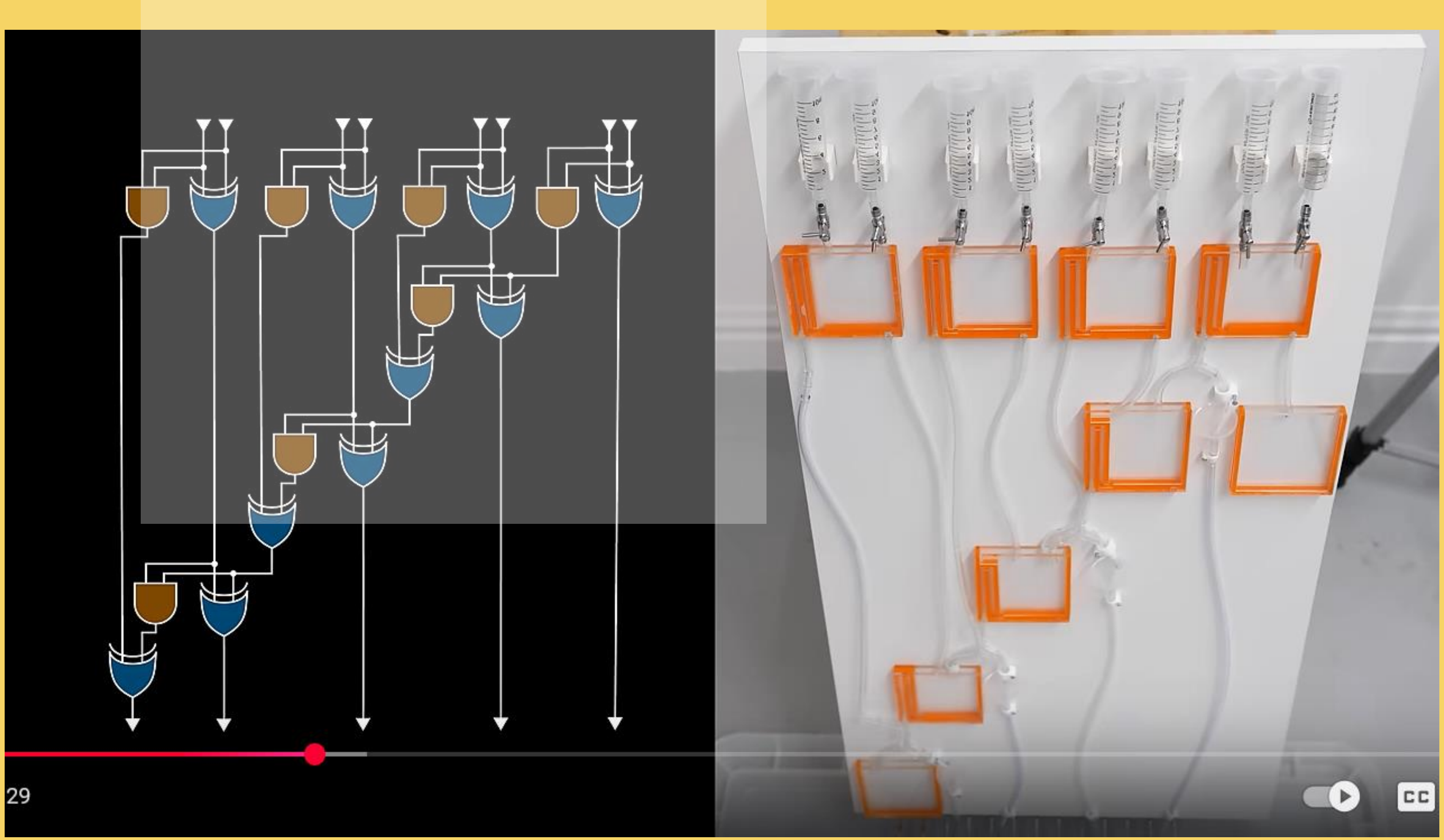
Problem Set 2 is due
This Friday, Jan 31 (10pm)



https://youtu.be/IxXaizglscw?si=iUw9bHqXyl_G5dWt&t=303

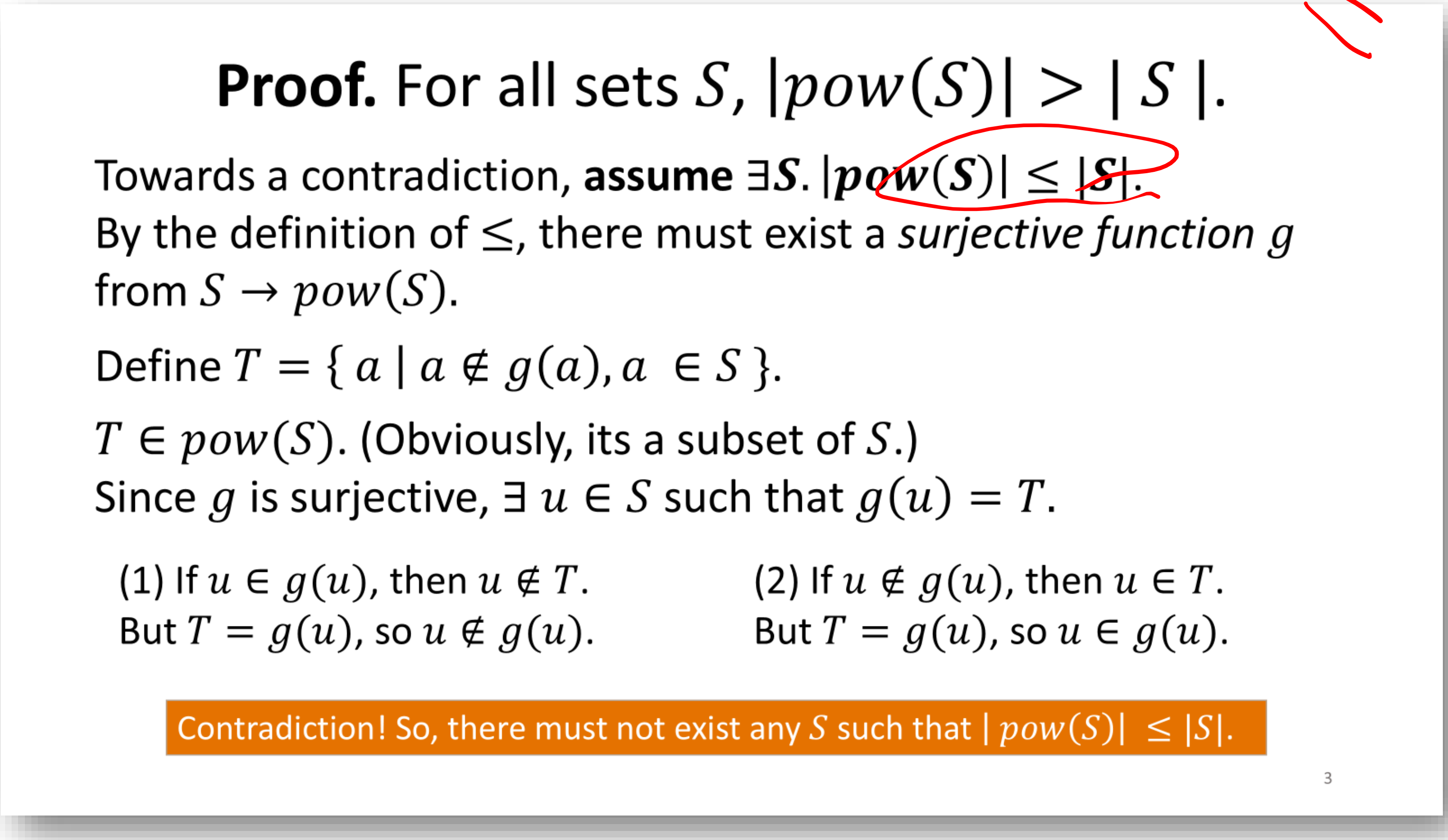
Class 5:
Boolean Gates.

University of Virginia
cs3120: DMT2
Wei-Kai Lin

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

$=$

#



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 $S \rightarrow pow(S)$.

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 $|\ pow(S)| \ \leq |S|$.

3

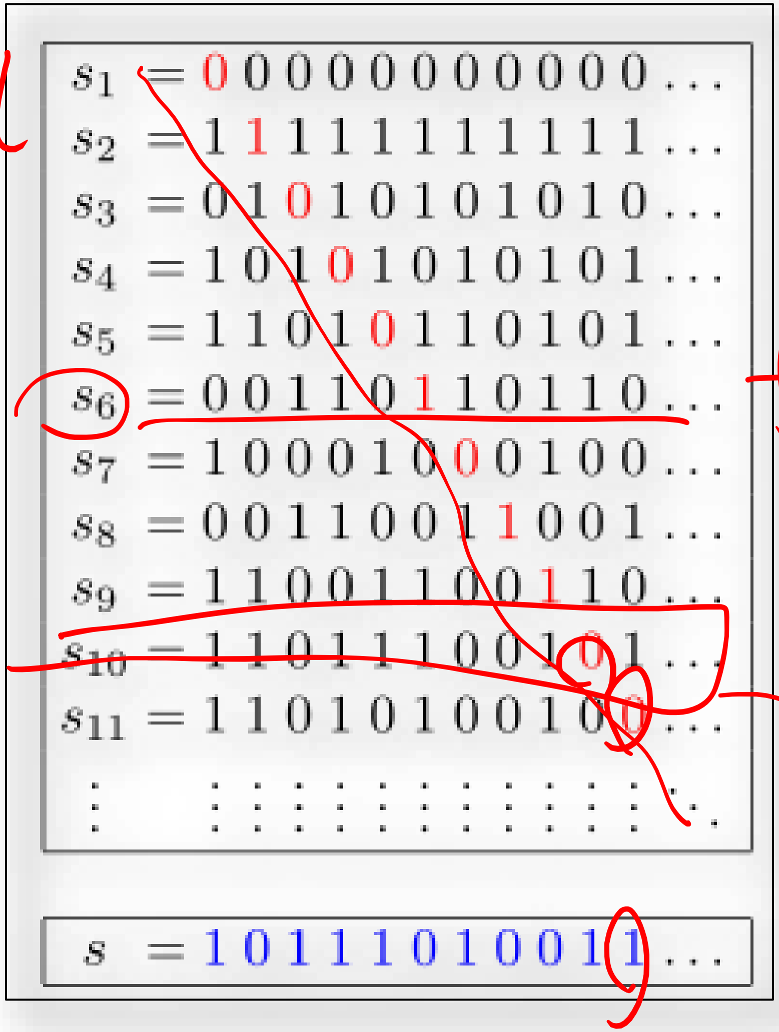
Recall: $\{0,1\}^\infty$ is Uncountable

($|\{0,1\}^\infty| > |\mathbb{N}|$)

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

Assume contra bijec $\{0.1\}^\infty \to \mathbb{N}$

bijec



$s_1 = 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \ldots$

$s_2 = 1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \ldots$

$s_3 = 0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0 \ldots$

$s_4 = 1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1 \ldots$

$s_5 = 1\,1\,0\,1\,0\,1\,1\,0\,1\,0\,1 \ldots$

$s_6 = 0\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0 \ldots$

$s_7 = 1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0 \ldots$

$s_8 = 0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1 \ldots$

$s_9 = 1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0 \ldots$

$s_{10} = 1\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1 \ldots$

$s_{11} = 1\,1\,0\,1\,0\,1\,0\,0\,1\,0\,0 \ldots$

$\vdots \quad \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots \ \ddots$

$s = 1\,0\,1\,1\,1\,0\,1\,0\,0\,1\,1 \ldots$

S_a

$f(a) \in \{0,1\}^\infty \quad \exists\ a \in \mathbb{N}$

$S_a = S \to \leftarrow$

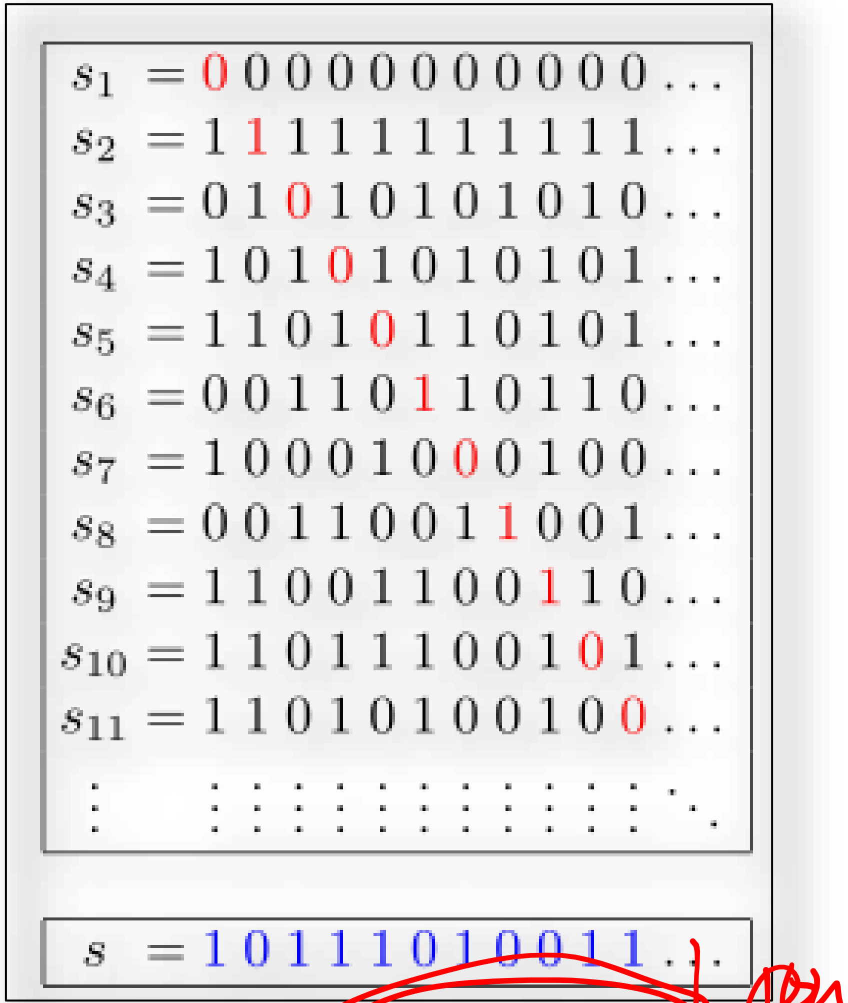
bit wise neg

$\neq$

$S[a] = \text{neg } S_a[a]$

https://en.wikipedia.org/wiki/Cantor%27s_diagonal_argument

Are they the same (or comparable)?



$s_1 = 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ \ldots$

$s_2 = 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ \ldots$

$s_3 = 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ \ldots$

$s_4 = 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ \ldots$

$s_5 = 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ \ldots$

$s_6 = 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ \ldots$

$s_7 = 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ \ldots$

$s_8 = 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ \ldots$

$s_9 = 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ \ldots$

$s_{10} = 1\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ \ldots$

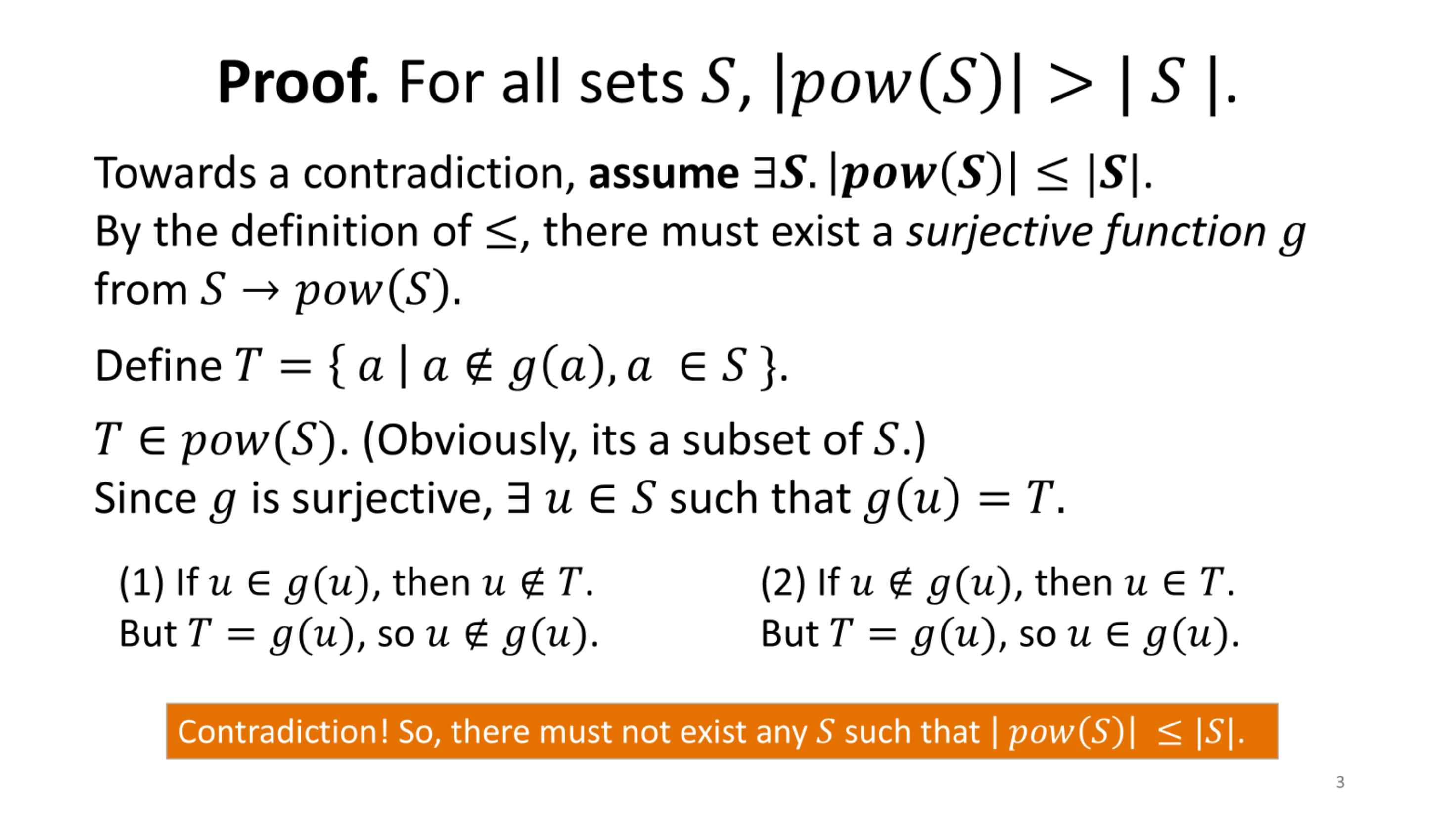
$s_{11} = 1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ \ldots$

$\vdots \quad \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \ddots$

$s = 1\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ \ldots$

$|\{\mathbf{0},\mathbf{1}\}^\infty| > |\mathbb{N}|$

$pow(\mathbb{N})$



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

Towards a contradiction, **assume** $\exists \boldsymbol{S}.\ |\boldsymbol{pow}(\boldsymbol{S})| \le |\boldsymbol{S}|$.
By the definition of $\le$, 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 $|\,pow(S)|\ \le |S|$.

3

$$\underline{|pow(\mathbb{N})| \overset{\text{biject}}{=} |\{0,1\}^{\infty}|} = |\underline{\{f : \mathbb{N} \to \{0,1\}| > \mathbb{N}}$$

$$= \{S \mid \underline{S \subseteq \mathbb{N}}\}$$

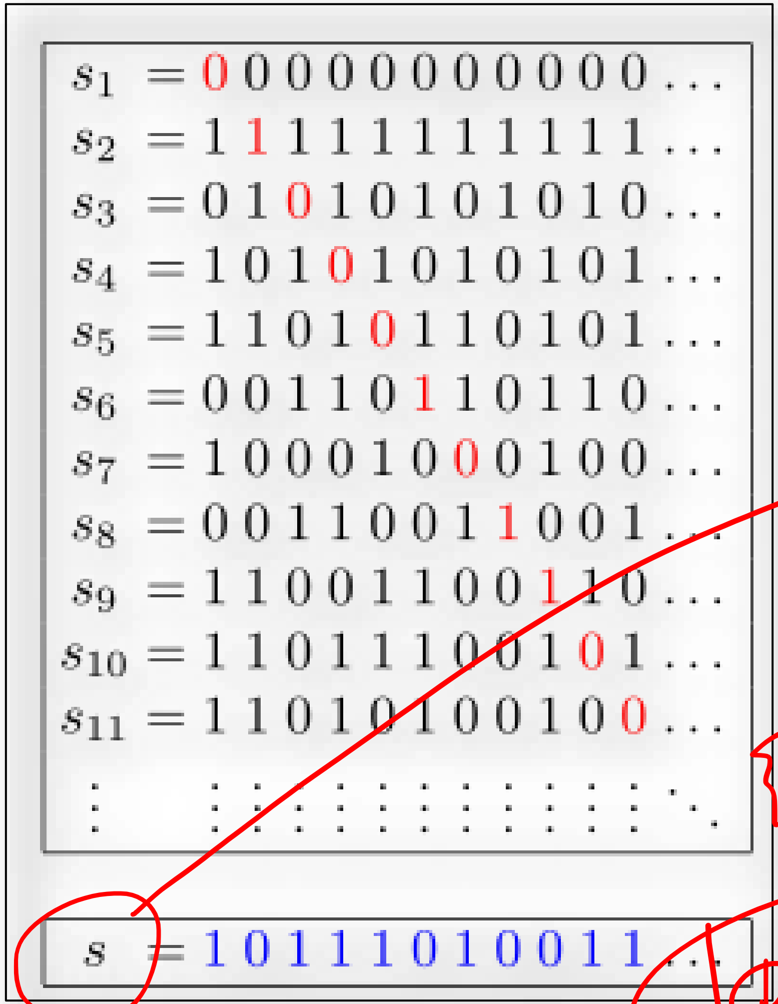
biject $T \in pow(\mathbb{N})$ $\quad T \subseteq \mathbb{N}$

$$f(T) = b_0 b_1 b_2 \cdots \qquad b_i = \begin{cases} 0 & \text{if } i \notin T \\ 1 & \text{o.w.} \end{cases}$$

Ex $T = \{3\}$ $\quad f(T) = 000100\cdots$

$\{3,2,6\}$ $\quad f(T) = 0011001\cdots$

Are they the same (or comparable)?



$s_1 = 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \ldots$

$s_2 = 1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \ldots$

$s_3 = 0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0 \ldots$

$s_4 = 1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1 \ldots$

$s_5 = 1\,1\,0\,1\,0\,1\,1\,0\,1\,0\,1 \ldots$

$s_6 = 0\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0 \ldots$

$s_7 = 1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0 \ldots$

$s_8 = 0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1 \ldots$

$s_9 = 1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0 \ldots$

$s_{10} = 1\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1 \ldots$

$s_{11} = 1\,1\,0\,1\,0\,1\,0\,0\,1\,0\,0 \ldots$

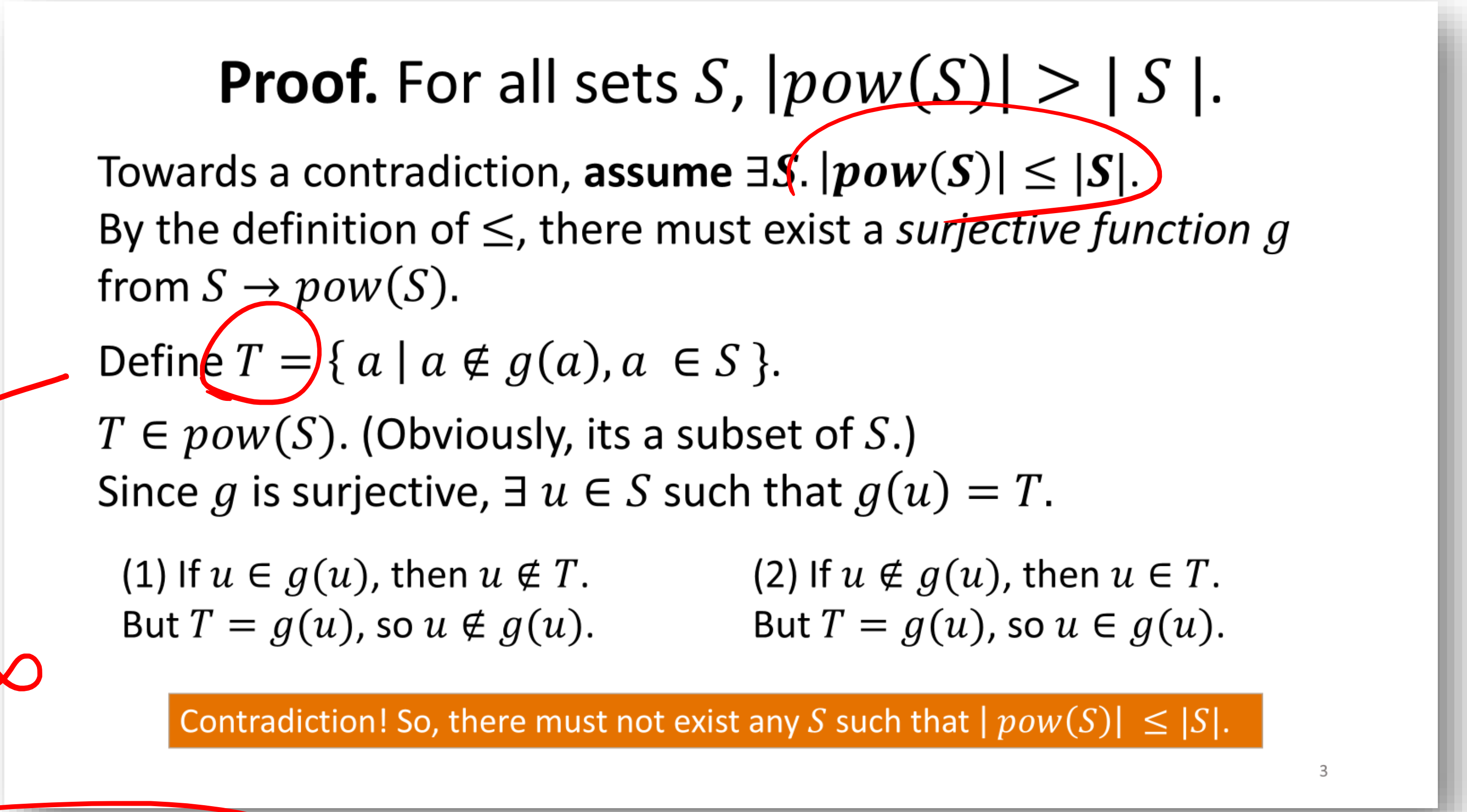
$\vdots \quad \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots \ \ddots$

$s = 1\,0\,1\,1\,1\,0\,1\,0\,0\,1\,1 \ldots$

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

$=$

$|pow(N)| \leq |N|$



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

Towards a contradiction, **assume** $\exists S.\ |\boldsymbol{pow}(\boldsymbol{S})| \leq |\boldsymbol{S}|$.
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 $u \in g(u)$.

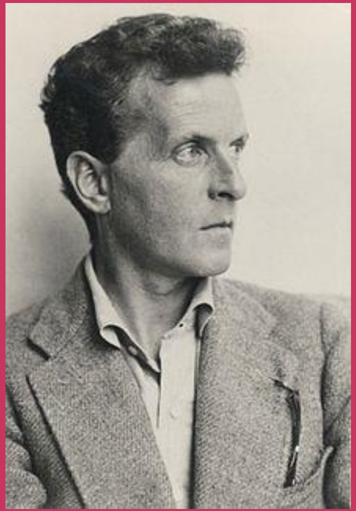
Contradiction! So, there must not exist any S such that $|pow(S)| \leq |S|$.

3

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

Any set bigger than $\mathbb{N}$?

2^{-1} 2^{-2} $\cdots$

$\underline{b_0} b_1 b_2 \cdots$

Yes: $|pow(\mathbb{N})| = |\underline{\{0,1\}}^{\infty}| = |\underline{[0,1]}|$

$\underline{0.d_1 d_2 \cdots}$

Any set bigger than $\mathbb{N}$?

biject

$\mathbb{R} \longrightarrow \{0,1\}^\infty$

total inject

Yes: $|pow(\mathbb{N})| = |\{0,1\}^\infty| = \underline{|[0,1]|}$

$\pm a . r \quad a \in \mathbb{N}$

$r \in [0,1]$

$\downarrow$

inf bin

- $a \in pow(\mathbb{N})$
- $f_a : \mathbb{N} \to \{0,1\}$ such that $f_a(i) = \begin{cases} 0 & if \;\; i \notin a \\ 1 & if \;\; i \in a \end{cases}$
- $(b_0, b_1, b_2, \ldots) \in \{0,1\}^\infty$ such that $b_i = \begin{cases} 0 & if \;\; i \notin a \\ 1 & if \;\; i \in a \end{cases}$
- $0.b_0 b_1 b_2 \ldots \in [0,1]$ in base 2

$(x_1, x_2) \in \mathbb{R}^2$

$x_1 \longmapsto b_0 \, b_1 \, b_2$

$x_2 \longmapsto b_0' \, b_1' \, b_2' \ldots$

$b_0 b_0' b_1 b_1' \ldots$

$e^{i\pi} + 1 = 0$

And also $|pow(\mathbb{N})| = |[0,1]^2| = |\mathbb{R}| = |\underline{\mathbb{R}^2}| = |\mathbb{C}|$

Exercise

$S \times T = \{(a,b) \mid a \in S, b \in T\}$

$S^2 = S \times S$, $S^* = \bigcup_{i=1}^{\infty} S^i$,

$[0,1]$ real $0 \leq r \leq 1$

$\{0,1\}^*$

Any set bigger than $\mathbb{N}$?

Yes:

$$|pow(\mathbb{N})| = |\{0,1\}^{\infty}| = |[0,1]| = |[0,1]^2| = |\mathbb{R}| = |\mathbb{R}^2| = |\mathbb{C}|$$

Any set bigger than [0, 1]?

yes: For **all** sets S, $|pow(S)| > |\ S\ |$

Aleph-Naught

$$\aleph_0 = |\mathbb{N}|$$

"smallest infinite cardinal number"

$$\aleph_1 = ?$$

"*second* smallest infinite cardinal number"

$$\aleph_0 = |\mathbb{N}|$$

“smallest infinite cardinal number”

$$\aleph_1 = ?$$

“*second* sm ite

card er”

Is there any set with card ween $\mathbb{N}$ and $pow(\mathbb{N})$?

It se $pow(\mathbb{N})| = |\mathbb{R}| = \aleph_1$

First of Hilbert's 23 problems presented in 1900

antor’s Continuum Hypothesis

https://en.wikipedia.org/wiki/Continuum_hypothesis
https://en.wikipedia.org/wiki/Aleph_number#Continuum_hypothesis

To conclude…

Infinities are not Intuitive, at least at first

From the paradise, that
Cantor created for us,
no-one can expel us.
David Hilbert

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

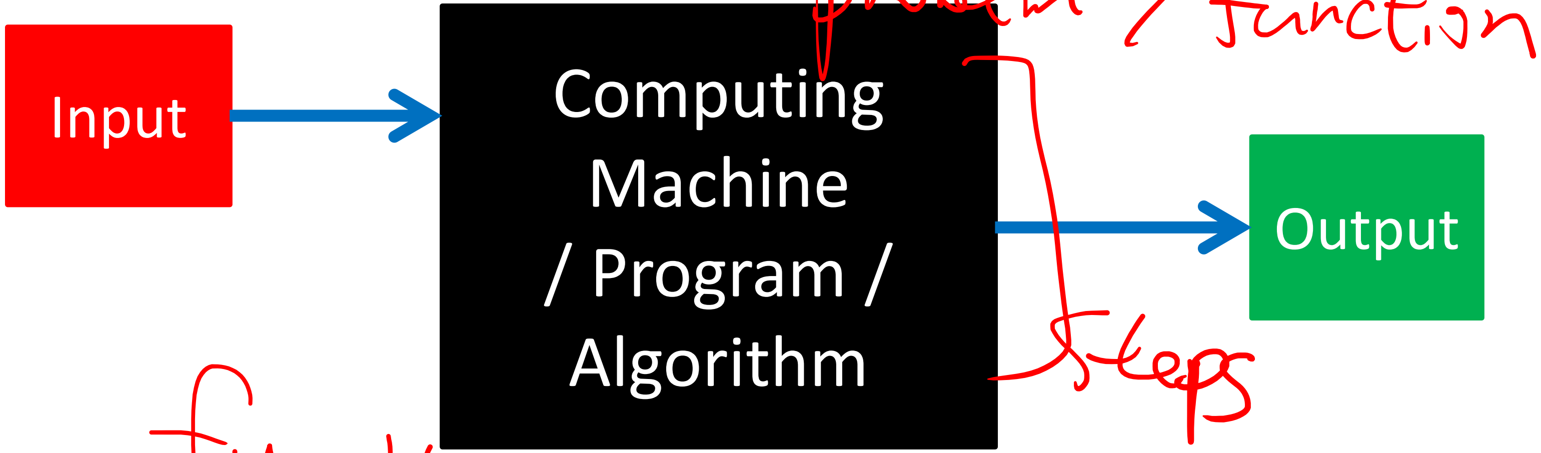
What do computers do?

- Solve problems. → Find proof.
- Precise list of steps, in-&-output
- Stop in some ~~f~~ time.

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.

problem / function.



Input

Computing Machine / Program / Algorithm

Output

Steps

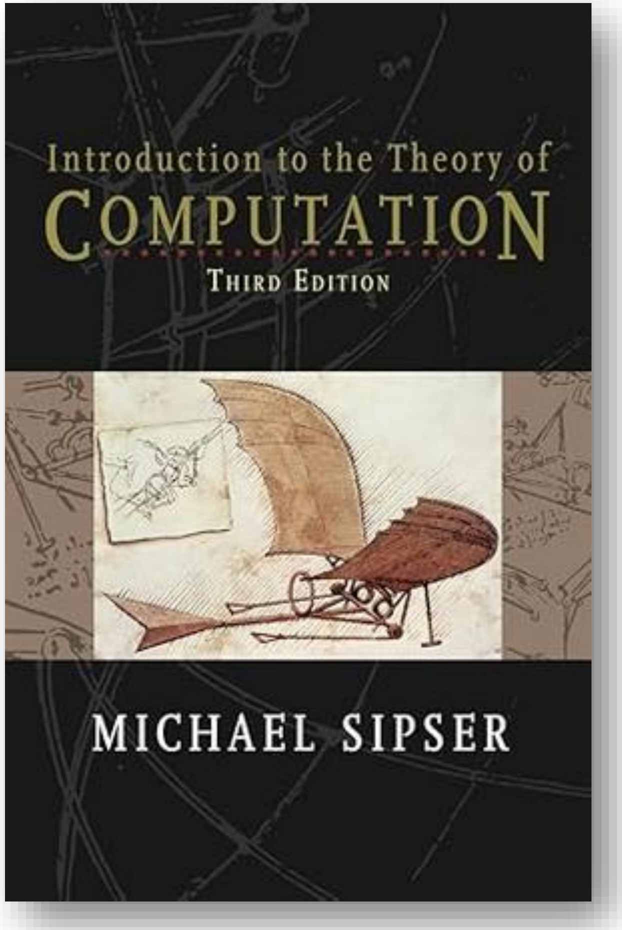
function

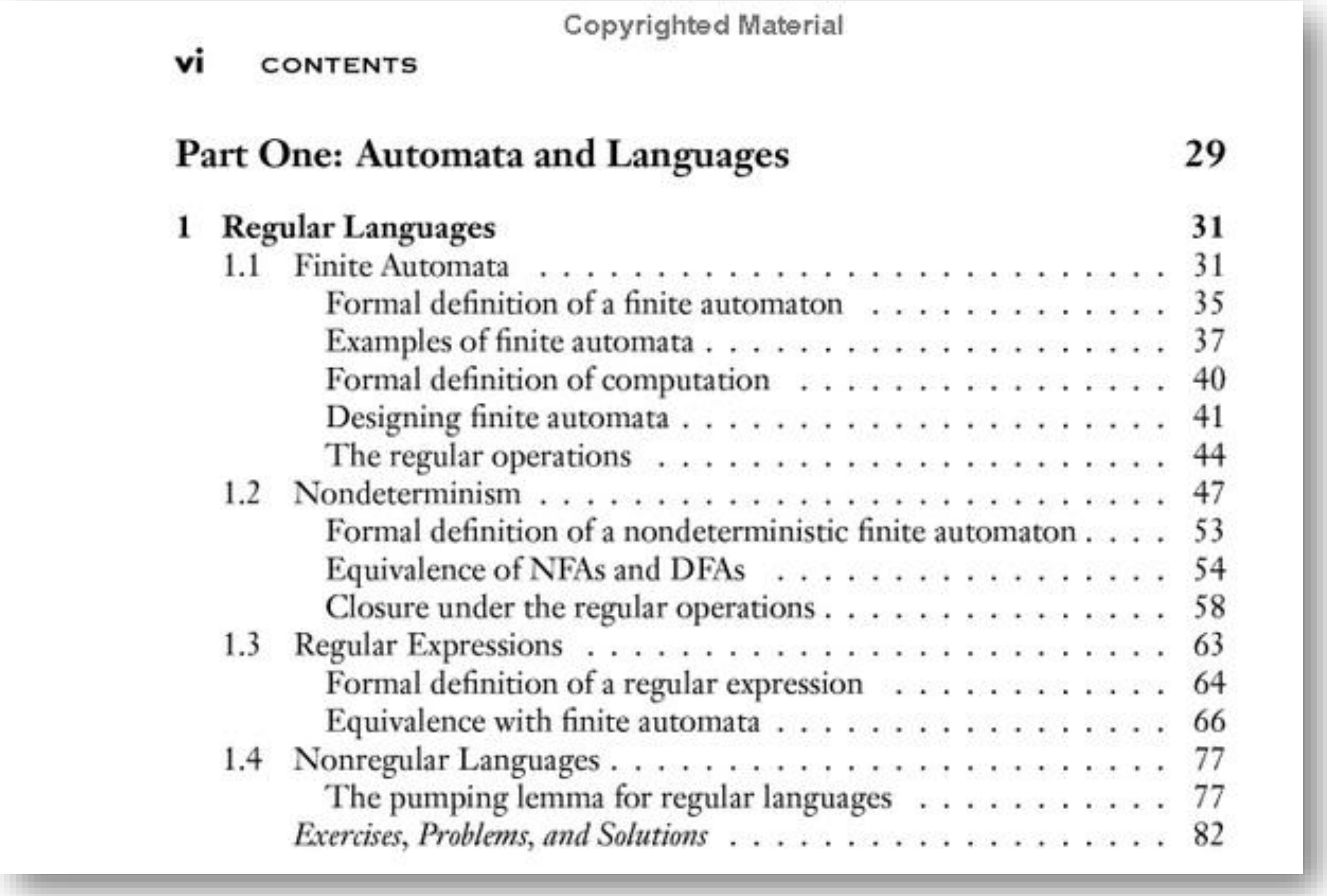
What goes in here?

Computational **Model**

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

python / C++ / Haskel OCamal





Part One: Automata and Languages 29

A simple model of computation

- Based on Boolean logical 'gates':
  - OR$\underbrace{\text{(a, b)}}_{2}$: outputs 1 iff a=1 **or** b=1
  - AND$\underbrace{\text{(a, b)}}_{2}$: outputs 1 iff a=1 **and** b=1
  - NOT$\underbrace{\text{(b)}}_{1}$: outputs 1 iff b=0

Output 0 otherwise

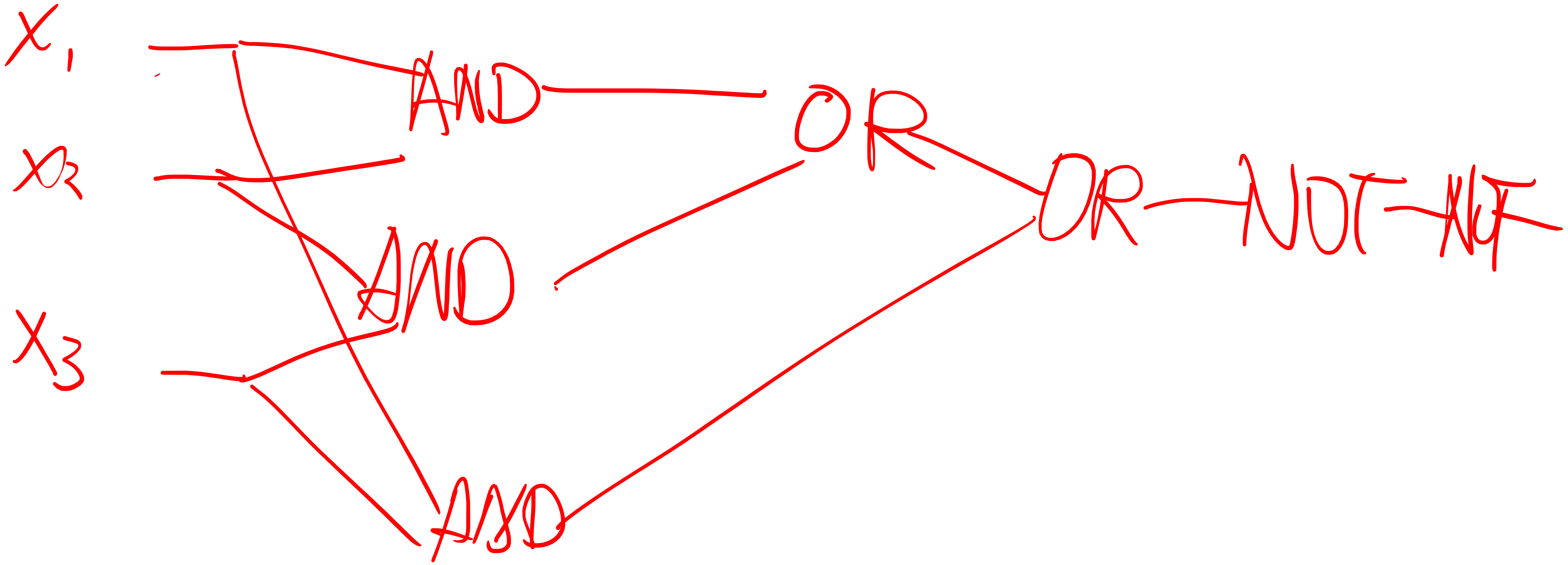
Towards Algorithms

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

x_1	0	0	0	0
x_2	0	0	1	1
x_3	0	1	0	1
MED	0	0	0	1

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

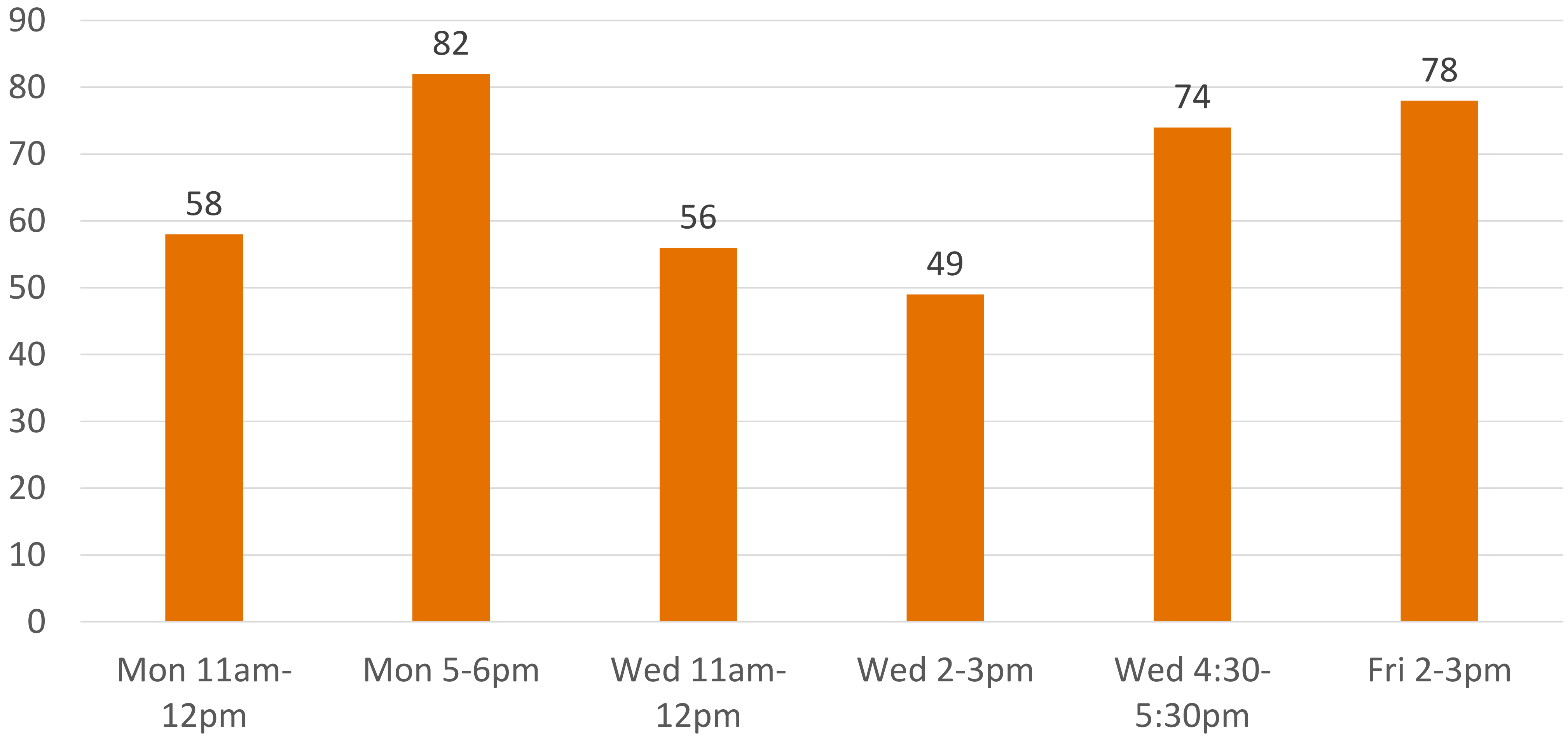
- Still a "math"-ish def/algorithm for MED:



Office Hours

- TA/Office Hours: We do not typically read your solution
  - Time constraint (there can be many students)
  - Independent and critical thinking! (It is easy to believe TA/teacher without thinking)
- Discussion is encouraged. Example:
  - A: “I started with X but then step Y is unclear. Does Y hold in general?”
  - B: “I can prove Y. Problem solved!”

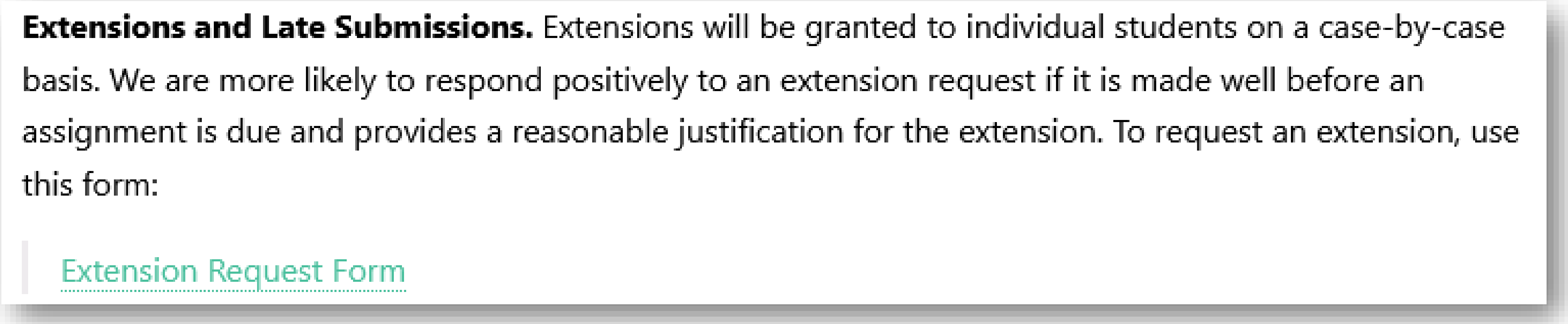
- Subscribe calendar: https://weikailin.github.io/cs3120-toc/calendar/



Popularity of Office Hours

What is the extension policy?

- Syllabus webpage:



Extensions and Late Submissions. Extensions will be granted to individual students on a case-by-case basis. We are more likely to respond positively to an extension request if it is made well before an assignment is due and provides a reasonable justification for the extension. To request an extension, use this form:

> Extension Request Form

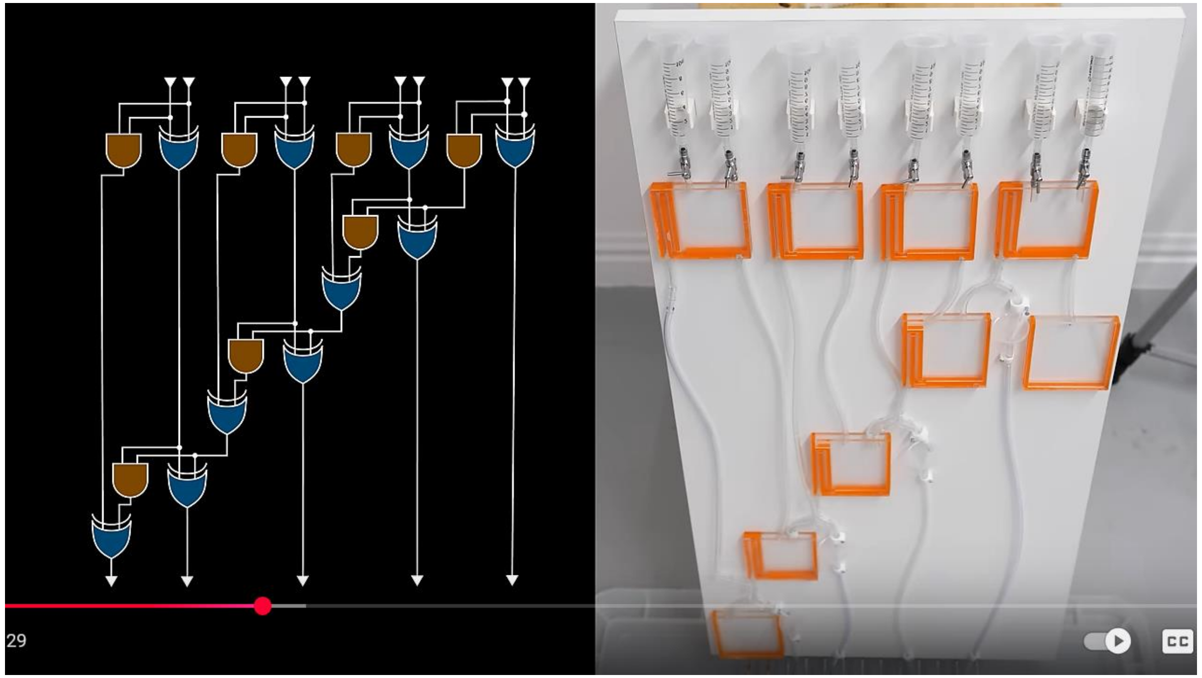
Charge

Set Cardinality

Cantor's Theorem

Computation Model

AND, OR, NOT



PS2: due this Friday 10:00pm