Discrete Mathematics & Mathematical Reasoning
Cardinality

Colin Stirling

Informatics
Finite and infinite sets

- $A = \{1, 2, 3\}$ is a finite set with 3 elements
Finite and infinite sets

- \( A = \{1, 2, 3\} \) is a finite set with 3 elements
- \( B = \{a, b, c, d\} \) and \( C = \{1, 2, 3, 4\} \) are finite sets with 4 elements
Finite and infinite sets

- $A = \{1, 2, 3\}$ is a finite set with 3 elements
- $B = \{a, b, c, d\}$ and $C = \{1, 2, 3, 4\}$ are finite sets with 4 elements
- For finite sets, $|X| \leq |Y|$ iff there is an injection $f : X \rightarrow Y$
Finite and infinite sets

• $A = \{1, 2, 3\}$ is a finite set with 3 elements
• $B = \{a, b, c, d\}$ and $C = \{1, 2, 3, 4\}$ are finite sets with 4 elements
• For finite sets, $|X| \leq |Y|$ iff there is an injection $f : X \rightarrow Y$
• For finite sets, $|X| = |Y|$ iff there is an bijection $f : X \rightarrow Y$
Finite and infinite sets

- \( A = \{1, 2, 3\} \) is a finite set with 3 elements
- \( B = \{a, b, c, d\} \) and \( C = \{1, 2, 3, 4\} \) are finite sets with 4 elements
- For finite sets, \(|X| \leq |Y|\) iff there is an injection \( f : X \to Y \)
- For finite sets, \(|X| = |Y|\) iff there is a bijection \( f : X \to Y \)
- \( \mathbb{Z}^+, \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R} \) are infinite sets
Finite and infinite sets

- $A = \{1, 2, 3\}$ is a finite set with 3 elements
- $B = \{a, b, c, d\}$ and $C = \{1, 2, 3, 4\}$ are finite sets with 4 elements
- For finite sets, $|X| \leq |Y|$ iff there is an injection $f : X \to Y$
- For finite sets, $|X| = |Y|$ iff there is an bijection $f : X \to Y$
- $\mathbb{Z}^+, \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are infinite sets
- When do two infinite sets have the same size?
Finite and infinite sets

- $A = \{1, 2, 3\}$ is a finite set with 3 elements
- $B = \{a, b, c, d\}$ and $C = \{1, 2, 3, 4\}$ are finite sets with 4 elements
- For finite sets, $|X| \leq |Y|$ iff there is an injection $f : X \rightarrow Y$
- For finite sets, $|X| = |Y|$ iff there is a bijection $f : X \rightarrow Y$
- $\mathbb{Z}^+, \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are infinite sets
- When do two infinite sets have the same size?
- Same answer
Cardinality of sets

Definition

- Two sets $A$ and $B$ have the same cardinality, $|A| = |B|$, iff there exists a bijection from $A$ to $B$
Cardinality of sets

Definition

- Two sets $A$ and $B$ have the same cardinality, $|A| = |B|$, iff there exists a bijection from $A$ to $B$.
- $|A| \leq |B|$ iff there exists an injection from $A$ to $B$.
Cardinality of sets

**Definition**

- Two sets $A$ and $B$ have the same cardinality, $|A| = |B|$, iff there exists a bijection from $A$ to $B$.
- $|A| \leq |B|$ iff there exists an injection from $A$ to $B$.
- $|A| < |B|$ iff $|A| \leq |B|$ and $|A| \neq |B|$ (A smaller cardinality than $B$).
Cardinality of sets

Definition

- Two sets $A$ and $B$ have the same cardinality, $|A| = |B|$, iff there exists a bijection from $A$ to $B$
- $|A| \leq |B|$ iff there exists an injection from $A$ to $B$
- $|A| < |B|$ iff $|A| \leq |B|$ and $|A| \neq |B|$ (A smaller cardinality than $B$)

Unlike finite sets, for infinite sets $A \subset B$ and $|A| = |B|$
Cardinality of sets

Definition

- Two sets $A$ and $B$ have the same cardinality, $|A| = |B|$, iff there exists a bijection from $A$ to $B$
- $|A| \leq |B|$ iff there exists an injection from $A$ to $B$
- $|A| < |B|$ iff $|A| \leq |B|$ and $|A| \neq |B|$ (A smaller cardinality than $B$)

Unlike finite sets, for infinite sets $A \subset B$ and $|A| = |B|$

$\text{Even} = \{2n \mid n \in \mathbb{N}\} \subset \mathbb{N}$ and $|\text{Even}| = |\mathbb{N}|$
Cardinality of sets

Definition

- Two sets $A$ and $B$ have the same cardinality, $|A| = |B|$, iff there exists a bijection from $A$ to $B$
- $|A| \leq |B|$ iff there exists an injection from $A$ to $B$
- $|A| < |B|$ iff $|A| \leq |B|$ and $|A| \neq |B|$ (A smaller cardinality than $B$)

Unlike finite sets, for infinite sets $A \subset B$ and $|A| = |B|$

Even $= \{2n \mid n \in \mathbb{N}\} \subset \mathbb{N}$ and $|Even| = |\mathbb{N}|$

$f : Even \rightarrow \mathbb{N}$ with $f(2n) = n$ is a bijection
Definition

A set $S$ is called countably infinite, iff it has the same cardinality as the positive integers, $|\mathbb{Z}^+| = |S|$.
Countable sets

**Definition**

- A set $S$ is called countably infinite, iff it has the same cardinality as the positive integers, $|\mathbb{Z}^+| = |S|$.
- A set is called countable iff it is either finite or countably infinite.
Countable sets

Definition

- A set $S$ is called countably infinite, iff it has the same cardinality as the positive integers, $|\mathbb{Z}^+| = |S|$
- A set is called countable iff it is either finite or countably infinite
- A set that is not countable is called uncountable
Countable sets

Definition

- A set $S$ is called countably infinite, iff it has the same cardinality as the positive integers, $|\mathbb{Z}^+| = |S|$
- A set is called countable iff it is either finite or countably infinite
- A set that is not countable is called uncountable

$\mathbb{N}$ is countably infinite; what is the bijection $f : \mathbb{Z}^+ \to \mathbb{N}$?
Definition

- A set $S$ is called countably infinite, iff it has the same cardinality as the positive integers, $|\mathbb{Z}^+| = |S|$
- A set is called countable iff it is either finite or countably infinite
- A set that is not countable is called uncountable

$\mathbb{N}$ is countably infinite; what is the bijection $f : \mathbb{Z}^+ \rightarrow \mathbb{N}$?

$\mathbb{Z}$ is countably infinite; what is the bijection $g : \mathbb{Z}^+ \rightarrow \mathbb{Z}$?
The positive rational numbers are countable

Construct a bijection \( f : \mathbb{Z}^+ \rightarrow \mathbb{Q}^+ \)
The positive rational numbers are countable

Construct a bijection $f : \mathbb{Z}^+ \rightarrow \mathbb{Q}^+$

List fractions $p/q$ with $q = n$ in the $n^{th}$ row
The positive rational numbers are countable

Construct a bijection \( f : \mathbb{Z}^+ \rightarrow \mathbb{Q}^+ \)

List fractions \( p/q \) with \( q = n \) in the \( n^{th} \) row

\( f \) traverses this list in the order for \( m = 2, 3, 4, \ldots \) visiting all \( p/q \) with \( p + q = m \) (and listing only new rationals)
The positive rational numbers are countable

Construct a bijection $f : \mathbb{Z}^+ \rightarrow \mathbb{Q}^+$

List fractions $p/q$ with $q = n$ in the $n^{th}$ row

$f$ traverses this list in the order for $m = 2, 3, 4, \ldots$ visiting all $p/q$ with $p + q = m$ (and listing only new rationals)
Theorem

If A and B are countable sets, then $A \cup B$ is countable
Countable sets

Theorem

If $A$ and $B$ are countable sets, then $A \cup B$ is countable

Proof in book
Countable sets

Theorem

If $A$ and $B$ are countable sets, then $A \cup B$ is countable

Proof in book

Theorem

If $I$ is countable and for each $i \in I$ the set $A_i$ is countable then $\bigcup_{i \in I} A_i$ is countable
Countable sets

**Theorem**

*If A and B are countable sets, then \( A \cup B \) is countable*

**Proof in book**

**Theorem**

*If \( I \) is countable and for each \( i \in I \) the set \( A_i \) is countable then \( \bigcup_{i \in I} A_i \) is countable*

**Proof in book**
Finite strings

Theorem

The set $\Sigma^*$ of all finite strings over a finite alphabet $\Sigma$ is countably infinite.

Proof.

First define an (alphabetical) ordering on the symbols in $\Sigma$.

Show that the strings can be listed in a sequence:

- First single string $\epsilon$ of length 0.
- Then all strings of length 1 in lexicographic order.
- Then all strings of length 2 in lexicographic order.
- ...
Finite strings

Theorem

The set $\Sigma^*$ of all finite strings over a finite alphabet $\Sigma$ is countably infinite

Proof.

First define an (alphabetical) ordering on the symbols in $\Sigma$.
Show that the strings can be listed in a sequence:

- First single string $\varepsilon$ of length 0
- Then all strings of length 1 in lexicographic order
- Then all strings of length 2 in lexicographic order

...
Finite strings

**Theorem**

\( \Sigma^* \) of all finite strings over a finite alphabet \( \Sigma \) is countably infinite

**Proof.**

- First define an (alphabetical) ordering on the symbols in \( \Sigma \).
- Show that the strings can be listed in a sequence:
  - First single string \( \varepsilon \) of length 0
  - Then all strings of length 1 in lexicographic order
  - Then all strings of length 2 in lexicographic order
  - ...
  - ...

- Each of these sets is countable; so is their union \( \Sigma^* \)
Finite strings

Theorem

The set $\Sigma^*$ of all finite strings over a finite alphabet $\Sigma$ is countably infinite

Proof.

- First define an (alphabetical) ordering on the symbols in $\Sigma$
  - Show that the strings can be listed in a sequence
    - First single string $\varepsilon$ of length 0
    - Then all strings of length 1 in lexicographic order
    - Then all strings of length 2 in lexicographic order
    - ...
    - ...
  - Each of these sets is countable; so is their union $\Sigma^*$

The set of Java-programs is countable; a program is just a finite string.
Infinite binary strings

- An infinite length string of bits 10010...
Infinite binary strings

- An infinite length string of bits 10010...
- Such a string is a function $d : \mathbb{Z}^+ \rightarrow \{0, 1\}$
Infinite binary strings

- An infinite length string of bits 10010...
- Such a string is a function $d : \mathbb{Z}^+ \to \{0, 1\}$
- With the property $d_m = d(m)$ is the $m$th symbol
Uncountable sets

Theorem

The set of infinite binary strings is uncountable

Proof. Let $X$ be the set of infinite binary strings. For a contradiction assume that a bijection $f : \mathbb{Z}^+ \rightarrow X$ exists. So, $f$ must be onto (surjective).

Assume that $f(i) = d_i$ for $i \in \mathbb{Z}^+$. So, $X = \{d_1, d_2, \ldots, d_m, \ldots\}$. Define the infinite binary string $d$ as follows: $d_n = (d_{n+1}) \mod 2$. But for each $m$, $d \neq d_m$ because $d_m \neq d_m$. So, $f$ is not a surjection.

The technique used here is called diagonalization. Similar argument shows that $\mathbb{R}$ via $[0, 1]$ is uncountable using infinite decimal strings (see book).
Uncountable sets

**Theorem**

*The set of infinite binary strings is uncountable*

**Proof.**

Let $X$ be the set of infinite binary strings. For a contradiction assume that a bijection $f : \mathbb{Z}^+ \rightarrow X$ exists. So, $f$ must be onto (surjective). Assume that $f(i) = d^i$ for $i \in \mathbb{Z}^+$. So, $X = \{d^1, d^2, \ldots, d^m, \ldots\}$. Define the infinite binary string $d$ as follows: $d_n = (d_n^i + 1) \mod 2$. But for each $m$, $d \neq d^m$ because $d_m \neq d_m^m$. So, $f$ is not a surjection. \qed
Theorem

The set of infinite binary strings is uncountable

Proof.

Let $X$ be the set of infinite binary strings. For a contradiction assume that a bijection $f : \mathbb{Z}^+ \rightarrow X$ exists. So, $f$ must be onto (surjective). Assume that $f(i) = d^i$ for $i \in \mathbb{Z}^+$. So, $X = \{d^1, d^2, \ldots, d^m, \ldots\}$. Define the infinite binary string $d$ as follows: $d_n = (d^n_n + 1) \mod 2$. But for each $m$, $d \neq d^m$ because $d_m \neq d^m_m$. So, $f$ is not a surjection.

The technique used here is called diagonalization
Uncountable sets

Theorem

The set of infinite binary strings is uncountable

Proof.

Let $X$ be the set of infinite binary strings. For a contradiction assume that a bijection $f : \mathbb{Z}^+ \rightarrow X$ exists. So, $f$ must be onto (surjective). Assume that $f(i) = d^i$ for $i \in \mathbb{Z}^+$. So, $X = \{d^1, d^2, \ldots, d^m, \ldots\}$. Define the infinite binary string $d$ as follows: $d_n = (d^n_n + 1) \mod 2$. But for each $m$, $d \neq d^m$ because $d_m \neq d^m_m$. So, $f$ is not a surjection.

The technique used here is called diagonalization.
Uncountable sets

Theorem

The set of infinite binary strings is uncountable

Proof.

Let $X$ be the set of infinite binary strings. For a contradiction assume that a bijection $f : \mathbb{Z}^+ \to X$ exists. So, $f$ must be onto (surjective). Assume that $f(i) = d^i$ for $i \in \mathbb{Z}^+$. So, $X = \{d^1, d^2, \ldots, d^m, \ldots\}$. Define the infinite binary string $d$ as follows: $d_n = (d_n^n + 1) \mod 2$. But for each $m$, $d \neq d^m$ because $d_m \neq d_m^m$. So, $f$ is not a surjection.

The technique used here is called diagonalization.

Similar argument shows that $\mathbb{R}$ via $[0, 1]$ is uncountable using infinite decimal strings (see book).
The set of functions $F = \{ f \mid f : \mathbb{Z} \to \mathbb{Z} \}$ is uncountable.

Therefore, "most functions" in $F$ are not computable!
More on the uncountable

Corollary

The set of functions \( F = \{ f \mid f : \mathbb{Z} \to \mathbb{Z} \} \) is uncountable

The set of functions \( C = \{ f \mid f : \mathbb{Z} \to \mathbb{Z} \text{ is computable} \} \) is countable
More on the uncountable

Corollary

The set of functions $F = \{ f \mid f : \mathbb{Z} \rightarrow \mathbb{Z} \}$ is uncountable

The set of functions $C = \{ f \mid f : \mathbb{Z} \rightarrow \mathbb{Z} \text{ is computable} \}$ is countable

Therefore, “most functions” in $F$ are not computable!
Theorem

If $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$
Schröder-Bernstein Theorem

**Theorem**

If $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$

- **Example** $|(0, 1)| = |(0, 1]|$
Schröder-Bernstein Theorem

Theorem

If \(|A| \leq |B|\) and \(|B| \leq |A|\) then \(|A| = |B|\)

- Example \(|(0, 1)| = |(0, 1]|\)
- \(|(0, 1)| \leq |(0, 1]|\) using identity function
Schröder-Bernstein Theorem

**Theorem**

*If* $|A| \leq |B|$ and $|B| \leq |A|$ *then* $|A| = |B|$ *

- **Example** $|(0, 1)| = |(0, 1]|$
- $|(0, 1)| \leq |(0, 1]|$ *using identity function*
- $|(0, 1]| \leq |(0, 1)|$ *use* $f(x) = x/2$ *as* $(0, 1/2] \subset (0, 1)$
Cantor’s theorem

**Theorem**

\[ |A| < |\mathcal{P}(A)| \]

**Proof.** Consider the injection \( f : A \to \mathcal{P}(A) \) with \( f(a) = \{a\} \) for any \( a \in A \). Therefore, \( |A| \leq |\mathcal{P}(A)| \).

Next we show there is not a surjection \( f : A \to \mathcal{P}(A) \). For a contradiction, assume that a surjection \( f \) exists. We define the set \( B \subseteq A \):

\[ B = \{ x \in A | x \not\in f(x) \} \]

Since \( f \) is a surjection, there must exist an \( a \in A \) s.t. \( B = f(a) \). Now there are two cases:

1. If \( a \in B \) then, by definition of \( B \), \( a \not\in B = f(a) \). Contradiction
2. If \( a \not\in B \) then \( a \not\in f(a) \); by definition of \( B \), \( a \in B \). Contradiction
Cantor’s theorem

Theorem

\[ |A| < |\mathcal{P}(A)| \]

Proof.

Consider the injection \( f : A \to \mathcal{P}(A) \) with \( f(a) = \{a\} \) for any \( a \in A \). Therefore, \( |A| \leq |\mathcal{P}(A)| \). Next we show there is not a surjection \( f : A \to \mathcal{P}(A) \). For a contradiction, assume that a surjection \( f \) exists. We define the set \( B \subseteq A : B = \{x \in A \mid x \notin f(x)\} \). Since \( f \) is a surjection, there must exist an \( a \in A \) s.t. \( B = f(a) \). Now there are two cases:

1. If \( a \in B \) then, by definition of \( B \), \( a \notin B = f(a) \). Contradiction
2. If \( a \notin B \) then \( a \notin f(a) \); by definition of \( B \), \( a \in B \). Contradiction
Implications of Cantor’s theorem

- \( \mathcal{P}(\mathbb{N}) \) is not countable (in fact, \( |\mathcal{P}(\mathbb{N})| = |\mathbb{R}| \))
Implications of Cantor’s theorem

- $\mathcal{P}(\mathbb{N})$ is not countable (in fact, $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$)
- The Continuum Hypothesis claims there is no set $S$ with $|\mathbb{N}| < |S| < |\mathbb{R}|$
Implications of Cantor’s theorem

- \( \mathcal{P}(\mathbb{N}) \) is not countable (in fact, \( |\mathcal{P}(\mathbb{N})| = |\mathbb{R}| \))
- The Continuum Hypothesis claims there is no set \( S \) with \(|\mathbb{N}| < |S| < |\mathbb{R}|\)
- It was 1st of Hilbert’s 23 open problems presented in 1900. Shown to be independent of ZFC set theory by Gödel/Cohen in 1963: cannot be proven/disproven in ZFC
Implications of Cantor’s theorem

- $\mathcal{P}(\mathbb{N})$ is not countable (in fact, $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$)
- The Continuum Hypothesis claims there is no set $S$ with $|\mathbb{N}| < |S| < |\mathbb{R}|$
- It was 1st of Hilbert’s 23 open problems presented in 1900. Shown to be independent of ZFC set theory by Gödel/Cohen in 1963: cannot be proven/disproven in ZFC
- There exists an infinite hierarchy of sets of ever larger cardinality
Implications of Cantor’s theorem

- $\mathcal{P}(\mathbb{N})$ is not countable (in fact, $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$)
- The Continuum Hypothesis claims there is no set $S$ with $|\mathbb{N}| < |S| < |\mathbb{R}|$
- It was 1st of Hilbert’s 23 open problems presented in 1900. Shown to be independent of ZFC set theory by Gödel/Cohen in 1963: cannot be proven/disproven in ZFC
- There exists an infinite hierarchy of sets of ever larger cardinality
- $S_0 = \mathbb{N}$ and $S_{i+1} = \mathcal{P}(S_i)$
**Implications of Cantor’s theorem**

- \(\mathcal{P}(\mathbb{N})\) is not countable (in fact, \(|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|\))
- The Continuum Hypothesis claims there is no set \(S\) with \(|\mathbb{N}| < |S| < |\mathbb{R}|\)
- It was 1st of Hilbert’s 23 open problems presented in 1900. Shown to be independent of ZFC set theory by Gödel/Cohen in 1963: cannot be proven/disproved in ZFC
- There exists an infinite hierarchy of sets of ever larger cardinality
- \(S_0 = \mathbb{N}\) and \(S_{i+1} = \mathcal{P}(S_i)\)
- \(|S_0| < |S_1| < \ldots < |S_i| < |S_{i+1}| < \ldots\)