Computer Science

Dr. Y. Liow (September 7, 2023)

Contents

debug: chap.tex

Chapter 7

Cantor set theory

7.1 Set cardinality, countability, and ordinals

Throughout this section, X is a set. Recall that I defined $|X|$ for finite sets, i.e., $|X|$ is the number of elements in X. $|X|$ is usually called the **size** or the **cardinality** of the set. Now I want to talk about infinite sets.

size
cardinality

Georg Cantor is usually considered the founder of modern set theory. He was the first to realized that although the idea of a set is simple, in fact other than finite sets, sets in general are very complex. Many of the concepts in this chapter was first defined by Richard Dedekind. But it was Cantor who realized their importance. Cantor and Dedekind were contemporary and were close friends and met frequently for discussion. But Dedekind acted more like a sounding board to Cantor's ideas. Cantor thoughts on set theory made him realized that when looking at infinite sets, it is still possible to differentiate between them. In other words, there are many different types of infinities. In a sense, this is somewhat similar to the study of functions: $f(x) = x$ and $g(x) = \ln x$ both go to infinity as x goes to infinity. But their order of growth are different. Cantor proved that there are not just different infinities, but there are *infinitely* many infinities! Cantor's contribution to set theory has important consequences to analysis, topology, logic, and Turing machines in the theory of automata and theoretical computational complexity. As a consequence of Cantor's work, you can for instance show that the set of C++ programs is countably infinite (I'll define this precisely later), but the set of boolean functions $\mathbb{N} \rightarrow \{0, 1\}$ is uncountably infinite. Note that both set are infinite but in different ways: there are more boolean functions $\mathbb{N} \rightarrow \{0, 1\}$ than there are C++ programs. Therefore Cantor's set theory tells you right away that there is a boolean function that cannot be computed by a C++ program.

Now ... on to infinite sets ...

Recall that a function $f : X \rightarrow Y$ is **one-to-one** (I'll write 1–1) or **injective** if $f(x) = f(x')$ implies $x = x'$. f is **onto** or **surjective** if for every $y \in Y$, there is some $x \in X$ such that $f(x) = y$. A **bijection** is a function that is both 1–1 and onto. If a function is a bijection I will say it is "1–1 and onto". A bijection is also called a **one-to-one correspondence**.

one-to-one
injective
onto
surjective
bijection
one-to-one correspondence

If we are going to only talk about finite sets then $|X| = |Y|$ means X and Y have the same number of distinct elements, $|X| < |Y|$ means that Y has strictly more elements than X. Etc. I'm going to generalize the above notions of $|X| = |Y|$, $|X| < |Y|$, $|X| \leq |Y|$ to include cases when X and Y are infinite.

Definition 7.1.1. Let X and Y be sets.

- We will write $|X| \leq |Y|$ if there is a 1–1 function $X \to Y$.
- If there is a bijection between X and Y, we write $|X| = |Y|$. If $|X| = |Y|$, I will also say that X and Y have the same **cardinality** or that they are **equinumerous**. I will write $|X| \neq |Y|$ if $|X| = |Y|$ is not true, i.e., if there is no 1–1 onto function from X to Y.
- I will write $|X| < |Y|$ if $|X| \leq |Y|$ but $|X| \neq |Y|$. In other words $|X| < |Y|$ means there is a 1–1 function from X to Y but there is no 1–1 and onto function from X to Y.

cardinality
equinumerous

Of course we define $|X| > |Y|$ if $|Y| < |X|$ and $|X| \geq |Y|$ if $|Y| \leq |X|$.

Note that the above definition generalizes the other simpler definition of $|X| \leq |Y|$ for the case when X and Y are finite. (Right?)

Definition 7.1.2. X is **infinite** iff $|X| = |X - \{x\}|$ for any $x \in X$.

infinite

Exercise 7.1.1. A set X is *finite* if there is some $n \in \mathbb{N}$ such that $|X| = |\{1, 2, 3, ..., n\}|$. But I can also define X to be finite if X is not infinite. Prove that the definitions are the same.

Definition 7.1.3. Let X be a set.

- We will say that X is **countable** if either X is finite or $|X| = |\mathbb{N}|$, i.e., there is a bijection between X and $\mathbb{N}$.
- X is **uncountable** if it is not countable.

countable
uncountable

Exercise 7.1.2. Prove the following:

- $|X| = |X|$ (easy)
- If $|X| \leq |Y|$ and $|Y| \leq |Z|$, then $|X| \leq |Z|$. Prove the same statement when $\leq$ is replaced by $<$ and then by $=$. □

Don't be fooled: The statement $|X| \leq |Y|, |Y| \leq |X| \implies |X| = |Y|$ is true, but the proof is not immediate. See next section on the Berstein–Schröder theorm.

Exercise 7.1.3. Prove that $\mathbb{N}$ is countably infinite.

Exercise 7.1.4. Let E be the set of even numbers. Since E is just half of $\mathbb{N}$, we must have $|E| < |\mathbb{N}|$, right? WRONG! Prove that $|E| = |\mathbb{N}|$.

Exercise 7.1.5. OK, but surely, $|\mathbb{Q}| > |\mathbb{N}|$, right? WRONG! Prove that $|\mathbb{Q}| = |\mathbb{N}|$.

Exercise 7.1.6. Prove that $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$. In fact $|\mathbb{N}^k| = |\mathbb{N}|$ for any integer $k > 0$. More generally, suppose $X_1, \ldots, X_n$ are countable sets, prove that $X_1 \times \cdots \times X_n$ is also countable.

Exercise 7.1.7. Prove that the subset of a countable set is countable. Prove that the superset of an uncountable set is uncountable.

Exercise 7.1.8. Let $X_1, X_2, \ldots, X_n$ be countable sets. Prove that $\bigcup_{i=1}^n X_i$ and $\bigcap_{i=1}^n X_i$ are both countable. In fact if you have countably many countable sets, $X_1, X_2, \ldots$, then $\bigcup_{i=1}^\infty X_i$ is countable. One would say "a countable union of countable sets is countable".

In the above "countable union" means the union of countably many sets. So this means that the sets of the union is finite, for instance

$$\bigcup_{i=1}^{5} X_i$$

where $X_i = [i, i+1)$ (intervals of $\mathbb{R}$), or

$$\bigcup_{i=1}^{\infty} X_i$$

In the second union, there are countable many X_i's.

An example of an uncountable union would be

$$\bigcup_{r \in [0,100)} X_r$$

where $X_r = [r, r+1)$. In this case there are uncountably many X_r's since the r runs through $[0, 100)$ which is not countable. For instance this union involves $[1, 2)$, $[3.5, 4.5)$, $[\sqrt{2}, \sqrt{2}+1)$, $[\pi, \pi+1)$, etc. Clearly there are uncountably many such X_r.

So what about $\mathbb{R}$? $\mathbb{R}$ is in fact uncountable. As a matter of fact, the interval $[0, 1)$ is uncountable. This was first proved by Cantor. The method of proof for this theorem discovered by Cantor is very important. Some people call this method the **diagonalization argument**.

diagonalization argument

Theorem 7.1.1. (Cantor) $[0, 1)$ *is uncountable.*

If you have taken discrete math, you should be able to give a proof (or a semi-proof close to the correct one.) You should attmept it.

SPOILER ALERT ... turn the page for the proof.

Proof. Every real number in $[0,1)$ looks like a decimal with no integer part. For instance $0.123 \in [0,1)$.

We prove by contradiction. Suppose $[0,1)$ is countable. So let's say the complete list of real numbers in $[0,1)$ is given by the list $x_1, x_2, x_3, \ldots$. Let's construct a real number $x \in [0,1)$ which is **not** in the above list. This will give us a contradiction. Right?

OK. So let's begin. I will construct x by giving you the decimal expansion. I will also“avoid” the list $x_1, x_2, x_3 \ldots$ so that x is not any of them.

Let's begin by "avoiding" x_1. Now x_1 is of the form $0.a...$ where a is a digit from 0 to 9. If $a = 0$, I will say that $x = 0.1\ldots$; otherwise, I will say that $x = 0.0\ldots$. So obviously $x \neq x_1$.

I'll repeat this for x_2. Say $x_2 = 0.bc\ldots$, then the second decimal place of x is 1 if $c = 0$; otherwise the second decimal place of x is 0. I have $x \neq x_2$.

I'll then make the 3rd decimal place of x different from the third decimal place of x_3.

Etc. Get it?

For instance suppose my list of $x_1, x_2, x_3, ...$ looks like this:

$$\begin{array}{cccccccccc}
x_1 & = & 0 & . & \boxed{1} & 3 & 0 & 2 & 9 & 0 \\
x_2 & = & 0 & . & 0 & \boxed{0} & 8 & 3 & 0 & 7 \\
x_3 & = & 0 & . & 3 & 1 & \boxed{3} & 1 & 3 & 1 \\
x_4 & = & 0 & . & 0 & 0 & 8 & \boxed{7} & 2 & 7 \\
x_5 & = & 0 & . & 1 & 2 & 8 & 0 & \boxed{2} & 7 \\
x_6 & = & 0 & . & 0 & 6 & 1 & 9 & 2 & \boxed{0}
\end{array}$$

So for the decimal places of x, I choose not 1, not 0, not 3, not 7, not 2, not 0, etc. For instance I can choose 0, 1, 0, 0, 0, 1, ... Hence for this case my x looks like

$$x = 0.010001...$$

So let's have a formal proof. Suppose x_i is

$$x_i = 0.x_{i,1}x_{i,2}x_{i,3}\ldots x_{i,i}\ldots$$

for $i = 1, 2, 3, \ldots$. Then we let x be the number

$$x = 0.y_1y_2y_3\ldots y_i\ldots$$

where

$$y_i = \begin{cases} 0 \text{ if } x_{i,i} \neq 0 \\ 1 \text{ if } x_{i,i} = 0 \end{cases}$$

Note in particular that $y_i \neq x_{i,i}$ for all $i > 0$. Then $x \neq x_i$ for all i. Why? Otherwise say $x = x_i$ for some i. But that implies that they have the same decimal expansion. In other words

$$y_j = x_{i,j}$$

for all j. But by construction,

$$y_i \neq x_{i,i}$$

Contradiction!!!

But wait, there's a ... **hole** in the proof. We assumed that if two real numbers are the same, they must then have the same decimal expansion. Is that true?

Exercise 7.1.9. Show that $0.09999\ldots = 0.1$ numerically although they are written differently. [Hint: Remember geometric series?

$$a + ar + ar^2 + ar^3 + \cdots = \frac{a}{1-r}$$

Don't just stare at it. Try to use this formula.]

Exercise 7.1.10. Complete the proof of Cantor's Theorem with the exercise on the previous page.

Exercise 7.1.11. This is something that is hard to believe: Prove that

$$[0,1] \text{ and } [0,1] \times [0,1] \text{ are equinumerous!!!}$$

The interval $[0,1]$ is called the **unit interval** and the product $[0,1] \times [0,1]$ is called the **unit square**. So basically there are as many points on the unit interval as there are on the unit square. (Cantor couldn't believe it when he proved the above fact. In a letter to Dedekind, he wrote, "I see it, but I don't believe it!")

unit interval

unit square

Exercise 7.1.12. Prove that there are uncountably many functions $\mathbb{N} \to \{0, 1\}$. [Hint: Diagonalization.]

Exercise 7.1.13. Is the set of polynomials with integer coefficients countable? Two polynomials are considered the same if their coefficients are the same. What about the set of polynomials with rational coefficients?

Exercise 7.1.14. We already know from a previous exercise that a finite product of countable sets is countable. Suppose $X_1, X_2, \ldots$ are countable. Is $X_1 \times X_2 \times X_2 \times \cdots$ countable?

You now know that $\mathbb{R}$ is not countable and $\mathbb{Q}$ is countable. So $\mathbb{R}$ is sort of "huge". In particular the set of $\mathbb{R} - \mathbb{Q}$ (irrational numbers) is "huge". You can actually subdivide $\mathbb{R}$ further. There is an important set of numbers, call the set of algebraic numbers in $\mathbb{R}$. I'll write A for the set of algebraic numbers. Some algebraic numbers are complex while some are real. Here's the definition of an algebraic number.

A number $\alpha \in \mathbb{C}$ is an **algebraic number** if α is the root of a polynomial with coefficients in $\mathbb{Q}$. Just for practice, show that $\mathbb{Q} \subset A$. Note that $\sqrt{2}$ is not rational. However $\sqrt{2}$ is algebraic. In fact show that if $x > 0$ and $y > 0$ are rational, then x^y is algebraic. Now show that i is algebraic where $i = \sqrt{-1}$.

algebraic number

The relationship between $\mathbb{Z}, \mathbb{Q}, A, \mathbb{R}, \mathbb{C}$ is:

$$\mathbb{Z} \subset \mathbb{Q} \subset A \cap \mathbb{R} \subset \mathbb{R} \subset \mathbb{C}$$

and

$$\mathbb{Z} \subset \mathbb{Q} \subset A \subset \mathbb{C}$$

In other words the set of algebraic numbers A is a subset of $\mathbb{C}$ and some algebraic numbers are real, but not all. Enough practice ... now for the real exercise:

Exercise 7.1.15. Prove that A is countable. □

Note that the set of algebraic numbers in $\mathbb{R}$ is countable: $A \cap \mathbb{R}$ is countable. But we know that $\mathbb{R}$ is uncountable. This means that there are non-algebraic numbers in $\mathbb{R}$. In fact there are uncountably many non-algebraic numbers in $\mathbb{R}$. These are called transendental numbers. In other words $\alpha \in \mathbb{C}$ is **transcendental** if α is not the root of a polynomial with rational coefficients. Here are two examples: π and e are transcendental.

transcendental

I'm sure you have heard in some previous classes that π and e are irrational. But π and e are more than irrational. They are transcendental.

Proving a number is transcendental is not easy! For instance to prove π is transcendental, by definition, you have to prove π is not algebraic. That means π is *not* the solution of *any* polynomial with $\mathbb{Q}$ coefficients.

While the ancient Greek philosophers discovered the existence of irrational numbers (example $\sqrt{2}$) around 300BC, the first transcendental number was only discovered around 1850:

$$\sum_{n=1}^{\infty} 10^{-n!}$$

Try to write down it's decimal representation up to say 50 decimal placed. This number was artificially created by Liouville to "avoid" polynomials with $\mathbb{Q}$ coefficients.

On the other hand π was proven to be transcendental in 1882 by von Lindemann and e was proven to be transcendental a couple of years early by Hermite in 1873. The fact that there are uncountably many transcendental numbers was proven by Cantor in 1874, one year after Hermite's result.

We actually know very little about transcendental numbers. For instance, we do not know if the following constant, the Euler–Mascheroni constant, is transcendental or not:

$$\gamma = \lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \ln n \right) = 0.5772...$$

($\ln = \log_e$). In fact, scratch that, we don't even know if γ is rational or irrational!!! This constant is ubiquitous and appears in CS, math, physics, etc.

Exercise 7.1.16. Prove that $P(\mathbb{N})$ is uncountable. This means $|\mathbb{N}| < |P(\mathbb{N})|$. In fact even more is true: if X is a set, then $|X| < |P(X)|$. (This is called Cantor's theorem and is extremely important. See later.)

Exercise 7.1.17.

- Prove that there are countably many C++ programs.
- Since there number of functions from $\mathbb{N}$ to $\{0, 1\}$ is uncountable, what does that tell you?

Theorem 7.1.2. (Cantor) *For any set X, $|X| < |P(X)|$.*

The fact $|X| \leq |P(X)|$ is easy.

Now I'm going to prove that you cannot find an onto function from X to $P(X)$. Suppose on the contrary that $f : X \to P(X)$ is an onto function. I need to arrive at a contradiction. How? Since f is onto, for any subset Y of X, there is some $x \in X$ such that $f(x) = Y$. I need to construct some Y that will cause some problem (contradiction).

Now Y would look like this: $Y = \{x \in X \mid P(x)\}$ where $P(x)$ is some condition. The condition $P(x)$ depends on whatever I have now. For instance $P(x)$ might depends on X, $P(X)$, f. So I want to say there is some $x' \in X$ such that

$$f(x') = \{x \in X \mid P(x)\}$$

will lead to a contradiction. The question is what should $P(x)$ be? What about this x'? How can it be used to craft a contradiction? Well x' is an element of X and $f(x')$ is a subset of X. The relationship between x' and $f(x')$ is either $x' \in f(x')$ or $x' \notin f(x')$. Suppose $x' \in f(x')$, i.e.,

$$x' \in f(x') = \{x \in X \mid P(x)\}$$

Since $x' \in \{x \in X \mid P(x)\}$, then of course x' satisfy $P(x')$. In other words

$$x' \in f(x') \implies P(x')$$

See a contradiction? Suppose $P(x)$ is "$x \notin f(x)$". Then

$$x' \in f(x') = \{x \in X \mid x \notin f(x)\}$$

i.e.,

$$x' \in f(x') \implies x' \notin f(x')$$

which is clearly a contradiction. However this is when I assume $x' \in f(x')$. What if $x' \notin f(x')$? Would the set $\{x \in X \mid x \notin f(x)\}$ still give me a contradiction? Why yes! Because if $x' \notin f(x')$, then x' does not satisfy $P(x)$, i.e., it is not true that $x' \notin f(x')$. So now we're ready to write the proof.

Proof. First we prove that $|X| \leq |P(X)$. Define the function $f : X \to P(X)$ to be $f(x) = \{x\}$. This function is 1–1: If $x, x' \in X$ and $f(x) = f(x')$, then $\{x\} = \{x'\}$ and hence $x = x'$. Therefore $|X| \leq |P(X)|$.

Now we will prove that $|X| \neq |P(X)|$. In other words, we will prove that there's no onto function from X to $P(X)$. Assume on the contrary that $f : X \to P(X)$ is an onto function. Let

$$Y = \{x \in X \mid x \not\in f(x)\}$$

Y is a subset of X. Since f is onto, there is some $x' \in X$ such that

$$f(x') = Y = \{x \in X \mid x \not\in f(x)\}$$

We will consider two cases: $x' \in f(x')$ and $x' \not\in f(x')$ and show that in each cases, we will arrive at a contradiction.

If $x' \in f(x')$, then

$$\begin{aligned} & x' \in f(x') = Y = \{x \in X \mid x \not\in f(x)\} \\ \therefore\ & x' \text{ satisfies the condition } x' \not\in f(x') \\ \therefore\ & x' \not\in f(x') \end{aligned}$$

which is a contradiction.

If $x' \not\in f(x')$, then

$$\begin{aligned} & x' \not\in f(x') = Y = \{x \in X \mid x \not\in f(x)\} \\ \therefore\ & x' \not\in \{x \in X \mid x \not\in f(x)\} \\ \therefore\ & x' \text{ does not satisfy the condition } x' \not\in f(x') \\ \therefore\ & x' \in f(x') \end{aligned}$$

which is a contradiction.

In both cases, I arrive at contradictions. Hence our assumption on the existence of an onto function from X to $P(X)$ does not hold. Hence there is no onto function from X to $P(X)$. □

ON NON-UNIQUENESS OF DECIMAL REPRESENTATIONS.

Here's a real number

$$1433.235246457234346$$

Of course a decimal expanion need no terminate. For instance π does not terminate and furthermore the pattern of the decimal expansion does not repeat. There are decimal expansion that repeats. For instance

$$0.9999999999\ldots$$

It can be shown (probably in precalc) that

$$0.9999999999\ldots = 1$$

The question is this:

Exercise 7.1.18. When does two decimal expansion represent the same real number?

If you have taken Calc 2, you should have enough background to answer this yourself. So you can treat this as an exercise and write a short paper on it. You should think about this question and try it out on your own. Maybe you want to chat or work with another student.

SPOILER ALERT ... turn the page for the answer.

Note that

$$0.99999\ldots$$

and

$$1.00000\ldots$$

represent the same real number. Also,

$$0.1234599999\ldots$$

and

$$0.1234600000\ldots$$

represent the same real number. In general when does distinct two decimal representations represent the same real number? First I'll focus on the representation problem in the interval $[0, 1)$.

Let $x = 0.x_1x_2x_3...$ and $y = 0.y_1y_2y_3....$ Assume the sequence of decimal places are different:

$$(x_i)_{i=1}^{\infty} \neq (y_i)_{i=1}^{\infty}$$

I claim that $x = y$ iff there is some N such that $x_i = y_i$ for $i < N$, $x_N = y_N - 1$, and $x_j = 9, y_j = 0$ for $j > N$, or the conditions are switched between x and y.

$\Longleftarrow$: This is easy.

$\Longrightarrow$: If

$$(x_i)_{i=1}^{\infty} \neq (y_i)_{i=1}^{\infty}$$

then there must be a smallest $N \geq 1$ such that

$$x_i = y_i$$

for $i < N$ and $x_N \neq y_N$. Of course either $x_N < y_N$ or $x_N > y_N$. Without loss of generalize, assume $x_N < y_N$. I want to prove that x_N, y_N differ by 1. Let's see what happens. Since $x = y$ and $x_i = y_i$ for $i < N$, I have

$$y - x = (y_N - x_N)10^{-N} + \sum_{j=N+1}^{\infty} (y_j - x_j)10^{-j}$$

I claim that in this case $y - x > 0$. Since $y - x = 0$,

$$0 = (y_N - x_N)10^{-N} + \sum_{j=N+1}^{\infty} (y_j - x_j)10^{-j}$$

i.e.,

$$(x_N - y_N)10^{-N} = \sum_{j=N+1}^{\infty} (y_j - x_j)10^{-j}$$

i.e.,

$$x_N - y_N = \sum_{j=1}^{\infty}(y_{N+j} - x_{N+j})10^{-j}$$

Now note that since x_j, y_j are integers in $[0, 9]$,

$$-9 \leq y_j - x_j \leq 9$$

Hence

$$-9\sum_{j=1}^{\infty} 10^{-j} \leq \sum_{j=1}^{\infty}(y_{N+j} - x_{N+j})10^{-j} \leq 9\sum_{j=1}^{\infty} 10^{-j}$$

i.e.,

$$-9 \cdot \frac{1}{10^1} \cdot \frac{1}{1 - 1/10} \leq \sum_{j=1}^{\infty}(y_{N+j} - x_{N+j})10^{-j} \leq 9 \cdot \frac{1}{10^1} \cdot \frac{1}{1 - 1/10}$$

i.e.,

$$-1 \leq \sum_{j=N+1}^{\infty} (y_{N+j} - x_{N+j})10^{-j} \leq 1$$

Together with the above equation

$$x_N - y_N = \sum_{j=1}^{\infty}(y_{N+j} - x_{N+j})10^{-j}$$

I get

$$-1 \leq x_N - y_N \leq 1$$

This means that $x_N - y_N$ is $-1, 0, 1$. But hang on: remember that $x_N \neq y_N$. So I now know that x_N, y_N differ by 1. Since I'm assuming $x_N < y_n$, I get

$$x_N = y_N - 1$$

So now from

$$x_N - y_N = \sum_{j=1}^{\infty}(y_{N+j} - x_{N+j})10^{-j}$$

I have

$$-1 = x_N - y_N = \sum_{j=1}^{\infty} (y_{N+j} - x_{N+j}) 10^{-j}$$

I claim that $y_{N+1} = 0$ and $x_{N+i} = 9$. From

$$-1 = \sum_{j=1}^{\infty} (y_{N+j} - x_{N+j}) 10^{-j}$$

I get

$$-1 - (y_{N+1} - x_{N+1}) 10^{-1} = \sum_{j=2}^{\infty} (y_{N+j} - x_{N+j}) 10^{-j}$$

and therefore

$$-10 - (y_{N+1} - x_{N+1}) = \sum_{j=2}^{\infty} (y_{N+j} - x_{N+j}) 10^{-j}$$

i.e.,

$$-10 - (y_{N+1} - x_{N+1}) = \sum_{j=1}^{\infty} (y_{N+1+j} - x_{N+1+j}) 10^{-j}$$

I claim that $y_{N+1} = 0$ and $x_{N+1} = 9$. The sum above can be bounded:

$$-1 = -9 \cdot \frac{1}{10} \cdot \frac{1}{1 - 1/10} \leq \sum_{j=1}^{\infty} (y_{N+1+j} - x_{N+1+j}) 10^{-j} \leq 9 \cdot \frac{1}{10} \cdot \frac{1}{1 - 1/10} = 1$$

Hence

$$-1 \leq -10 - (y_{N+1} - x_{N+1}) \leq 1$$

i.e.

$$9 \leq -(y_{N+1} - x_{N+1}) \leq 11$$

i.e.,

$$-9 \geq y_{N+1} - x_{N+1} \geq -11$$

However the since x_j, y_j are in $[0, 9]$,

$$-9 \leq y_{N+1} - x_{N+1} \leq 9$$

Hence

$$y_{N+1} - x_{N+1} = -9$$

which is achieved only when

$$y_{N+1} = 0, \;\; x_{N+1} = 9$$

which is what I claimed earlier. With this information,

$$-10 - (y_{N+1} - x_{N+1}) = \sum_{j=1}^{\infty} (y_{N+1+j} - x_{N+1+j}) 10^{-j}$$

becomes

$$-1 = \sum_{j=1}^{\infty} (y_{N+1+j} - x_{N+1+j}) 10^{-j}$$

and the same argument would yield

$$y_{N+2} = 0, x_{N+2} = 9$$

Etc. By induction, one can prove that

$$y_{N+j} = 0, x_{N+j} = 9$$

for $j = 1, 2, 3, ...$

I have now shown that if $0.x_1x_2x_3...$ and $0.y_1y_2y_3...$ are two decimal representations, then either $x_i = y_i$ for all i or, if not, then there is a smallest N such that $x_i = y_i$ for $i < N$, and $x_N \neq y_N$. Furthermore, x_N and y_N differs by exactly 1. Without loss of generality, if $x_N = y_N - 1$, then $x_j = 9$ and $y_j = 0$ for $j > N$.

What about decimal representations with nonzero integer part? Easy! Consider

$$x = x_{-m}x_{-m+1}x_{-m+2} \cdots x_0 \ . \ x_1x_2x_3...$$

and

$$y = y_{-n}y_{-n+1}y_{-n+2} \cdots y_0 \ . \ y_1y_2y_3...$$

All I need to do is to multiply these two numbers by 10^{-k} for a sufficiently large k so that $x \cdot 10^{-k}$ and $y \cdot 10^{-k}$ are two numbers in $[0, 1)$. (Basically I'm moving their decimal point to the left by the same number of steps.) Then use the above result to get the following: Either $x_i = y_i$ for all i of there is some N such that $x_i = y_i$ for $i < N$, $x_N \neq y_N$. Furthermore x_N, y_N differs by 1. Assuming $x_N = y_N - 1$, then $x_j = 9$ and $y_j = 0$ for $j > N$.

Let me state this as a theorem. I'm going to use descending index values.

Theorem 7.1.3. *Let x and y be real numbers. Suppose*

$$x = x_m x_{m-1} \ldots x_0 \cdot x_{-1} x_{-2} \ldots$$

and

$$y = y_m y_{m-1} \ldots y_0 \cdot y_{-1} y_{-2} \ldots$$

be decimal representations for x and y. Then $x = y$ iff either $x_i = y_i$ for all $i \leq m$ or there is some N such that

(a) *$x_i = y_i$ for $m \leq i < N$*
(b) *$x_N = y_N - 1$ (or $y_N = x_N - 1$), and*
(c) *$x_j = 9$, $y_j = 0$ for $j < N$ (or $x_j = 0$, $y_j = 9$ for $j < N$, respectively)*

The above is also true (and the proof is similar), if the base of the representation is changed to any base $B > 1$. In that case, the "9" in the statement of the theorem has to be changed to $B - 1$.

□

7.2 Berstein-Schröder Theorem

Suppose you have two finite sets X and Y. If X and Y has the same number of elements, then of course I can find a 1–1 and onto from X and Y.

Now suppose I have two finite sets X and Y but I only tell you there is a 1–1 function from X to Y. What can you tell me about the sizes $|X$ and $|Y|$? Then it must be true that

$$|X| \leq |Y|$$

What if I tell you there's also a 1–1 function from Y to X, Then of course

$$|Y| \leq |X|$$

Since $|X|$ and $|Y|$ are finite, I get

$$|X| = |Y|$$

right away. That's because for integers a and b,

$$a \leq b \text{ and } b \leq a$$

implies

$$a = b$$

However if X and Y are sets in general (i.e., not neceesarily finite) and I know that

$$|X| \leq |Y| \text{ and } |Y| \leq |X|$$

it seems to be true that

$$|X| = |Y|$$

but hang on ... you should not think of numbers here. When it comes to infinities, you always have to be careful. What I'm saying above is this: If

$$|X| \leq |Y| \text{ and } |Y| \leq |X|$$

i.e.

$$\text{there is a 1–1 function } X \to Y$$

and

$$\text{there is a 1–1 function } Y \to X$$

then

$$|X| = |Y|$$

i.e.,

$$\text{there is a 1–1 onto function } X \to Y$$

So I'm making this statement: If there are 1–1 functions

$$X \to Y, \;\; Y \to X$$

then there is a 1–1 and onto function

$$X \to Y$$

If you think the proof easy, go ahead and try it. This is not a trick question. The above statement is actually true. I'll state it as a theorem for reference, but without proof. The theorem is usually called the Bernstein–Schröder theorem. The statement was first stated by Cantor in 1887. Bernstein and Schröder provided proofs 1897. It was later found (1902) that Schröder's proof is incorrect. Unknown to everyone, Dedekind already had a proof in 1887.

Theorem 7.2.1. Bernstein–Schröder *Let X and Y be sets such that*

Bernstein–Schröder

$$|X| \leq |Y| \textit{ and } |Y| \leq |X|$$

Then

$$|Y| = |X|$$

What does the Berstein–Schröfer theorem gives you? Well if you want to show $|X| = |Y|$, you can try to find a 1–1 and onto function from X to Y. Or, by Bernstein–Schroeder, you can find a 1–1 function from X to Y and another 1–1 function from Y to X. In some cases, finding a 1–1 and onto function might be harder. The reason is because you need to find one function that satisfies *two* conditions. It's true that using Bernstein–Schroeder requires you to find *two* functions. However in many cases finding two functions each satisfying *one* condition (i.e., 1–1) is actually easier.

Exercise 7.2.1. Note that Berstein-Schroeder says

$$|X| \leq |Y|, \ \ |Y| \leq |X| \implies |X| = |Y|$$

Show that the converse is true, i.e., show that

$$|X| = |Y| \implies |X| \leq |Y|, \ \ |Y| \leq |X|$$

□

Exercise 7.2.2. Let $a < b$ and $c < d$ where a, b, c, d are real numbers. Prove that $|(a, b)| = |(c, d)|$. Here (a, b) is the open interval from a to b. How about (a, b) and $(c, d]$? Do they have the same cardinality? What about (a, b) and $[c, d]$? □

Exercise 7.2.3. Is it true that $|(0,1)| = |\mathbb{R}|$? What about $|[0,1)| = |\mathbb{R}|$ □

Exercise 7.2.4. Is it true that $|\mathbb{R}| = |\mathbb{R}^2|$? What about $|[0,1]| = |[0,1]^2|$? □

Exercise 7.2.5. Prove that $|P(\mathbb{N})| = |\mathbb{R}|$.

SPOILER ALERT ... turn the page for the solution.

Proof. I will show $|P(\mathbb{N})| = |[0,1)|$. A real number x in $[0,1)$ can be writing in binary representation

$$x = 0.x_1 x_2 x_3 \ldots$$

I will assume that x does not have a string of 1s as the tail end of the binary sequence, i.e., there is no N such that $x_i = 1$ for all $i > N$. Define a set

$$f(x) \subseteq \mathbb{N}$$

where

$$n \in f(x) \iff x_n > 0$$

For instance if $x = 0.001101$, then

$$f(x) = \{3, 4, 6\}$$

and if $x = 0.0101010101010\ldots$, then

$$f(x) = \{2, 4, 6, 8, 10, 12, ...\}$$

i.e., it's the set of positive even integer. Now I'll show that f is 1–1. If $f(x) = f(x')$, then the $x_i = 1$ iff $x'_i = 1$. Hence x and x' has the same binary representation. Therefore $x = x'$. Hence f is 1–1. To show f is onto, if X is a subset of $\mathbb{N}$, from X I construct x as $x = 0.x_1 x_2 x_3 \ldots$ where $x_i = 1$ iff $i \in X$. Hence $|P(\mathbb{N})| = |[0,1)|$. □

Note that Cantor's theorem

$$|X| < |P(X)|$$

implies that there there is no "largest" set since

$$|X| < |P(X)| < |P(P(X))| < |P(P(P(X)))| < \cdots$$

In particular we have $|\mathbb{N}| < |P(\mathbb{N})|$. From the above exercise, $|P(\mathbb{N})| = |\mathbb{R}|$. Hence

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

An interesting question is whether you can find a set X such that

$$|\mathbb{N}| < |X| < |\mathbb{R}|$$

In other words, is there anything in between $|\mathbb{N}|$ and $|\mathbb{R}|$? In some books you will find the symbol $\aleph_0$ (pronounced "$\aleph$-null", google for the pronounciation of $\aleph$) which stands for $|\mathbb{N}|$; we also write $2^{\aleph_0}$ for $|P(\mathbb{N})|$. The orders of infinite sets together with natural numbers are called **ordinals**. You can think of ordinals as sizes of sets. Here are some ordinals:

$\aleph_0$

$2^{\aleph_0}$

ordinals

$$0 < 1 < 2 < 3 < \ldots < |\mathbb{N}| < |P(\mathbb{N})| = |\mathbb{R}| < |P(\mathbb{R})| < |P(P(\mathbb{R}))| < |P(P(P(\mathbb{R})))| < \ldots$$

So the above question can be rephrased as whether there is any ordinal x such that $\aleph_0 < x < 2^{\aleph_0}$. Cantor asked this question 1878 and believed that there is no such x. This is called the **continuum hypothesis CH**:

continuum hypothesis

CH

Continuum Hypothesis. There is no ordinal x between $|\mathbb{N}|$ and $|\mathbb{R}|$, i.e., there is no ordinal x such that

$$\aleph_0 < x < 2^{\alpha_0}$$

Cantor spent his whole life trying to prove the CH but was not able to. The continuum hypothesis is so important that it was one of the famous 23 problems of David Hilbert announced at the 1900 centennial meeting of the international congress of mathematicians. Without going into details, it was later proved that CH can neither be proved right nor proved wrong. Specifically, in 1940 Gödel proved that the statement "there is *some* x such that $|\mathbb{N}| < x < |\mathbb{R}|$" cannot be proven and then in 1963 Paul Cohen proved that the statement "there is *no* x such that $|\mathbb{N}| < x < |\mathbb{R}|$" cannot be proven, both proved under some "general and reasonably assumptions on what is meant by sets and logic". It's important to understand that Godel and Cohen did not say that CH is true. And they did not say it's false. They are saying that CH and the logical opposite of CH, i.e., $\neg$ CH cannot be proved. Set theory and logic of this type is still under active research.

Index