2,3\rangle) = 8, \quad \ldots$$

would be helpful. To calculate the position of each pair in the enumeration, we can use the function below. (The exact derivation of the function is somewhat messy, so we are skipping it here.)

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

Accordingly, the pair $\langle 2, 3\rangle$ is in position $((2+3-2)(2+3-1)/2)+2 = (3\cdot 4/2)+2 = (12/2)+2 = 8$; pair $\langle 3, 7\rangle$ is in position $((3+7-2)(3+7-1)/2)+3 = 39$.

Functions like g above, i.e., inverses of enumerations of sets of pairs, are called *pairing functions*.

Definition siz.8 (Pairing function)**.** A function $f\colon X \times Y \to \mathbb{Z}^+$ is an arithmetical *pairing function* if f is total and injective. We also say that f *encodes* $X \times Y$, and that for $f(\langle x, y\rangle) = n$, n is the *code* for $\langle x, y\rangle$.

The idea is that we can use such functions to encode, e.g., pairs of positive integers in $\mathbb{Z}^+$, or, in other words, represent pairs of positive integers as positive integers. Using the inverse of the pairing function, we can *decode* the integer, i.e., find out which pair of positive integers is represented. explanation

There are other enumerations of $(\mathbb{Z}^+)^2$ 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 1 in the first place (i.e., pairs $\langle 1, m\rangle$), put the first (i.e., $\langle 1, 1\rangle$) in the first empty place, then skip an empty space, put the second (i.e., $\langle 1, 2\rangle$) in the next empty place, skip one again, and so forth. The (incomplete) beginning of our enumeration now looks like this

$f(1)$	$f(2)$	$f(3)$	$f(4)$	$f(5)$	$f(6)$	$f(7)$	$f(8)$	$f(9)$	$f(10)$	$\dots$
$\langle 1, 1\rangle$		$\langle 1, 2\rangle$		$\langle 1, 3\rangle$		$\langle 1, 4\rangle$		$\langle 1, 5\rangle$		$\dots$

Repeat this with pairs $\langle 2, m\rangle$ for the place that still remain empty, again skipping every other empty place:

$f(1)$	$f(2)$	$f(3)$	$f(4)$	$f(5)$	$f(6)$	$f(7)$	$f(8)$	$f(9)$	$f(10)$	$\dots$
$\langle 1, 1\rangle$	$\langle 2, 1\rangle$	$\langle 1, 2\rangle$		$\langle 1, 3\rangle$	$\langle 2, 2\rangle$	$\langle 1, 4\rangle$		$\langle 1, 5\rangle$	$\langle 2, 3\rangle$	$\dots$

Enter pairs $\langle 3, m\rangle$, $\langle 4, m\rangle$, etc., in the same way. Our completed enumeration thus starts like this:

$f(1)$	$f(2)$	$f(3)$	$f(4)$	$f(5)$	$f(6)$	$f(7)$	$f(8)$	$f(9)$	$f(10)$	$\dots$
$\langle 1, 1\rangle$	$\langle 2, 1\rangle$	$\langle 1, 2\rangle$	$\langle 3, 1\rangle$	$\langle 1, 3\rangle$	$\langle 2, 2\rangle$	$\langle 1, 4\rangle$	$\langle 4, 1\rangle$	$\langle 1, 5\rangle$	$\langle 2, 3\rangle$	$\dots$

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:

	1	**2**	**3**	**4**	**5**	**6**	$\dots$
1	1	3	5	7	9	11	$\dots$
2	2	6	10	14	18	$\dots$	$\dots$
3	4	12	20	28	$\dots$	$\dots$	$\dots$
4	8	24	40	$\dots$	$\dots$	$\dots$	$\dots$
5	16	48	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
6	32	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

We can see that the pairs in the first row are in the odd numbered places of our enumeration, i.e., pair $\langle 1, m\rangle$ 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, $\langle 1, m\rangle$, 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, $1, 2, 4, 8, \dots$, are powers of 2: $2^0, 2^1, 2^2, 2^3, \dots$ In fact, the relevant exponent is one less than the first member of the pair in question. Thus, for pair $\langle n, m\rangle$ the factor is $n-1$. This gives us the general formula: $2^{n-1} \cdot (2m-1)$, and hence:

Example siz.9. The function $f\colon (\mathbb{Z}^+)^2 \to \mathbb{Z}^+$ given by

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

is a pairing function for the set of pairs of positive integers $(\mathbb{Z}^+)^2$.

Accordingly, in our second enumeration of $(\mathbb{Z}^+)^2$, the pair $\langle 2,3\rangle$ is in position $2^{2-1}\cdot(2\cdot 3-1) = 2\cdot 5 = 10$; pair $\langle 3,7\rangle$ is in position $2^{3-1}\cdot(2\cdot 7-1) = 52$. explanation

Another common pairing function that encodes $(\mathbb{Z}^+)^2$ is the following:

Example siz.10. The function $f\colon (\mathbb{Z}^+)^2 \to \mathbb{Z}^+$ given by

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

is a pairing function for the set of pairs of positive integers $(\mathbb{Z}^+)^2$.

j is injective, but nor surjective. That means the inverse of j is a partial, surjective function, and hence an enumeration of $(\mathbb{Z}^+)^2$. (Exercise.) explanation

Problem siz.5. Give an enumeration of the set of all positive rational numbers. (A positive rational number is one that can be written as a fraction n/m with $n, m \in \mathbb{Z}^+$).

Problem siz.6. Show that $\mathbb{Q}$ is enumerable. (A rational number is one that can be written as a fraction z/m with $z \in \mathbb{Z}$, $m \in \mathbb{Z}^+$).

Problem siz.7. Define an enumeration of $\mathbb{B}^*$.

Problem siz.8. 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 siz.9. Show that the set of all finite subsets of an arbitrary infinite enumerable set is enumerable.

Problem siz.10. A set of positive integers is said to be *cofinite* iff it is the complement of a finite set of positive integers. Let I be the set that contains all the finite and cofinite sets of positive integers. Show that I is enumerable.

Problem siz.11. Show that the enumerable union of enumerable sets is enumerable. That is, whenever X_1, X_2, ... are sets, and each X_i is enumerable, then the union $\bigcup_{i=1}^{\infty} X_i$ of all of them is also enumerable.

Problem siz.12. Let $f : X \times Y \to \mathbb{Z}^+$ be an arbitrary pairing function. Show that the inverse of f is an enumeration of $X \times Y$.

Problem siz.13. Specify a function that encodes $\mathbb{N}^3$.

siz.3 Non-enumerable Sets

sfr:siz:nen:sec

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 X there is a surjective function $f\colon \mathbb{Z}^+ \to X$. If a set is non-enumerable there is no such function. That is, no function mapping the infinitely many elements of $\mathbb{Z}^+$ to X can exhaust all of X. So there are "more" elements of X 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 X cannot be enumerated in a one way infinite list. The best way to do this is to show that every list of elements of X must leave at least one element out; or that no function $f\colon \mathbb{Z}^+ \to X$ can be surjective. We can do this using Cantor's *diagonal method*. Given a list of elements of X, say, $x_1, x_2, \ldots$, we construct another element of X 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 siz.11. *$\mathbb{B}^\omega$ 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 $s_1, s_2, s_3, s_4, \ldots$ 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 $s_1, s_2, \ldots$; 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 $s_1, s_2, \ldots$. 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 1

to a 0. 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 a non-gappy 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 siz.12. *$\wp(\mathbb{Z}^+)$ 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 $\{1, 2, 3, \dots\}$, $\{2, 4, 6, \dots\}$, $\{1, 2, 5\}$, and $\{3, 4, 5, \dots\}$. Then the array would begin with

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

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 siz.14. Show that $\wp(\mathbb{N})$ is non-enumerable by a diagonal argument.

Problem siz.15. Show that the set of functions $f\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ is non-enumerable by an explicit diagonal argument. That is, show that if f_1, f_2, ..., is a list of functions and each $f_i\colon \mathbb{Z}^+ \to \mathbb{Z}^+$, then there is some $\overline{f}\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ not on this list.

siz.4 Reduction

sfr:siz:red:sec

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

Problem siz.16. Show that if there is an injective function $g\colon Y \to X$, and Y is non-enumerable, then so is X. Do this by showing how you can use g to turn an enumeration of X into one of Y.

Proof of Theorem siz.12 by reduction. Suppose that $\wp(\mathbb{Z}^+)$ were enumerable, and thus that there is an enumeration of it, Z_1, Z_2, Z_3, ...

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 $2\mathbb{Z}^+ = \{2, 4, 6, \dots\}$ of positive even numbers gets mapped to the sequence $010101\dots$, the empty set gets mapped to $0000\dots$ and the set $\mathbb{Z}^+$ itself to $1111\dots$.

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

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

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 $\wp(\mathbb{Z}^+)$ were enumerable, $\mathbb{B}^\omega$ would be enumerable. But $\mathbb{B}^\omega$ is non-enumerable (Theorem siz.11). Hence $\wp(\mathbb{Z}^+)$ is non-enumerable. □

explanation

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

$$h(n) = \underbrace{000\dots0}_{n\text{ 0's}}$$

is a function, but $\mathbb{Z}^+$ is enumerable.

Problem siz.17. Show that the set of all *sets of* pairs of positive integers is non-enumerable by a reduction argument.

Problem siz.18. Show that $\mathbb{N}^\omega$, the set of infinite sequences of natural numbers, is non-enumerable by a reduction argument.

Problem siz.19. 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 siz.20. 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 siz.21. Show that the set $\mathbb{R}$ of all real numbers is non-enumerable.

set.5 Equinumerous Sets

intro

sfr:set: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 with defining when sets are the same size. Let's say sets of the same size are *equinumerous*. We want the formal notion of equinumerosity to correspond with our intuitive notion of "same size," hence the formal notion ought to satisfy the following properties:

Reflexivity: Every set is equinumerous with itself.

Symmetry: For any sets X and Y, if X is equinumerous with Y, then Y is equinumerous with X.

Transitivity: For any sets X, Y, and Z, if X is equinumerous with Y and Y is equinumerous with Z, then X is equinumerous with Z.

In other words, we want equinumerosity to be an *equivalence relation*.

Definition set.13. A set X is *equinumerous* with a set Y, $X \approx Y$, if and only if there is a bijective $f\colon X \to Y$.

Proposition set.14. *Equinumerosity defines an equivalence relation.*

Proof. Let X, Y, and Z be sets.

Reflexivity: Using the identity map $1_X\colon X \to X$, where $1_X(x) = x$ for all $x \in X$, we see that X is equinumerous with itself (clearly, 1_X is bijective).

Symmetry: Suppose that X is equinumerous with Y. Then there is a bijective $f\colon X \to Y$. Since f is bijective, its inverse f^{-1} exists and also bijective. Hence, $f^{-1}\colon Y \to X$ is a bijective function from Y to X, so Y is also equinumerous with X.

Transitivity: Suppose that X is equinumerous with Y via the bijective function $f\colon X \to Y$ and that Y is equinumerous with Z via the bijective function $g\colon Y \to Z$. Then the composition of $g \circ f\colon X \to Z$ is bijective, and X is thus equinumerous with Z.

Therefore, equinumerosity is an equivalence relation. □

Theorem set.15. *Suppose X and Y are equinumerous. Then X is enumerable if and only if Y is.*

Proof. Let X and Y be equinumerous. Suppose that X is enumerable. Then either $X = \emptyset$ or there is a surjective function $f\colon \mathbb{Z}^+ \to X$. Since X and Y are equinumerous, there is a bijective $g\colon X \to Y$. If $X = \emptyset$, then $Y = \emptyset$ also (otherwise there would be an element $y \in Y$ but no $x \in X$ with $g(x) = y$). If, on the other hand, $f\colon \mathbb{Z}^+ \to X$ is surjective, then $g \circ f\colon \mathbb{Z}^+ \to Y$ is surjective. To see this, let $y \in Y$. Since g is surjective, there is an $x \in X$ 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 Y, and so Y is enumerable. □

Problem set.22. Show that if X is equinumerous with U and and Y is equinumerous with V, and the intersections $X \cap Y$ and $U \cap V$ are empty, then the unions $X \cup Y$ and $U \cup V$ are equinumerous.

Problem set.23. Show that if X is infinite and enumerable, then it is equinumerous with the positive integers $\mathbb{Z}^+$.

siz.6 Comparing Sizes of Sets

sfr:siz:car:sec

Just like we were able to make precise when two sets have the same size in a way that also accounts for the size of infinite sets, we can also compare the sizes of sets in a precise way. Our definition of "is smaller than (or equinumerous)" will require, instead of a bijection between the sets, a total injective function 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 injective function 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. explanation

Definition siz.16. X is *no larger than* Y, $X \preceq Y$, if and only if there is an injective function $f\colon X \to Y$.

Theorem siz.17 (Schröder-Bernstein)**.** *Let X and Y be sets. If $X \preceq Y$ and $Y \preceq X$, then $X \approx Y$.*

In other words, if there is a total injective function from X to Y, and if there is a total injective function from Y back to X, then there is a total bijection from X to Y. Sometimes, it can be difficult to think of a bijection between two equinumerous sets, so the Schröder-Bernstein theorem allows us to break the comparison down into cases so we only have to think of an injection from explanation

the first to the second, and vice-versa. The Schröder-Bernstein theorem, apart from being convenient, justifies the act of discussing the "sizes" of sets, for it tells us that set cardinalities have the familiar anti-symmetric property that numbers have.

Definition siz.18. X is *smaller than* Y, $X \prec Y$, if and only if there is an injective function $f\colon X \to Y$ but no bijective $g\colon X \to Y$.

Theorem siz.19 (Cantor)**.** *For all X, $X \prec \wp(X)$.*

sfr:siz:car:thm:cantor

Proof. The function $f\colon X \to \wp(X)$ that maps any $x \in X$ to its singleton $\{x\}$ is injective, since if $x \neq y$ then also $f(x) = \{x\} \neq \{y\} = f(y)$.

There cannot be a surjective function $g\colon X \to \wp(X)$, let alone a bijective one. For suppose that $g\colon X \to \wp(X)$. Since g is total, every $x \in X$ is mapped to a subset $g(x) \subseteq X$. We show that g cannot be surjective. To do this, we define a subset $Y \subseteq X$ which by definition cannot be in the range of g. Let

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

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

explanation

It's instructive to compare the proof of Theorem siz.19 to that of Theorem siz.12. 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 and $\overline{Z}$ but not the other. We follow the same idea here, except the indices n are now elements of X instead of $\mathbb{Z}^+$. The set $\overline{Y}$ is defined so that it is different from $g(x)$ for each $x \in X$, because $x \in g(x)$ iff $x \notin \overline{Y}$. Again, there is always an element of X which is an element of one of $g(x)$ and $\overline{Y}$ but not the other. And just as $\overline{Z}$ therefore cannot be on the list Z_1, Z_2, ..., $\overline{Y}$ cannot be in the range of g.

Problem siz.24. Show that there cannot be an injective function $g\colon \wp(X) \to X$, for any set X. Hint: Suppose $g\colon \wp(X) \to X$ is injective. Then for each $x \in X$ there is at most one $Y \subseteq X$ such that $g(Y) = x$. Define a set $\overline{Y}$ such that for every $x \in X$, $g(\overline{Y}) \neq x$.

Photo Credits

Bibliography