Counting
Countable and Uncountable Sets
Continuum Hypothesis (or Problem)
Truth, Proofs, and Axioms
Final Remarks

Tetsuya Ishiu
Department of Mathematics
Miami University
February 21, 2011
Today, I would like to talk about “the size of infinite sets”.

Well, “infinity is infinity, nothing different” may be a good and consistent attitude. But modern mathematicians do not think so.

Before thinking about infinite sets, review how to count finite things (and make sure you are smarter than my 4-year old).
Counting finite sets

Let’s count them!
Counting finite sets

What rules do you have to follow when counting?
Counting can be considered as a function $f$ from \{1, 2, 3, \ldots, n\} into the set in question.

First, you must count each thing only once. It can be described as “if $n \neq m$, then $f(n) \neq f(m)$”. This property is called “one-to-one”.

You must also count all of them without ignoring any. This property is called “onto”

So, counting a finite set is, mathematically, to find a one-to-one onto function from \{1, 2, 3, \ldots, n\} into the set in question.
You can compare the sizes of two finite sets without using numbers.

Apple  Honey  Banana  Carrot  Milk

So, this set of animals and the set of foods have the same size!
How about infinite sets?

Why don’t we do the same for infinite sets?

Say two infinite sets have the same size if there is a one-to-one onto function from one to the other.

Does it work?
This was done by Galileo Galilei. Recall that an integer $n$ is a *perfect square* if and only if $n = m^2$ for some integer $m$.

Then, we can “count” the set of perfect squares as

\[
\begin{array}{cccccccc}
1 & 4 & 9 & 16 & 25 & 36 & 49 & 64 & \cdots \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \\
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \cdots \\
\end{array}
\]

So, the set of perfect squares has the same size as the set $\mathbb{N}$ of positive integers, though it is a subset of $\mathbb{N}$ with many missing elements. That is crazy!

This was the conclusion Galileo reached: You cannot talk about less, equal, or greater for infinite sets!
Not so fast!

In 19th century, G. Cantor viewed the same situation in a totally different way.

“This you can talk about the size of infinite sets. Just an infinite set can have the same size as its proper subset” (Y is a proper subset of X if and only if Y is a subset of X but Y $\neq X$).

So, he (and all other mathematicians) entered a new world, where even Galileo did not step in.
Cantor defined the following notion.

**Definition**

Two sets $X$ and $Y$ have the same cardinality if and only if there is a one-to-one onto function $f$ from $X$ into $Y$.

**Definition**

If a set $X$ has the same cardinality as $\mathbb{N}$, $X$ is called countable.
Examples of countable sets

The following sets are known to be countable.

- $\mathbb{N}$, the set of natural numbers.
- $\mathbb{Z}$, the set of integers.
- The set of finite sequences of natural numbers.
- $\mathbb{Q}$, the set of rational numbers.

But do there really exist “big infinity” and “small infinity”? That is, are there any “uncountable” set?
Yes, there is beyond infinity! Cantor proved the following theorem.

**Theorem**

*There is no onto function from \( \mathbb{N} \) to the set \( \mathbb{R} \) of all real numbers.*

So, \( \mathbb{R} \) is a larger infinite set than \( \mathbb{N} \).
Is $\mathbb{R}$ the largest? NO!

**Definition**

The powerset $\mathcal{P}(X)$ of a set $X$ is the set of all subsets of $X$.

For example, 
\{0\}, \{0, 1, 2, 3, 5\}, \{even integers\}, \{perfect squares\} are all elements of $\mathcal{P}(\mathbb{N})$. 
Theorem (Cantor)

For every (infinite) set $X$, there is no onto function from $X$ into $\mathcal{P}(X)$.

So, you can create bigger and bigger infinite sets, by taking $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))$, $\ldots$. 
Why does it matter?

But so what? Is it just a toy for crazy mathematicians?

We can define a function $\mu$ from most of the regions in the $xy$-plane into $[0, \infty)$ such that

1. $\mu(\{p\}) = 0$ for every point $p$,
2. if $R$ is a rectangle, then $\mu(R)$ is equal to the area of $R$,
3. (countably additive) if $\{D_n\}$ is a sequence of disjoint regions, then $\mu(\bigcup_n D_n) = \Sigma_n \mu(D_n)$, and
4. (translation invariant) if $D$ is some region and $x, y$ are real numbers, then $\mu(\{(a + x, b + y) : (a, b) \in D\}) = \mu(D)$. 
Not uncountably additive

In particular, if \( \mu(D_n) = 0 \), then

\[
\mu(\bigcup D_n) = 0
\]

However, you cannot extend it to an uncountable sequence, because for every \( x \in \mathbb{R} \), \( \mu(\{x\}) = 0 \), but

\[
\mu \left( \bigcup_{x \in \mathbb{R}} \{x\} \right) = \mu(\mathbb{R}) = \infty
\]

So, there is a big difference between countable sets and uncountable sets.
Continuum Problem

However, the following big question remains.

**Question**

Are there any set that has the size strictly between that of $\mathbb{N}$ and $\mathbb{R}$? Equivalently, are there any uncountable set of reals that has smaller size than $\mathbb{R}$?

This is called the *Continuum Problem*, which D. Hilbert picked as the first problem in his famous list.

The *Continuum Hypothesis* (written as CH) denotes the assertion that there is no uncountable set of reals that has strictly smaller size than $\mathbb{R}$. 
Twisted answer

This problem was kind of “solved”. However, the answer is not so clear cut.

What we found is that

- there is a “reasonable” universe of mathematics that satisfies CH, and
- there also is a “reasonable” universe of mathematics that does not satisfy CH, and
Truth and proof

Consider “$x^2 + 1 \geq 0$ for every real number $x$”.

This statement is (of course) true because no matter what real number $x$ you take, $x^2 + 1 \geq 0$. e.g. $1^2 + 1 = 2 \geq 0$, $(-2)^2 + 1 \geq 0$, $(-\pi)^2 + 1 \geq 0$, ….

However, we cannot check it for every real number because there are infinitely many (even uncountably many) real numbers, and we can compute only finitely many times.

So, we write proofs. But what is a proof?
A proof in mathematics is (roughly) a logical argument from a set of axioms that the desired statement is correct.

Axioms are the statements that are always assumed to be true under the context.

So, to prove something, you need to set up a system of axioms that describe the objects to work on.
<table>
<thead>
<tr>
<th>Axiom</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Closed under addition) ( \forall x, y \in \mathbb{R} (x + y \in \mathbb{R}) ).</td>
</tr>
<tr>
<td>(Closed under multiplication) ( \forall x, y \in \mathbb{R} (xy \in \mathbb{R}) ).</td>
</tr>
<tr>
<td>(Associative under addition) ( \forall x, y, z \in \mathbb{R} ((x + y) + z = x + (y + z)) ).</td>
</tr>
<tr>
<td>(Associative under multiplication) ( \forall x, y, z \in \mathbb{R} ((xy)z = x(yz)) ).</td>
</tr>
<tr>
<td>(Commutative under addition) ( \forall x, y \in \mathbb{R} (x + y = y + x) ).</td>
</tr>
<tr>
<td>(Commutative under multiplication) ( \forall x, y \in \mathbb{R} (xy = yx) ).</td>
</tr>
<tr>
<td>(Additive identity) ( \forall x \in \mathbb{R} (x + 0 = 0 + x = x) ).</td>
</tr>
<tr>
<td>(Multiplicative identity) ( \forall x \in \mathbb{R} (x \cdot 1 = 1 \cdot x = x) ).</td>
</tr>
<tr>
<td>(Identity elements axiom) ( 0 \neq 1 ).</td>
</tr>
<tr>
<td>(Additive inverse) ( \forall x \in \mathbb{R} \exists y \in \mathbb{R} (x + y = 0) ).</td>
</tr>
<tr>
<td>(Multiplicative inverse) ( \forall x \in \mathbb{R} (x \neq 0 \rightarrow \exists y \in \mathbb{R} (xy = 1)) ).</td>
</tr>
<tr>
<td>(Distributive) ( \forall x, y, z \in \mathbb{R} ((x + y)z = xz + yz) ).</td>
</tr>
<tr>
<td>(Trichotomy) ( \forall x, y \in \mathbb{R} (\text{exactly one of } x = y, x &gt; y, \text{ or } x &lt; y \text{ holds}) ).</td>
</tr>
<tr>
<td>(Transitivity) ( \forall x, y, z \in \mathbb{R} (x &gt; y \wedge y &lt; z \rightarrow x &lt; z) ).</td>
</tr>
<tr>
<td>(Additive compatibility) ( \forall x, y, z \in \mathbb{R} (x &lt; y \rightarrow x + z &lt; y + z) ).</td>
</tr>
<tr>
<td>(Multiplicative compatibility) ( \forall x, y, z \in \mathbb{R} (x &lt; y \wedge z &gt; 0 \rightarrow xz &lt; yz) ).</td>
</tr>
<tr>
<td>(Completeness) ( \forall X \subseteq \mathbb{R} (\exists y \in \mathbb{R} \forall x \in X (x \leq y) \rightarrow \exists z \in R (\forall x \in X (x \leq z) \wedge \forall y &lt; z \exists x \in X (y \leq x))) ).</td>
</tr>
</tbody>
</table>
The most standard system of axioms for “the whole universe of mathematics” is called “Zermelo-Fraenkel Axiom of Set Theory with Axiom of Choice”, denoted by ZFC.

This is a very powerful system, by which we can do most of mathematics by it.

So, in most cases, to prove something in mathematics means to prove it from ZFC.
However, K. Gödel proved “Incompleteness Theorem”, which says that every humanly describable system of axioms has a statement that can be neither proved nor disproved. (Well, this is a quite vague way to put it, though).

You may extend ZFC as much as you want, but every extension has an “undecidable” statement. So, there can be many universes of mathematics that look reasonable to human beings.
K. Gödel showed that there is a reasonable universe of mathematics that satisfies CH.

P. Cohen showed that there is a reasonable universe of mathematics that does not satisfy CH.

Such a statement is called *independent*. This settles the Continuum Problem, in a sense.
Still going!

However, there are still many research projects going on around CH.

- Can we determine it by thinking harder about mathematical universe?
  - K. Gödel pursued this very seriously.
  - Many set theorists including H. Woodin (P. Larson’s thesis adviser) are working on this approach.
- What happens if we assume CH? What happens if we assume not CH?
- What are common?
What I like about set theory

I like set theory because it is so crazy:

1. Counting infinity!
2. Extending the universe!
3. Shrinking the universe!
4. Building a miniture universe!
5. and so on, so forth.

Obviously, some people dislike it by exactly the same reason...