Discrete Mathematics & Mathematical Reasoning
Cardinality

Colin Stirling

Informatics

Some slides based on ones by Myrto Arapinis and by Richard Mayr

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)

When A and B are finite $|A| = |B|$ iff they have same size

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)

When A and B are finite $|A| = |B|$ iff they have same size

$\mathbb{N}$ and its subset Even $= \{2n \mid n \in \mathbb{N}\}$ have the same cardinality, because $f : \mathbb{N} \to$ Even where $f(n) = 2n$ is a bijection

Countable Sets

Definition

- A set S is called countably infinite, iff it has the same cardinality as the natural numbers, $|S| = |\mathbb{N}|$

Countable Sets

Definition

- A set S is called countably infinite, iff it has the same cardinality as the natural numbers, $|S| = |\mathbb{N}|$
- 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 natural numbers, $|S| = |\mathbb{N}|$
- A set is called countable iff it is either finite or countably infinite
- A set that is not countable is called uncountable

The positive rational numbers are countable

Construct a bijection $f : \mathbb{N} \to \mathbb{Q}^+$

The positive rational numbers are countable

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

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

The positive rational numbers are countable

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

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

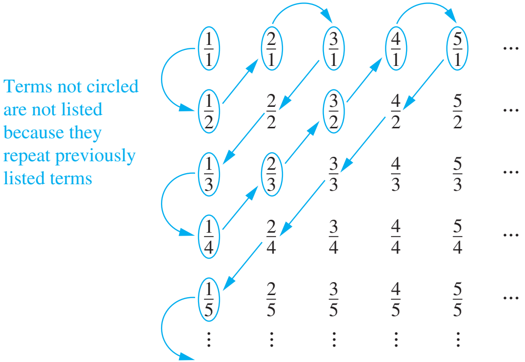
f traverses this list in the order for $m = 2, 3, 4, \ldots$ visiting all p/q with $p + q = m$ (and listing only new rationals)

The positive rational numbers are countable

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

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)



Finite strings

Theorem

The set Σ^* of all finite strings over a finite alphabet Σ is countably infinite

Finite strings

Theorem

The set Σ^* of all finite strings over a finite alphabet Σ is countably infinite

Proof.

- First define an (alphabetical) ordering on the symbols in Σ
  Show that the strings can be listed in a sequence
  - First single string ε of length 0
  - Then all strings of length 1 in lexicographic order
  - Then all strings of length 2 in lexicographic order
  - etc

Finite strings

Theorem

The set Σ^* of all finite strings over a finite alphabet Σ is countably infinite

Proof.

- First define an (alphabetical) ordering on the symbols in Σ
  Show that the strings can be listed in a sequence
    - First single string ε of length 0
    - Then all strings of length 1 in lexicographic order
    - Then all strings of length 2 in lexicographic order
    - etc
- This implies a bijection from $\mathbb{N}$ to Σ^*

□

Finite strings

Theorem

The set Σ^* of all finite strings over a finite alphabet Σ is countably infinite

Proof.

- First define an (alphabetical) ordering on the symbols in Σ
  Show that the strings can be listed in a sequence
  - First single string ε of length 0
  - Then all strings of length 1 in lexicographic order
  - Then all strings of length 2 in lexicographic order
  - etc
- This implies a bijection from $\mathbb{N}$ to Σ^*

□

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 $d : \mathbb{N} \to \{0, 1\}$

Infinite binary strings

- An infinite length string of bits 10010 ...
- Such a string is a function $d : \mathbb{N} \rightarrow \{0, 1\}$
- with the property $d_m = d(m)$ is the mth symbol (starting from 0)

Uncountable sets

Theorem

The set of infinite binary strings is uncountable

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 $f : \mathbb{N} \to X$ exists. So, f must be onto (surjective). Assume that $f(i) = d^i$ for $i \in \mathbb{N}$. So, $X = \{d^0, d^1, \ldots, d^m, \ldots\}$. Define the infinite binary string d as follows: $d_n = (d^n_n + 1) \bmod 2$. But for each m, $d \neq d^m$ because $d_m \neq d^m_m$. So, f is not a surjection. $\square$

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 $f : \mathbb{N} \to X$ exists. So, f must be onto (surjective). Assume that $f(i) = d^i$ for $i \in \mathbb{N}$. So, $X = \{d^0, d^1, \ldots, d^m, \ldots\}$. 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 $f : \mathbb{N} \rightarrow X$ exists. So, f must be onto (surjective). Assume that $f(i) = d^i$ for $i \in \mathbb{N}$. So, $X = \{d^0, d^1, \ldots, d^m, \ldots\}$. 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. $\square$

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 $f : \mathbb{N} \rightarrow X$ exists. So, f must be onto (surjective). Assume that $f(i) = d^i$ for $i \in \mathbb{N}$. So, $X = \{d^0, d^1, \ldots, d^m, \ldots\}$. Define the infinite binary string d as follows: $d_n = (d^n_n + 1) \bmod 2$. But for each m, $d \neq d^m$ because $d_m \neq d^m_m$. So, f is not a surjection. $\square$

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 $f : \mathbb{N} \rightarrow X$ exists. So, f must be onto (surjective). Assume that $f(i) = d^i$ for $i \in \mathbb{N}$. So, $X = \{d^0, d^1, \ldots, d^m, \ldots\}$. Define the infinite binary string d as follows: $d_n = (d_n^n + 1) \bmod 2$. But for each m, $d \neq d^m$ because $d_m \neq d_m^m$. So, f is not a surjection. $\square$

The technique used here is called diagonalization

Similar argument shows that $\mathbb{R}$ via $[0, 1]$ is uncountable using infinite decimal strings (see book). "Most functions" are not computable!

Schröder-Bernstein Theorem

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

$|A| < |\mathcal{P}(A)|$

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, $a \notin f(a) = B$. Contradiction
2. If $a \notin B$ then $a \notin f(a)$. Thus, 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 ZF set theory by Gödel/Cohen in 1963: cannot be proven/disproven in ZF

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 ZF set theory by Gödel/Cohen in 1963: cannot be proven/disproven in ZF
- 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 ZF set theory by Gödel/Cohen in 1963: cannot be proven/disproven in ZF
- 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 ZF set theory by Gödel/Cohen in 1963: cannot be proven/disproven in ZF
- There exists an infinite hierarchy of sets of ever larger cardinality
- $S_0 := \mathbb{N}$ and $S_{i+1} := \mathcal{P}(S_i)$
- $|S_0| < |S_1| < \ldots < |S_i| < |S_{i+1}| < \ldots$