Intro to Theory of Computation

CS 332

LECTURE 14

Last time

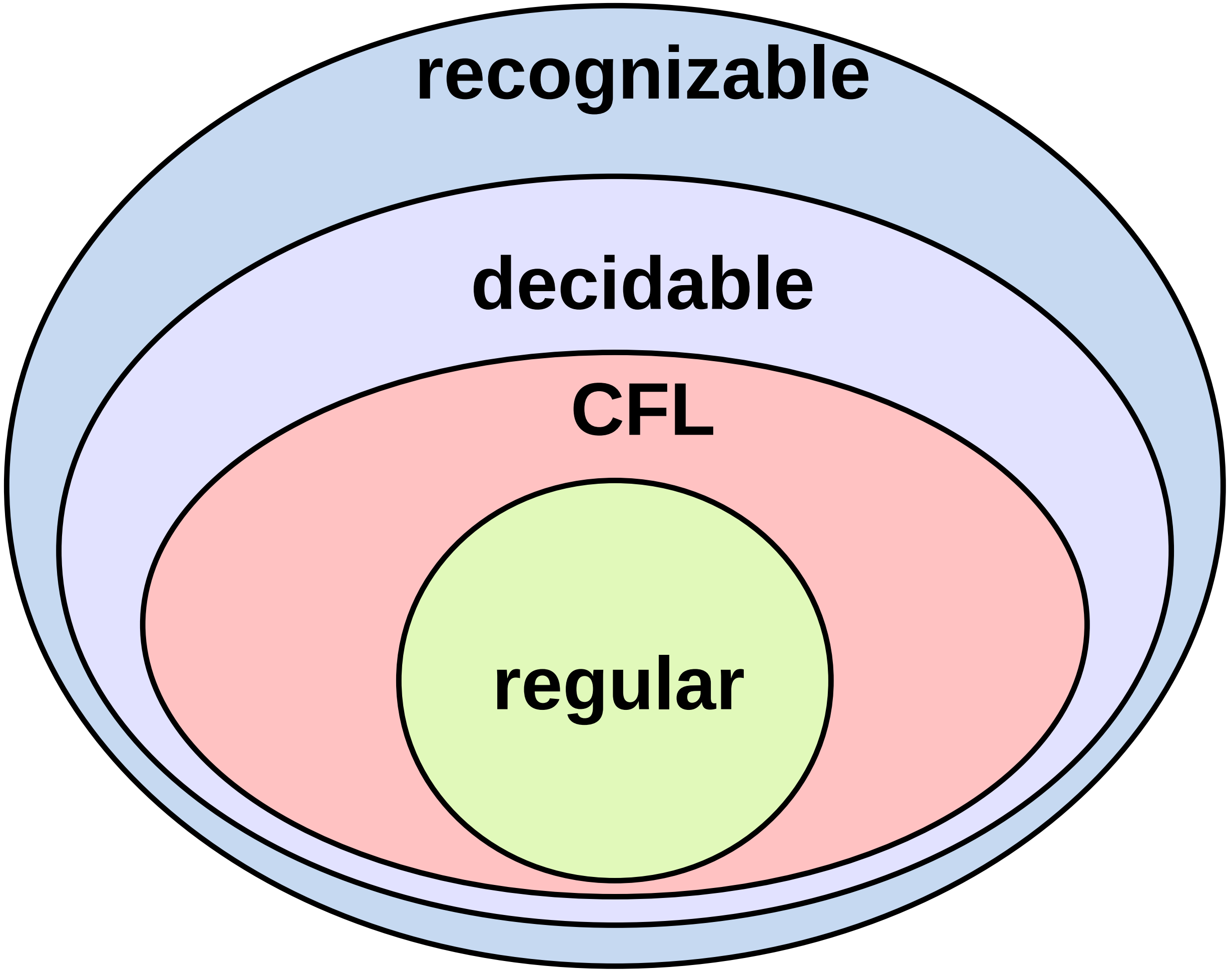
- Decidable languages
- Designing deciders

Today

- Undecidable languages
- Diagonalization

Sofya Raskhodnikova

Classes of languages



CS 332

Problems in language theory

A_{DFA} decidable	A_{CFG} decidable	A_{TM} ?
E_{DFA} decidable	E_{CFG} decidable	E_{TM} ?
EQ_{DFA} decidable	EQ_{CFG} ?	EQ_{TM} ?

Undecidability

We will prove that there are some undecidable languages:

- i.e., problems a computer cannot solve no matter how long it computes

The proof idea is "simple:"

There are more languages than there are Turing Machines.

A language L is undecidable if

there is no TM that decides L.

If L is undecidable, then every TM must either:

1. **Accept (infinitely many) strings s ∉ L.**
2. **Reject (infinitely many) strings s ∈ L.**
3. **Loop forever on (infinitely many) strings.**

POP **QUIZ**

Let $\mathbb{N}$ = {1,2,…} be the natural numbers.

Let E = {2,4,6,…} be the even natural numbers.

Let $\mathbb{Z}$ = {…,-2,-1,0,1,2,…} be the integers.

Which one is largest?

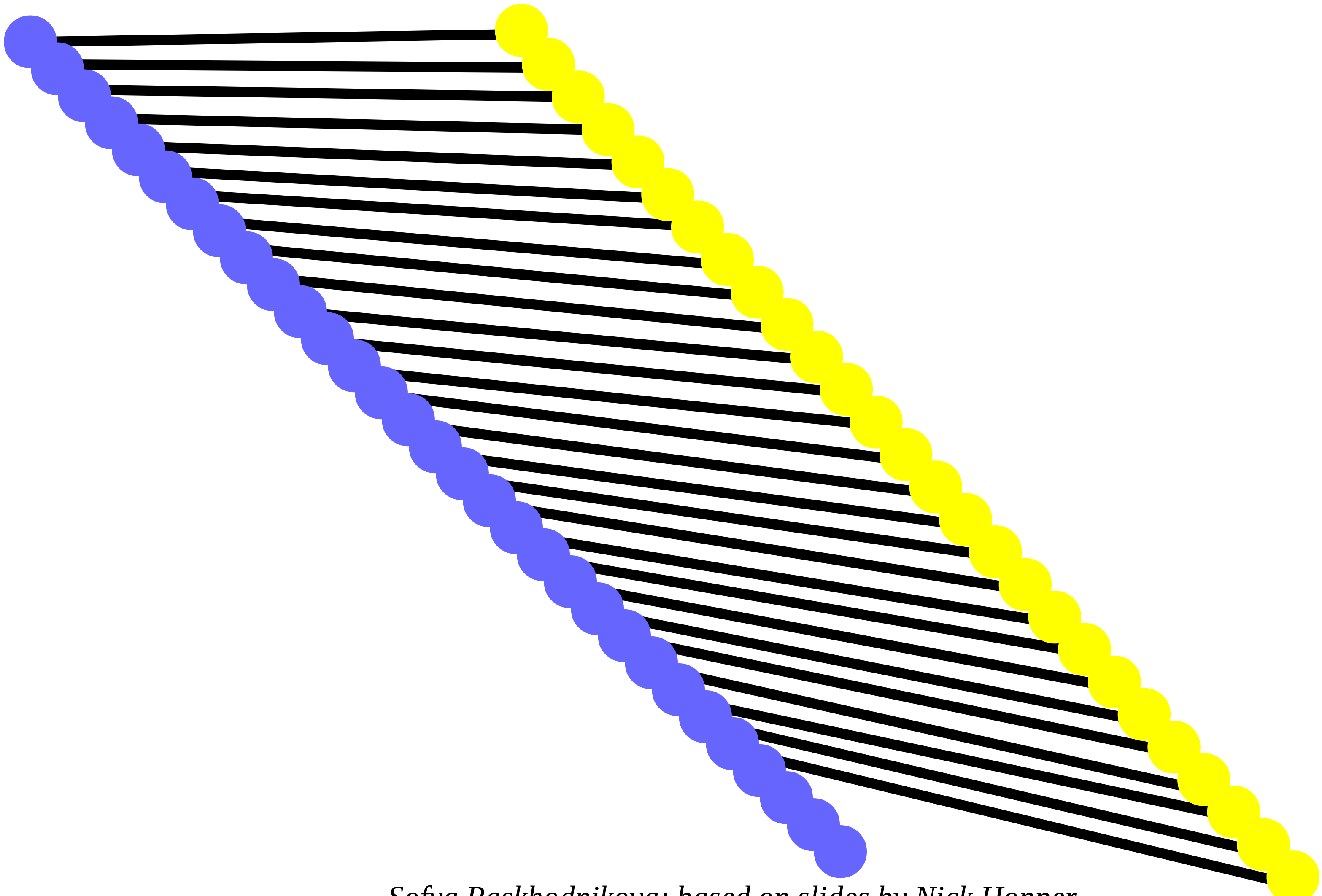
A. $\mathbb{N}$

B. E

C. $\mathbb{Z}$

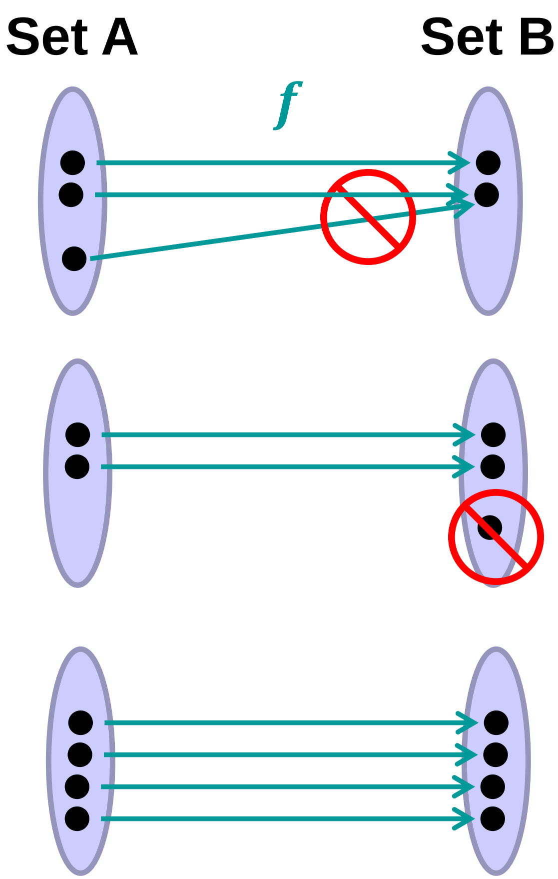
D. the same size.

Are there more blue or yellow dots?



CS 332

Set Theory 101



A function $f: A \to B$ is

- **1-*to*-1** (or ***injective***) if

  $f(a) \neq f(b)$ for $a \neq b$.

- ***onto*** (or ***surjective***) if for all $b \in B$, some $a \in A$ maps to b: $f(a) = b$.

- ***correspondence*** (or ***bijective***) if

  it is 1-to-1 and onto, i.e.,

  each $a \in A$ maps to a unique $b \in B$, and each $b \in B$ has a unique $a \in A$ mapping to it.

How to compare sizes of infinite sets?

- Two sets are **the same size** if there is a bijection between them.
- A set is **countable** if it is
  - finite or
  - it has the same size as ℕ, the set of natural numbers

Examples of countable sets

Ø, {0}, {0,1}, {0,1, …, 255}

E = {2,4,6,…}

O = {1,3,5,7,…}

SQUARES = {1,4,9,16,25…}

POWERS = {1,2,4,8,16,32…}

|POWERS| = |SQUARES| = |E| = |O| = $|\mathbb{N}|$

There is a bijection between $\mathbb{N}$ and $\mathbb{N} \times \mathbb{N}$.

(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	…
(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	…
(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	…
(3,0)	(3,1)	(3,2)	(3,3)	(3,4)	…
(4,0)	(4,1)	(4,2)	(4,3)	(4,4)	…

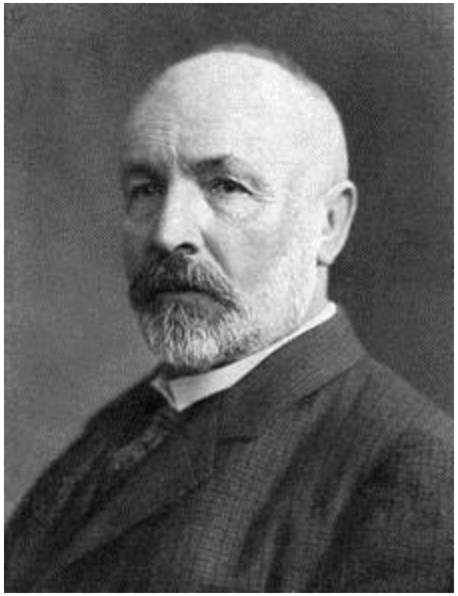
$\{0,1\}^*$ is countable

$\{ \langle M \rangle \mid M \text{ is a TM} \}$ is countable

$Q^+ = \{ p/q \mid p,q \in Z^+ \}$ is countable!

Is any set *uncountable?*

Creator of Set Theory



Georg Cantor
1845--1918

CS 332

Theorem. There is no bijection from the positive integers to the real interval (0,1)

Proof: Suppose f is such a function:

n	f(n)
1	0.**2**8347279…
2	0.8**8**388384…
3	0.77**6**35284…
4	0.111**1**1111…
5	0.1234**5**678…
⋮	⋮

Construct $b \in (0,1)$ that does not appear in the table.

b=0.$d_1 d_2 d_3 \ldots$, where $d_i \neq$ digit i of $f(i)$.

Diagonalization

The process of constructing a counterexample by "contradicting the diagonal" is called DIAGONALIZATION

What if we try this argument on $\mathbb{Q}$ instead of $\mathbb{R}$?

Proof: Suppose f is such a function:

n	f(n)
1	0.28347279…
2	0.88388384…
3	0.77635284…
4	0.11111111…
5	0.12345678…
:	:

Construct $b \in (0,1)$ that does not appear in the table.

b=0.$d_1 d_2 d_3 \ldots$, where $d_i \neq$ digit i of $f(i)$.

Exercise

What if we try Cantor's diagonalization argument on $\mathbb{Q}$ instead of $\mathbb{R}$?

A. It works.

B. It fails because there are some rational numbers that cannot be represented in decimal point notation.

C. It fails because the i-th number might have no digit in the i-th position after the decimal point.

D. It fails because the constructed number is not rational.

E. None of the above.

Let L be any set and P(L) be the power set of L

Theorem: There is no bijection from L to P(L)

Proof: **Assume, for a contradiction, that there is bijection $f : L \rightarrow P(L)$**

We construct a set S that cannot be the output, f(y), for any $y \in L$.

Use diagonalization

x	$y_1 \in f(x)$?	$y_2 \in f(x)$?	$y_3 \in f(x)$?	$y_4 \in f(x)$?	…
y_1	Y	N	Y	Y	
y_2	N	Y	N	Y	
y_3	N	N	N	N	
y_4	Y	N	N	Y	
⋮					⋱

Define set S by flipping the diagonal:

$(y_i \in S)$ = Y iff $(y_i \in f(y_i))$ = N

CS 332

EXAMPLE

Let L = {0,1,2}. Then P(L) =
{Ø, {0}, {1}, {2}, {0,1}, {0,2}, {1,2}, {0,1,2}}

Let f(0) = {1}, f(1) = Ø, f(2) = {0,2}. Then:

x	0 ∈ f(x)?	1 ∈ f(x)?	2 ∈ f(x)?
0	N	Y	N
1	N	N	N
2	Y	N	Y

S = {0,1}

Let L be any set and P(L) be the power set of L

Theorem: There is no bijection from L to P(L)

Proof: Assume, for a contradiction, that there is bijection $f : L \rightarrow P(L)$

We construct a set S that cannot be the output, $f(y)$, for any $y \in L$.

$$\text{Let } S = \{ x \in L \mid x \notin f(x) \}$$

If $S = f(y)$ then $y \in S$ if and only if $y \notin S$

For all sets L,
P(L) has more elements than L

Not all languages over {0,1} are decidable

TM Deciders

Strings of 0s and 1s

L

Languages over {0,1}

Sets of strings of 0s and 1s

P(L)

Not all languages over {0,1} are recognizable

Turing Machines	Languages over {0,1}
Strings of 0s and 1s	Sets of strings of 0s and 1s
L	**P(L)**

A specific undecidable language

A_{TM} = $\{\langle M, w\rangle$ | M is a TM, w is a string, and M accepts w $\}$

Theorem. A_{TM} is undecidable.

Proof: For contradiction, suppose a TM H decides A_{TM}.

$$H(\langle M, w\rangle) = \begin{cases} \text{accept} & \text{if } M \text{ accepts } w \\ \text{reject} & \text{if } M \text{ doesn't accept } w \end{cases}$$

Idea: Use H to check what TM M does on its own description (and do the opposite).

TM D = `` On input $\langle M\rangle$, where M is a TM:

1. **Run H on input <M, $\langle M\rangle$>.**
2. **Accept if it rejects. O.w. reject.”**

D is a decider. What does it do on $\langle D\rangle$?

CS 332

Is it diagonalization again? Does M accept $\langle M \rangle$?

TMs	$\langle M_1 \rangle$	$\langle M_2 \rangle$	$\langle M_3 \rangle$	$\langle M_4 \rangle$	…
M_1	Y	N	Y	Y	
M_2	N	Y	N	Y	
M_3	N	N	N	N	
M_4	Y	N	N	Y	
$\vdots$					$\ddots$

D accepts $\langle M_i \rangle$ iff entry (i, i) is N .

CS 332 Is it diagonalization again? Does M accept $\langle M \rangle$?

TMs	$\langle M_1 \rangle$	$\langle M_2 \rangle$	$\langle M_3 \rangle$	$\langle M_4 \rangle$	…	$\langle D \rangle$	…
M_1	Y	N	Y	Y			
M_2	N	Y	N	Y			
M_3	N	N	N	N			
M_4	Y	N	N	Y			
⋮					⋱		
D						?	
⋮							⋱

CS 332

A movie about undecidability of the Halting Problem

https://www.youtube.com/watch?v=92WHN-pAFCs