5 The Cantor-Bernstein Theorem (continued)

Some applications of the Cantor-Bernstein theorem

Theorem 5.1. \( \mathbb{N} \sim \mathbb{Q} \).

Proof. First define a function \( f : \mathbb{N} \to \mathbb{Q} \) by \( f(n) = n \). Clearly \( f \) is an injection and so \( \mathbb{N} \leq \mathbb{Q} \).

Now define a function \( g : \mathbb{Q} \to \mathbb{N} \) as follows. First suppose that \( 0 \neq q \in \mathbb{Q} \). Then we can uniquely express \( q = \frac{\epsilon a}{b} \) where \( \epsilon = \pm 1 \) and \( a, b \in \mathbb{N} \) are positive and relatively prime. Then we define \( g(q) = 2^{\epsilon + 1}3^a5^b \).

Finally define \( g(0) = 7 \). Clearly \( g \) is an injection and so \( \mathbb{Q} \leq \mathbb{N} \).

By Cantor-Bernstein, \( \mathbb{N} \sim \mathbb{Q} \).

Theorem 5.2. \( \mathbb{R} \sim \mathcal{P}(\mathbb{N}) \).

We shall make use of the following result.

Lemma 5.3. \((0, 1) \sim \mathbb{R}\).

Proof of Lemma 5.3. By Calc I, we can define a bijection \( f : (0, 1) \to \mathbb{R} \) by \( f(x) = \tan(\pi x - \pi/2) \).

Proof of Theorem 5.2. By the lemma, it is enough to show that \( (0, 1) \sim \mathcal{P}(\mathbb{N}) \). We shall make use of the fact that each \( r \in (0, 1) \) has a unique decimal expansion

\[ r = 0.r_1r_2r_3\ldots r_n\ldots \]

so that

1. \( 0 \leq r_n < 9 \)

2. the expansion does not terminate with infinitely many 9s. (This is to avoid two expansions such as 0.5000\ldots = 0.4999\ldots)

First we define \( f : (0, 1) \to \mathcal{P}(\mathbb{N}) \) as follows. If

\[ r = 0.r_0r_1r_2\ldots r_n\ldots \]

then

\[ f(r) = \{2^{r_0+1}, 3^{r_1+1}, \ldots, p_n^{r_n+1}, \ldots\} \]

where \( p_n \) is the \( n \)th prime. Clearly \( f \) is an injection and so \( (0, 1) \leq \mathcal{P}(\mathbb{N}) \).

Next we define a function \( g : \mathcal{P}(\mathbb{N}) \to (0, 1) \) as follows: If \( \emptyset \neq S \subseteq \mathbb{N} \) then

\[ g(S) = 0.s_0s_1s_2\ldots s_n\ldots \]

where

\[ s_n = 0 \text{ if } n \in S \]
\[ s_n = 1 \text{ if } n \notin S. \]

Finally, \( g(\emptyset) = 0.5 \). Clearly \( g \) is an injection and so \( \mathcal{P}(\mathbb{N}) \leq (0, 1) \).

By Cantor-Bernstein, \((0, 1) \sim \mathcal{P}(\mathbb{N})\). 

\[ \square \]
The following result says that “\( \mathbb{N} \) has the smallest infinite size.”

**Theorem 5.4.** If \( S \subseteq \mathbb{N} \), then either \( S \) is finite or \( \mathbb{N} \sim S \).

**Proof.** Suppose that \( S \) is infinite. Let
\[ s_0, s_1, s_2, \ldots, s_n, \ldots \]
be the increasing enumeration of the elements of \( S \). This list witnesses that \( \mathbb{N} \sim S \). \( \square \)

The **Continuum Hypothesis (CH)** If \( S \subseteq \mathbb{R} \), then either \( S \) is countable or \( \mathbb{R} \sim S \).

**Theorem 5.5.** (Gödel 1930s, Cohen 1960s) If the axioms of set theory are consistent, then CH can neither be proved nor disproved from these axioms.

**Definition 5.6.** \( \text{Fin}(\mathbb{N}) \) is the set of all finite subsets of \( \mathbb{N} \).

**Theorem 5.7.** \( \mathbb{N} \sim \text{Fin}(\mathbb{N}) \).

**Proof.** First define \( f : \mathbb{N} \to \text{Fin}(\mathbb{N}) \) by \( f(n) = \{ n \} \). Clearly \( f \) is an injection and so \( \mathbb{N} \leq \text{Fin}(\mathbb{N}) \). Now define \( g : \text{Fin}(\mathbb{N}) \to \mathbb{N} \) as follows. If \( s = \{ s_0, s_1, s_2, \ldots, s_n \} \) where \( s_0 < s_1 < \ldots < s_n \), then
\[ g(S) = 2^{s_0+1}3^{s_1+1}\cdots p_{s_n+1}^{s_n} \]
where \( p_i \) is the \( i \)th prime. Also we define \( g(\emptyset) = 1 \). Clearly \( g \) is an injection and so \( \text{Fin}(\mathbb{N}) \leq \mathbb{N} \).

By Cantor-Bernstein, \( \mathbb{N} \sim \text{Fin}(\mathbb{N}) \). \( \square \)

**Exercise 5.8.** If \( a < b \) are reals, then \( (a, b) \sim (0, 1) \).

**Exercise 5.9.** If \( a < b \) are reals, then \( [a, b] \sim (0, 1) \).

**Exercise 5.10.** \( \mathbb{N} \sim \mathbb{N} \times \mathbb{N} \).

**Exercise 5.11.** If \( A \sim B \) and \( C \sim D \), then \( A \times C \sim B \times D \).

**Definition 5.12.** If \( A \) and \( B \) are sets, then
\[ B^A = \{ f \mid f : A \to B \} \]

**Theorem 5.13.** \( \mathcal{P}(\mathbb{N}) \sim \mathbb{N}^\mathbb{N} \).

**Proof.** For each \( S \subseteq \mathbb{N} \) we define the corresponding characteristic function \( \chi_S : \mathbb{N} \to \{0, 1\} \) by
\[ \chi_S(n) = 1 \text{ if } n \in S \]
\[ \chi_S(n) = 0 \text{ if } n \notin S \]
Let \( f : \mathcal{P}(\mathbb{N}) \to \mathbb{N}^\mathbb{N} \) be the function defined by \( f(S) = \chi_S \). Clearly \( f \) is an injection and so \( \mathcal{P}(\mathbb{N}) \leq \mathbb{N}^\mathbb{N} \).

Now we define a function \( g : \mathbb{N}^\mathbb{N} \to \mathcal{P}(\mathbb{N}) \) by
\[ g(\pi) = \{ 2^{\pi(0)+1}, 3^{\pi(1)+1}, \ldots, p_n^{\pi(n)+1}, \ldots \} \]
\( \square \)

2006/01/30
where \( p_n \) is the \( n \)th prime. Clearly \( g \) is an injection. Hence \( \mathbb{N}^\mathbb{N} \preceq \mathcal{P}(\mathbb{N}) \).

By Cantor-Bernstein, \( \mathcal{P}(\mathbb{N}) \sim \mathbb{N}^\mathbb{N} \).

**Heuristic Principle** Let \( S \) be an infinite set.

1. If each \( s \in S \) is determined by a *finite* amount of data, then \( S \) is countable.
2. If each \( s \in S \) is determined by *infinitely many independent* pieces of data, then \( S \) is uncountable.

**Definition 5.14.** A function \( f : \mathbb{N} \rightarrow \mathbb{N} \) is *eventually constant* iff there exists \( a, b \in \mathbb{N} \) such that

\[
f(n) = b \quad \text{for all } n \geq a.
\]

\( \text{EC}(\mathbb{N}) = \{ f \in \mathbb{N}^\mathbb{N} \mid f \text{ is eventually constant} \} \).

**Theorem 5.15.** \( \mathbb{N} \sim \text{EC}(\mathbb{N}) \).

**Proof.** For each \( n \in \mathbb{N} \), let \( c_n : \mathbb{N} \rightarrow \mathbb{N} \) be the function defined by

\[
c_n(t) = n \quad \text{for all } t \in \mathbb{N}.
\]

Then we can define an injection \( f : \mathbb{N} \rightarrow \text{EC}(\mathbb{N}) \) by \( f(n) = c_n \). Hence \( \mathbb{N} \preceq \text{EC}(\mathbb{N}) \).

Next we define a function \( g : \text{EC}(\mathbb{N}) \rightarrow \mathbb{N} \) as follows. Let \( \pi \in \text{EC}(\mathbb{N}) \). Let \( a, b \in \mathbb{N} \) be chosen so that:

1. \( \pi(n) = b \) for all \( n \geq a \)
2. \( a \) is the least such integer.

Then

\[
g(\pi) = 2^{\pi(0)+1}3^{\pi(1)+1}\ldots p_a^{\pi(a)+1}
\]

where \( p_i \) is the \( i \)th prime. Clearly \( g \) is an injection. Thus \( \text{EC}(\mathbb{N}) \preceq \mathbb{N} \).

By Cantor-Bernstein, \( \mathbb{N} \sim \text{EC}(\mathbb{N}) \). \( \square \)

**6 The proof of Cantor-Bernstein**

Next we turn to the proof of the Cantor-Bernstein Theorem. We shall make use of the following result.

**Definition 6.1.** If \( f : A \rightarrow B \) and \( C \subseteq A \), then

\[
f[C] = \{ f(c) \mid c \in C \}.
\]

**Lemma 6.2.** If \( f : A \rightarrow B \) is an injection and \( C \subseteq A \), then

\[
f[A \setminus C] = f[A] \setminus f[C].
\]
Proof. Suppose that \( x \in f[A \setminus C] \). Then there exists \( a \in A \setminus C \) such that \( f(a) = x \). In particular \( x \in f[A] \). Suppose that \( x \in f[C] \). Then there exists \( c \in C \) such that \( f(c) = x \). But \( a \neq c \) and so this contradicts the fact that \( f \) is an injection. Hence \( x \notin f[C] \) and so \( x \in f[A] \setminus f[C] \).

Conversely suppose that \( x \in f[A] \setminus f[C] \). Since \( x \in f[A] \), there exists \( a \in A \) such that \( f(a) = x \). Since \( x \notin f[C] \), it follows that \( a \notin C \). Thus \( a \in A \setminus C \) and \( x = f(a) \in f[A \setminus C] \).

Theorem 6.3. (Cantor-Bernstein) If \( A \not\preceq B \) and \( B \not\preceq A \), then \( A \sim B \).

Proof. Since \( A \not\preceq B \) and \( B \not\preceq A \), there exists injections \( f : A \to B \) and \( g : B \to A \). Let \( C = g[B] = \{ g(b) \mid b \in B \} \).

Claim 6.4. \( B \sim C \).

Proof of Claim 6.4. The map \( b \mapsto g(b) \) is a bijection from \( B \) to \( C \).

Thus it is enough to prove that \( A \sim C \). For then, \( A \sim C \) and \( C \sim B \), which implies that \( A \sim B \).

Let \( h = g \circ f : A \to C \). Then \( h \) is an injection.

Define by induction on \( n \geq 0 \).

\[
\begin{align*}
A_0 &= A \\
A_{n+1} &= h[A_n] \\
C_0 &= C \\
C_{n+1} &= h[C_n]
\end{align*}
\]

Define \( k : A \to C \) by \( k(x) = h(x) \) if \( x \in A_n \setminus C_n \) for some \( n \)

\[
= x \text{ otherwise}
\]

Claim 6.5. \( k \) is an injection.

Proof of Claim 6.5. Suppose that \( x \neq x' \) are distinct elements of \( A \). We consider three cases.

Case 1:

Suppose that \( x \in A_n \setminus C_n \) and \( x' \in A_m \setminus C_m \) for some \( n, m \). Since \( h \) is an injection, \( k(x) = h(x) = x \neq x' = h(x) = k(x) \).

Case 2:

Suppose that \( x \notin A_n \setminus C_n \) for all \( n \) and that \( x' \notin A_n \setminus C_n \) for all \( n \). Then \( k(x) = x \neq x' = k(x) \).

Case 3:

Suppose that \( x \notin A_n \setminus C_n \) and \( x' \notin A_m \setminus C_m \) for all \( m \). Then \( k(x) = h(x) \in h[A_n \setminus C_n] \)

and \( h[A_n \setminus C_n] = h[A_n] \setminus h[C_n] = A_{n+1} \setminus C_{n+1} \).
Hence \( k(x) = h(x) \neq x' = k(x') \).

**Claim 6.6.** \( k \) is a surjection.

*Proof of Claim 6.6.* Let \( x \in C \). There are two cases to consider.

**Case 1:**
Suppose that \( x \notin A_n \setminus C_n \) for all \( n \). Then \( k(x) = x \).

**Case 2:**
Suppose that \( x \in A_n \setminus C_n \). Since \( x \in C \), we must have that \( n = m + 1 \) for some \( m \). Since
\[
h[A_m \setminus C_m] = A_n \setminus C_n,
\]
there exists \( y \in A_m \setminus C_m \) such that \( k(y) = h(y) = x \).

This completes the proof of the Cantor-Bernstein Theorem.

**Theorem 6.7.** \( \mathbb{R} \sim \mathbb{R} \times \mathbb{R} \)

*Proof.* Since \( (0, 1) \sim \mathbb{R} \), it follows that \( (0, 1) \times (0, 1) \sim \mathbb{R} \times \mathbb{R} \). Hence it is enough to prove that \( (0, 1) \sim (0, 1) \times (0, 1) \).

First define \( f : (0, 1) \rightarrow (0, 1) \times (0, 1) \) by \( f(r) = \langle r, r \rangle \). Clearly \( f \) is an injection and so \( (0, 1) \sim (0, 1) \times (0, 1) \).

Next define \( g : (0, 1) \times (0, 1) \rightarrow (0, 1) \) as follows. Suppose that \( r, s \in (0, 1) \) have decimal expansions
\[
r = 0.r_0r_1\ldots r_n\ldots
\]
\[
s = 0.s_0s_1\ldots s_n\ldots
\]
Then
\[
g(\langle r, s \rangle) = 0.r_0s_0r_1s_1\ldots r_ns_n\ldots
\]
Clearly \( g \) is an injection and so \( (0, 1) \times (0, 1) \sim (0, 1) \).

By Cantor-Bernstein, \( (0, 1) \sim (0, 1) \times (0, 1) \).

**Exercise 6.8.** \( \mathbb{R} \setminus \mathbb{N} \sim \mathbb{R} \)

**Exercise 6.9.** \( \mathbb{R} \setminus \mathbb{Q} \sim \mathbb{R} \)

**Exercise 6.10.** Let \( \text{Sym}(\mathbb{N}) = \{ f \mid f : \mathbb{N} \rightarrow \mathbb{N} \text{ is a bijection} \} \). Prove that \( \mathcal{P}(\mathbb{N}) \sim \text{Sym}(\mathbb{N}) \).

**Definition 6.11.** Let \( A \) be any set. Then a *finite sequence* of elements of \( A \) is an object \( \langle a_0, a_1, \ldots, a_n \rangle, \ n \geq 0 \) so that each \( a_i \in A \), chosen so that \( \langle a_0, a_1, \ldots, a_n \rangle = \langle b_0, b_1, \ldots, b_n \rangle \) iff \( n = m \) and \( a_i = b_i \) for \( 0 \leq i \leq n \).

\( \text{FinSeq}(A) \) is the set of all finite sequences of elements of \( A \).
Theorem 6.12. If $A$ is a nonempty countable set, then $\mathbb{N} \sim \text{FinSeq}(A)$.

Proof. First we prove that $\mathbb{N} \leq \text{FinSeq}(A)$. Fix some $a \in A$. Then we define $f : \mathbb{N} \to \text{FinSeq}(A)$ by

$$f(n) = \langle a, a, a, a, \ldots, a \rangle_{n + 1 \text{ times}}.$$ 

Clearly $f$ is an injection and so $\mathbb{N} \leq \text{FinSeq}(A)$.

Next we prove that $\text{FinSeq}(A) \leq \mathbb{N}$. Since $A$ is countable, there exists an injection $e : A \to \mathbb{N}$. Define $g : \text{FinSeq}(A) \to \mathbb{N}$ by

$$g(\langle a_0, a_1, \ldots, a_n \rangle) = 2^{e(a_0)+1} \cdots p_{e(a_n)+1}^{e(a_n)+1}$$

where $p_i$ is the $i^{\text{th}}$ prime. Clearly $g$ is an injection. Hence $\text{FinSeq}(A) \leq \mathbb{N}$.

By Cantor-Bernstein, $\mathbb{N} \sim \text{FinSeq}(A)$. \qed