CSE 431: Theory of computation Instructor: James Lee
Lecture 1: Cantor, set theory, and diagonalization

We're all familiar with finite sets, e.g. $X = \{1,2,4,\{2,3\},4.7\}$, and the various options we can perform on them, e.g. $X \cap Y = \{x : x \in X \text{ and } x \in Y\}$. Or we can consider the **power set of X** which is the set of all subsets of X:

$$2^X = \{S : S \subseteq X\}$$

For instance, if $X = \{a, b, c\}$ then $2^X = \big\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\big\}$.

There are also many infinite sets we're accustomed to, like the naturals, integers, and rationals:

$$\mathbb{N} = \{0,1,2,3, \dots\}, \quad \mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}, \quad \mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\right\}.$$

We also have the set of real numbers $\mathbb{R}$. We can write the real numbers between 0 and 1 using their decimal expansion

$$[0,1] = \big\{0.x_1x_2x_3x_4 \dots : x_i \in \{0,1, \dots, 9\}\big\}.$$

Sizes of infinity?

Cantor asked the question of whether there are different sizes of infinite sets. Two sets A and B have the same **cardinality** if there is a 1-1 correspondence $f : A \to B$. Recall that a mapping is a **1-1 correspondence** (or a "bijection") if

(i) [it is injective or "into"] For every $x, x' \in A$ with $x \neq x'$, we have $f(x) \neq f(x')$.
(ii) [it is surjective or "onto"] For every $y \in B$ there is an $x \in A$ with $f(x) = y$.

With this definition in place, we can make a few observations.

Fact: $\mathbb{N}$ and $\mathbb{Z}$ have the same cardinality.

Proof: Consider the 1-1 correspondence $f : \mathbb{N} \to \mathbb{Z}$ given by

$$f(n) = -\frac{n}{2} \text{ if } n \text{ is even and } \quad f(n) = \frac{n+1}{2} \text{ if } n \text{ is odd.}$$

Note that f naturally lists the elements of $\mathbb{Z}$ as $0, -1, 1, -2, 2, -3, 3, \dots$

Let's argue carefully that f is a 1-1 correspondence. First, if $f(n) = f(n')$ then by the formulas above, we must have $n = n'$. Hence f is injective (satisfies property (i)). Now consider any integer $x \in \mathbb{Z}$.

If $x > 0$ then $2x - 1 \in \mathbb{N}$ and $f(2x-1) = x$. If $x \leq 0$, then $-2x \in \mathbb{N}$ and $f(-2x) = x$. Thus f is surjective as well (satisfies property (ii)). Putting these together, we see that f is a 1-1 correspondence.

Definition: A set S is *countable* if it has the same cardinality as $\mathbb{N}$.

Thus above we have proved that $\mathbb{Z}$ is countable.

It is a more surprising fact, perhaps, that the rational numbers $\mathbb{Q}$ are countable.

To prove this, it helps to have two lemmas.

Lemma 1: If S is countable and $A \subseteq S$ is infinite, then A is countable.

Proof (sketch): Since S is countable, it is in 1-1 correspondence with $\mathbb{N}$, so it suffices to prove that an infinite subset $A \subseteq \mathbb{N}$ is countable. We define a 1-1 correspondence $g : \mathbb{N} \to A$ inductively as follows: $g(0) = \min(A)$. Given that $g(0), g(1), \dots, g(i)$ are defined, we put $g(i+1) = \min(A \setminus \{g(0), g(1), \dots, g(i)\})$. One can easily verify that this map is 1-1. A different way of stating this: We simply sort A and output a list of the elements in sorted order.

Lemma 2 : If A and B are countable, then so is $A \times B$.

Proof: Recall the Cartesian product $A \times B = \{(a,b) : a \in A, b \in B\}$. Since A is countable, we may list its elements as $A = \{a_1, a_2, a_3, \dots.\}$, and similarly for $B = \{b_1, b_2, b_3, \dots\}$. Now we give a list of the elements of the Cartesian product:

$$A \times B = \{(a_1,b_1), (a_1,b_2), (a_2,b_1), (a_1,b_3), (a_2,b_2), (a_3,b_1), \dots\}$$

Here we are ordering the elements of $A \times B$ by the **sum** of their indices, i.e. by the value $i + j$ for the pair (a_i, b_j). First we list the pair with $i + j = 2$, then the two pairs with $i + j = 3$, then the three pairs with $i + j = 4$, etc. The important point is that for any element (a_i, b_j) of $A \times B$, it occurs at a finite place in the list.

One can actually describe this 1-1 correspondence by a formula. Let $f : A \times B \to \mathbb{N}$ be given by

$$f : (a_i, b_j) \mapsto \frac{1}{2}(i+j-1)(i+j-2) - i$$

though it seems easier to think about sorting by the sum of the indices.

Theorem: $\mathbb{Q}$ is countable.

Proof: With Lemmas 1 and 2 in hand, we can easily prove that $\mathbb{Q}$ is countable. Notice that for any fraction a/b we can write it as p/q where $q \neq 0$ and p and q have no common factors, and this representation is unique. This allows us to put $\mathbb{Q}$ in 1-1 correspondence with a subset of $\mathbb{Z} \times \mathbb{Z}$: Let the map $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ be defined by $f\left(\frac{a}{b}\right) = (p, q)$. But from Lemma 2, we know that $\mathbb{Z} \times \mathbb{Z}$ is countable (since we know that $\mathbb{Z}$ is). Thus from Lemma 1, we know that any infinite subset of $\mathbb{Z} \times \mathbb{Z}$ is countable. So since $\mathbb{Q}$ is infinite, and we have put it in 1-1 correspondence with a subset of $\mathbb{Z} \times \mathbb{Z}$, we can conclude that $\mathbb{Q}$ is countable.

At this point, one might start to think that all infinite sets are countable, but one of Cantor's amazing insights is that the real numbers are **uncountable**. This is proved using "diagonalization," a proof technique we will see many times. Let's prove it \ for the real numbers between 0 and 1.

Theorem: [0,1] is uncountable.

Proof: Suppose, for the sake of contradiction, that [0,1] **is** countable. In that case, we can write a list enumerating all these numbers:

$$0.x_{11}x_{12}x_{13}x_{14}x_{15}x_{16}\ldots$$

$$0.x_{21}x_{22}x_{23}x_{24}x_{25}x_{26}\ldots$$

$$0.x_{31}x_{32}x_{33}x_{34}x_{35}x_{36}\ldots$$

$$0.x_{41}x_{42}x_{43}x_{44}x_{45}x_{46}\ldots$$

Etc. Here, x_{ij} represents the jth digit after the decimal point of the ith number in the list. We will derive a contradiction by producing a real number $y \in [0,1]$ that is not on the list. We do this simply by defining $y = 0.y_1y_2y_3y_4y_5y_6\ldots$ where

$$y_i = 1 \text{ if } x_{ii} \neq 1 \text{ and } y_i = 0 \text{ if } x_i = 1$$

Now suppose that y appears somewhere in the purported list above. It cannot be the ith element in the list because it differs from that number in the ith digit, i.e. $y_i \neq x_{ii}$ by construction. Thus the list is incomplete, contradicting our initial assumption.

Cantor noticed more: Given any set X, the power set 2^X will always have cardinality bigger than X, i.e. there is no surjective (i.e., onto) mapping $f : X \to 2^X$. This will also use diagonalization.

Proof: Suppose (for the sake of contradiction) there is a surjective map $f : X \to 2^X$. Consider the subset

$$S = \{x : x \notin f(x)\}$$

Now, S is a subset of X. So since f is surjective, there must be an element $x \in X$ such that $f(x) = S$. Now consider two possibilities:

If $x \in S$ then $x \in f(x)$ which implies $x \notin S$ by the definition of S.

But if $x \notin S$ then $x \notin f(x)$ which implies that $x \in S$ by the definition of S.

Thus we get a contradiction, and no such mapping f cannot exist.

Paradoxes in naïve set theory

Cantor noticed something fishy about the fact that 2^X always has a larger cardinality than X. If we let $\mathcal{S}$ denote the **set of all possible sets** then it should have the largest cardinality, but still it must be that $2^{\mathcal{S}}$ is even bigger!

Bertrand Russell set about to resolve this "paradox." In the process, he found an even simpler paradox of naïve set theory. Consider a barber that shaves all those men who don't shave themselves (and no one else). If the barber shaves himself, then he doesn't shave himself. But if he doesn't shave himself, then by definition, he shaves himself! So such a barber cannot exist. Similarly, consider the set of all sets that don't contain themselves as a member:

$$\mathcal{B} = \{S : S \notin S\}$$

If $\mathcal{B} \in \mathcal{B}$ then by definition $\mathcal{B} \notin \mathcal{B}$. But if $\mathcal{B} \notin \mathcal{B}$ then $\mathcal{B} \in \mathcal{B}$! So such a set $\mathcal{B}$ cannot exist.

Both of these examples illustrate that if we allow sets to become too big (or too "powerful") then they can diagonalize against themselves! We will see the same phenomenon come up in computation: Since computer programs can manipulate and simulate other computer programs, there must be limitations on what they could do. If they were too powerful, they could diagonalize against themselves, leading to a contradiction. (We'll see this very clearly soon.)