Countability

November 4, 2009

Does it make any sense to talk about the size of an *infinite* set? For instance, do the set $\mathbb{Z}$ of integers and the set $2\mathbb{Z}$ of even integers have the same size? One might say "no", since $2\mathbb{Z}$ is a proper subset of $\mathbb{Z}$. But one might also say "yes", since there is a bijection $f : \mathbb{Z} \to 2\mathbb{Z}$ given by $f(n) = 2n$. It turns out that the second answer is more useful (neither is false – we are free to choose how to extend the definition). In general, we say that two sets A and B have the same *cardinality* if there is a bijection from A to B. If there is no such bijection, but there is an injection $g : A \to B$, then we say that the cardinality of A is less than that of B, and that the cardinality of B is greater than that of A. Note that for finite sets, cardinality really does just measure the size of a set, i.e., the number of its elements. The point is that we can now state that the (sets of) integers $\mathbb{Z}$, the even integers $2\mathbb{Z}$ and the natural numbers $\mathbb{N}$ all have the same cardinality.

A set A is said to be *countable* if it is either finite or its cardinality is that of $\mathbb{N}$. Equivalently, there should be an injection $g : A \to \mathbb{N}$. So a countable set has cardinality less than or equal to that of the natural numbers. All finite sets are countable. So are $\mathbb{N}$ and $\mathbb{Z}$. You might think that the set $\mathbb{Q}$ of rationals is bigger than these, i.e., that it is not countable, but in fact:

- $\mathbb{Q}$ is countable

The proof of this (in outline) is to write all the positive rationals in an infinite square array, and to sweep through the array in some "diagonal" manner. This proves that the set of positive rationals is countable, and hence so is $\mathbb{Q}$.

The interesting thing about this theorem is that, at first glance, $\mathbb{Q}$ really does seem to be much bigger than $\mathbb{N}$. For instance, between any two real numbers x and y, *however close*, there are an infinite number of rationals. But still, there is a bijection $f : \mathbb{Q} \to \mathbb{N}$.

$\mathbb{Q}$ is the quintessential example of a set which seems larger than it actually is (in the sense of cardinality). But there are even "larger-seeming" sets which are also countable, for example, the set of algebraic numbers. In fact:

- The union of a countable number of countable sets is countable

The proof of this is essentially the same as the proof that $\mathbb{Q}$ is countable (except that this time we have to use the axiom of (countable) choice). An equivalent way of saying this is:

- **Countability pigeonhole principle** Uncountably many items, countably many boxes $\Rightarrow$ some box contains uncountably many items

This is of course useless unless some sets are uncountable. As it happens:

- $\mathbb{R}$ is uncountable

This was proved by Cantor using his famous "diagonal" argument. The argument really shows that there is no surjection from a set X onto its power set $\mathcal{P}(X)$, or equivalently that a set always has lower cardinality than its power set. Suppose (only for simplicity of notation) that $X = \{x_1, x_2, \ldots\}$ is countable but not finite, and that there exists a surjection $f : X \to \mathcal{P}(X)$. The idea is to consider the array

$$\begin{array}{cl}
f(x_1) & \mathbf{1}10101001010 \\
f(x_2) & 0\mathbf{0}1111001010 \\
f(x_3) & 11\mathbf{0}101010111 \\
f(x_4) & 010\mathbf{1}11001010 \\
. & \ldots \\
. & \ldots \\
. & \ldots
\end{array}$$

where next to $f(x_i)$ I've just indicated the elements in the set $f(x_i)$ by putting a 1 in the j^{th} place if $x_j \in f(x_i)$, and a 0 in the j^{th} place if $x_j \notin f(x_i)$. In this way, I've represented each set $A \subset X$ as an infinite binary decimal. Now, I can also consider the set $B \subset X$ corresponding to the infinite binary decimal along the diagonal of the array (indicated in bold), and its complement $B^C = C \subset X$. In symbols,

$$C = \{x \in X : x \notin f(x)\}$$

Now f is a bijection, so $C = f(y)$ for some y. The question is: do we have $y \in f(y)$? If $y \in f(y)$, then $y \in C$, so $y \notin f(y)$. But if $y \notin f(y)$, then $y \in C$, so $y \in f(y)$. Contradiction. Pictorially, the "flipped diagonal" $0110\cdots$ must be one of the rows in the table, but it cannot actually be *any* of the rows, since it was constructed to be different from *each* row.

This is a very important style of argument in mathematics, and it crops up all over the place. It is essentially the same as "Russell's paradox" – the set of all sets which don't contain themselves – and it is implicit in Turing's proof that the **halting problem** is undecidable. (For the halting problem, the additional key idea is that a set of symbols can be considered both as a program and as an input to a program. With this understood, one simply creates an array as above, where this time the rows are *programs*, the columns are *inputs*, and there is a 1 in the ij^{th} place if program i halts with input j. The "flipped diagonal" can easily be made into a program P, which halts with input i if and only if program i does not halt with input i. However, P can also be considered as an *input*, and the question as to whether the program P halts with input P leads to a contradiction.)

Now for some problems.

1. (Putnam 1989) Can a countably infinite set have an uncountable collection of nonempty subsets such that the intersection of any two of them is finite?

2. Can a countably infinite set have an uncountable collection of *nested* subsets (i.e. an uncountable collection $\mathcal{A}$ such that for $A, B \in \mathcal{A}$, either $A \subset B$ or $B \subset A$)?

Homework

1. For every $x \in \mathbb{R}$, assign a finite set $A(x) \subset \mathbb{R} \setminus \{x\}$. Call a set $I \subset \mathbb{R}$ *independent* if for all $x, y \in I$ we have $x \notin A(y)$: in short $I \cap A(I) = \emptyset$. Prove that there exists an uncountable independent set.
[**Hint.** For every $x \in \mathbb{R}$ there is an interval J with rational endpoints such that $x \in J$ and $J \cap A(x) = \emptyset$. Apply the countability pigeonhole principle.]

This result was proved by Lázár in 1936.