Cantor’s Theory of Infinite Sets

COMPSCI 230 — Discrete Math

February 7, 2017
Outline

1. Infinite Sets
2. The Cardinality of the Integers: Bijections
3. The Cardinality of the Rationals: Dovetailing
4. The Cardinality of the Reals: Diagonalization
Comparing Infinities

• For finite sets, \( A \subset B \Rightarrow |A| < |B| \)
• \( \{a, c\} \subset \{a, b, c\} \) and \( 2 < 3 \)
• For infinite sets, \( \subset \) is defined, while \( |\cdot| \) is not
• \( \{x \mid x \text{ is prime}\} \subset \mathbb{N} \)
  But what are \( |\{x \mid x \text{ is prime}\}| \) and \( |\mathbb{N}|? \)
• So from \( A \subset B \) we cannot conclude anything about \( |A| \) or \( |B| \) for infinite sets
• We need a new way to measure \( |A| \)
• No necessary contradiction between \( A \subset B \) and \( |A| = |B| \) for infinite sets
Cantor’s Equality for Cardinality

- \(|A| = |B| \iff \text{there exists a bijection between } A \text{ and } B\)
- Bijection: injection both ways
- Associate exactly one \(b \in B\) to each \(a \in A\), and associate exactly one \(a \in A\) to each \(b \in B\)
- Works for finite sets!
- Cantor’s program:
  - Instead of associating number \(|A|\) to set \(A\) ... group all sets such that sets in the same group have equal cardinality
  - We do not have the number \(|A|\), but we can order sets by their cardinality
  - Given any two sets \(A, B\) (finite or infinite), we can say exactly one of \(|A| = |B|\) or \(|A| < |B|\) or \(|B| < |A|\)
  - Defining cardinality by abstraction
  - Analogous to defining parity by congruence
Proving or Disproving Equality

• Proving equality:
  • Constructive method: Make a conceptual “table” of \((a, b)\) pairs with no gaps or repetitions
  • Constructive method: Devise an algorithm to compute \(b\) from \(a\) and vice versa and show that each is an injection
  • Non-constructive method: Argue that such a bijection must exist

• Proving inequality is harder:
  • To prove that \(|A| \neq |B|\) we need to show that no bijection can possibly exist
  • \textit{Any} function we may find between \(A\) and \(B\) will have gaps or repetitions
  • Once we prove inequality, we usually also know whether \(|A| < |B|\) (different cardinalities and \(A \subset B\)) or \(|B| < |A|\)
Define classes (sets of sets) of cardinalities: 
\{A_1, A_2, \ldots \} such that |A_1| = |A_2| = \ldots

Start with \( A_1 = \mathbb{N} \) and let \(|\mathbb{N}| = \aleph_0 \) (“aleph nought”)

Any set \( A \) with \(|A| = \aleph_0 \) is countably infinite

What other sets have the same cardinality?

Even naturals: \( n \leftrightarrow 2n \)

\[
\begin{array}{c|c}
  a & b \\
  \hline
  0 & 0 \\
  1 & 2 \\
  2 & 4 \\
  \vdots & \vdots \\
\end{array}
\]

A bijection: \(|E| = |\mathbb{N}| = \aleph_0\) 
(E is the set of even numbers)
Proving Bijection

- Bijection: injection both ways
- \( b = f(a) = 2a \) for \( a \in \mathbb{N} \) and \( b \in \mathbb{E} \) is an injection:
- \( a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2) \)
- Proof:
  - Let \( a_1, a_2 \in \mathbb{N} \) with \( a_1 \neq a_2 \)
  - Then, \( a_1 - a_2 \neq 0 \)
  - Let \( b_1 = f(a_1) = 2a_1 \) and \( b_2 = f(a_2) = 2a_2 \)
  - Then, \( b_1, b_2 \in \mathbb{E} \)
  - Also, \( b_1 - b_2 = 2a_1 - 2a_2 = 2(a_1 - a_2) \neq 0 \)
  - Therefore, \( b_1 \neq b_2 \)
  - Therefore, \( b = 2a \) is an injection

- Similar reasoning for \( a = f^{-1}(b) = b/2 \) for even \( b \) shows that \( f^{-1} \) is an injection
A Slightly Harder Example

\[ |\{ x \mid x \text{ is prime}\}| = ? \]

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
</tr>
</tbody>
</table>

• What do we need to show?
  • 0. No repetitions on either side (up to us!)
  • 1. No primes are skipped
  • 2. The table never stops
• Constructive argument for 1: Use the sieve
• Non-constructive argument for 2: Euclid’s 2nd theorem: The number of primes is infinite
The Number of Primes is Infinite

• Proof by contradiction:
  Assume the opposite, and derive a contradiction
• Assume that the number of primes is finite
• So there must be a largest prime, call it $p_n$
• Let $p_0, \ldots, p_n$ be all primes
• Let $q = 1 + p_0 \cdot \ldots \cdot p_n$
• Example: $q = 1 + 2 \cdot 3 \cdot 5 \cdot 7 = 211$
• None of $p_0, \ldots, p_n$ divides $q$ (remainder of 1)
• Either $q$ is divisible by a bigger prime than $p_n$, or $q$ is a prime itself
• Either way, there is a prime greater than $p_n$
• This contradicts our assumption
• The number of primes is infinite
There Are $\aleph_0$ Primes

<table>
<thead>
<tr>
<th>$a$</th>
<th>$b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
</tbody>
</table>

- Table construction $\Rightarrow$ No repetitions on either side
- Sieve of Erathostenes $\Rightarrow$ No primes are skipped
- Euclid’s 2nd theorem $\Rightarrow$ The table never stops
- Found a bijection between $\mathbb{N}$ and the primes
- We can write a Python generator of primes
- There are as many primes as there are naturals

$|\{x \mid x \text{ is prime}\}| = \aleph_0$, even if $|\{x \mid x \text{ is prime}\}| \subset \mathbb{N}$
The Cardinality of the Rationals: Dovetailing

|\( |\mathbb{Q} | = ? \) |

- Can we make a table to match \( \mathbb{N} \) and \( \mathbb{Q} \)?
- Can we write a Python generator for the rationals?
- How many positive rationals are there? \(|\mathbb{N}^+| = |\mathbb{Q}^+|?\)
- **Dovetailing:**

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1/1</td>
<td>1/2</td>
<td>1/3</td>
<td>1/4</td>
<td>1/5</td>
</tr>
<tr>
<td>2</td>
<td>1/2</td>
<td>2/2</td>
<td>2/3</td>
<td>2/4</td>
<td>2/5</td>
</tr>
<tr>
<td>3</td>
<td>2/3</td>
<td>3/2</td>
<td>3/3</td>
<td>3/4</td>
<td>3/5</td>
</tr>
<tr>
<td>4</td>
<td>3/1</td>
<td>3/2</td>
<td>3/3</td>
<td>3/4</td>
<td>3/5</td>
</tr>
<tr>
<td>5</td>
<td>4/1</td>
<td>4/2</td>
<td>4/3</td>
<td>4/4</td>
<td>4/5</td>
</tr>
</tbody>
</table>

Dovetailing:
Dovetailing

<table>
<thead>
<tr>
<th>n</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>r</td>
<td>1/1</td>
<td>2/1</td>
<td>1/2</td>
<td>3/1</td>
<td>4/1</td>
</tr>
</tbody>
</table>

• Skip repetitions (require gcd(num, denom) = 1)

| n  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 | ...
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>r</td>
<td>1/1</td>
<td>2/1</td>
<td>1/2</td>
<td>3/1</td>
<td>4/1</td>
<td>3/2</td>
<td>2/3</td>
<td>1/4</td>
<td>1/5</td>
<td>5/1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

• Can include zero and negatives by starting with zero, then alternating signs in the list

| n  | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 | 12 | 13 | ...
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>r</td>
<td>0</td>
<td>1/1</td>
<td>-1/1</td>
<td>2/1</td>
<td>-2/1</td>
<td>1/2</td>
<td>-1/2</td>
<td>1/3</td>
<td>-1/3</td>
<td>3/1</td>
<td>-3/1</td>
<td>4/1</td>
<td>-4/1</td>
<td>3/2</td>
<td></td>
</tr>
</tbody>
</table>

• $|\mathbb{Q}| = \aleph_0$
The Cardinality of the Reals: Diagonalization

$|\mathbb{R}| = ?$

- Let’s just take a small piece of $\mathbb{R}$:
  $U = \{x \mid x \in \mathbb{R}, 0 < x < 1\}$

- We will show that even the reals on the open unit interval $U$ are more than the naturals: $|U| > \aleph_0$

- Again by contradiction: *Diagonalization*

- Structure of the proof:
  - Assume that we can make a bijective table of the reals in $U$, listed *in any order whatsoever*
    The last qualification means: we cannot make any assumption about ordering in our argument
  - Then, we give a way to construct a real number that is not in the table
  - This contradicts our assumption, so the reals are not countably infinite
\[ |U| > \aleph_0 \]

- Every number in \( U \) can be written as \( 0.d_1d_2d_3 \ldots \).
- Only ambiguity is of the form
  \[ 0.d_0 \ldots d_{k-1}d_k000 \ldots = 0.d_0 \ldots d_{k-1}(d_k - 1)999 \ldots \]
- Example: \( 0.347000 \ldots = 0.346999 \ldots \) (exactly two representations)
- So a table looks like this:

<table>
<thead>
<tr>
<th>( n )</th>
<th>( r_n )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>( 0.d_0^{(0)}d_1^{(0)}d_2^{(0)}d_3^{(0)} \ldots )</td>
</tr>
<tr>
<td>1</td>
<td>( 0.d_0^{(1)}d_1^{(1)}d_2^{(1)}d_3^{(1)} \ldots )</td>
</tr>
<tr>
<td>2</td>
<td>( 0.d_0^{(2)}d_1^{(2)}d_2^{(2)}d_3^{(2)} \ldots )</td>
</tr>
<tr>
<td>3</td>
<td>( 0.d_0^{(3)}d_1^{(3)}d_2^{(3)}d_3^{(3)} \ldots )</td>
</tr>
</tbody>
</table>
\[ |U| > \aleph_0 \]

\[
\begin{array}{c|c}
 n & r_n \\
\hline
 0 & 0.d_0^{(0)} d_1^{(0)} d_2^{(0)} d_3^{(0)} \ldots \\
 1 & 0.d_0^{(1)} d_1^{(1)} d_2^{(1)} d_3^{(1)} \ldots \\
 2 & 0.d_0^{(2)} d_1^{(2)} d_2^{(2)} d_3^{(2)} \ldots \\
 3 & 0.d_0^{(3)} d_1^{(3)} d_2^{(3)} d_3^{(3)} \ldots \\
\end{array}
\]

- A number not on the table:

\[ e = 0.e_0 e_1 e_2 e_3 \ldots \quad \text{where} \quad e_n = (d_n^{(n)} + 1) \mod 10 \]

- \( e \neq r_0 \) because they differ in the first digit
- ...
- \( |U| > \aleph_0 \) uncountable
What about $|\mathbb{R}|$?

- Claim: $|U| = |\mathbb{R}|$
- Any bijection between $U$ and $\mathbb{R}$ will do
- Example: $r = \tan[\pi(u - \frac{1}{2})]$
- $u \to 0 \Rightarrow \pi(u - \frac{1}{2}) \to -\frac{\pi}{2} \Rightarrow r \to -\infty$
- $u \to 1 \Rightarrow \pi(u - \frac{1}{2}) \to \frac{\pi}{2} \Rightarrow r \to \infty$
- Monotonic $\Rightarrow$ invertible $\Rightarrow$ bijection!

- $|U| = |\mathbb{R}|
- \aleph_0 = |\mathbb{N}| = |\mathbb{Q}| < |U| = |\mathbb{R}| = c$
  (pronounce “cee”)
- Surprising, given that $\mathbb{N}$ is not dense in $\mathbb{Q}$ and $\mathbb{Q}$ is dense in $\mathbb{R}$
- $[A$ is dense in $B$ if every $b \in B$ is either in $A$ or arbitrarily close to some $a \in A]$