Basic set theory II

Richard Pettigrew

March 1, 2012

1 Cardinality

One of Cantor's central motivations when he inaugurated the mathematical study of sets was to explore the relative *sizes* or *cardinalities* of sets, in particular, infinite or transfinite sets.

1.1 Functions

To give Cantor's central definitions, we must begin with some terminology for discussing functions:

- A binary relation is a set of ordered pairs.
- A binary relation R is a *(unary) function* if whenever $(x, y) \in R$ and $(x, z) \in R$, we have $y = z$.
- Given a function f:
  - The domain of f is $\{x : \exists y[(x, y) \in f]\}$
  - The range of f is $\{y : \exists x[(x, y) \in f]\}$
- If f is a function and x is in the range of f, we write $f(x)$ for the unique y such that $(x, y) \in f$.
- If $f : a \to b$, then we say that f *is one-one* or *injective* if, for every $x, y \in a$, if $x \neq y$, then $f(x) \neq f(y)$.
- If $f : a \to b$, then we say that f *is onto* or *surjective* if, for every $y \in b$, there is $x \in a$ such that $f(x) = y$. That is, the range of f is b.
- If $f : a \to b$, then we say that f *is a one-one correspondence* or *bijective* if f is one-one and onto: that is, injective and surjective.

1.2 Definition of cardinality

Definition 1.1 *Given two sets a and b, we say that a* is the same size as *b iff there is a bijective function $f : a \to b$. We write $a \cong b$.*

Definition 1.2 *Given two sets a and b, we say that b* is at least as big as *a iff there is an injective function $f : a \to b$. We write $a \leq b$.*

Definition 1.3 *Given two sets a and b, we say that a* is strictly smaller than$b$ *iff $a \leq b$ and $b \not\leq a$. We write $a < b$.*

Theorem 1.4 (Cantor-Bernstein-Schröder) *If $a \leq b$ and $b \leq a$, then $a \cong b$.*

1.3 Some cardinality facts

Notation:

- $\mathbb{N}$ is the set of natural numbers. I.e.

$$\mathbb{N} = \{0, 1, 2, \ldots\}.$$

- $\mathbb{Q}$ is the set of rational numbers. I.e.

$$\mathbb{Q} = \{i\frac{m}{n} : i \in \{-1, 1\} \text{ and } m, n \in \mathbb{N} \text{ and } n \neq 0 \text{ and } m, n \text{ coprime}\}$$

- $\mathbb{R}$ is the set of real numbers.

Theorem 1.5 $\mathbb{N} \cong \{x \in \mathbb{N} : x$ *is even*$\}$

Proof. Define $f : \mathbb{N} \to \{x \in \mathbb{N} : x \text{ is even}\}$ as follows: $f(n) = 2n$. Then f is bijective. □

Theorem 1.6 $\mathbb{N} \cong \mathbb{Q}$

Proof. Define $f : \mathbb{N} \to \mathbb{Q}$ using the following diagram:

$$\begin{tikzcd}
\frac{1}{1} \arrow[r] & -\frac{1}{1} \arrow[dl] & \frac{2}{1} \arrow[r] & -\frac{2}{1} \arrow[dl] & \frac{3}{1} \arrow[r] & \cdots \\
\frac{1}{2} \arrow[d] & -\frac{1}{2} \arrow[ur] & \frac{2}{2} \arrow[dl] & -\frac{2}{2} \arrow[ur] & \frac{3}{5} & \cdots \\
\frac{1}{3} \arrow[ur] & -\frac{1}{3} \arrow[dl] & \frac{2}{3} \arrow[ur] & -\frac{2}{3} & \frac{3}{3} & \cdots \\
\frac{1}{4} \arrow[d] & -\frac{1}{4} \arrow[ur] & \frac{2}{4} & -\frac{2}{4} & \frac{3}{4} & \cdots \\
\frac{1}{5} \arrow[ur] & -\frac{1}{5} & \frac{2}{5} & -\frac{2}{5} & \frac{3}{5} & \cdots \\
\vdots & \vdots & \vdots & & &
\end{tikzcd}$$

Let $f(1) = \frac{1}{1}$, $f(2) = -\frac{1}{1}$, $f(3) = \frac{1}{2}$, $f(4) = \frac{1}{3}$, and so on. Whenever you come to a rational that has already been taken by an earlier number, skip over it and take the next one that hasn't been taken. Then f is a bijection. □

Theorem 1.7 (Cantor) $\mathbb{N} < \mathbb{R}$

Proof. Define $f : \mathbb{N} \to \mathbb{R}$ by $f(n) = n$. Then f is a bijection. So $\mathbb{N} \leq \mathbb{R}$. Now suppose, for the sake of contradiction that there is a bijection $g : \mathbb{N} \to \mathbb{R}$. Then write:

$$\begin{array}{rcl} g(0) & = & 3.7898234\ldots \\ g(1) & = & 8.0912384\ldots \\ g(2) & = & 2.0982348\ldots \\ \vdots & \vdots & \vdots \end{array}$$

Then, for every real r, there is a natural n such that $g(n) = r$. Now define a real number r^* using the following algorithm:

- Let the number before the decimal point in r^* be 0.
- Let the first number after the decimal point in r^* be given by taking the first number after the decimal point in $g(0)$ and adding one (if the number is 9, use 0). Thus, in our example, the first number after the decimal point in r^* will be 8.
- Let the second number after the decimal point in r^* be given by taking the second number after the decimal point in $g(1)$ and adding one (if the number is 9, use 0). Thus, in our example, the first number after the decimal point in r^* will be 0.
- Let the third number after the decimal point in r^* be given by taking the third number after the decimal point in $g(2)$ and adding one (if the number is 9, use 0). Thus, in our example, the third number after the decimal point in r^* will be 9.
- And so on.

This gives us a number that cannot possibly be in our list, since it differs from $g(0)$ in the first digit after the decimal point, from $g(1)$ in the second digit after the decimal point, and so on. Thus, there is no n such that $g(n) = r^*$. We have a contradiction. Thus, there is no bijection between $\mathbb{N}$ and $\mathbb{R}$. $\square$

There is another, more general way to see this point.

Definition 1.8 *Suppose x is a set. Let $2^x := \{f : x \to \{0,1\}\}$.*

Theorem 1.9 $\mathcal{P}(x) \cong 2^x$

Proof. Define the following function $f : \mathcal{P}(x) \to 2^x$. For $y \subseteq x$, let $f(y)$ be the characteristic function $\chi_y : x \to \{0,1\}$ of y. That is,

$$\chi_y(z) = \begin{cases} 0 & \text{if } z \notin y \\ 1 & \text{if } z \in y \end{cases}$$

Then f is a bijection. $\square$

Theorem 1.10 $\mathbb{R} \cong 2^{\mathbb{N}}$

Proof. Define $f : \mathbb{R} \to 2^{\mathbb{N}}$ as follows: for real number r, $f(r)$ is the function from $\mathbb{N}$ into $\{0,1\}$ that gives the infinite binary expansion of r. This is a bijection. $\square$

Theorem 1.11 (Cantor) *For all x, $x < \mathcal{P}(x)$.*

Proof. Define $f : x \to \mathcal{P}(x)$ as follows: For $z \in x$, $f(z) = \{z\}$. Now suppose there is a bijection $g : x \to \mathcal{P}(x)$. Then define the following subset $y \subseteq x$:

$$y := \{z \in x : z \notin g(z)\}.$$

Now suppose that there is $z \in x$ such that $g(z) = y$. Now, suppose $z \in g(z) = y$. Then, by definition, $z \notin g(z) = y$. On the other hand, suppose $z \notin g(z) = y$. Then, by definition, $z \in g(z) = y$. Thus, we have $z \in y \leftrightarrow z \notin y$, which is a contradiction. □

The power of this result is that it provides us with a way of producing larger and larger sets. It also gives rise to Cantor's Continuum Hypothesis (CH):

(CH) There is no set x such that $\mathbb{N} < x < \mathbb{R}$.

This claim cannot be proved or disproved in standard set theory. It is independent of the ZFC axioms. Gödel proved that $ZFC \nvdash \neg CH$; Cohen proved that $ZFC \nvdash CH$.

2 Cumulative hierarchy

The other upshot of Cantor's Theorem is that it suggests the *cumulative hierarchy* picture of the universe of sets.

2.1 Ordinals

Definition 2.1 (Well-ordering) *A relation $\leq$ on a set S is a* well-ordering *if it has the following properties:*

(i) *If $a \leq b$ and $b \leq a$, then $a = b$.* (Anti-symmetry)

(ii) *If $a \leq b$ and $b \leq c$, then $a \leq c$.* (Transitivity)

(iii) *For all $a, b \in S$, $a \leq b$ or $b \leq a$.* (Totality)

(iv) *For all non-empty subsets $A \subseteq S$, there is a $\leq$-least element of A.* (Well-ordering)

Definition 2.2 *Two well-orderings $(S, \leq_S)$ and $(T, \leq_T)$ have the same order type if there is a bijection $f : S \to T$ such that*

$$a \leq_S b \Leftrightarrow f(a) \leq_T f(b)$$

We write $(S, \leq_S) \cong (T, \leq_T)$.

Definition 2.3 *A set S is a von Neumann ordinal if:*

(i) *S is transitive (that is, if $x \in S$, then $x \subseteq S$).*

(ii) *S is well-ordered by $\in$.*

Theorem 2.4 (ZF) *If $(S, \leq)$ is a well-ordering, then there is a von Neumann ordinal x such that*

$$(S, \leq) \cong (x, \in)$$

This theorem shows that we won't go wrong if we simply let the von Neumann ordinals be our privileged exemplars of well-orderings and discuss everything to do with well-orderings in terms of them alone.

Definition 2.5 (Cumulative hierarchy) *Define:*

$$\begin{aligned} V_0 &= \varnothing \\ V_{\alpha+1} &= \mathcal{P}(V_\alpha) \\ V_\lambda &= \bigcup_{\alpha<\lambda} V_\alpha \end{aligned}$$

Theorem 2.6 *For $\lambda < \kappa$, $V_\lambda \subseteq V_\kappa$.*

Theorem 2.7 (ZF) *For all sets x, there is an ordinal α such that $x \in V_\alpha$.*

This gives us the following characterization of the universe of sets:

$$V = \bigcup_\alpha V_\alpha$$

Note that, by Cantor's Theorem, we have $V_\alpha < V_{\alpha+1}$.

3 Axiom of Choice

So far, everything we have said has been provable using only the Zermelo-Fraenkel axioms. But they are not powerful enough to prove a principle that is often required in mathematics. This is called the Axiom of Choice (AC):

Axiom 1 (Axiom of Choice) *For every set X of non-empty sets, there is a function $f : X \to \bigcup X$ such that, for all non-empty sets $x \in X$, $f(x) \in x$.*

That AC is independent of ZF was proved by Gödel and Cohen: Gödel showed that $ZF \nvdash \neg AC$ using the method of inner models; Cohen showed that $ZF \nvdash AC$ using the method of forcing.

The power of AC is witnessed by the string of important mathematical principles to which it is equivalent:

Theorem 3.1 *The following propositions are equivalent (relative to ZF):*

- *The Axiom of Choice*
- *The Well-Ordering Principle: Every set can be well-ordered.*
- *Zorn's lemma: Every non-empty partially ordered set in which every chain (i.e. totally ordered subset) has an upper bound contains at least one maximal element.*
- *Every vector space has a basis.*