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

- **HW 0 due this Friday, Jan 23 (10:00pm)**
- **Quiz 1 w due next Mon, Jan 26 (10:00pm)**
- **HW 1 coming soon, due next Friday**

Class 3: *Infinity*

University of Virginia
CS3120: DMT2
https://weikailin.github.io/cs3120-toc
Wei-Kai Lin

Survey: A (common) question for the course

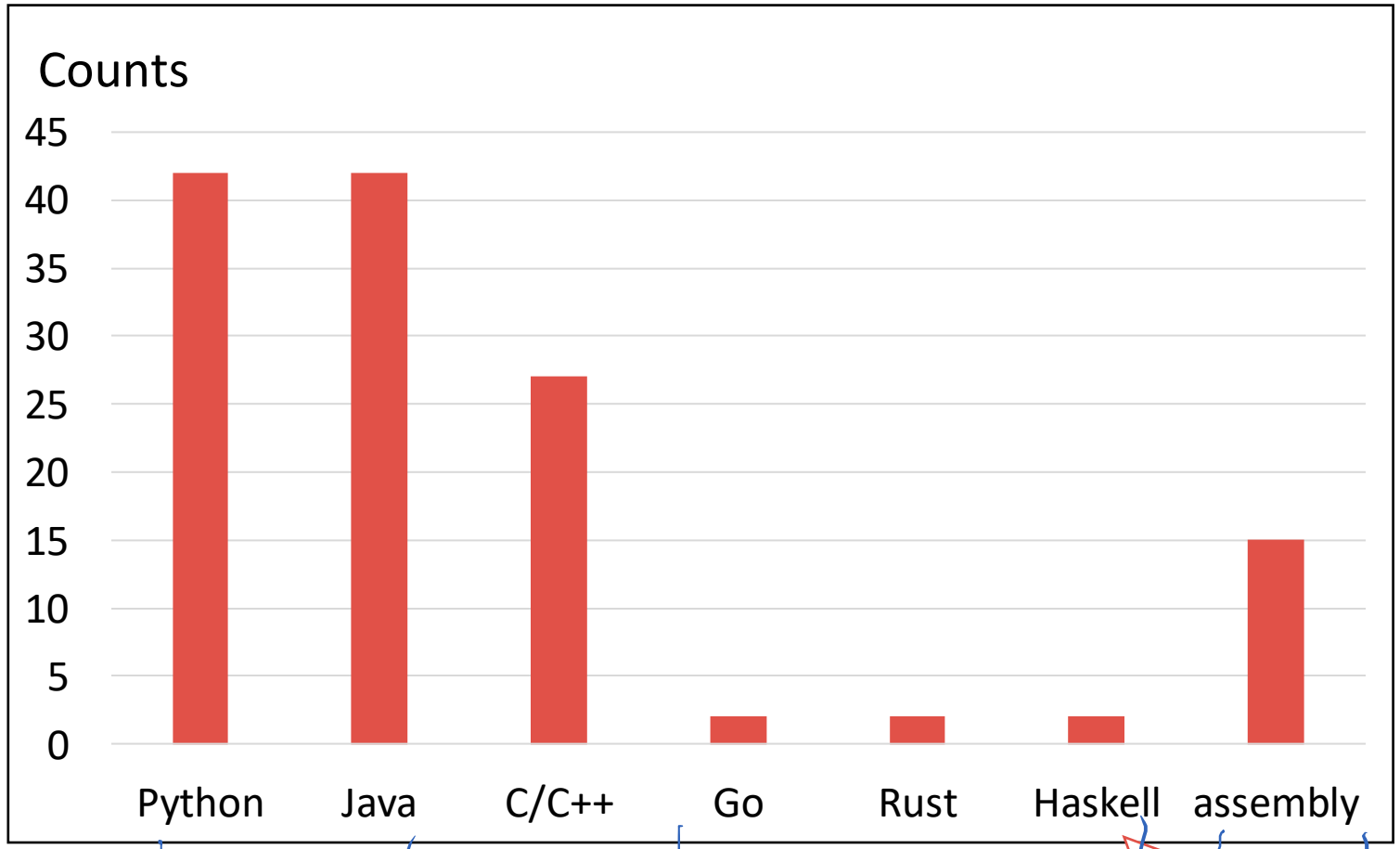
- How this course can be applied to real-world contexts, especially for SWE jobs?
  - Many different answers, here is one:

Many programming languages (if not all) are rooted in the theory. Thus, this course speeds up the learning of PLs.

- Hold on or ask for other answers.

Q3.1 Programming languages

Select all programming languages which you consider yourself competent in.



Or other functional programming languages

Definition. For any two natural numbers, n and m, we define equality (=) as:

(1) if n is $\mathbf{0}$: $n = m$ iff m is $\mathbf{0}$.

(2) otherwise, n is $\boldsymbol{S}(p)$ for some natural number p.

(2a) If m is $\mathbf{0}$, n is not equal to m.

(2b) Otherwise, m is $\boldsymbol{S}(q)$ for some natural number q, then $n = m$ iff $p = q$.

Class 1, Equality

HW 0 also

The Haskell Quicksort

Haskell

```haskell
quicksort :: (Ord a) => [a] -> [a]
quicksort [] = []
quicksort (x:xs) =
    let smallerSorted = quicksort [a | a <- xs, a <= x]
        biggerSorted  = quicksort [a | a <- xs, a > x]
    in  smallerSorted ++ [x] ++ biggerSorted
```

Plan

Cardinality of Sets

Countable

Diagonalization

Cantor's Theorem

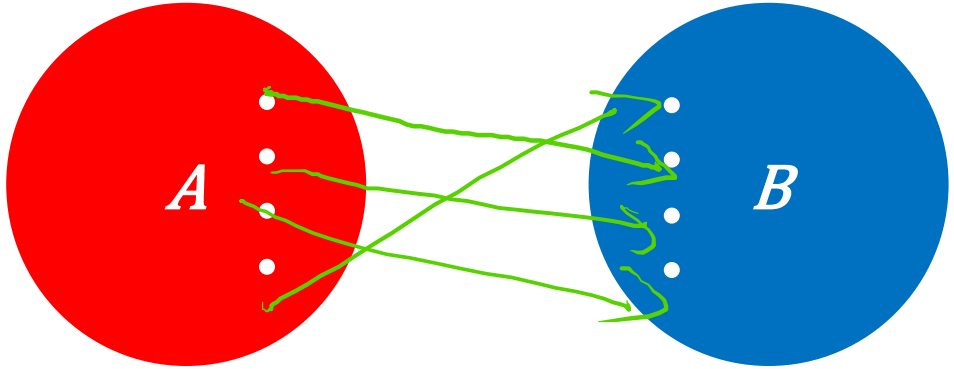
Section

Today: Chapter 2.4 in the TCS book

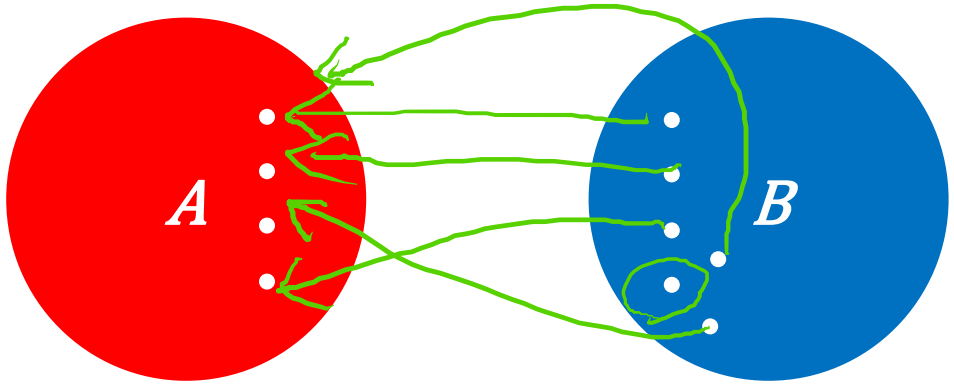
https://introtcs.org/public/lec_02_representation.html#cantorsec

Recap: Cardinality of (Infinite) Sets

Definition. Two sets have the *same cardinality* if there is a bijection between the two sets. We denote this as $|A| = |B|$.



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 $|A| \leq |B|$.



Q: Do we have $|A| \geq |B|$ defined?
Q: Do we have $|A| < |B|$ defined?

$|B| \leq |A|$ iff $A \to B$
$|A| \leq |B|$ and not $|A| = |B|$

Example: $EVEN$ and $\mathbb{N}$

$\mathbb{N} = \{0,1,2,3,\dots\}$, $EVEN = \{0,2,4,6,\dots\}$

Is $\mathbb{N} \subseteq EVEN$? $EVEN \subseteq \mathbb{N}$? $EVEN \subseteq \mathbb{N}$?

Is $|\mathbb{N}| \leq |EVEN|$?

Surjective $g(x) = x/2$ from EVEN to N

Is $|\mathbb{N}| \geq |EVEN|$?

Surjective $h(x) = 2x$ from N to EVEN

Is $|\mathbb{N}| = |EVEN|$?

Bijection g

Do infinite sets even *exist*?


Was ſind und was ſollen
die
Zahlen?

Von

Richard Dedekind

Dritte unveränderte Auflage

Braunſchweig
Druck und Verlag von Friedr. Vieweg & Sohn
1911

Pronounce “Dedekind”: https://www.youtube.com/watch?v=s5pbbwGrH14

Do infinite sets even *exist*?

[Dedekind 1888, Beman 1901]

¶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.

Footnote of Dedekind

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

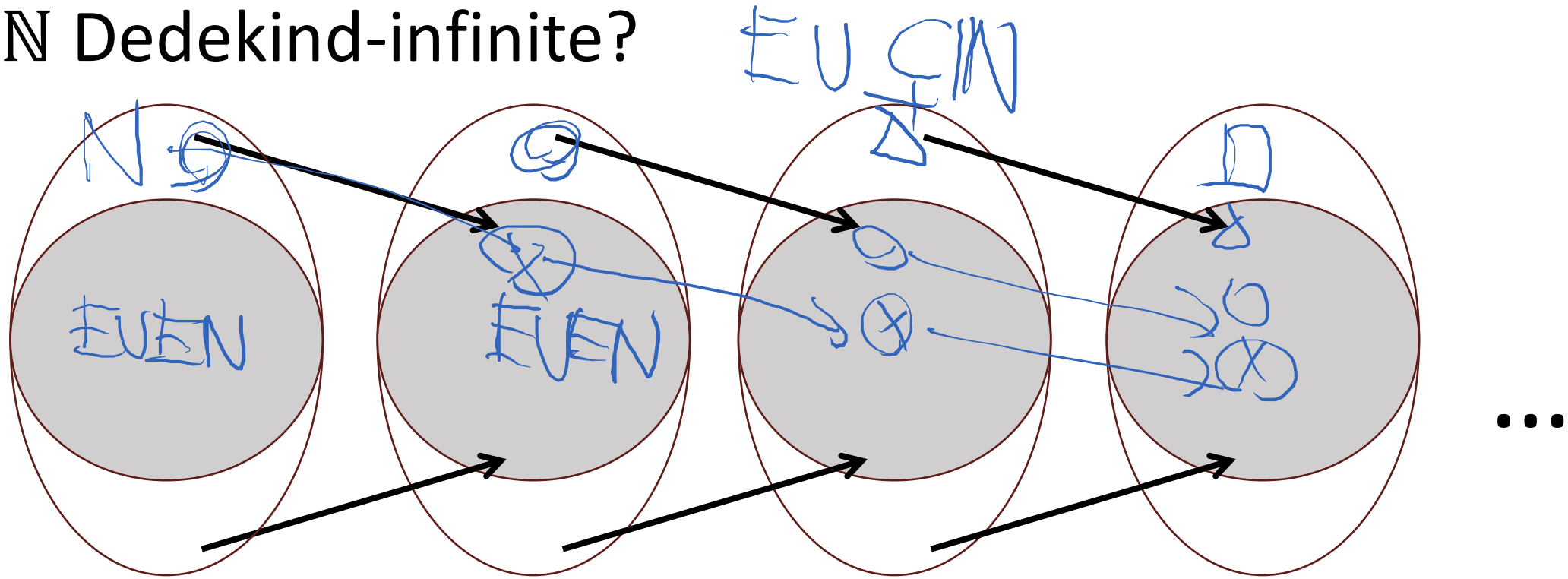
Do infinite sets even *exist*?

¶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.

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.

Alternative Definition. A set S is *infinite*, if there is no bijection between S and any $[k], k \in \mathbb{N}$.

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.

Q: Is $\mathbb{N}$ countable?

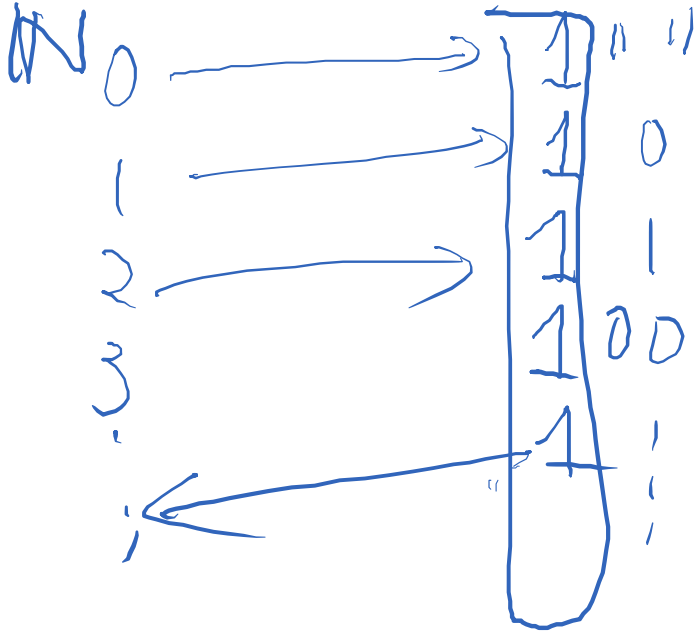
Y. $|\mathbb{N}| = |\mathbb{N}|$ biject

How about Binary Strings?

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*.

$\{0,1\}^*$



Proof.

Want a surjective function g from $\mathbb{N}$ to $\{0,1\}^*$.

$g(x)$ = ? $x \in \mathbb{N}$

1. write bin $(x+1)$
2. remove the leading 1

Argue g is surjective.

$\forall s \in \{0,1\}^*$

$\exists x \in \mathbb{N}, g(x) = s$

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.

Proved

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

$\{0,1\}^* \supsetneq T$

$|\{0,1\}^*| = |T|$,

$T = \{ s \in \{0,1\}^* \mid s \text{ begins w/ } 1 \}$

bijection is ~~rev~~ * remove the leading 1

prepend 1

$11 \in \{0,1\}^*$

$11 \notin T$

Why care countable or infinite?

- Is the set of Python programs countable or infinite?
- How about Java, Go, or Assembly programs?
- Is there any “programming language” uncountable?

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

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.

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*.

$\Rightarrow$ easy

"$\Leftarrow$" $|S| \leq |\mathbb{N}|$ by countable

Want $|S| \geq |\mathbb{N}|$ (then by Theorem on Jan 20)

$T \subsetneq S$, $|T| = |S|$ (To be posted)

Uncountable

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

- $\{(x, y) \mid x \in \mathbb{N}, y \in \mathbb{N}\}$
  that is, 2-dimensional grid points

$|\mathbb{N}^2| \leq |\mathbb{N}|$

- $\{(x_0, x_1, \ldots, x_n) \mid n \in \mathbb{N}, x_i \in \{0,1,2,3\} \text{ for all } i \in [n]\}$
  ternary strings

- $\{(x_0, x_1, \ldots, x_n) \mid n \in \mathbb{N}, x_i \in \mathbb{N} \text{ for all } i \in [n]\}$
  strings of natural numbers

(0 — 9 ,)

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

$\{0,1\}^\infty = \{f \mid f : \mathbb{N} \to \{0,1\}\}$

Can the *Infinite* Binary Strings be counted?

No.

Proof. Assume for contradiction, $\{0,1\}^\infty$ is infinite but countable.

We have bijection g between $\{0,1\}^\infty$ and $\mathbb{N}$ by Theorem (above).

Diagon.

$x \in \mathbb{N}$	$g(x)[0]$	$g(x)[1]$	$g(x)[2]$	$g(x)[3]$	...
0	0	0	0	0	...
1	1	0	0	0	...
2					
3					
4					
⋮					
⋮					
⋮					

Assume $g: \mathbb{N} \to \{0,1\}^\infty$ a bijection.

$y \in \mathbb{N}$	g(y)[0]	g(y)[1]	g(y)[2]	g(y)[3]	g(y)[4]	g(y)[5]	
0	0	1	1	0	1	0	…
1	1	1	0	1	0	1	…
2	0	1	1	0	1	0	…
3	0	0	1	0	1	1	…
4	1	1	0	1	0	1	…
5	0	1	0	1	1	0	…
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

Let s := (¬g(0)[0], ¬g(1)[1], ¬g(2)[2], ¬g(3)[3], …).

$s \in \{0,1\}^\infty$ by definition of $\{0,1\}^\infty$.

Is there any $y \in \mathbb{N}$ s.t. $g(y) = s$?

Power Sets

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

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

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

Sometime $pow(A)$ is written as $P(A)$ or 2^A

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

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, $|pow(S)| > |S|$.

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

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

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

$2^{|S|} > |S|$

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

Bogus non-proof:

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

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

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

$2^{|S|} > |S|$

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

Bogus non-proof:

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

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

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

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

*Which is the **first** incorrect step?*

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

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

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

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

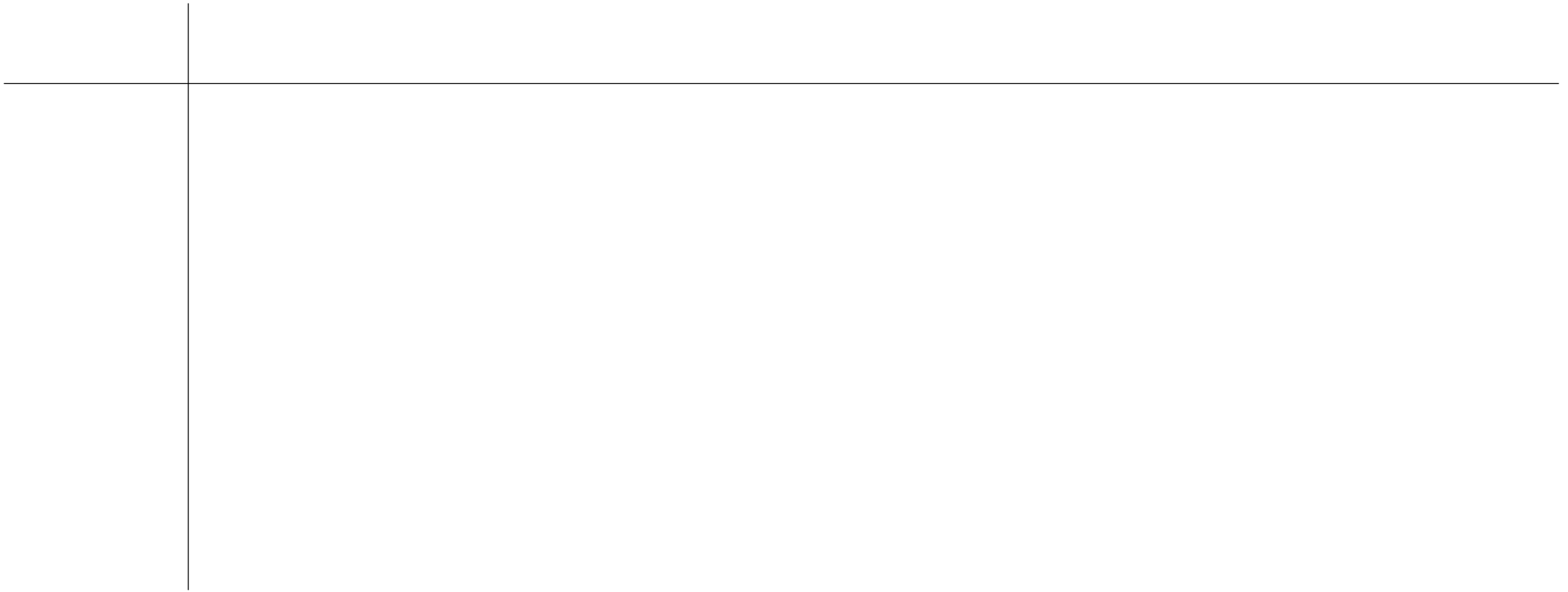
(~1874)

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

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).

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

Proof. Assume for contradiction, $|pow(S)| \leq |S|$.



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

Proof. Assume for contradiction, $|pow(S)| \leq |S|$. $\exists$ surjective $g: S \to pow(S)$

$y \in S$	$a_0 \in g(y)$	$a_1 \in g(y)$	$a_2 \in g(y)$	$a_3 \in g(y)$	$a_4 \in g(y)$	...
a_0	0	0	0	1	0	
a_1	1	1	1	1	1	
a_2	0	1	0	0	0	
a_3	1	1	0	0	0	
a_4	1	1	0	0	1	
a_5	1	1	0	0	0	
⋮						

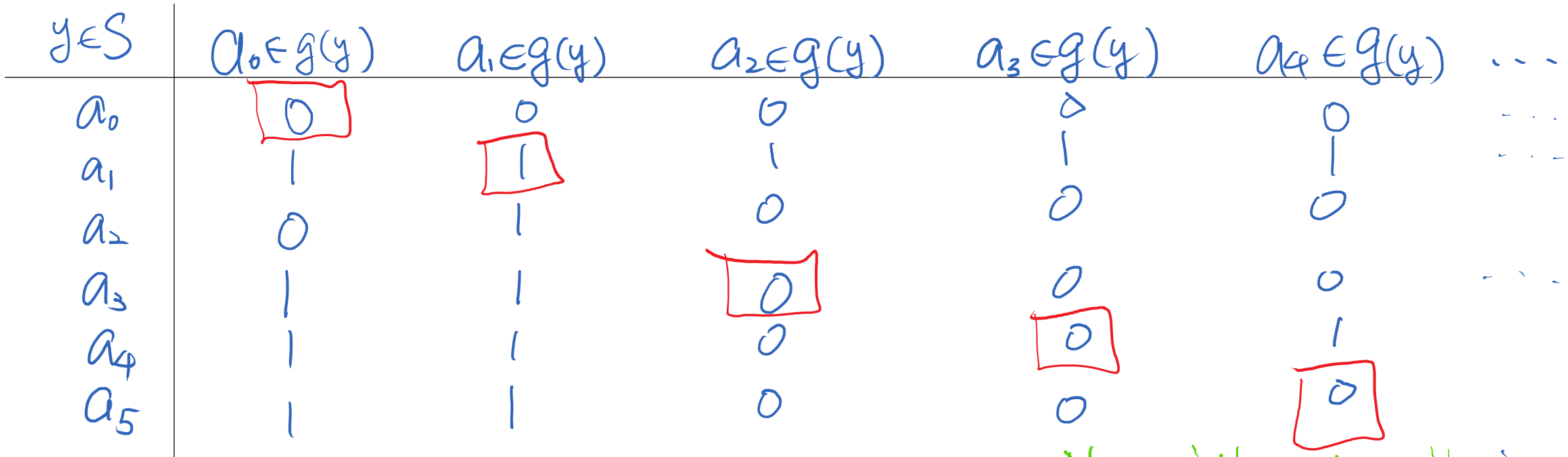
0 : Not in

1 : in

Good illustration, but S can be uncountable, so this is NOT precise

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

Proof. Assume for contradiction, $|pow(S)| \leq |S|$. $\exists$ surjective $g : S \to pow(S)$



Negate diagonal $T := \{ y \in S \mid y \notin g(y) \}$ ← Neg intentionally

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

Negate diagonal $T := \{a \in S \mid a \notin g(a)\}$

$T \subseteq S$, so $T \in pow(S)$.

g is surjective, there is $u \in S$ s.t. $g(u) = T$.

Want a contradiction: no such u !

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

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

Define $T = \{a \in A \mid a \notin g(a)\}$ ($\star$).

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

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

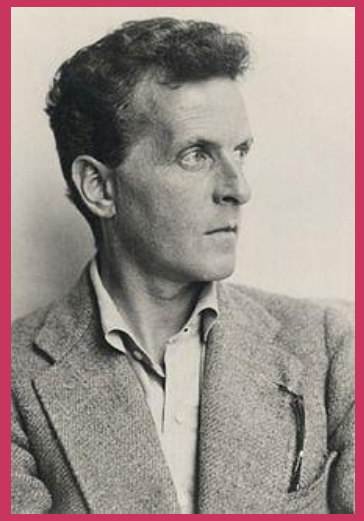
(2) If $u \notin g(u)$, then $u \in T$ by $\star$.
But $T = g(u)$, so $u \in g(u)$.

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

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

Logistics

- This concludes Module 1 in CS 3120
- Midterm 0 covers this module (Feb 3, 20 min.)
- HW 1 will be posted in 24 hours,
  due Jan 30 (Fri) 10pm

- Next: finite automata and regular expressions

Wrap up

Today: Chapter 2.4 in the TCS book

Cardinality of Sets

Countable and Infinite

Power Set

Cantor's Theorem