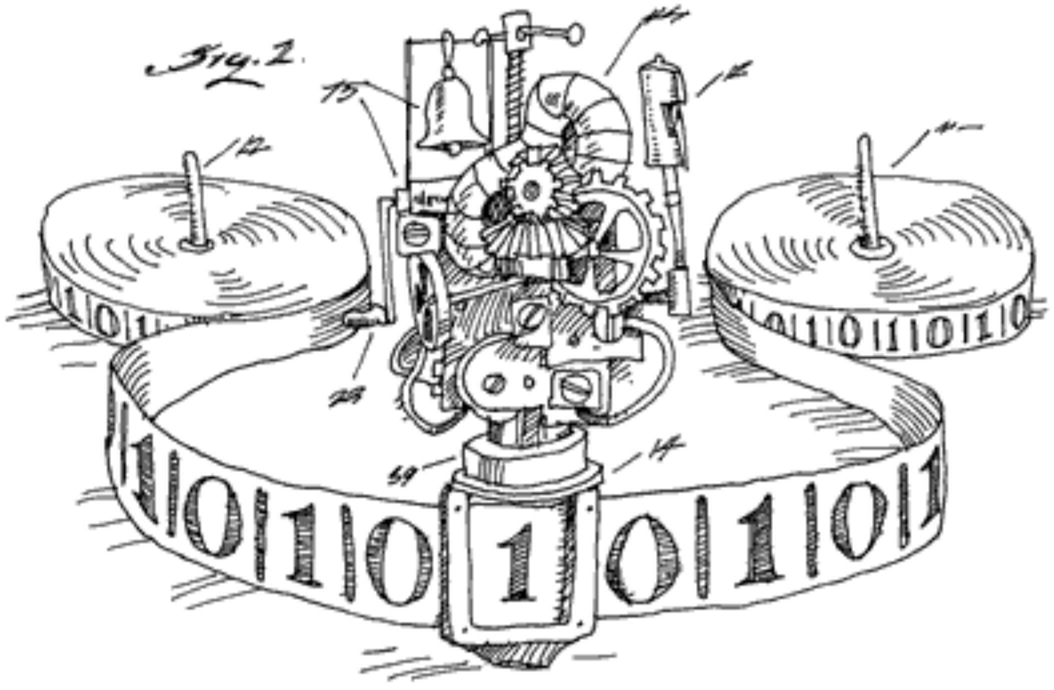
CSC4010: Introduction to Theoretical Computer Science



Tutorial 1

Recap: Cardinality of Infinite Sets

Recap: Cardinality of Infinite Sets

Definition: Two (infinite/finite) sets A, B have the same cardinality $|A| = |B|$ if and only if there is a bijection from A to B.

Recap: Cardinality of Infinite Sets

Definition: Two (infinite/finite) sets A, B have the same cardinality $|A| = |B|$ if and only if there is a bijection from A to B.

Claim: For $\mathbb{Z}^+ = \{1,2,\cdots\}$ **and** $\mathbb{N} = \{0,1,2,\cdots\}$**,** $|\mathbb{Z}^+| = |\mathbb{N}|$.

Recap: Cardinality of Infinite Sets

Definition: Two (infinite/finite) sets A, B have the same cardinality $|A| = |B|$ if and only if there is a bijection from A to B .

Claim: For $\mathbb{Z}^+ = \{1,2,\cdots\}$ **and** $\mathbb{N} = \{0,1,2,\cdots\}$**,** $|\mathbb{Z}^+| = |\mathbb{N}|$.

Equivalent Definition: Two (infinite/finite) sets A, B have the same cardinality $|A| = |B|$ if and only if

a) There is a one-one function $f : A \to B$, and
b) there is a one-one function from $g : B \to A$.

Example 2: $|\mathbb{N}| = |\mathbb{Z}|$

Example 2: $|\mathbb{N}| = |\mathbb{Z}|$

Equivalent Definition: Two (infinite/finite) sets A, B have the same cardinality $|A| = |B|$ if and only if

a) There is a one-one function $f : A \to B$, and

b) there is a one-one function from $g : B \to A$.

Example 2: $|\mathbb{N}| = |\mathbb{Z}|$

Equivalent Definition: Two (infinite/finite) sets A, B have the same cardinality $|A| = |B|$ if and only if
a) There is a one-one function $f : A \to B$, and
b) there is a one-one function from $g : B \to A$.

- **Recall:** $\mathbb{N} = \{0,1,2,3,\cdots\}$ and $\mathbb{Z} = \{0,1,-1,2,-2,\cdots\}$.
- **(Easy Case):** $f : \mathbb{N} \to \mathbb{Z}$ that is one-one.

Define $f(x) = x$

Example 2: $|\mathbb{N}| = |\mathbb{Z}|$

Equivalent Definition: Two (infinite/finite) sets A, B have the same cardinality $|A| = |B|$ if and only if

a) There is a one-one function $f : A \to B$, and

b) there is a one-one function from $g : B \to A$.

- **Recall:** $\mathbb{N} = \{0,1,2,3,\cdots\}$ and $\mathbb{Z} = \{0,1,-1,2,-2,\cdots\}$.
- **(Easy Case):** $f : \mathbb{N} \to \mathbb{Z}$ that is one-one.

  Define $f(x) = x$
- **(Hard Case):** $g : \mathbb{Z} \to \mathbb{N}$ that is one-one.

Example 2: $|\mathbb{N}| = |\mathbb{Z}|$

Equivalent Definition: Two (infinite/finite) sets A, B have the same cardinality $|A| = |B|$ if and only if
a) There is a one-one function $f : A \to B$, and
b) there is a one-one function from $g : B \to A$.

- **Recall:** $\mathbb{N} = \{0,1,2,3,\cdots\}$ and $\mathbb{Z} = \{0,1,-1,2,-2,\cdots\}$.
- **(Easy Case):** $f : \mathbb{N} \to \mathbb{Z}$ that is one-one.

  Define $f(x) = x$
- **(Hard Case):** $g : \mathbb{Z} \to \mathbb{N}$ that is one-one.

$$
\begin{array}{lllllllll}
\mathbb{Z}: & 0, & 1, & -1, & 2, & -2, & 3, & -3 & \cdots \\
 & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
\mathbb{N}: & 0, & 1, & 2, & 3, & 4, & 5 & 6 &
\end{array}
$$

Example 2: $|\mathbb{N}| = |\mathbb{Z}|$

Equivalent Definition: Two (infinite/finite) sets A, B have the same cardinality $|A| = |B|$ if and only if
a) There is a one-one function $f : A \to B$, and
b) there is a one-one function from $g : B \to A$.

- **Recall:** $\mathbb{N} = \{0,1,2,3,\cdots\}$ and $\mathbb{Z} = \{0,1,-1,2,-2,\cdots\}$.
- **(Easy Case):** $f : \mathbb{N} \to \mathbb{Z}$ that is one-one.

Define $f(x) = x$

- **(Hard Case):** $g : \mathbb{Z} \to \mathbb{N}$ that is one-one.

$$\begin{array}{l}
\mathbb{Z} : 0,1,-1,2,-2,3,-3\cdots \\
\quad\;\; \downarrow\;\downarrow\;\;\;\downarrow\;\downarrow\;\;\;\downarrow\;\downarrow\;\;\;\downarrow \\
\mathbb{N} : 0,1,\;\;2,3,\;\;4,5\;\;\;6
\end{array}$$

$g(x) = 2x - 1$ if $x > 0$,
$-2x$ if $x \le 0$.

Example 2: $|\mathbb{N}| = |\mathbb{Z}|$

$$
\begin{array}{ccccccccc}
\mathbb{Z}: & 0, & 1, & -1, & 2, & -2, & 3, & -3 & \cdots \\
 & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
\mathbb{N}: & 0, & 1, & 2, & 3, & 4, & 5 & 6 &
\end{array}
$$

$g(x) = 2x - 1$ if $x > 0$,
$-2x$ if $x \leq 0$.

Example 2: $|\mathbb{N}| = |\mathbb{Z}|$

$$\begin{array}{l}
\mathbb{Z} : 0, 1, -1, 2, -2, 3, -3 \cdots \\
\quad\ \ \downarrow\ \downarrow\quad\ \downarrow\ \downarrow\quad\ \downarrow\ \downarrow\quad\ \downarrow \\
\mathbb{N} : 0, 1,\quad 2, 3,\quad 4, 5\quad 6
\end{array}$$

$$g(x) = 2x - 1 \text{ if } x > 0, \quad -2x \text{ if } x \leq 0.$$

- **(Hard Case):** $g : \mathbb{Z} \to \mathbb{N}$ that is one-one. This is equivalent to listing out all the infinitely many element of $\mathbb{Z}$ such that each $x \in \mathbb{Z}$ has a finite position on this list.

Example 2: $|\mathbb{N}| = |\mathbb{Z}|$

$$
\begin{array}{l}
\mathbb{Z} : 0,1,-1,2,-2,3,-3\cdots \\
\quad\ \ \downarrow\ \downarrow\quad \downarrow\ \downarrow\quad \downarrow\ \downarrow\quad \downarrow \\
\mathbb{N} : 0,1,\ \ 2,3,\ \ 4,5\ \ \ 6
\end{array}
$$

$g(x) = 2x - 1$ if $x > 0$,
$-2x$ if $x \leq 0$.

- **(Hard Case):** $g : \mathbb{Z} \to \mathbb{N}$ that is one-one. This is equivalent to listing out all the infinitely many element of $\mathbb{Z}$ such that each $x \in \mathbb{Z}$ has a finite position on this list.

- Another (wrong but natural) way to list: List $\mathbb{Z}^+ \cup \{0\}$ first, and then $\mathbb{Z}^-$. But $\mathbb{Z}^+ \cup \{0\}$ is infinite! So, we do not have a finite position for -1.

Definitions

- **Definition:** A set is countable if $|A| \leq |\mathbb{N}|$. This is the same as saying there is a one-one function from A to $\mathbb{N}$.

- **Definition:** A set is countably infinite if $|A| = |\mathbb{N}|$.

Example 3: $\mathbb{N}^2$ is countably infinite

Example 3: $\mathbb{N}^2$ is countably infinite

Equivalent Definition: Two (infinite/finite) sets A, B have the same cardinality $|A| = |B|$ if and only if

a) There is a one-one function $f : A \rightarrow B$, and

b) there is a one-one function from $g : B \rightarrow A$.

Example 3: $\mathbb{N}^2$ is countably infinite

Equivalent Definition: Two (infinite/finite) sets A, B have the same cardinality $|A| = |B|$ if and only if

a) There is a one-one function $f : A \to B$, and

b) there is a one-one function from $g : B \to A$.

- **Recall:** $\mathbb{N}^2 = \{(x, y) \mid x, y \in \mathbb{N}\}$.
- **(Easy Case):** $f : \mathbb{N} \to \mathbb{N}^2$ that is one-one.

Define $f(x) = (x,0)$.

Example 3: $\mathbb{N}^2$ is countably infinite

Equivalent Definition: Two (infinite/finite) sets A, B have the same cardinality $|A| = |B|$ if and only if

a) There is a one-one function $f : A \to B$, and

b) there is a one-one function from $g : B \to A$.

- **Recall:** $\mathbb{N}^2 = \{(x, y) \mid x, y \in \mathbb{N}\}$.

- **(Easy Case):** $f : \mathbb{N} \to \mathbb{N}^2$ that is one-one.

  Define $f(x) = (x,0)$.

- **(Hard Case):** $g : \mathbb{N}^2 \to \mathbb{N}$ that is one-one.

  Define $g((x, y)) = 2^x 3^y$

Example 4: $\mathbb{N}^3$ is countably infinite

Example 4: $\mathbb{N}^3$ is countably infinite

Equivalent Definition: Two (infinite/finite) sets A, B have the same cardinality $|A| = |B|$ if and only if

a) There is a one-one function $f : A \to B$, and

b) there is a one-one function from $g : B \to A$.

Example 4: $\mathbb{N}^3$ is countably infinite

Equivalent Definition: Two (infinite/finite) sets A, B have the same cardinality $|A| = |B|$ if and only if
a) There is a one-one function $f : A \to B$, and
b) there is a one-one function from $g : B \to A$.

- **Recall:** $\mathbb{N}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{N}\}$.
- **(Easy Case):** $f : \mathbb{N} \to \mathbb{N}^3$ that is one-one.

  Define $f(x) = (x,0,0)$.

Example 4: $\mathbb{N}^3$ is countably infinite

Equivalent Definition: Two (infinite/finite) sets A, B have the same cardinality $|A| = |B|$ if and only if

a) There is a one-one function $f : A \to B$, and

b) there is a one-one function from $g : B \to A$.

- **Recall:** $\mathbb{N}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{N}\}$.
- **(Easy Case):** $f : \mathbb{N} \to \mathbb{N}^3$ that is one-one.

  Define $f(x) = (x,0,0)$.
- **(Hard Case):** $g : \mathbb{N}^3 \to \mathbb{N}$ that is one-one.

  Define $g((x, y, z)) = 2^x 3^y 5^z$

Example 5: $\mathbb{N}^k$ is countably infinite

Example 5: $\mathbb{N}^k$ is countably infinite

Claim: For any $k \in \mathbb{Z}^+$, $\mathbb{N}^k$ is countably infinite.

Example 5: $\mathbb{N}^k$ is countably infinite

Claim: For any $k \in \mathbb{Z}^+$, $\mathbb{N}^k$ is countably infinite.

- **(Hard Case):** $g : \mathbb{N}^k \to \mathbb{N}$ that is one-one.

  Define $g((x_1, x_2, \cdots, x_k)) = p_1^{x_1} p_2^{x_2} \ldots p_k^{x_k}$

  Where p_i is the ith prime number.

Another Way to Prove Countably Infinite

Another Way to Prove Countably Infinite

- Finding an explicit one-one function can be hard!

- **How do you prove B is countably infinite:**
    - This is equivalent to listing out all the infinitely many element of B such that each $x \in B$ has a finite position on this list.

Example 7: $\mathbb{Q}$ is countably infinite

Example 7: $\mathbb{Q}$ is countably infinite

Claim: $|\mathbb{Q}| = |\mathbb{N}|$ **is countably infinite.**

Example 7: $\mathbb{Q}$ is countably infinite

Claim: $|\mathbb{Q}| = |\mathbb{N}|$ **is countably infinite.**

- **Recall:** $\mathbb{Q} = \{\frac{x}{y} \mid x, y \in \mathbb{N}^+\}$.

Example 7: $\mathbb{Q}$ is countably infinite

Claim: $|\mathbb{Q}| = |\mathbb{N}|$ **is countably infinite.**

- **Recall:** $\mathbb{Q} = \{\frac{x}{y} \mid x, y \in \mathbb{N}^+\}$.

- Instead of finding a one-one function, we will list out all the infinitely many element of $\mathbb{Q}$ such that each $\frac{x}{y} \in \mathbb{Q}$ has a finite position on this list.

Example 7: $\mathbb{Q}$ is countably infinite

Claim: $|\mathbb{Q}| = |\mathbb{N}|$ **is countably infinite.**

- **Recall:** $\mathbb{Q} = \{\frac{x}{y} \mid x, y \in \mathbb{N}^+\}$.

- Instead of finding a one-one function, we will list out all the infinitely many element of $\mathbb{Q}$ such that each $\frac{x}{y} \in \mathbb{Q}$ has a finite position on this list.

1/1	1/2	1/3	1/4	$\cdots$
2/1	2/2	2/3	2/4	$\cdots$
3/1	3/2	3/3	3/4	$\cdots$
4/1	4/2	4/3	4/4	$\cdots$
5/1	5/2	5/3	5/4	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Example 7: $\mathbb{Q}$ is countably infinite

Claim: $|\mathbb{Q}| = |\mathbb{N}|$ **is countably infinite.**

- **Recall:** $\mathbb{Q} = \{\frac{x}{y} \mid x, y \in \mathbb{N}^+\}$.

- Instead of finding a one-one function, we will list out all the infinitely many element of $\mathbb{Q}$ such that each $\frac{x}{y} \in \mathbb{Q}$ has a finite position on this list.

1/1	1/2	1/3	1/4	$\cdots$
2/1	2/2	2/3	2/4	$\cdots$
3/1	3/2	3/3	3/4	$\cdots$
4/1	4/2	4/3	4/4	$\cdots$
5/1	5/2	5/3	5/4	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Convert this matrix into a list!

1) Read off row by row.

2) Read off column by column.

Example 7: $\mathbb{Q}$ is countably infinite

Claim: $|\mathbb{Q}| = |\mathbb{N}|$ **is countably infinite.**

- **Recall:** $\mathbb{Q} = \{\frac{x}{y} \mid x, y \in \mathbb{N}^+\}$.
- Instead of finding a one-one function, we will list out all the infinitely many element of $\mathbb{Q}$ such that each $\frac{x}{y} \in \mathbb{Q}$ has a finite position on this list.

1/1	1/2	1/3	1/4	$\cdots$
2/1	2/2	2/3	2/4	$\cdots$
3/1	3/2	3/3	3/4	$\cdots$
4/1	4/2	4/3	4/4	$\cdots$
5/1	5/2	5/3	5/4	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Convert this matrix into a list!

1) Read off row by row. ☠
2) Read off column by column. ☠

Example 7: $\mathbb{Q}$ is countably infinite

1/1	1/2	1/3	1/4	$\cdots$
2/1	2/2	2/3	2/4	$\cdots$
3/1	3/2	3/3	3/4	$\cdots$
4/1	4/2	4/3	4/4	$\cdots$
5/1	5/2	5/3	5/4	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Our list is: $D_1, D_2, D_3, \cdots$

What is the finite position of $\dfrac{x}{y}$? We can compute! We know:

a) $|D_i| = i$ and $x + y \in D_{x+y-1}$.

b) Thus, we know the position of the first element of D_{x+y-1}.

c) We know the position of x/y in D_{x+y-1}.

General Principle

To prove B is countably infinite:

a) Write $B = \cup_{i>0} L_i$, where $|L_i|$ is finite.
b) Arrange elements of each L_i in a fixed order.
c) The first element of L_i has index $\sum_{j=1}^{i-1} |L_j|$.
e) We know position of $x \in L_i$.

Example 6: The set of all finite binary strings

- Let $\{0,1\}^k$ be the collection of all strings of length k .
- For example: $\{0,1\}^2 = \{00,01,10,11\}$.
- $\{0,1\}^0$ is the empty string, denoted ε.
- $\{0,1\}^* = \cup_{k \geqslant 0} \{0,1\}^k$ be the collection of all finite strings.

Example 6: The set of all finite binary strings

- Let $\{0,1\}^k$ be the collection of all strings of length k.
- For example: $\{0,1\}^2 = \{00,01,10,11\}$.
- $\{0,1\}^0$ is the empty string, denoted ε.
- $\{0,1\}^* = \cup_{k \geqslant 0} \{0,1\}^k$ be the collection of all finite strings.

Claim: $\{0,1\}^*$ is countably infinite.

Example 6: The set of all finite binary strings

- Let $\{0,1\}^k$ be the collection of all strings of length k.
- For example: $\{0,1\}^2 = \{00,01,10,11\}$.
- $\{0,1\}^0$ is the empty string, denoted ε.
- $\{0,1\}^* = \cup_{k \geqslant 0} \{0,1\}^k$ be the collection of all finite strings.

Example 6: The set of all finite binary strings

- Let $\{0,1\}^k$ be the collection of all strings of length k .
- For example: $\{0,1\}^2 = \{00,01,10,11\}$.
- $\{0,1\}^0$ is the empty string, denoted ε.
- $\{0,1\}^* = \cup_{k\geqslant 0} \{0,1\}^k$ be the collection of all finite strings.

Claim: $\{0,1\}^*$ is countably infinite.

Example 6: The set of all finite binary strings

- Let $\{0,1\}^k$ be the collection of all strings of length k.
- For example: $\{0,1\}^2 = \{00,01,10,11\}$.
- $\{0,1\}^0$ is the empty string, denoted ε.
- $\{0,1\}^* = \cup_{k \geqslant 0} \{0,1\}^k$ be the collection of all finite strings.

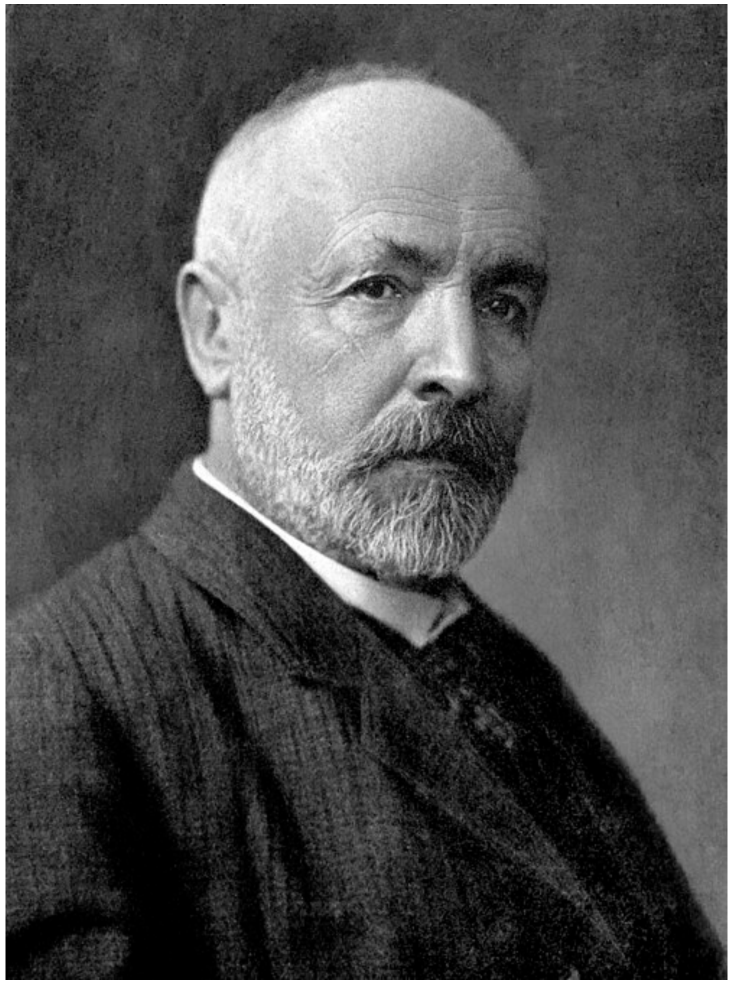
Claim: $\{0,1\}^*$ is countably infinite.

- First order every string by length. These are L_i's and $|L_i| = 2^i$.
- Within each length, order by dictionary order.

Next Class: Is Everything Countable?

Bonus Slides

Our Hero For this Lecture



Georg Cantor
(1845-1918)
“Father of Set Theory”

Some of Cantor's Contributions

- The study of infinite sets.
- Definition and use of bijections to compare the cardinality of sets.
- There are different levels of infinity. (Infinitely many levels in fact.)
- $|\mathbb{N}| = |\mathbb{Z}|$ even though $\mathbb{N} \subseteq \mathbb{Z}$.
- $|\mathbb{Z}| < |\mathbb{R}|$ even though both are infinite.
- The diagonal argument for proving one infinite set is larger than another. (We will see this in next class.)

Infinity in Mathematics

Before Cantor:

"We must not treat infinite sets as if they have an existence exactly comparable to the existence of finite sets."

- Carl Friedrich Gauss

Infinity in Mathematics

Before Cantor:

"We must not treat infinite sets as if they have an existence exactly comparable to the existence of finite sets."

- Carl Friedrich Gauss

After Cantor:

Infinite sets are mathematical objects just like finite sets.

Reaction to Cantor’s Ideas at the Time

Reaction to Cantor's Ideas at the Time

"Most of the ideas of Cantorian set theory should be banished from mathematics once and for all!"

- Henri Poincare (1854-1912)
(mathematician, physicist, engineer)

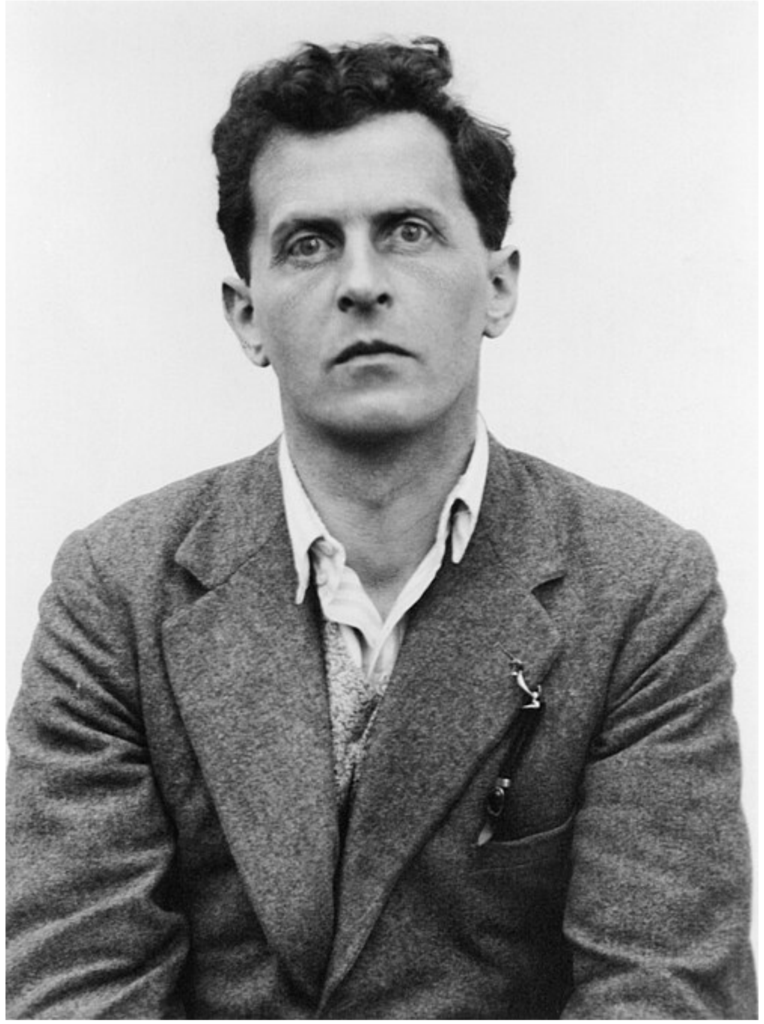
Reaction to Cantor's Ideas at the Time

"Scientific charlatan."
"Corrupter of youth."

- Leopold Kronecker (1823-1891)
(Mathematician)

Reaction to Cantor's Ideas at the Time

"Utter nonsense."
- Ludwig Wittgenstein (1889-1951)
(Logician, philosopher of science)



Reaction to Cantor’s Ideas at the Time

“No one should expel us from the Paradise
that Cantor has created.”
- David Hilbert (1862-1943) (Mathematician)

lernt, lehrt und anwendet, zu Ungereimtheiten. Und wo soll sonst Sicherheit und Wahrheit zu finden sein, wenn sogar das mathematische Denken versagt?

Aber es gibt einen völlig befriedigenden Weg, den Paradoxien zu entgehen, ohne Verrat an unserer Wissenschaft zu üben. Die Gesichtspunkte zur Auffindung dieses Weges und die Wünsche, die uns die Richtung weisen, sind diese:

1. Fruchtbaren Begriffsbildungen und Schlußweisen wollen wir, wo immer nur die geringste Aussicht sich bietet, sorgfältig nachspüren und sie pflegen, stützen und gebrauchsfähig machen. Aus dem Paradies, das Cantor uns geschaffen, soll uns niemand vertreiben können.

2. Es ist nötig, durchweg dieselbe Sicherheit des Schließens herzustellen, wie sie in der gewöhnlichen niederen Zahlentheorie vorhanden ist, an der niemand zweifelt und wo Widersprüche und Paradoxien nur durch unsere Unaufmerksamkeit entstehen.

Die Erreichung dieser Ziele ist offenbar nur möglich, wenn uns die volle Aufklärung über *das Wesen des Unendlichen* gelingt.

Next Class: Cantor’s Argument and Introduction to Computability Theory