Set Cardinality

Prof. Dan A. Simovici

UMB
1 Set cardinality

2 Pairing Functions
**Definition**

Two sets, $A, B$ have the same **cardinality**, written $A \sim B$, if there exists a bijection $f : A \rightarrow B$.

**Example**

The set of even numbers, $E = \{ n \mid n = 2k, \text{ for some } k \in \mathbb{N} \}$ and the set $\mathbb{N}$ have the same cardinality, because $f : \mathbb{N} \rightarrow E$ defined by $f(n) = 2n$ is a bijection.
Theorem

The relation $\sim$ is an equivalence relation.

Proof.

For every set $A$, $1_A : A \rightarrow A$ is a bijection. Therefore, $A \sim A$ for every $A$, so $\sim$ is reflexive. If $f : A \rightarrow B$ is a bijection, then $f^{-1} : A \rightarrow A$ is a bijection, so $A \sim B$ implies $B \sim A$, which shows that $\sim$ is symmetric. Transitivity follows from the fact that the composition of two bijections is a bijection.
Theorem

If $A \sim B$, then $\mathcal{P}(A) \sim \mathcal{P}(B)$.

Proof.

Let $f : A \rightarrow B$ be a bijection between $A$ and $B$. Define the mapping $F : \mathcal{P}(A) \rightarrow \mathcal{P}(B)$ by $F(L) = \{ b \in B \mid b = f(a) \text{ for some } a \in L \}$ for every $L \in \mathcal{P}(A)$. It is easy to verify that $F$ is a bijection. Thus, $\mathcal{P}(A) \sim \mathcal{P}(B)$. 

\square
Definition

A set $A$ is **countable** if it has the same cardinality as a subset of $\mathbb{N}$. $A$ is **finite** if there is an integer $k \in \mathbb{N}$ such that $A$ has the same cardinality as a subset of $\{0, 1, \ldots, k\}$. 
Note that any finite set is countable. The following theorem will help us enumerate finite sets.

**Theorem**

*If A is finite, then there is a unique $k \in \mathbb{N}$ for which $A \sim \{0, 1, \ldots, k - 1\}$. In this case, we write $|A| = k$ and say that “A has $k$ elements.”*

**Proof.**

Assume $A$ is finite. Let $M = \{m \in \mathbb{N} \mid A$ has the same cardinality as some subset of $\{0, 1, \ldots, m - 1\}\}$. Since $A$ is finite, $M \neq \emptyset$, so $M$ has a least element, $k$, which clearly satisfies the requirements of the theorem. [QED]
Often it is desirable to be able explicitly to enumerate the elements of \( A \). If \( A \) is finite, with \( |A| = k \), then there is a bijection \( f : \{0, 1, \ldots, k - 1\} \longrightarrow A \), and we can enumerate \( A = \{a_0, a_1, \ldots, a_{k-1}\} \), where \( a_i = f(i) \).

If \( A \) is infinite but countable, we write \( |A| = \aleph_0 \) and say “\( A \) is countably infinite.” (The symbol \( \aleph \) (pronounced “aleph”) is the first letter of the Hebrew alphabet).
Theorem

If $|A| = \aleph_0$, then there is a bijection $f : \mathbb{N} \rightarrow A$.

Proof.

Since $A$ is countable, there is a bijection $g : A \rightarrow S \subseteq \mathbb{N}$. To define $f : \mathbb{N} \rightarrow A$ inductively, we simultaneously define both $f$ and a subset of $S$. Let $f(0) = g^{-1}(s_0)$, where $s_0$ is the smallest element in $S$. Assume $\{f(0), f(1), \ldots f(k-1)\}$ and $\{s_0, s_1, \ldots s_{k-1}\}$ have been defined. Then define $f(k) = g^{-1}(s_k)$, where $s_k$ is the smallest element in $S - \{s_0, s_1, \ldots s_{k-1}\}$. Since $A$ is infinite, $S$ is also infinite, so $S - \{s_0, s_1, \ldots s_{k-1}\} \neq \emptyset$, and a smallest element always exists. By construction, if $m_0 < m_1$ then $f(m_1) \not\in \{f(0), f(1), \ldots f(m_0)\}$, since $g$ is a bijection (and hence $g^{-1}$ is, too.) So, if $f(m_0) = f(m_1)$ then clearly $m_0 = m_1$. We have to check that $f$ is also onto. An easy induction shows that $s_k \geq k$, for all $k \in \mathbb{N}$. Let $a \in A$, with $g(a) = m$. Then, $m = s_j$ for some $j \leq m$, so $f(s_j) = a$. 

\qed
Corollary

If $|A| = \aleph_0$, then there is a bijection $g : A \rightarrow \mathbb{N}$.

Proof.

This follows from the fact that the inverse of a bijection is again a bijection.
Theorem

Let $A, B$ be two countable sets. Then, $A \cup B$ is countable.

Proof.

Assume $A, B$ are two countable sets, and let $f : A \to \mathbb{N}$ and $g : B \to \mathbb{N}$ be injections. Define $h : A \cup B \to \mathbb{N}$ by

$$h(x) = \begin{cases} 
2f(x) & \text{if } x \in A - B \\
2g(x) + 1 & \text{if } x \in B.
\end{cases}$$

The function $h : A \cup B \to \mathbb{N}$ is easily seen to be an injection; hence, $A \cup B$ is countable.
Corollary

The union of any finite collection of countable sets is countable.
Theorem

Let $A, B, C$ be sets, where $A$ is countable.

1. If there is a surjection $f : A \rightarrow B$, then $B$ is countable.
2. If there is an injection $\ell : C \rightarrow A$, then $C$ is countable.

Proof.

For the first part of the theorem assume $A$ is countable and $f : A \rightarrow B$ is a surjection. Since $A$ is countable, there is an injection $g : A \rightarrow \mathbb{N}$. Define $h : B \rightarrow \mathbb{N}$ by

$$h(b) = \min \{g(a) \mid f(a) = b\}.$$

We need to verify that $h$ is an injection. Let $b_0, b_1 \in B$ such that $h(b_0) = h(b_1)$. Let $a_i \in A$ be the element such that $h(b_i) = g(a_i)$ for $i = 0, 1$. Then, $g(a_0) = g(a_1)$, and since $g$ is an injection, $a_0 = a_1$, so $f(a_0) = f(a_1)$, and thus $b_0 = b_1$.

For the second part note that the function $g\ell : C \rightarrow \mathbb{N}$ is an injection; this implies immediately the countability of $C$. 

\[\Box\]
Let $A, B$ be two sets. If $f : A \to B$ is a bijection, then $A$ is countable if and only if $B$ is countable.

Let $A, B$ be two sets. If $f : A \to B$ is an injection and $A$ is not countable, then $B$ is not countable.
Theorem

Any subset of a countable set is countable.

Proof.

Assume $B \subseteq A$, where $A$ is countable. If $B = \emptyset$, then it is clearly countable. If $B \neq \emptyset$, pick $b \in B$, and define $f : A \rightarrow B$ by

$$f(x) = \begin{cases} x & \text{if } x \in B \\ b & \text{if } x \notin B. \end{cases}$$

The function $f$ is clearly a surjection, so $B$ is countable.
Theorem

Let $A_0, \ldots, A_{n-1}$ be $n$ countable sets. The Cartesian product $A_0 \times \cdots \times A_{n-1}$ is countable.
Proof

Since $A_0, \ldots, A_{n-1}$ are countable sets, there exist injections $f_i : A_i \longrightarrow \mathbb{N}$ for $0 \leq i \leq n - 1$. For $(a_0, \ldots, a_{n-1}) \in A_0 \times \cdots \times A_{n-1}$, define

$$h(a_0, \ldots, a_{n-1}) = 2^{f_0(a_0)} \cdot 3^{f_1(a_1)} \cdots \cdot p^{a_{n-1}}_{n-1},$$

where $p_{i-1}$ is the $i^{th}$ prime number for $0 \leq i \leq n - 1$. By the Fundamental Theorem of Arithmetic $h : A_0 \times \cdots \times A_{n-1} \longrightarrow \mathbb{N}$ is an injection, so $A_0 \times \cdots \times A_{n-1}$ is countable. (The Fundamental Theorem of Arithmetic states that each natural number larger than one can be written uniquely as a product powers of primes.)
Example
Let $D$ be a countable set. The set $D^n$ of sequences of length $n$ of elements of $D$ is a countable set for every $n \in \mathbb{N}$. 
Theorem

The union of a countable collection of countable sets that are pairwise disjoint, is a countable set.
Proof

Let $K$ be a countable set, and let each $\{A_k \mid k \in K\}$ be countable. Then there are injections $f : K \rightarrow \mathbb{N}$ and $g_k : A_k \rightarrow \mathbb{N}$ for each $k \in K$. Assume that $A_i \cap A_j = \emptyset$ for $i \neq j \in K$. To show that $A = \bigcup_{k \in K} A_k$ is countable, we define an injection $h : A \rightarrow \mathbb{N}$. Let $P = \{p_0, p_1, \ldots\}$ be an enumeration of the prime numbers. Since the sets $A_k$ are pairwise disjoint, given any $a \in A$, there is a unique $k$ with $a \in A_k$. We use this fact to define

$$h(a) = p_{g_k(a)}^{f(k)}.$$

It follows from the Fundamental Theorem of Arithmetic that $h$ is an injection, and thus $A$ is countable.
Example

if $D$ is a countable set, the set of sequences of length $n$, $\text{Seq}_n(D)$ is countable. Therefore, the set of all sequences $\text{Seq}(D) = \bigcup \{D^n \mid n \in \mathbb{N}\}$ is countable as a union of a countable collection of sets.
Definition

A pairing function is a bijection $\varphi : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$. 
**Example**

There are many possible pairing functions, but consider the one suggested by the following picture:

<table>
<thead>
<tr>
<th>( \varphi(i, j) )</th>
<th>( i )</th>
<th>( 0 )</th>
<th>( 1 )</th>
<th>( 2 )</th>
<th>( 3 )</th>
<th>( 4 )</th>
<th>( 5 )</th>
<th>( \ldots )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( i )</td>
<td>0</td>
<td>0 1</td>
<td>3 6</td>
<td>10</td>
<td>( \ldots )</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2 4 7</td>
<td>( \ldots )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>5 8 12</td>
<td>( \ldots )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>9 13 ( \ldots )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>14 ( \ldots )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \ldots )</td>
<td>( \ldots )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The diagonal $D_m$ that contains all pairs $(i, j)$ such that $i + j = m$ contains $m + 1$ pairs. The pair $(i, j)$ is located on the diagonal $D_{i+j}$ and that this diagonal is preceded by the diagonals $D_0, \ldots, D_{i+j-1}$ that have a total of $1 + 2 + \cdots + (i + j) = (i + j)(i + j + 1)/2$ elements. Thus, the pair $(i, j)$ is enumerated on the place $(i + j)(i + j + 1)/2 + i$ and this shows that the mapping $\varphi : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ given by

$$\varphi(i, j) = \frac{1}{2}[(i + j)^2 + 3i + j]$$

is a bijection.
It is important to realize that not all sets are countable. Consider $\mathcal{P}(\mathbb{N})$, the power set of $\mathbb{N}$. This certainly has at least as many elements as $\mathbb{N}$, since $\{k\}$ is in $\mathcal{P}(\mathbb{N})$ for each $k \in \mathbb{N}$. However, it has so many more sets that it is not possible to count them all.

**Theorem**

*The set $\mathcal{P}(\mathbb{N})$ is not countable.*
Proof

Assume that $\mathcal{P}(\mathbb{N})$ were countable. Then there would be an bijection $f : \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N})$; i.e., for each $n \in \mathbb{N}$, we would have a distinct subset $f(n) \subseteq \mathbb{N}$. We show that the existence of this bijection leads to a contradiction.

Define the $D = \{ n \mid n \not\in f(n) \}$. Clearly, $D \subseteq \mathbb{N}$, so we must have $D = f(k)$ for some $k \in \mathbb{N}$. We must now have one of two situations: either $k \in D$, or $k \not\in D$. First, suppose that $k \in D$. Then, by the definition of $D$, $k \not\in f(k)$, but $f(k) = D$, so we have that $k \in D$ implies that $k \not\in D$; this cannot be. Suppose, on the other hand, that $k \not\in D$. Then, by the definition of $D$, $k \in f(k)$, and since $f(k) = D$, we have $k \not\in D$ implies $k \in D$. Again, this cannot be. Either way, we have a contradiction. From this, we necessarily conclude that the assumed bijection $f$ cannot exist.
Another Look to the Previous Proof

If there were a bijection $f : \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N})$, then we could have the following list:

\[
\begin{align*}
0 : & \quad a_{00} \ a_{01} \ a_{02} \ a_{03} \ a_{04} \ldots \\
1 : & \quad a_{10} \ a_{11} \ a_{12} \ a_{13} \ a_{14} \ldots \\
2 : & \quad a_{20} \ a_{21} \ a_{22} \ a_{23} \ a_{24} \ldots \\
3 : & \quad a_{30} \ a_{31} \ a_{32} \ a_{33} \ a_{34} \ldots \\
4 : & \quad a_{40} \ a_{41} \ a_{42} \ a_{43} \ a_{44} \ldots \\
5 : & \quad a_{50} \ a_{51} \ a_{52} \ a_{53} \ a_{54} \ldots \\
& \vdots \\
k : & \quad a_{k0} \ a_{k1} \ a_{k2} \ a_{k3} \ a_{k4} \ldots \ a_{kk}
\end{align*}
\]

where

\[
a_{ij} = \begin{cases} 
0 & \text{if } j \notin f(i) \\
1 & \text{if } j \in f(i).
\end{cases}
\]
The set $D$ is formed by “going down the diagonal” and spoiling the possibility that $D = f(k)$, for each $k$. At row $k$, we look at $a_{kk}$ in column $k$. If this is 1, i.e., if $k \in f(k)$, then we make sure that the corresponding position for the set $D$ has a 0 in it by saying that $k \notin D$. On the other hand, if $a_{kk}$ is a 0, i.e., $k \notin f(k)$, then we force the corresponding position for the set $D$ to be a 1 by putting $k$ into $D$. This guarantees that $D \neq f(k)$, because its characteristic functions differs from that of $f(k)$ in column $k$.

This proof technique, usually referred to as diagonalization, first appeared in an 1891 paper of Georg Cantor (1845–1918); it has found many applications in the theory of computation.
Corollary

If $A$ is a countably infinite set, then $\mathcal{P}(A)$ is not countable.

Proof.

Let $A$ be a countably infinite set. Since $A \sim \mathbb{N}$, we have $\mathbb{N} \sim A$, so there is a bijection $F : \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(A)$. If $\mathcal{P}(A)$ were countable (and, therefore, countably infinite), this would imply the existence of a bijection $G : \mathcal{P}(A) \rightarrow \mathbb{N}$, so we would obtain a bijection between $\mathcal{P}(\mathbb{N})$ and $\mathbb{N}$. \qed
Example

Let $F_2$ be the set of all functions of the form $f : \mathbb{N} \rightarrow \{0, 1\}$. Define the mapping $\phi : F_2 \rightarrow \mathcal{P}(\mathbb{N})$ by $\phi(f) = \{n \in \mathbb{N} \mid f(n) = 1\}$. It is not difficult to see that $\phi$ is a bijection. Indeed, suppose that $\phi(f) = \phi(g)$, that is $\{n \in \mathbb{N} \mid f(n) = 1\} = \{n \in \mathbb{N} \mid g(n) = 1\}$. 
This means that $f(n) = 1$ if and only if $g(n) = 1$ for $n \in \mathbb{N}$, so $f = g$, which means that $\phi$ is an injection. To prove that $\phi$ is a bijection consider an arbitrary subset $K$ of $\mathbb{N}$. Then, for its characteristic function $f_K$ (given by $f_K(n) = 1$ if $n \in K$ and $f_K(n) = 0$, otherwise) we have $\phi(f_K) = K$, so $\phi$ is also a surjection, and therefore, a bijection. Thus, we conclude that the set $F_2$ is not countable.

If $F$ is the set of functions of the form $f : \mathbb{N} \rightarrow \mathbb{N}$, then the uncountability of $F_2$ implies the uncountability of $F$. 