Problem Set 1 is due
This Friday, Jan 24 (10pm)

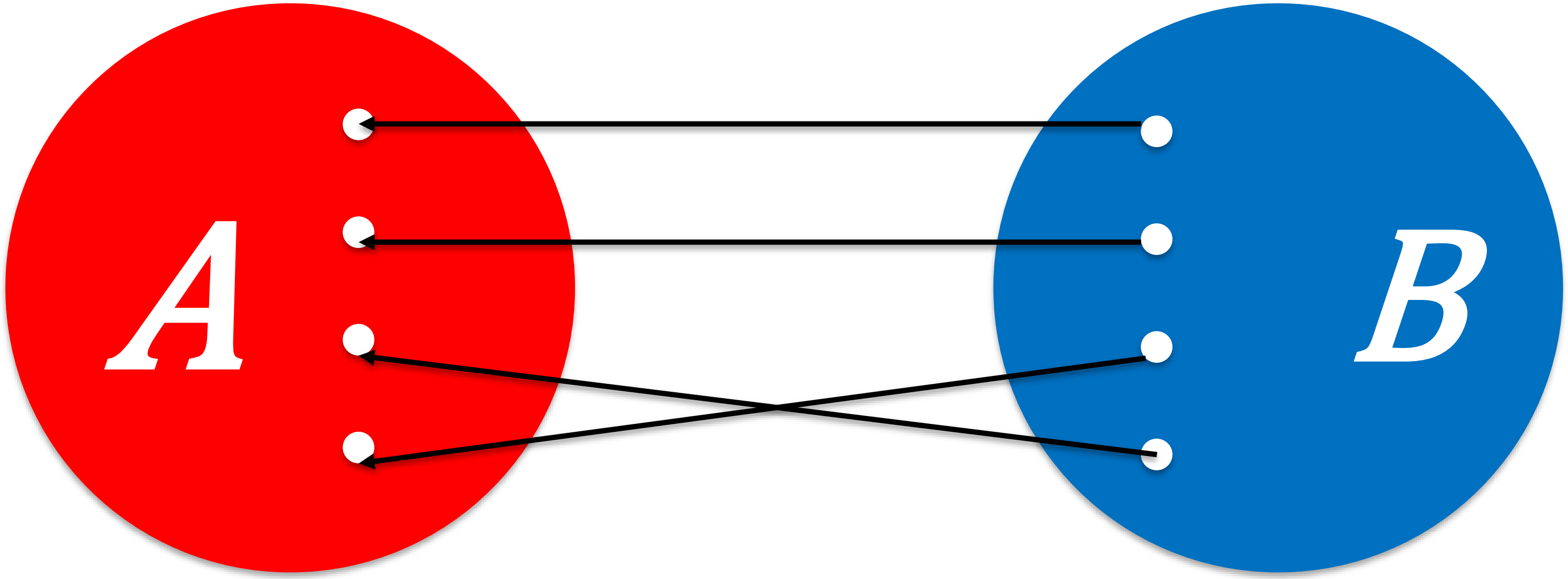
https://en.wikipedia.org/wiki/Print_Gallery_(M._C._Escher)

Class 4: *Cardinality. Boolean Gates.*

University of Virginia
cs3120: DMT2
Wei-Kai Lin

Recap: *same* cardinality

Definition. Two sets have the *same cardinality* if there is a bijection between the two sets.

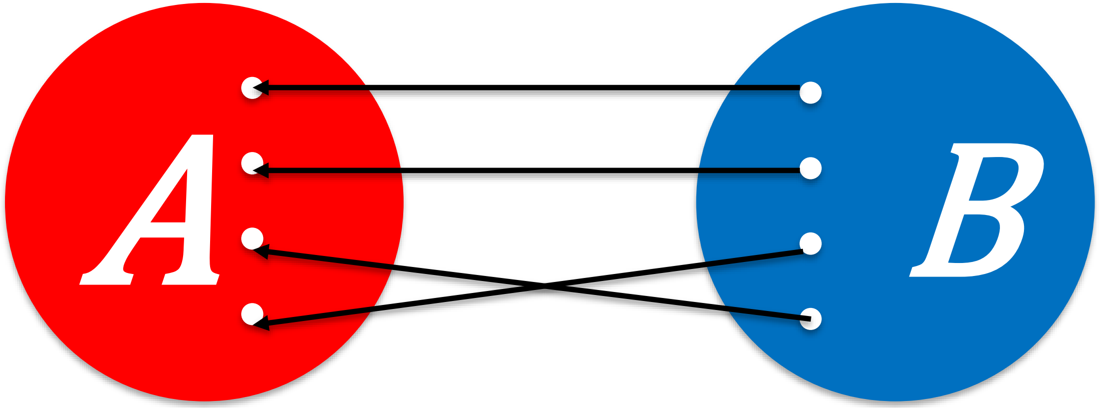


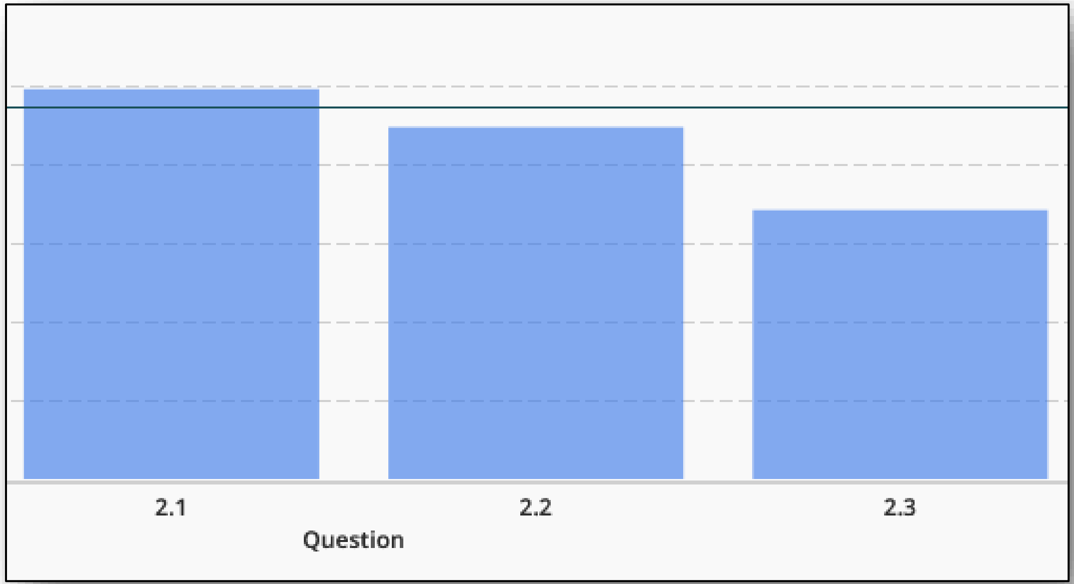
bijective: $=1$ in

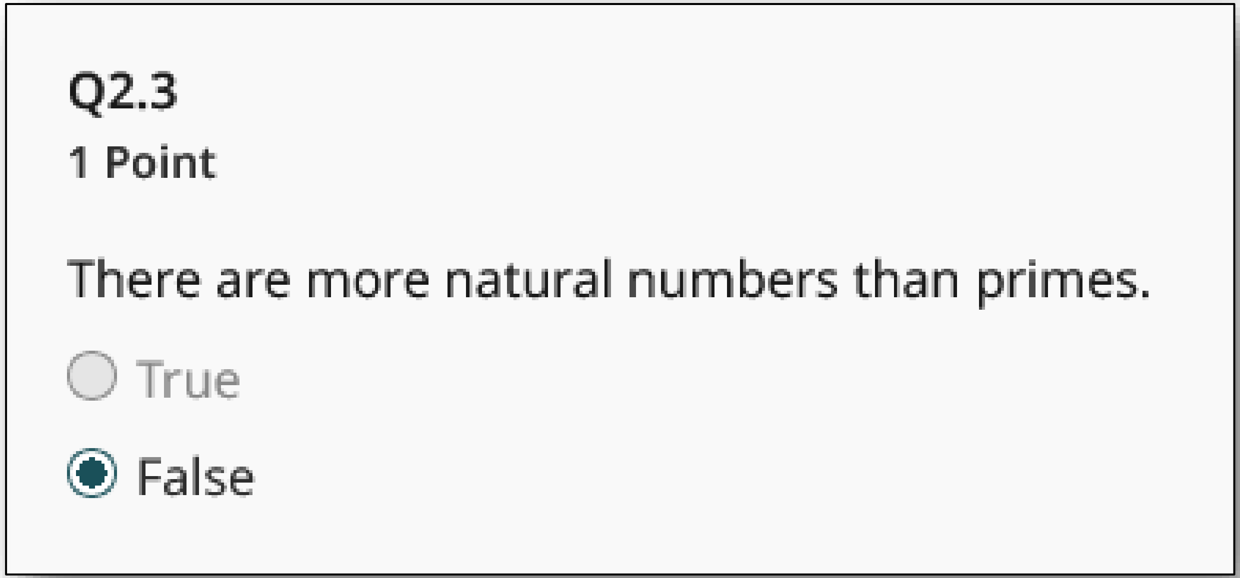
bijective: $=1$ out

Recap: *same* cardinality

Definition. Two sets have the *same cardinality* if there is a bijection between the two sets.

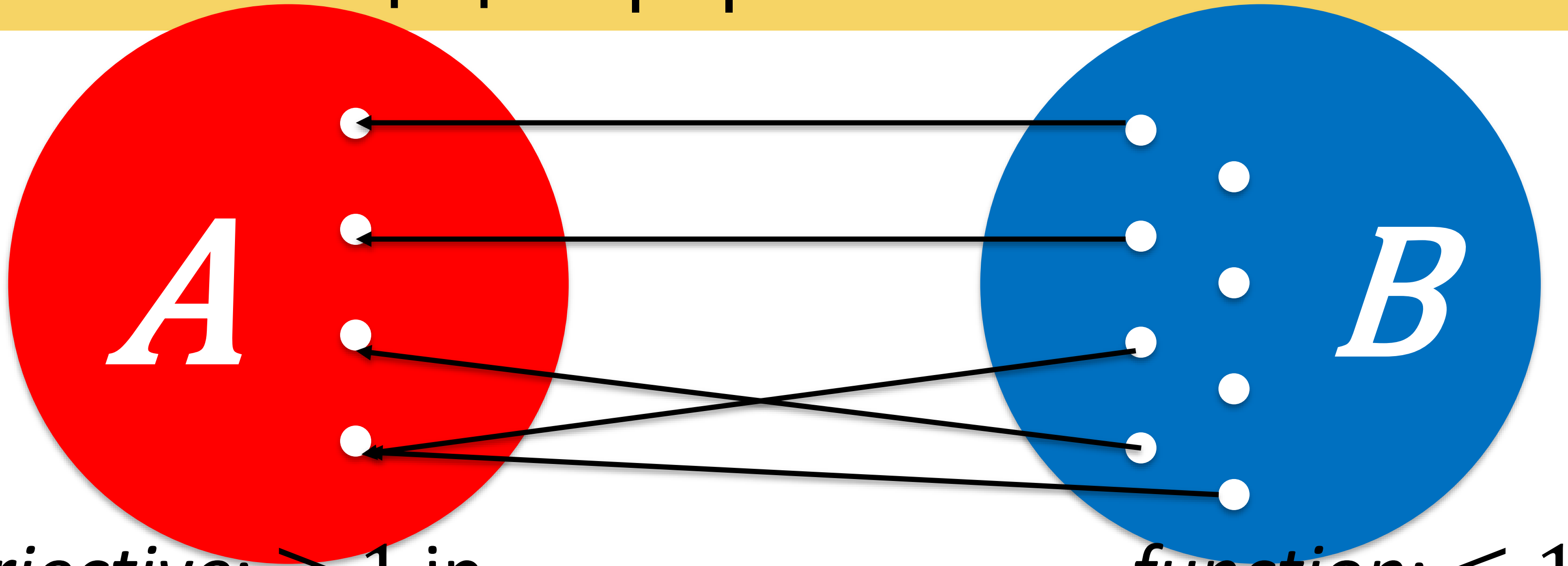






Recap: cardinality $|A| \leq |B|$

Definition. If there exists a **surjective function** from sets B to A, then we say the cardinality of B is ***greater than or equal to*** the cardinality of A.
We denote this as $|A| \leq |B|$.



surjective: ≥ 1 in

function: ≤ 1 out

Cardinality of (Infinite) Sets

Definition. Two sets have the *same cardinality* if there is a bijection between the two sets.

Definition. If there exists a **surjective function** from sets B to A, then we say the cardinality of B is ***greater than or equal to*** the cardinality of A.
We denote this as $|A| \leq |B|$.

Two Useful (Intuitively obvious?) Facts

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

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

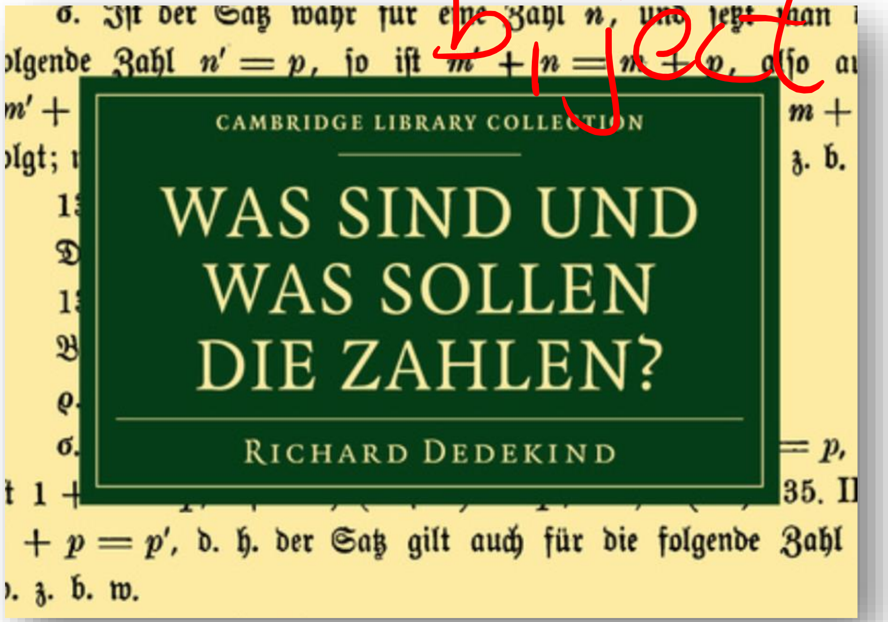
Are these “obvious” facts, or do we need a proof?

Two Useful Theorems

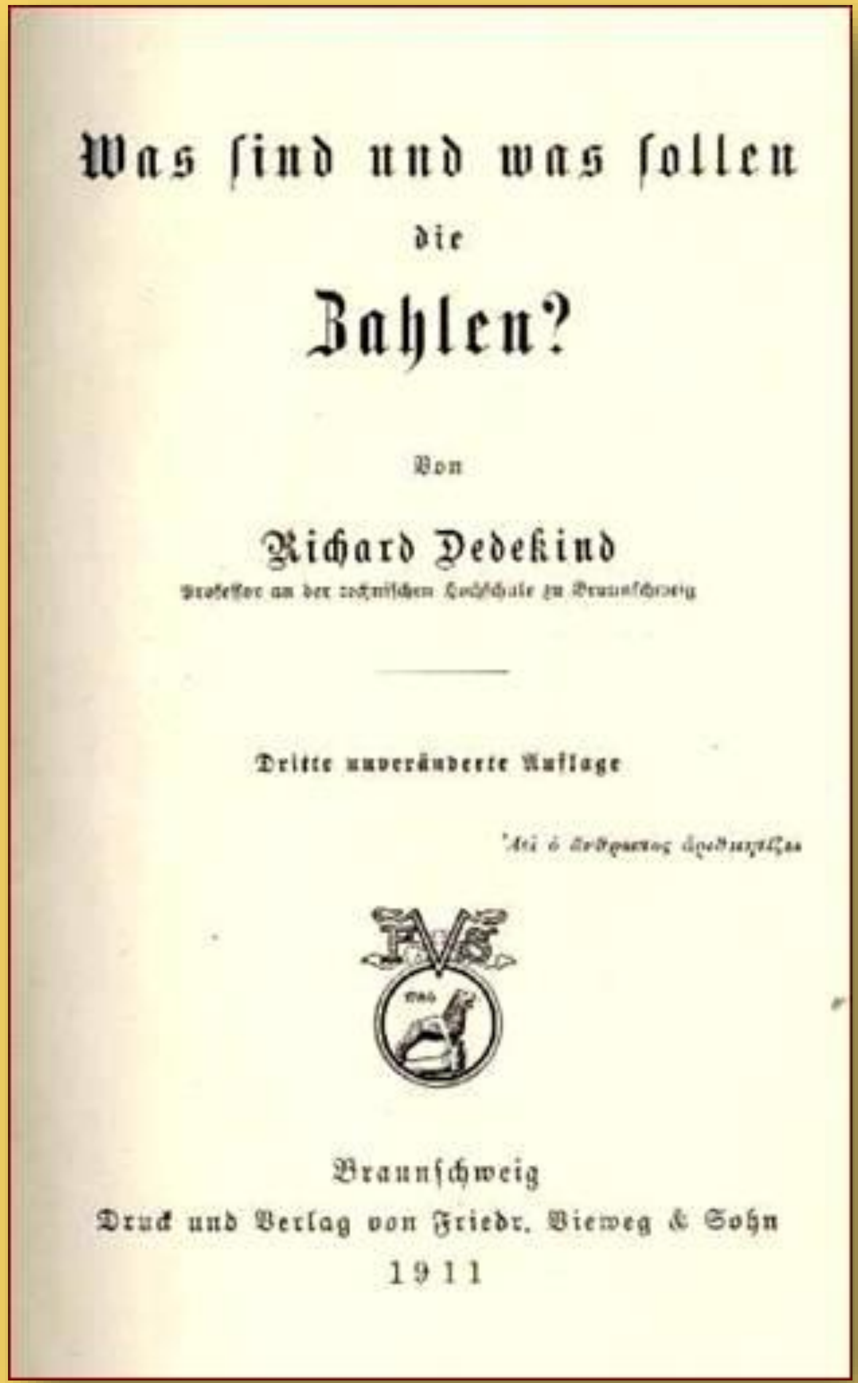
1. If $|A| = |B|$ then $|A| \leq |B|$ and $|B| \leq |A|$.
   biject surj surj
2. If $|A| \leq |B|$ and $|B| \leq |A|$ then $\cancel{|A| = |B|}$. find biject
   surj surj

(Cantor-) Schröder–Bernstein theorem

First stated (but not proven) by Cantor (1887)
First proven (but not published) by Dedekind (1887)
First proof announced by Schroder in 1896 (but its incorrect)
First correct proof by Bernstein (1897) (student in Cantor's class)



Do infinite sets even *exist*?



Was sind und was sollen
die
Zahlen?

Von

Richard Dedekind
Professor an der technischen Hochschule zu Braunschweig

Dritte unveränderte Auflage

Ἀεὶ ὁ ἄνθρωπος ἀριθμητίζει

Braunschweig
Druck und Verlag von Friedr. Vieweg & Sohn
1911

Do infinite sets even *exist*?

¶64. *Definition.* A set S is said to be *infinite* when it is similar to a proper subset of itself, otherwise it is said to be *finite*. Dedekind's footnote to this definition contains some important historical notes.

> In this form I submitted the definition of the infinite which forms the core of my whole investigation in September, 1882, to G. Cantor and several years earlier to Schwarz and Weber. All other attempts that have come to my knowledge to distinguish the infinite from the finite seem to me to have met with so little success that I think I may be permitted to forego any criticism of them.

David Joyce's *Notes on Richard Dedekind's Was sind und was sollen die Zahlen?*
https://mathcs.clarku.edu/~djoyce/numbers/dedekind.pdf

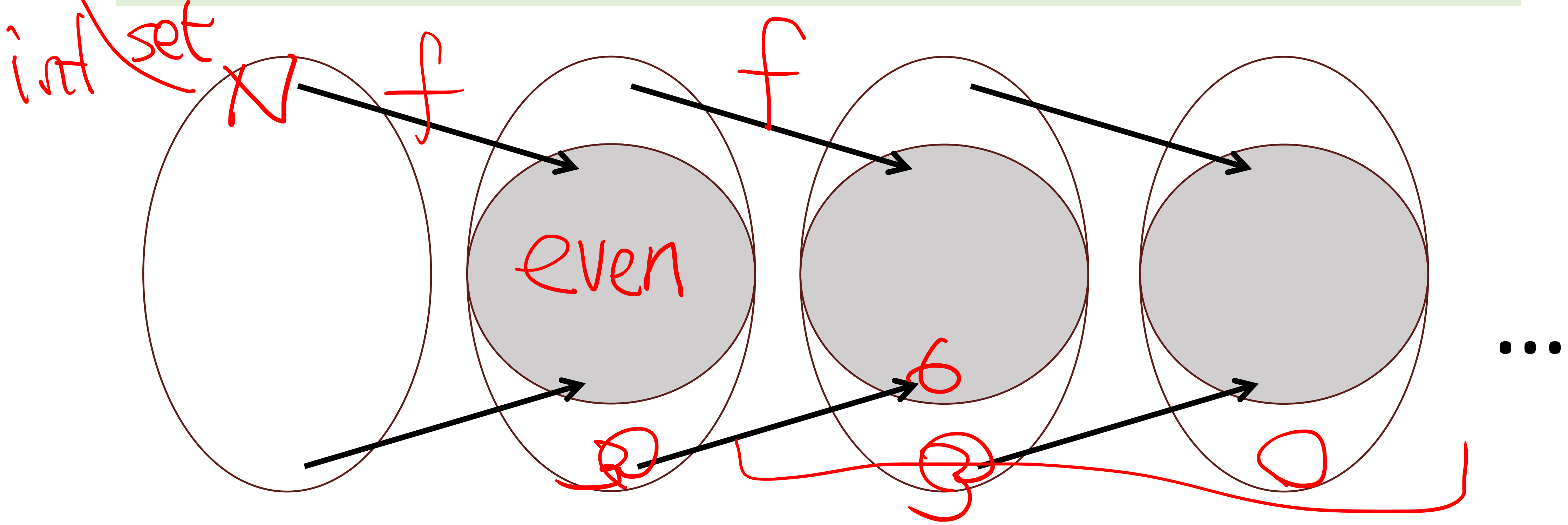
Do infinite sets even *exist*?

¶64. *Definition.* A set S is said to be *infinite* when it is similar to a proper subset of itself, otherwise it is said to be *finite*. Dedekind's footnote to this definition contains some important historical notes.

Definition. A set is ***Dedekind***-*infinite* if and only if it has the same cardinality as some **strict subset** of itself.

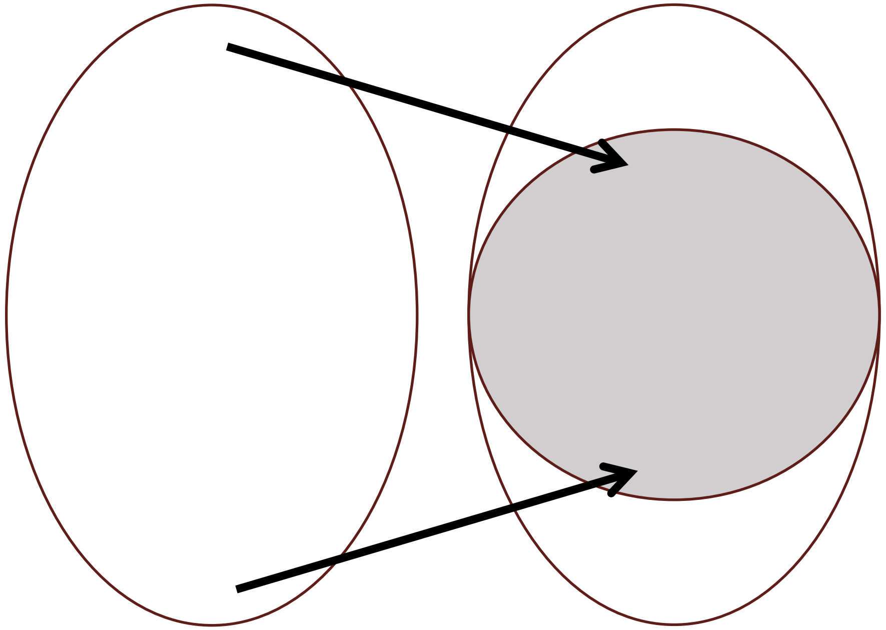
David Joyce's *Notes on Richard Dedekind's Was sind und was sollen die Zahlen?*
https://mathcs.clarku.edu/~djoyce/numbers/dedekind.pdf

Definition. A set is *Dedekind-infinite* if and only if it has the same cardinality as some **strict subset** of itself.



Definition. A set is *Dedekind-infinite* if and only if it has the same cardinality as some **strict subset** of itself.

Is $\mathbb{N}$ Dedekind-infinite?



Equivalent Definitions?

Definition. A set is ***Dedekind***-*infinite* if and only if it has the same cardinality as some **strict subset** of itself.

Previous Definition. A set S is *infinite*, if there is no bijection between S and any $[k]$.

this equivalence cannot be proved with the axioms of Zermelo–Fraenkel set theory without the axiom of choice

Countable

Definition. A set S is *countable* if and only if

$$|S| \leq |\mathbb{N}|$$

Definition. If there exists a **surjective function** from sets B to A, then we say the cardinality of B is ***greater than or equal to*** the cardinality of A. We denote this as $|A| \leq |B|$.

Countable

Definition. A set S is *countable* if and only if $|S| \leq |\mathbb{N}|$.

Definition. If there exists a **surjective function** from sets B to A, then we say the cardinality of B is ***greater than or equal to*** the cardinality of A. We denote this as $|A| \leq |B|$.

(Equivalent) Definition. A set S is *countable* if and only if there exists a *surjective function* from $\mathbb{N}$ to S.

A set S is *countable* if and only if there exists a *surjective function* from $\mathbb{N}$ to S.

Theorem: The set of finite Binary Strings is *countable*.

bijective

$|\{0,1\}^*| \leq |\mathbb{N}|$

$\mathbb{N}$	$\{0,1\}^*$
0 = 0	“”
1 = S(0)	0
2 = S(S(0))	1
3 = S(S(S(0)))	00
4 = …	01
5 = …	10
…	11
	…

Countably Infinite

A set S is *countable* if and only if there exists a *surjective function* from $\mathbb{N}$ to S.

A set is ***Dedekind***-*infinite* iff it has the same cardinality as some **strict subset** of itself.

Definition. A ~~***countably infinite*** set~~ is a set that is *countable* and *infinite*.

Prove Binary Strings is *countably infinite*

A set S is *countable* if and only if there exists a *surjective function* from $\mathbb{N}$ to S.

A set is ***Dedekind**-infinite* iff it has the same cardinality as some **strict subset** of itself.

biject

$\mathbb{N}$	$\{0,1\}^*$		Strict subset of $\{0,1\}^*$
0 = 0	“”	0	~~“”~~
1 = S(0)	0	1	0
2 = S(S(0))	1	2	~~1~~
3 = S(S(S(0)))	00		00
4 = …	01		~~01~~
5 = …	10		~~10~~
…	11		~~11~~
	…		…

Theorem?: A set S is *countably infinite* if and only if there exists a bijection between S and $\mathbb{N}$.

Two sets have the *same cardinality* if there is a bijection between the two sets.

$S = \{0,1\}^*$ inf

$|S| = |\mathbb{N}|$

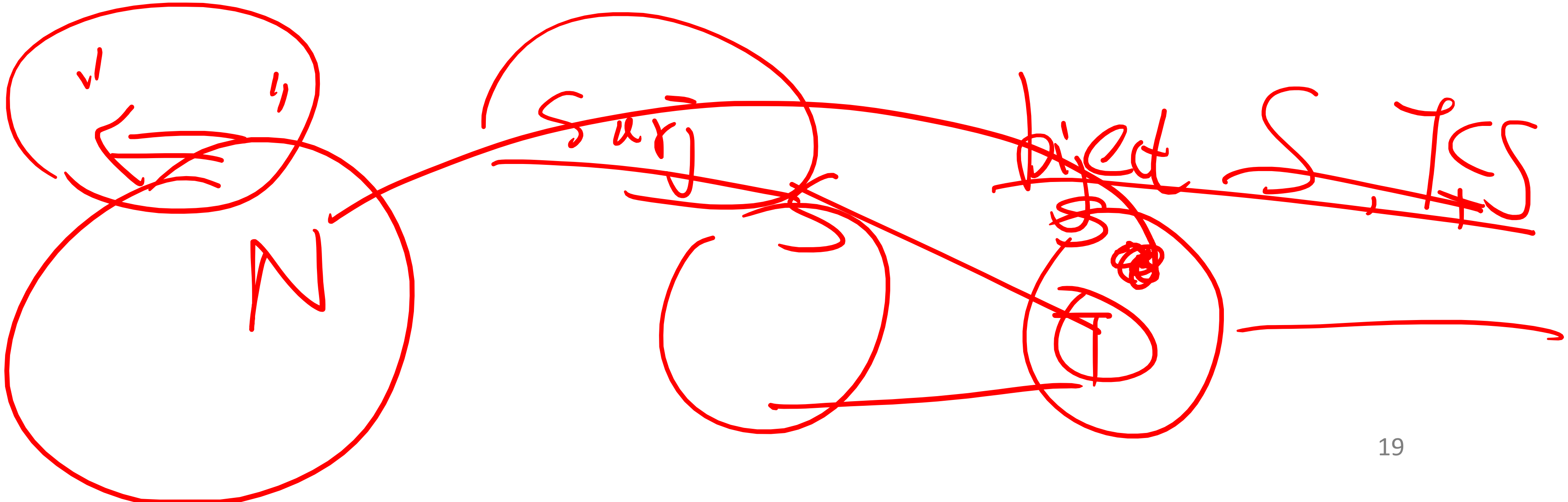
A set S is *countable* if and only if there exists a *surjective function* from $\mathbb{N}$ to S.

A set is ***Dedekind**-infinite* iff it has the same cardinality as some **strict subset** of itself.

A ***countably infinite*** set is a set that is *countable* and *infinite*.

$\Longrightarrow$

biject



Title slide: Escher's Print Gallery. https://www.youtube.com/watch?v=dzCEf8mwgDU

Is there an ***un***countable set?

$\mathbb{R}$, $\cancel{\mathbb{Q}}$ $\mathbb{R} \setminus \mathbb{Q}$, $\mathbb{C}$, $\mathbb{I}$

$\{0,1\}^\infty$

$\{0,1\}^\infty$

Can the *Infinite* Binary Strings be counted?

Assume for contra, countable

bijeet $\{0,1\}^\infty$, $\mathbb{N}$

$$\begin{array}{cccccc}
0 & b_{01} & b_{02} & b_{03} & \cdots & \\
1 & b_{11} & b_{12} & b_{13} & \cdots & \\
2 & \vdots & & & \ddots & \\
3 & & & & & \\
\vdots & \vdots & & & &
\end{array}$$

b_{01} b_{12} b_{23} $\vdots$

$\{0,1\}^\infty$

Can the *Infinite* Binary Strings be counted?

Power Sets

Definition. The *power set* of a set A is the set of all subsets of A.

$$B \in pow(A) \Leftrightarrow B \subseteq A$$

What is the cardinality of $pow(S)$?

Cardinality of $pow(S)$ for finite set S

$= 2^{|S|}$

Proof

Induction

$a \in pow(S)$ $\quad 2^{|S|}$ string

$f(a) \longleftrightarrow$ "$0\,1\,0 \cdots 0$"

iff ith elem of S $\in a$

Cardinality of $pow(S)$ for finite set S

Proof by induction on $\mathbb{N}$:

Inductive hypothesis: $P(n)$ = for all sets A of cardinality n, $|pow(A)| = 2^n$

Base case: $P(0)$: $pow(S) = \{\emptyset\}$. $|pow(S)| = 1 = 2^0 = 2^{|S|}$.

Inductive case: $\forall m \in \mathbb{N}. P(m) \Rightarrow P(m+1)$.

For all sets T with $|T| = m+1, \exists S$ where $|S| = m, x \notin S.\ T = S \cup \{x\}$

By the inductive hypothesis, $P(m) \Rightarrow |pow(S)| = 2^{|S|}$

Since $pow(T)$ includes all elements of $pow(S)$ as well as each of those elements with $\{x\}$ inserted, this means

$$|pow(T)| = 2 \cdot |pow(S)| = 2 \cdot 2^{|S|} = 2^{|S|+1} = 2^{|T|}.$$

QED: For all finite sets S, $|pow(S)| = 2^{|S|}$.

Theorem: For all **finite** sets S, $|pow(S)| > |S|$.

$2^n > n$

Theorem: For all **finite** sets S, $|pow(S)| > |S|$.

Proof by induction on $\mathbb{N}$:

$P(n) ::= \forall$ sets S where $|S| = n \,.\, |pow(S)| > |S|$.

Base case: $P(0){:}\, S = \emptyset$.

$pow(S) = \{\emptyset\}$. $|\,pow(S)| = 1 > \,|\,S\,| = 0$.

Inductive case: $\forall m \in \mathbb{N}.\, P(m) \Rightarrow P(m+1)$.

for all sets T where $|T| = m + 1, \exists S$ where $|S| = m, x \notin S \,.\, T = S \cup \{\, x \,\}$

$P(m) \Rightarrow |pow(S)| > |S| \Rightarrow |pow(S)| + 1 > |S| + 1$

Since $pow(T)$ includes all elements of $pow(S)$ and includes $\{\, x \,\}$, this means

$|\,pow(T)\,| \geq |pow(S)| + 1 > |S| + 1 = |T| \Rightarrow P(m+1)$.

Therefore, $P(n)$ always holds, so we can conclude for all sets S, $|pow(S)| > |\,S\,|$.

For **ALL** sets S, $|pow(S)| > |\, S\,|$.

Bogus non-proof:

Proof by induction on $\mathbb{N}$:

$$P(n) ::= \ \forall \text{ sets } S \text{ where } |S| = n\,.\,|pow(S)| > |S|.$$

Base case: $P(0)$: $S = \emptyset$.

$$pow(S) = \{\emptyset\}.\ |\,pow(S)| = 1 > |\,S\,| = 0.$$

Inductive case: $\forall m \in \mathbb{N}.\, P(m) \Rightarrow P(m+1)$.

for all sets T where $|T| = m + 1, \exists S$ where $|S| = m, x \notin S\,.\,T = S \cup \{\,x\,\}$

$P(m) \Rightarrow |pow(S)| > |S| \Rightarrow |pow(S)| + 1 > |S| + 1$

Since $pow(T)$ includes all elements of $pow(S)$ and includes $\{\,x\,\}$, this means

$$|\,pow(T)\,| \geq |pow(S)| + 1 > |S| + 1 = |T| \Rightarrow P(m+1).$$

Therefore, $P(n)$ always holds, so we can conclude for all sets S, $|pow(S)| > |\,S\,|$.

For **ALL** sets S, $|pow(S)| > |S|$.

Bogus non-proof:

1 **Proof by induction on $\mathbb{N}$:**

2 $P(n) ::= \ \forall$ sets S where $|S| = n \,.\, |pow(S)| > |S|$.

3 **Base case:** $P(0)$: $S = \emptyset$.

4 $pow(S) = \{\emptyset\}$. $|pow(S)| = 1 > |S| = 0$.

5 **Inductive case:** $\forall m \in \mathbb{N}.\, P(m) \Rightarrow P(m+1)$.

6 for all sets T where $|T| = m + 1, \exists S$ where $|S| = m, x \notin S \,.\, T = S \cup \{x\}$

7 $P(m) \Rightarrow |pow(S)| > |S| \Rightarrow |pow(S)| + 1 > |S| + 1$

8 Since $pow(T)$ includes all elements of $pow(S)$ and includes $\{x\}$, this means

9 $|pow(T)| \geq |pow(S)| + 1 > |S| + 1 = |T| \Rightarrow P(m+1)$.

10 Therefore, $P(n)$ always holds, so we can conclude for all sets S, $|pow(S)| > |S|$.

Which is the first incorrect step?

Principle of Induction: Suppose that $\boldsymbol{X}$ is a subset of $\mathbb{N}$ that satisfies these two properties: (1) $\mathbf{0} \in \boldsymbol{X}$ (2) if $n \in \boldsymbol{X}$, then $\boldsymbol{S}(n) \in \boldsymbol{X}$. Then, $\boldsymbol{X} = \mathbb{N}$.

Proof by Induction: For any predicate $\boldsymbol{P}(\mathbb{N})$, showing (1) $\boldsymbol{P}(\mathbf{0})$ and (2) if for any $n \in \mathbb{N}$ if $\boldsymbol{P}(n)$ then $\boldsymbol{P}(\boldsymbol{S}(n))$ proves $\boldsymbol{P}$ holds for all $\mathbb{N}$.

Principle of Induction starts from a subset of $\mathbb{N}$ and proves that it is equal to $\mathbb{N}$. You can only use induction to prove a property about a set if we can map that set to a subset of $\mathbb{N}$.


Georg Cantor
(1845-1918)

Georg Cantor’s Shocking Result

(~1874)

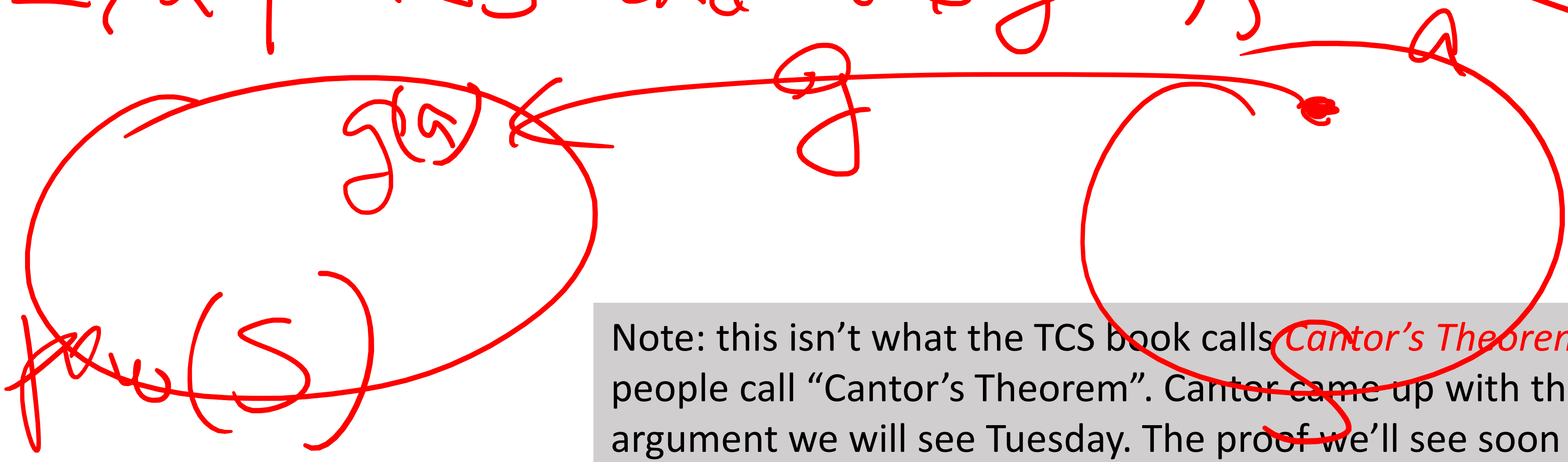
For **all** sets S, $|pow(S)| > |S|$.

Cantor's Theorem:
For all sets S, $|pow(S)| > |S|$.

By contradict, $\exists S$, $|pow(S)| \le |S|$

$\exists$ surject $g : S \to pow(S)$

$T = \{a \mid a \in S \text{ and } a \notin g(a)\} \subseteq S$



Note: this isn't what the TCS book calls *Cantor's Theorem* but is what most people call "Cantor's Theorem". Cantor came up with the diagonalization argument we will see Tuesday. The proof we'll see soon of Cantor's Theorem is believed to have been first done by Hessenberg (1906).

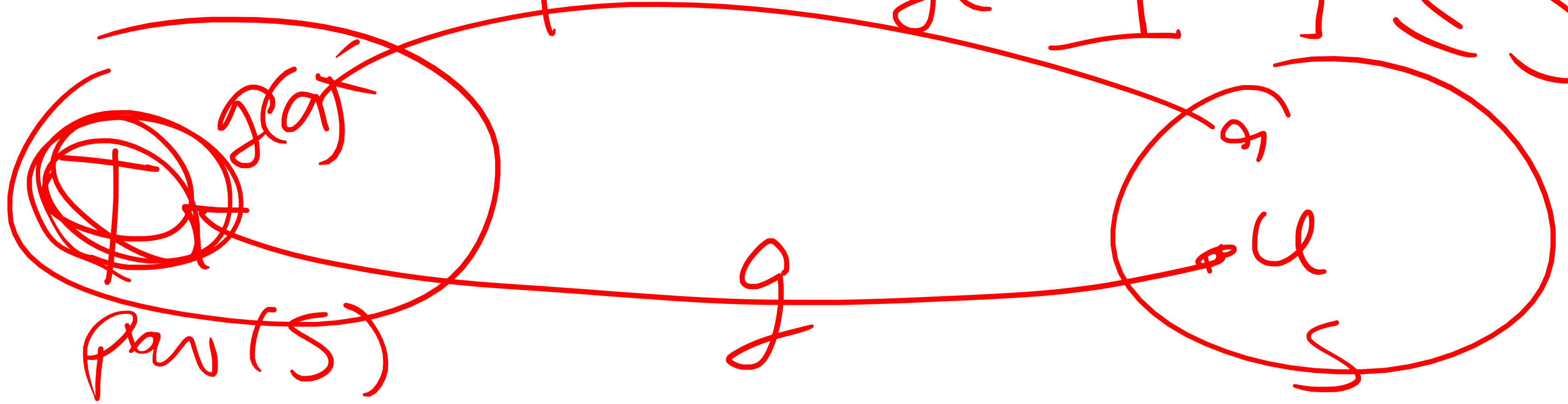
For all sets S, $|pow(S)| > |S|$.

$\exists u$ s.t. $g(u) = T$

1. $u \in T = g(u) \Rightarrow u \in g(u) \Rightarrow u \notin T$ $\lightning$

2. $u \notin T = g(u) \Rightarrow u \notin g(u) \Rightarrow u \in T$ $\lightning$

$T = \{a \mid a \in S, g(a) \not\ni a\}$ $\square$



Proof. For all sets S, $|pow(S)| > |S|$.

Towards a contradiction, **assume** $\exists \boldsymbol{S}. |\boldsymbol{pow}(\boldsymbol{S})| \leq |\boldsymbol{S}|$.
By the definition of $\leq$, there must exist a *surjective function* g from $S \to pow(S)$.

Define $T = \{ a \mid a \notin g(a), a \in S \}$.

$T \in pow(S)$. (Obviously, its a subset of S.)
Since g is surjective, $\exists\, u \in S$ such that $g(u) = T$.

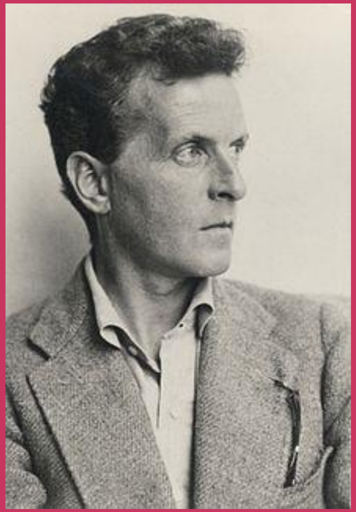
(1) If $u \in g(u)$, then $u \notin T$.
But $T = g(u)$, so $u \notin g(u)$.

(2) If $u \notin g(u)$, then $u \in T$.
But $T = g(u)$, so $u \in g(u)$.

Contradiction! So, there must not exist any S such that $|pow(S)| \leq |S|$.

Georg Cantor
(1845-1918)

“corruptor of youth”
Leopold Kronecker



“utter nonsense”
Ludwig Wittgenstein

“grave disease”
Henri Poincaré

Georg Cantor
(1845-1918)

My theory stands as firm as a rock; every arrow directed against it will return quickly to its archer. How do I know this? Because I have studied it from all sides for many years; because I have examined all objections which have ever been made against the infinite numbers; and above all, because I have followed its roots, so to speak, to the first infallible cause of all created things.

Georg Cantor, 1887 Letter to K. F. Heman

Defining Computation

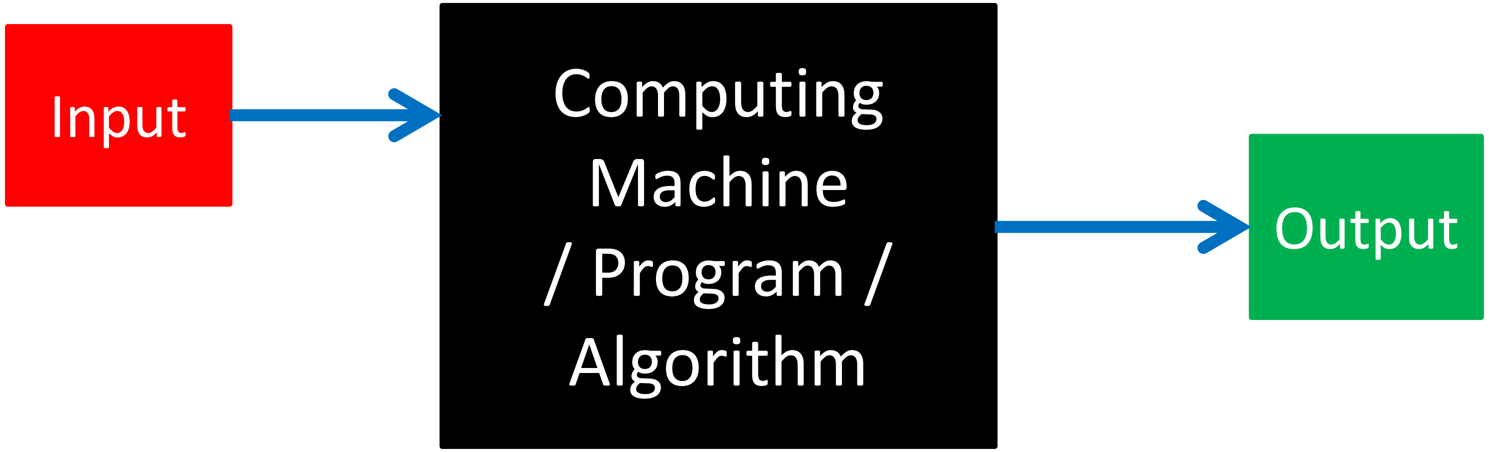
Story so far

- Defining things Precisely:
  – Natural numbers
  – Sets
  – Cardinality
  – Infinity
  – Countability
- Goal of the class:
  – Think precisely about computing
- Next:
  – Precise definition of computing

What do computers do?

What computers do

- A "computer" is something that "performs" a “mapping” from inputs to outputs (strings?)
  - It is the actual process.
  - Different from the specification.



What goes in here?

Computational **Model**

- The **particular way** of implementing the computation process
- Examples:

A simple model of computation

- Based on Boolean logical 'gates':
  - OR(a, b): outputs 1 iff a=1 **or** b=1
  - AND(a, b): outputs 1 iff a=1 **and** b=1
  - NOT(b): outputs 1 iff b=0

Output 0 otherwise

Towards Algorithms

- Example: “median"
  - Median is 1 **if at least half** of inputs are 1
- Math definition of MED on 3 inputs:

Computing MED using **A**nd/**O**r/**N** ot

- Still a “math”-ish def/algorithm for MED:

A formal programming language

- **AON Straightline** programs
  - Python-like language
  - Define functions that take Boolean inputs
  - Use AND/OR/NOT within
  - Assign results of AND/OR/NOT to variables
  - The result of variables can be used later as inputs
  - Return some of the obtained result(s) as output

More things to program

- NAND

- XOR

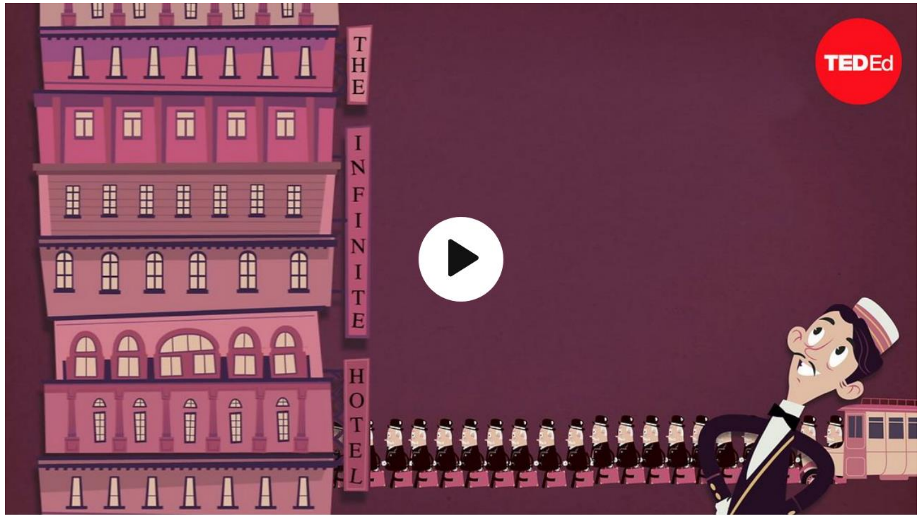
Charge

Set Cardinality

Infinite

Countable

Power set



Computation Model

PS1: due tomorrow (Friday) 10:00pm
PRR2: due Monday, Jan 27, 10:00pm
PS2: due next Friday, Jan 31, 10:00pm

Survey: which TA / Office hour work for you?