CS 70 Discrete Mathematics for CS
Spring 2007 Luca Trevisan

Lecture 27

Infinity and Countability

Consider a function f that maps elements of a set A (called the domain of f) to elements of set B (called the range of f). Recall that we write this as $f : A \to B$. We say that f is a bijection if every element $a \in A$ has a unique image $b = f(a) \in B$, and every element $b \in B$ has a unique pre-image $a \in A$: $f(a) = b$.

f is a *one-to-one function* (or an *injection*) then if f maps distinct inputs to distinct outputs. More rigorously, f is one-to-one if the following holds: $x \neq y \Rightarrow f(x) \neq f(y)$.

The next property we are interested in is functions that are *onto* (or *surjective*). A mapping that is onto essentially "hits" every element in the range (i.e., each element in the range has at least one pre-image). More precisely, a mapping function f is onto if the following holds: $\forall y, \exists x : f(x) = y$.

For example, if $\mathbb{R}$ is the set of real numbers, here are some examples of functions $f : \mathbb{R} \to \mathbb{R}$:

- The function $f(x) = x^2$ is not one-to-one (because $f(3) = f(-3)$, for example) and it is not onto (because there is no x such that $f(x) = -1$, for example).
- The function $f(x) = e^x$ is one-to-one but it is not onto (the output is always positive).
- The function $f(x) = x^3 - x$ is onto but it is not one-to-one (for example, $f(0) = f(1) = 0$).
- The function $f(x) = 1 + 3x$ is a bijection.

Note that according to our definition a function is a bijection iff it is both one-to-one and onto.

Cardinality

How can we determine whether two sets have the same cardinality (or size)? The answer to this question reassuringly lies in early grade school memories: by demonstrating a pairing between elements of the two sets. Saying this more formally, it is by demonstrating a bijection f between the two sets. The bijection sets up a one to one correspondence or pairing between elements of the two sets. We know how this works for finite sets. In this lecture, we will see what it tells us about infinite sets.

Are there more natural numbers $\mathbb{N}$ than there are positive integers $\mathbb{Z}^+$? It is tempting to answer yes, since every positive integer is also a natural number, but the natural numbers have one extra element $0 \notin \mathbb{Z}^+$. Upon more careful observation though, we see that we can generate a mapping between the positive integers and the natural numbers as follows:

$$f(x) = x - 1$$

Why is this mapping a bijection? Clearly, the function $f : \mathbb{Z}^+ \to \mathbb{N}$ is one-to-one (prove it). The mapping is also onto because every image $n \in \mathbb{N}$ is hit: the pre-image $n+1$ maps to it. We will never run out of positive integers; informally this says "$\infty + 1 = \infty$."

Since we have shown a bijection between $\mathbb{N}$ and $\mathbb{Z}^+$, this tells us that there are as many natural numbers as there are positive integers! What about the infinite set of even natural numbers $2\mathbb{N} = \{0, 2, 4, 6, ...\}$? In the previous example, the difference was just one element. But in this example, there seems to be twice as many natural numbers as there are even natural numbers. Surely, the cardinality of $\mathbb{N}$ must be larger than $2\mathbb{N}$ since $\mathbb{N}$ contains all of the odd natural numbers! Though it might seem to be a more difficult task, let us attempt to find a bijection between the two sets with this mapping:

$$f(x) = \frac{x}{2}$$

The mapping in this example is also a bijection. f is clearly one-to-one, since distinct even natural numbers get mapped to distinct natural numbers. Can you prove this more rigorously? The mapping is also onto, since every n in the range is hit: its pre-image is $2n$. Since we have found a bijection between these two sets, this tells us that in fact $\mathbb{N}$ and $2\mathbb{N}$ actually have the same cardinality!

In this lecture, we will see that there are different "orders" of infinity. If we are given a set B and can find a bijective function from $\mathbb{N}$ or some subset of $\mathbb{N}$ to our set, then we will call B a **countable set** (this name was chosen since the natural numbers are often considered the "counting" numbers).

What about the set of all integers, $\mathbb{Z}$? At first glance, it may seem obvious that the set of integers is larger than the set of natural numbers, since it includes negative numbers! However, as it turns out, it is possible to find a bijection between the two sets, meaning that the two sets have the same size! Consider the following mapping:

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

We will prove that this function $f : \mathbb{N} \to \mathbb{Z}$ is a bijection, by first showing that it is one-to-one and then showing that it is onto.

Proof (one-to-one): Suppose towards a contradiction that $f(x) = f(y)$. Then they both must have the same sign. Therefore either $f(x) = \frac{x}{2}$ and $f(y) = \frac{y}{2}$. So $f(x) = f(y) \Rightarrow \frac{x}{2} = \frac{y}{2} \Rightarrow x = y$. Contradiction. The second case is very similar, $f(x) = \frac{-(x+1)}{2}$ and $f(y) = \frac{-(y+1)}{2}$. So $f(x) = f(y) \Rightarrow \frac{-(x+1)}{2} = \frac{-(y+1)}{2} \Rightarrow x = y$. Contradiction, and thus f is one-to-one.

Proof (onto): If y is positive, then $f(2y) = y$. Therefore, y has a pre-image. If y is negative, then $f(-(2y+1)) = y$. Therefore, y has a pre-image. Thus, f is onto.

Since f is a bijective function, this tells us that $\mathbb{N}$ and $\mathbb{Z}$ have the same size! Another way to describe this mapping is: positive integers $\leftrightarrow$ even natural numbers, negative integers $\leftrightarrow$ odd natural numbers. What about the set of all rational numbers? Recall that $\mathbb{Q} = \{\frac{x}{y} \mid x, y \in \mathbb{Z}, y \neq 0\}$. Informally, we are asking the question: $\infty \times \infty > \infty$?

Surely there are more rational numbers than natural numbers. After all there are infinitely many rational numbers between any two natural numbers. Surprisingly, the two sets have the same cardinality! To see this, let us introduce another way of comparing the cardinality of two sets:

If there is a one-to-one function $f : A \to B$, then the cardinality of A is less than or equal to that of B. Now to show that the cardinality of A and B are the same we can show that $|A| \leq |B|$ and $|B| \leq |A|$. This corresponds to showing that there is a one-to-one function $f : A \to B$ and a one-to-one function $g : B \to A$. The existence of these two one-to-one functions implies that there is a bijection $h : A \to B$, thus showing that A and B have the same cardinality. The proof of this fact, which is called the Cantor-Bernstein theorem, is actually quite hard, and we will skip it here.

Back to comparing the natural numbers and the integers, we are going to describe an injective function $f : \mathbf{Q} \to \mathbf{N}$:

$$f(x) = \begin{cases} 2^a \cdot 3^b, & \text{if } x > 0 \text{ and it } x = \frac{a}{b} \text{ in simplified form} \\ 1, & \text{if } x = 0 \\ 2^a \cdot 3^b \cdot 5, & \text{if } x < 0 \text{ and it } x = -\frac{a}{b} \text{ in simplified form} \end{cases}$$

This tells us that $|\mathbb{Q}| \leq |\mathbb{N}|$. Since $\mathbb{N} \subseteq \mathbb{Q}$, it is easy to see that $|\mathbb{N}| \leq |\mathbb{Q}|$ (how do you show this formally?). Combining these two facts, it must be the case that $\mathbb{N}$ and $\mathbb{Q}$ have the same size!

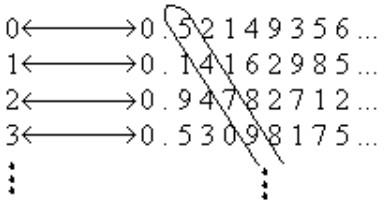
Cantor's Diagonalization

So we have established that $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ all have the same cardinality! What about the real numbers, the set of all points on the real line? Surely they are countable too. After all, the rational numbers are dense (i.e., between any two rational numbers there is a rational number).

In fact, between any two real numbers there is always a rational number. It is really surprising, then, that there are more real numbers than rationals! That is, there is no bijection between the rationals (or the natural numbers) and the reals. In fact, we will show something even stronger, even the real numbers in the interval $[0,1]$ are uncountable!

Recall that a real number can be written out in an infinite decimal expansion. A real number in the interval $[0,1]$ can be written as $0.d_1d_2d_3...$ (note that this representation is not unique; for example, $1 = 0.999...$). [1]

Cantor's Diagonalization Proof: Suppose towards a contradiction that there is a bijection $f : \mathbb{N} \to \mathbb{R}[0,1]$. Then, we can enumerate the infinite list as follows:



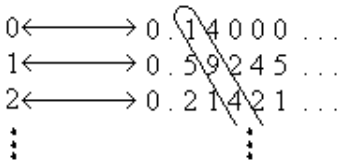
[1]

$$\begin{aligned} x &= .999\ldots \\ 10x &= 9.999\ldots \\ 9x &= 9 \\ x &= 1 \end{aligned}$$

The number circled in the diagonal is some real number r, since it is an infinite decimal expansion. Now consider the real number s obtained by modifying every digit of r, say by replacing each digit d with $d+5 \bmod 10$. We claim that s does not occur in our infinite list of real numbers. Suppose for contradiction that it did, and that it was the n^{th} number in the list. Then r and s differ in the n^{th} digit - the n^{th} digit of s is the n^{th} digit of r plus 5 mod 10. So we have a real number s that is not in the range of f. But this contradicts the assertion that f is a bijection. Thus the real numbers are not countable.

Let us remark that the reason that we modified each digit by adding 5 mod 10 as opposed to adding 1 is that the same real number can have two decimal expansions; for example $0.999... = 1.000....$ But if two real numbers differ by more than 1 in any digit they cannot be equal.

With Cantor's diagonalization method, we proved that $\mathbb{R}$ is uncountable. What happens if we apply the same method to $\mathbb{Q}$, in a futile attempt to show the rationals are uncountable? Well, suppose for a contradiction that our bijective function $f : \mathbb{N} \to \mathbb{Q}[0,1]$ produces the following mapping:



This time, let us consider the number q obtained by modifying every digit of the diagonal, say by replacing each digit d with $d+2 \bmod 10$. Then $q = 0.316...$, and we want to try to show that it does not occur in our infinite list of rational numbers. However, we do not know if q is rational (in fact, it is extremely unlikely for the decimal expansion of q to be periodic). This is why the method fails when applied to the rationals. When dealing with the reals, the modified diagonal number was guaranteed to be a real number - a number with an infinite decimal expansion.

The Halting Problem

Cantor's proof inspired a result of Turing, which is seen as one of the first results ever in computer science. (It predates the construction of the first computer by almost ten years.) Turing proved that the *Halting Problem*, a seemingly simple computational problem cannot be solved by *any algorithms whatsoever*. The Halting Problem is a software verification problem: we are given in input the code of a program P and a test input x. We want to know whether P, on input x, ever halts, or whether it runs forever, getting stuck in some kind of infinite loop.

Suppose, towards a contradiction, that there were an algorithm A that correctly solves the Halting Program. Now write a new program, called T, that, on input a program P, does the following

- T (program P)
  - run A to determine whether P halts when given in input P
  - if P halts on input P, then run forever
  - else, halt

That is, T receives an input the code of a program P. It uses the algorithm for the Halting Problem to determine whether the program P *when given its own code as an input* halts or not. Then T does the

opposite: if P halts when given its own code, T enters an infinite loop; if P does not halt when given its own code, T stops.

Consider now the behavior of T *when given its own code as input*. You see that T halts if and only if it does not halt, which is a contradiction.