# CS 121: Lecture 14
# Uncomputability

Madhu Sudan

https://madhu.seas.Harvard.edu/courses/Fall2020

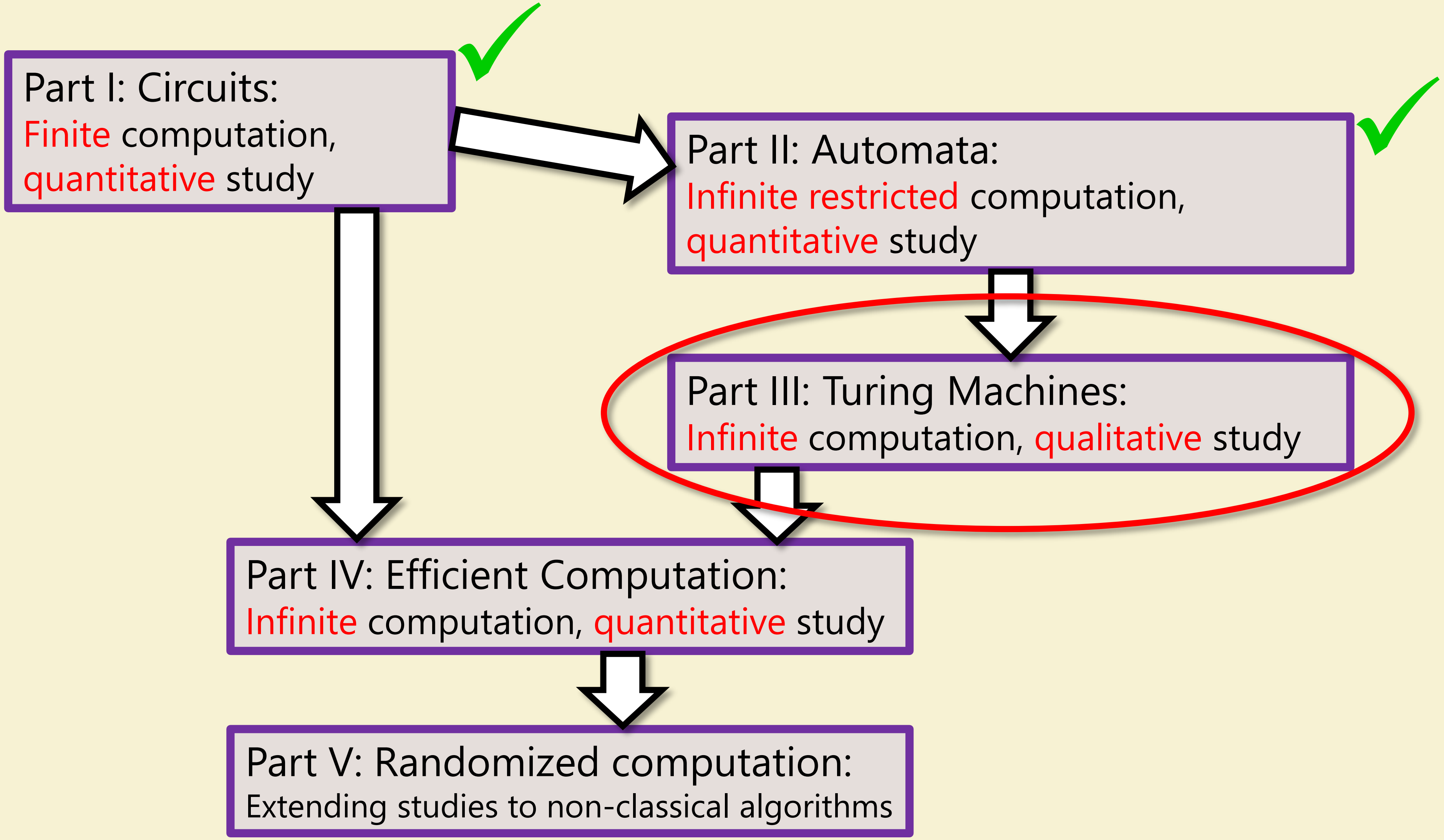
Book: https://introtcs.org

How to contact us
- The whole staff (faster response): [CS 121 Piazza]
- Only the course heads (slower): cs121.fall2020.course.heads@gmail.com

# Announcements:

- Midterm 1 graded. Solutions to be posted today-ish.
- Homework 4 due in 9 days.
- Thanks for participating in Midterm Feedback Survey.

# Where we are:


Part I: Circuits:
Finite computation, quantitative study
Part II: Automata:
Infinite restricted computation, quantitative study
Part III: Turing Machines:
Infinite computation, qualitative study
Part IV: Efficient Computation:
Infinite computation, quantitative study
Part V: Randomized computation:
Extending studies to non-classical algorithms

# Today:

- Finiteness and Infinities
- Cantor: #Reals > #Rationals (Uncountable vs. Countable sets)
- Uncomputable function by counting
- Explicit Uncomputable function: H~~ALT~~ CANTOR

# Background: Finiteness & Infinities

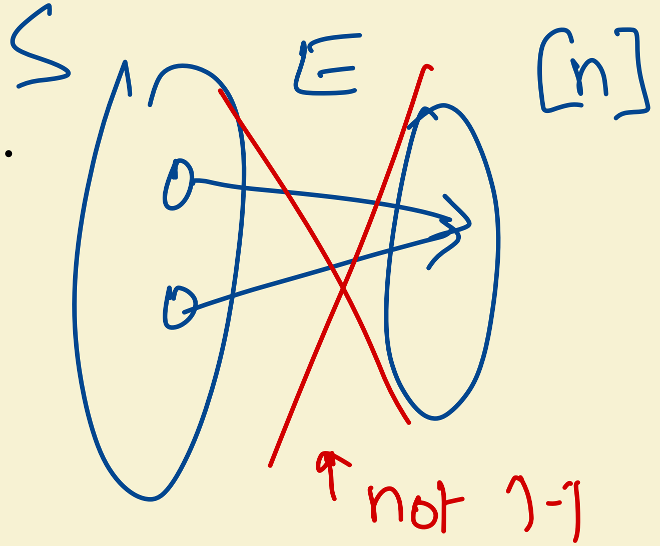
Think: $\rightarrow E: \mathbb{Z}^2 \rightarrow \mathbb{Z}$ ?

$\exists E: \mathbb{Z} \xrightarrow{1-1} \mathbb{Z}^2$ ; Proof: $z \rightarrow (z, 0)$ or $z \rightarrow (z, z)$

Glossary of terms:
- $\mathbb{N}$ = Natural numbers
- $\mathbb{Z}$ = Integers
- $\mathbb{Q}$ = Rationals
- $\mathbb{R}$= Reals
- $[0,1] = \{x \in \mathbb{R} | 0 \leq x \leq 1\}$

- $E: A \rightarrow B$ 1-1 (aka injective): $E(a) = E(a') \Rightarrow a = a'$
- $F: B \rightarrow A$ onto (aka surjective): $\forall a \in A\, \exists b \in B\, s.t.\, F(b) = a$

- Back prior to1800s:
  - Understood finite vs. infinite
    - Set $S$ is finite if $\exists\ n \in \mathbb{N}$ s.t. $\exists$ 1-1 function $E: S \rightarrow [n]$
    - Infinite otherwise.
      - Example infinite sets: $\mathbb{N}, \mathbb{Z}, \mathbb{Z}^2, \mathbb{R}, \mathbb{R}^{10}$ $\quad \{0,1\}^*$
    - Thinking then: All of same size? No point comparing?
- …, Cantor '1800s:
  - $|S| \leq |T| \Leftrightarrow \exists\ 1-1\ E: S \rightarrow T$ : Applies also to infinite sets.
  - Examples: $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = |\mathbb{Z}^2| = |\{0,1\}^*|$
  - Thm: No 1-1 function $E: \mathbb{R} \rightarrow \mathbb{Z}$ exists. ($|\mathbb{Q}| < |\mathbb{R}|$)



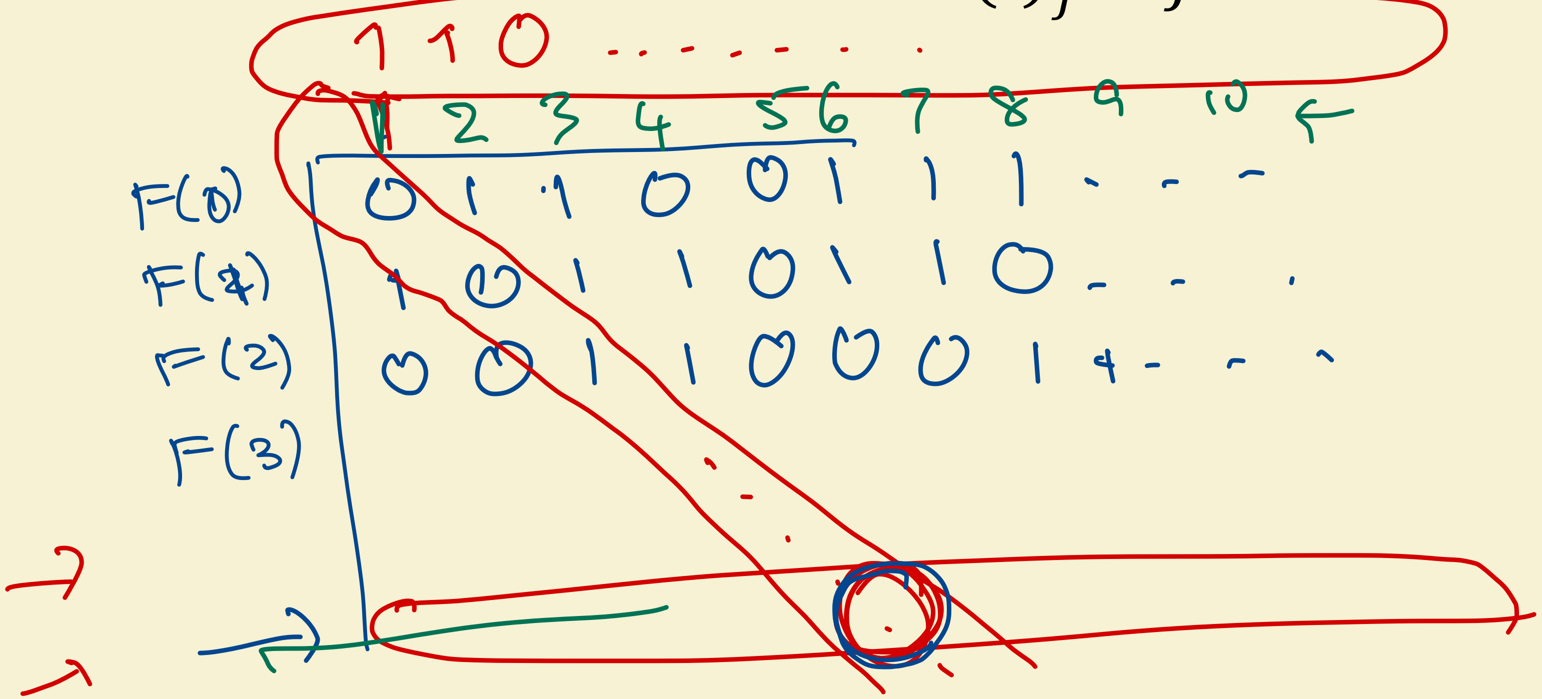
# Cantor's Proof

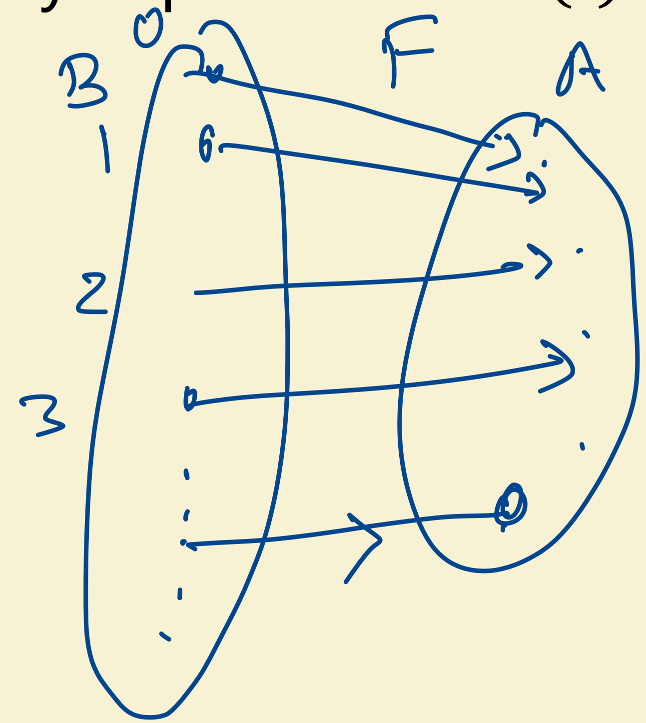
$E: A \to B$ $1-1$ $\iff$ $F: B \to A$ onto

$.101101\ldots$

$.011000011\ldots$

- Suppose $\exists$ $1-1$ $E: [0,1] \to \mathbb{N}$. Then $\exists$ onto $F: \mathbb{N} \to [0,1]$
- Then … can draw matrix with $F(i)_j = j$th bit in binary expansion of $F(i)$.




- Consider $\bar{F} = \overline{F(0)_0}\ \overline{F(1)_1}\ \overline{F(2)_2}\ \overline{F(3)_3} \cdots$ where does it lie? [Can't be $i$th row.]
- Doesn't! Hence $F$ can't exist!

# Uncomputable functions by counting

- Q1: How many computable functions are there?
  - Claim: At most $|\{0,1\}^*|$ ← Since Turing machines can be described with finite # of bits
  - Why?
- Q2: How many functions $f: \{0,1\}^* \to \{0,1\}$
  - Claim: $|[0,1]|$
- Put together: $|R| < |ALL|$, where

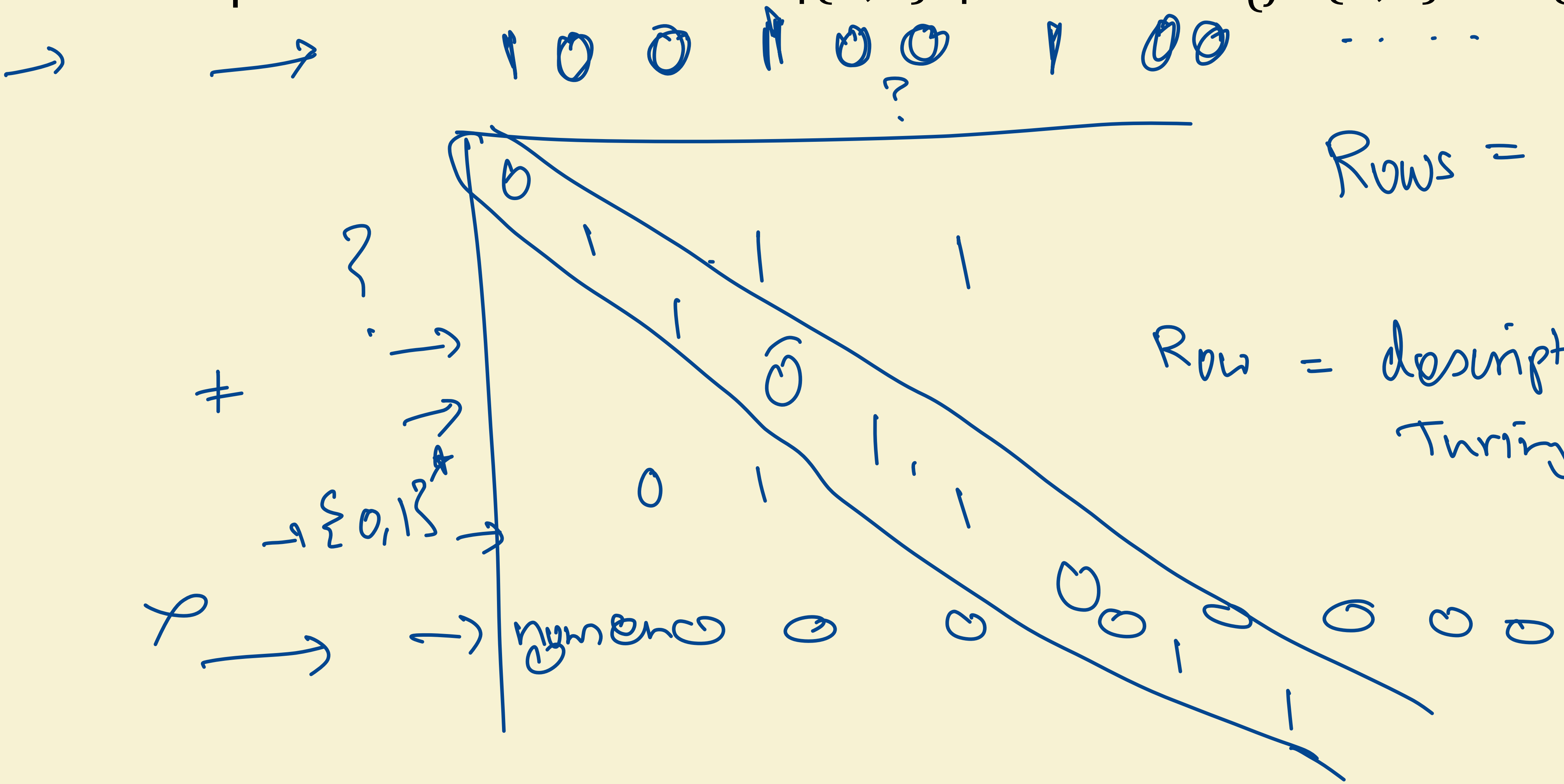
$$R = \{F: \{0,1\}^* \to \{0,1\} | F \text{ is computable}\};$$

$$ALL = \left\{F: \{0,1\}^* \to \{0,1\}\right\}$$

  - $\Rightarrow \exists F \in ALL \setminus R$

# Exercise Break 1

Give direct proof a la Cantor that $|\{0,1\}^*| < \text{ALL} \overset{\text{def}}{=} \{f: \{0,1\}^* \to \{0,1\}\}$




Rows = computable functions

Row = description of Turing machines

| | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | .... |
|---|---|---|---|---|---|---|---|---|---|
| $f \to$ | 0 | 1 | 0 | 1 | ...... | | | | |

→ Rows ≥ All Turing Machines

$$f: \{0,1\}^* \to \{0,1\}$$

$$\Downarrow$$

$$f(\text{""}),\ f(0),\ f(1),\ f(00),\ f(01) \ldots$$

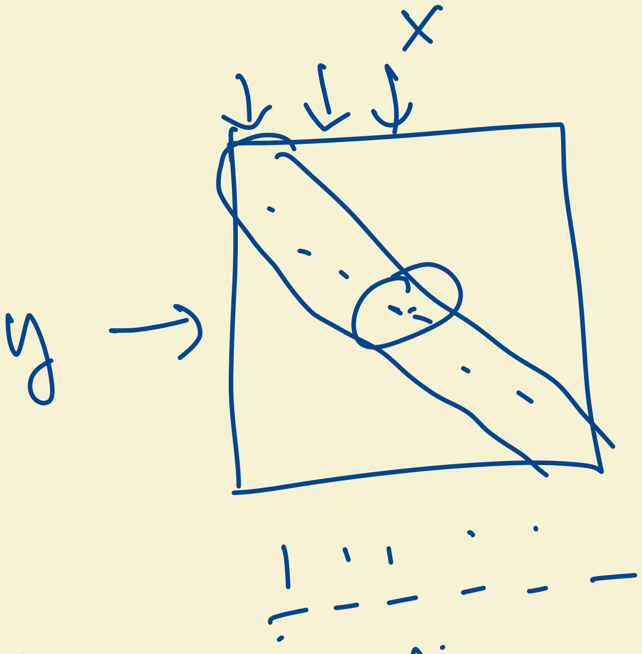
all finite strings enumerated in order of increasing length

→ Columns = enumeration of inputs to function

→ Matrix = evaluation of row on column.

Rows of matrix are $\{0,1\}^*$ ←

Columns of matrix are $\{0,1\}^*$




$\overline{\text{Diag}}: \{0,1\}^* \to \{0,1\}$

Entry of matrix at row y column x

: if y = encoding of Turing Machine M

& then matrix at $(y, x)$ = $M(x)$. [if M halts & outputs a bit]

[in all other cases, write 0]

# Explicit Uncomputable Functions?

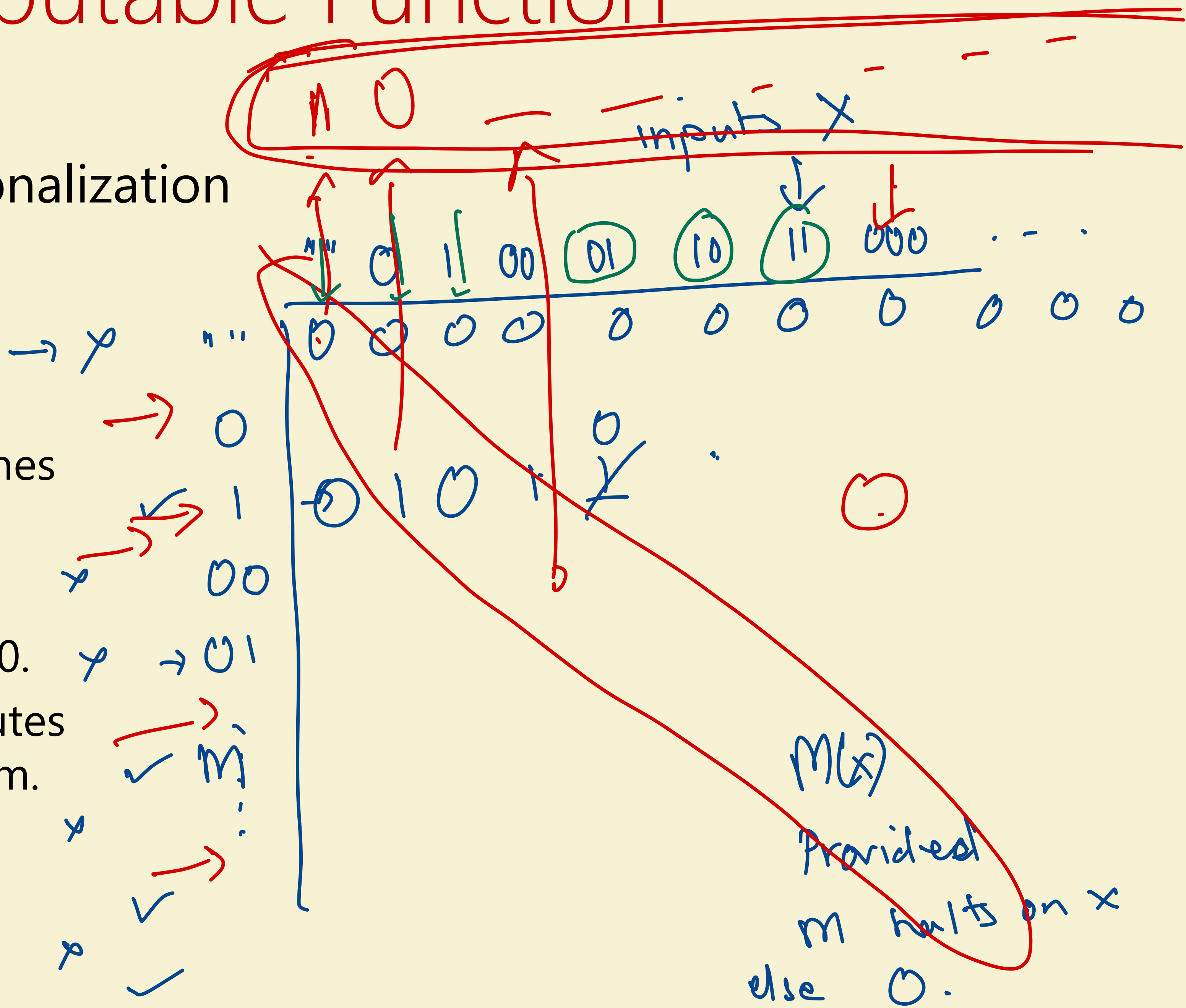
- Motivation: Are "uncomputable" functions of interest to us?
  - Maybe they exist but can't even be described.
    - (#describable functions = countable! By definition!)
  - If they can't be described why would we be interested in computing them?
  - Turns out: Many natural problems uncomputable.
  - As we will see, the following (very describable!) problem is uncomputable.

- $\mathrm{HALT}(M, x) = 1 \text{ if } M \text{ halts on input } x$

  $\qquad\qquad\qquad = 0 \text{ otherwise}$
- Will see in next lecture: $\mathrm{HALT}$ is uncomputable

# An Explicit Uncomputable Function

- Cantor inspired by the diagonalization proof
- Idea:
  - columns = $\{0,1\}^*$ = inputs
  - rows = $\{0,1\}^* \supseteq$ Turing machines
  - $M$th row, $x$th column = $(M, x)$
  - If row not TM – fill with 0s.
  - If $M$ does not halt on $x$ enter 0.
  - Consider function that computes diagonal entries and flips them.




- $\text{Cantor}(M) = \overline{M(M)}$

# Exercise Break 2

- Prove Cantor is uncomputable, where $\text{Cantor}(M) = \overline{M(M)}$

- say $\exists$ turing machine that computes Cantor
- say X is encoding of this Turing Machine

$\forall\, m \qquad X(m) = \text{Cantor}(m)$

What is $X(X)$ ?

$X(X) = \text{Cantor}(X) = \overline{m(m)}\Big|_{m=X} = \overline{X(X)}$

# Proof:

- Assume for contradiction that Turing Machine $A$ computes $\mathrm{Cantor}$
- Then we have $\forall M \quad A(M) = \overline{M(M)}$
- So $A(A) = \overline{M(M)}|_{M=A} = \overline{A(A)}.$ … Contradiction!!

# Next Lecture: More Uncomputability

- Uncomputability of new problems
  - HALT, HALT_ON_ZERO
- Two proof techniques
  - Using presumed (non-existent) Turing Machine
  - REDUCTIONS!!!
    - Using a hard problem to show other problems are also hard.