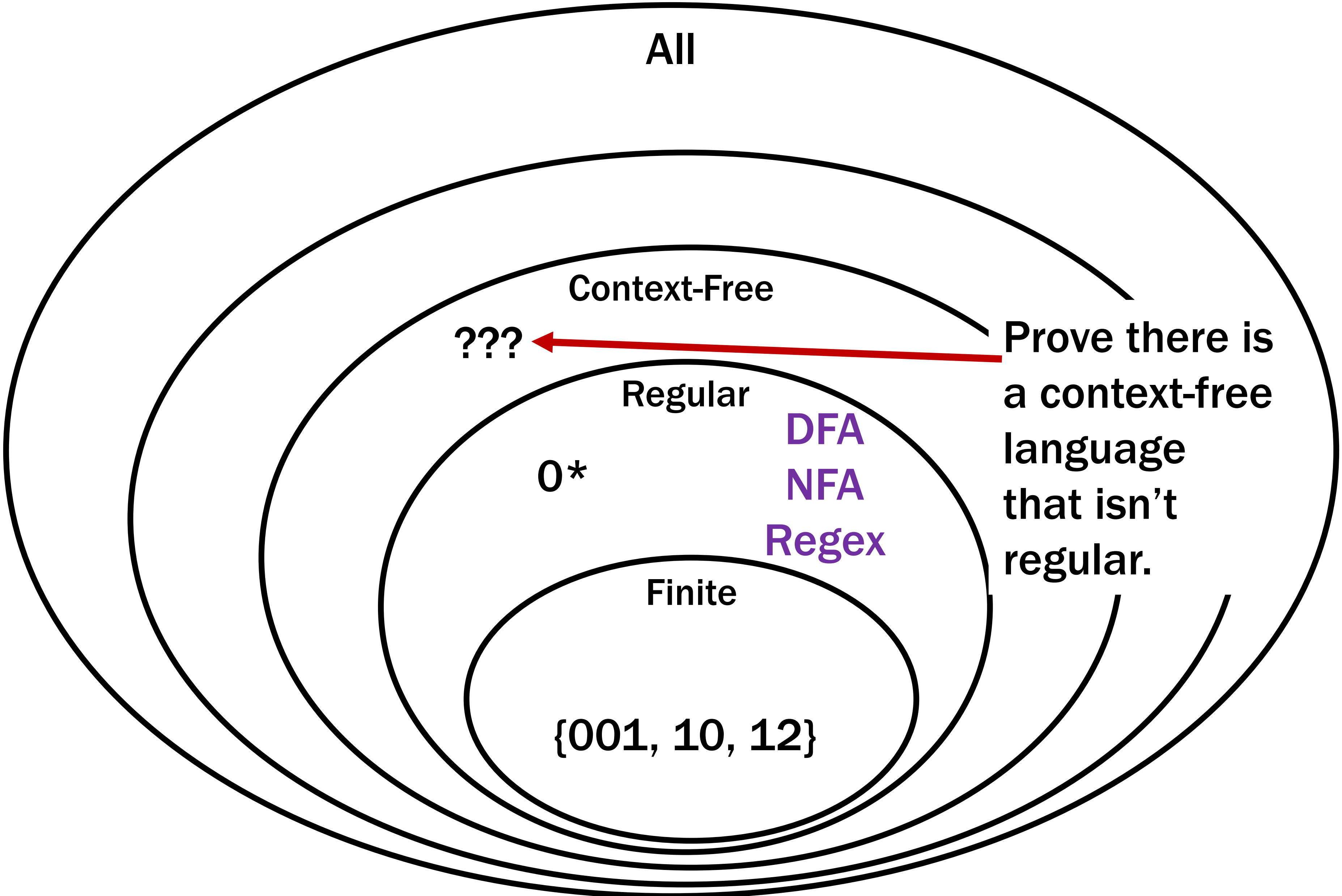
CSE 311: Foundations of Computing

Lecture 26: More on Limits of FSMs, Cardinality

Last time: Languages and Representations



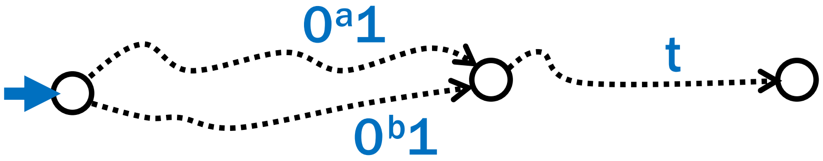
Prove there is a context-free language that isn't regular.

B = {binary palindromes} can't be recognized by any DFA

The general proof strategy is:

- Assume (for contradiction) that some DFA (call it M) exists that recognizes B
- We want to show: M accepts or rejects a string it shouldn't.

Key Idea 1: If two strings "collide", a DFA cannot distinguish between their common extension!



Key Idea 2: Our machine M has a finite number of states which means if we have infinitely many strings, two of them must collide!

B = {binary palindromes} can't be recognized by any DFA

The general proof strategy is:

- Assume (for contradiction) that some DFA (call it M) exists that recognizes B
- We want to show: M accepts or rejects a string it shouldn't.

We choose an **INFINITE** set S of "half strings" (which we intend to complete later). It is imperative that for ***every pair*** of strings in our set there is an "accept" completion that the two strings DO NOT SHARE.

1______
01______
001______
0001______
00001______
....

B = {binary palindromes} can't be recognized by any DFA

Suppose for contradiction that some DFA, M, recognizes B.

We show that M accepts or rejects a string it shouldn't.

Consider S={1, 01, 001, 0001, 00001, ...} = $\{0^n1 : n \geq 0\}$.

Since there are finitely many states in M and infinitely many strings in S, ***there exist strings*** $0^a1 \in S$ ***and*** $0^b1 \in S$ ***with*** $a \neq b$ ***that end in the same state of M.***

SUPER IMPORTANT POINT: You do not get to choose what a and b are. Remember, we've proven they exist…we have to take the ones we're given!

B = {binary palindromes} can't be recognized by any DFA

Suppose for contradiction that some DFA, M, recognizes B.

We show that M accepts or rejects a string it shouldn't.

Consider $S = \{0^n1 : n \geq 0\}$.

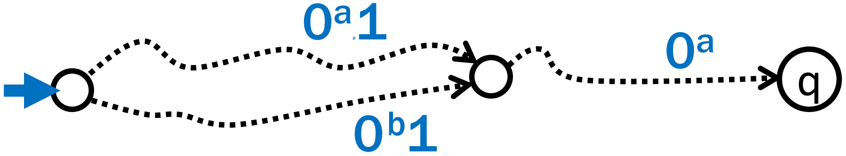
Since there are finitely many states in M and infinitely many strings in S**, there exist strings** $0^a1 \in S$ **and** $0^b1 \in S$ **with** $a \neq b$ **that end in the same state of M.**

Now, consider appending 0^a **to both strings.**

$0^a 1 0^a \in B$

$0^b 1 0^a \notin B$

$0^a 1 0^b \notin B$, $0^b 1 0^b \in B$



Then, since 0^a1 ***and*** 0^b1 ***end in the same state,*** 0^a10^a ***and*** 0^b10^a ***also end in the same state, call it*** q***. But then M must make a mistake:*** q ***needs to be an accept state since*** $0^a10^a \in$ ***B, but then M would accept*** $0^b10^a \notin$ ***B which is an error.***

B = {binary palindromes} can't be recognized by any DFA

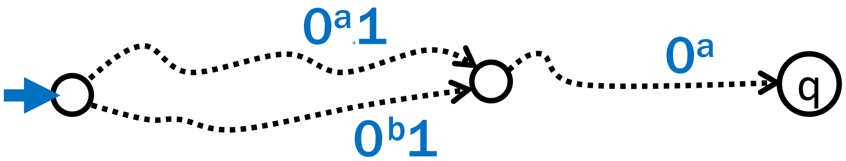
Suppose for contradiction that some DFA, M, recognizes B.

We show that M accepts or rejects a string it shouldn't.

Consider $S = \{0^n1 : n \geq 0\}$.

Since there are finitely many states in M and infinitely many strings in S, there exist strings $0^a1 \in S$ and $0^b1 \in S$ with $a \neq b$ that end in the same state of M.

Now, consider appending 0^a to both strings.



Then, since 0^a1 and 0^b1 end in the same state, 0^a10^a and 0^b10^a also end in the same state, call it q. But then M must make a mistake: q needs to be an accept state since $0^a10^a \in B$, but then M would accept $0^b10^a \notin B$ which is an error.

This is a contradiction, since we assumed that M recognizes B. Since M was arbitrary, ***there is no DFA that** recognizes **B.***

Showing that a Language L is not regular

1. "Suppose for contradiction that some DFA M recognizes L."
2. Consider an **INFINITE** set S of "half strings" (which we intend to complete later). It is imperative that for ***every pair*** of strings in our set there is an "accept" completion that the two strings DO NOT SHARE.
3. "Since **S** is infinite and **M** has finitely many states, there must be two strings $\mathbf{s_a}$ and $\mathbf{s_b}$ in **S** for some $\mathbf{s_a \neq s_b}$ that end up at the same state of **M**."
4. Consider appending the completion **t** that the two strings don't share (say $\mathbf{s_a t} \in \mathbf{L}$ and $\mathbf{s_b t} \notin \mathbf{L}$).
5. "Since $\mathbf{s_a}$ and $\mathbf{s_b}$ end up at the same state of **M**, and we appended the same string **t**, both $\mathbf{s_a t}$ and $\mathbf{s_b t}$ end up at the same state **q** of **M.** Since $\mathbf{s_a t} \in \mathbf{L}$, **q** is an accept state but then **M** also accepts $\mathbf{s_b t} \notin \mathbf{L}$**.** So, **M** does not recognize **L**."
6. "Since **M** was arbitrary, no DFA recognizes **L**."

Prove A = $\{0^n1^n : n \geq 0\}$ is not regular

Suppose for contradiction that some DFA, M, accepts A.

Let S =

Prove A = $\{0^n 1^n : n \geq 0\}$ is not regular

Suppose for contradiction that some DFA, M, recognizes A.

Let S = $\{0^n : n \geq 0\}$**. Since S is infinite and M has finitely many states, there must be two strings,** 0^a **and** 0^b **for some** $a \neq b$ **that end in the same state in M.**

Prove A = $\{0^n 1^n : n \geq 0\}$ is not regular

Suppose for contradiction that some DFA, M, recognizes A.

Let S = $\{0^n : n \geq 0\}$. Since S is infinite and M has finitely many states, there must be two strings, 0^a and 0^b for some $a \neq b$ that end in the same state in M.

Consider appending 1^a to both strings.

Prove A = $\{0^n1^n : n \geq 0\}$ is not regular

Suppose for contradiction that some DFA, M, recognizes A.

Let S = $\{0^n : n \geq 0\}$. Since S is infinite and M has finitely many states, there must be two strings, 0^a and 0^b for some $a \neq b$ that end in the same state in M.

Consider appending 1^a to both strings.

Note that $0^a1^a \in$ A, **but** $0^b1^a \notin$ A since $a \neq b$. But they both end up in the same state of M, call it **q**. Since $0^a1^a \in$ A, state **q** must be an accept state but then M would incorrectly accept $0^b1^a \notin$ A so M does not recognize A.

Since M was arbitrary, no DFA recognizes A.

Prove P = {balanced parentheses} **is not regular**

( )

Suppose for contradiction that some DFA, M, accepts P.

Let S = ~~{ (, ()(, ()()(, ()()()(, ... }~~

t =)(

Prove P = {balanced parentheses} is not regular

Suppose for contradiction that some DFA, M, recognizes P.

Let S = $\{ (^n : n \geq 0\}$. Since S is infinite and M has finitely many states, there must be two strings, $(^a$ and $(^b$ for some $a \neq b$ that end in the same state in M.

Consider appending $)^a$ to both strings.

Prove P = {balanced parentheses} **is not regular**

Suppose for contradiction that some DFA, M, recognizes P.

Let S = $\{ (^n : n \geq 0\}$**. Since S is infinite and M has finitely many states, there must be two strings,** $(^a$ **and** $(^b$ **for some** $a \neq b$ **that end in the same state in M.**

Consider appending $)^a$ **to both strings.**

Note that $(^a)^a \in$ **P, but** $(^b)^a \notin$ **P since** $a \neq b$**. But they both end up in the same state of M, call it q. Since** $(^a)^a \in$ **P, state q must be an accept state but then M would incorrectly accept** $(^b)^a \notin$ **P so M does not recognize P.**

Since M was arbitrary, no DFA recognizes P.

General Computation

Computers from Thought

Computers as we know them grew out of a desire to avoid bugs in mathematical reasoning.

Hilbert in a famous speech at the International Congress of Mathematicians in 1900 set out the goal to mechanize all of mathematics.

In the 1930s, work of Gödel and Turing showed that Hilbert's program is impossible.

Gödel's incompleteness theorem
Undecidability of the Halting Problem

Both of these employ an idea we will see called diagonalization.

The ideas are simple but so revolutionary that their inventor Georg Cantor was shunned by the mathematical leaders of the time:

Poincaré referred to them as a "grave disease infecting mathematics."

Kronecker fought to keep Cantor's papers out of his journals.

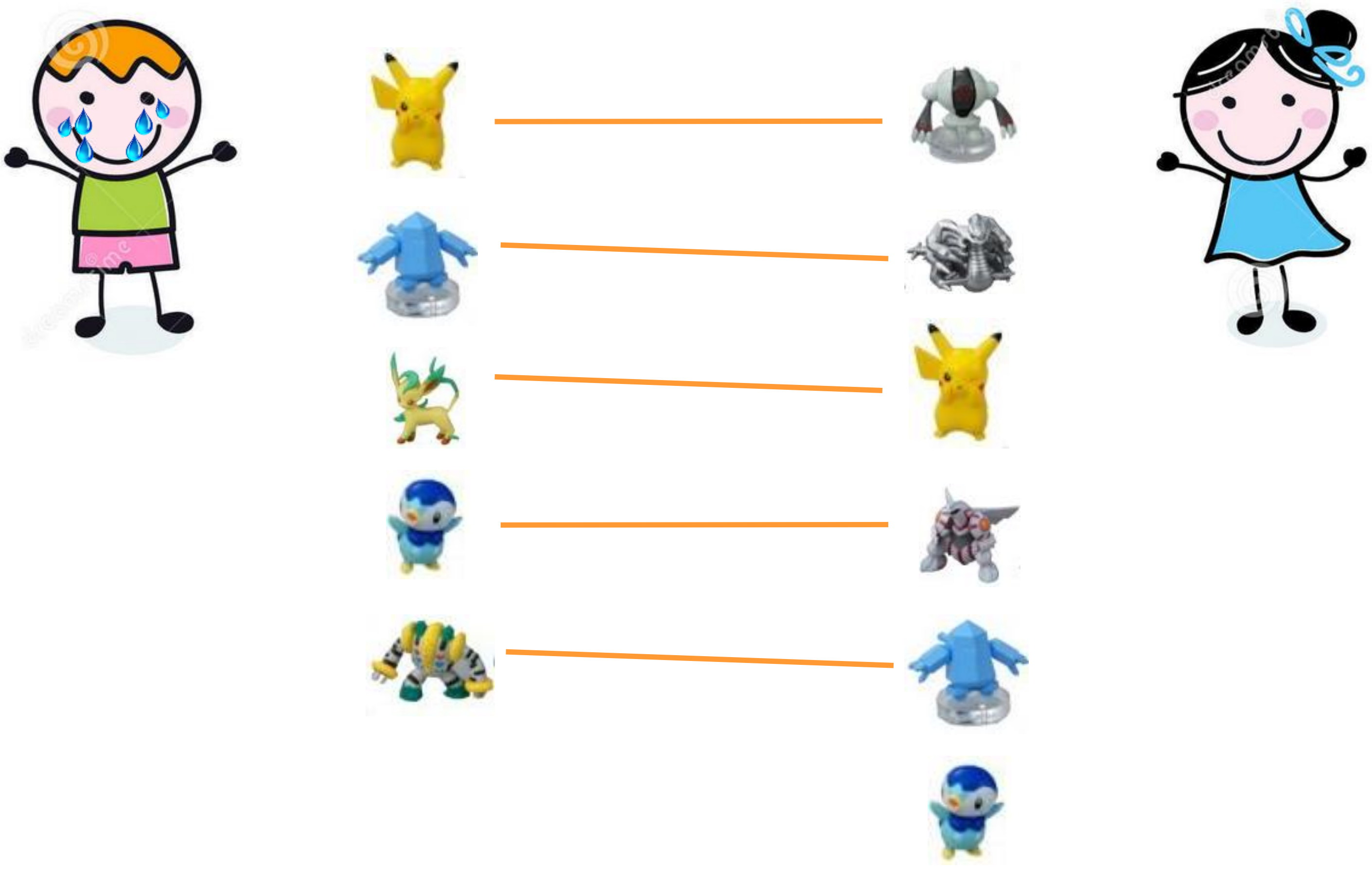
Cantor spent the last 30 years of his life battling depression, living often in "sanatoriums" (psychiatric hospitals).

Cardinality

What does it mean that two sets have the same size?

Cardinality

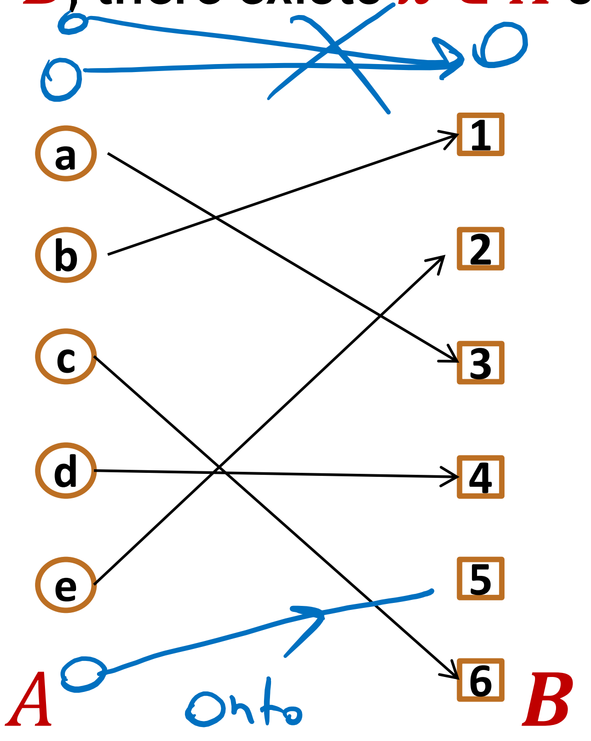
What does it mean that two sets have the same size?



1-1 and onto

A **function** $f : A \to B$ is **one-to-one** (1-1) if every output corresponds to at most one input;
i.e. $f(x) = f(x') \Rightarrow x = x'$ for all $x, x' \in A$.

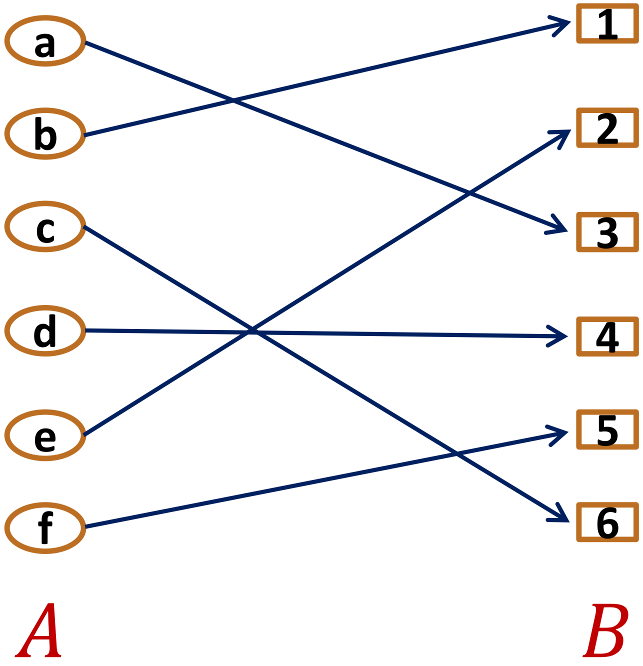
A **function** $f : A \to B$ is **onto** if every output gets hit;
i.e. for every $y \in B$, there exists $x \in A$ such that $f(x) = y$.



1-1 but not onto

Cardinality

Definition: Two sets A and B have the same **cardinality** if there is a one-to-one correspondence between the elements of A and those of B.
More precisely, if there is a **1-1 and onto** function $f : A \to B$.



The definition also makes sense for infinite sets!

Cardinality

Do the natural numbers and the even natural numbers have the same cardinality?

Yes!

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	…
0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	…

$f(x) = 2x$

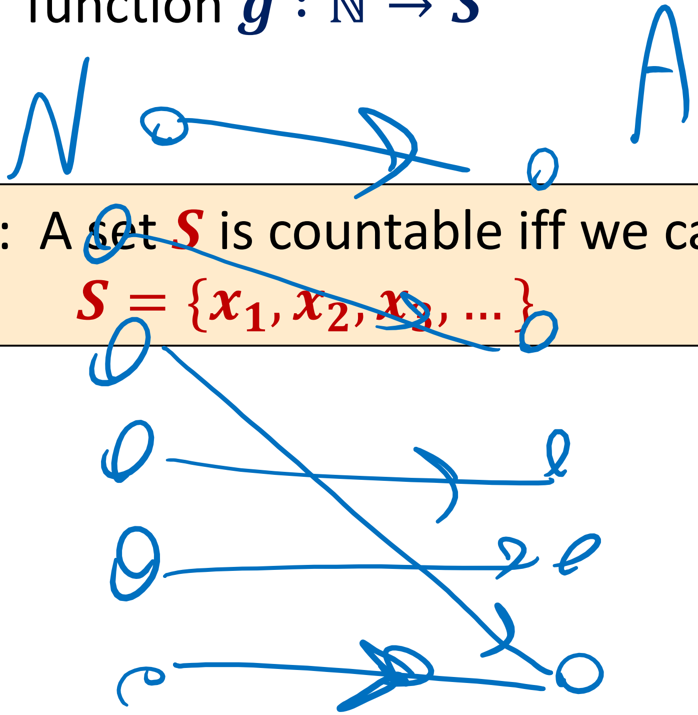
What's the map $\boldsymbol{f} : \mathbb{N} \to \mathbf{2}\mathbb{N}$? $\boldsymbol{f(n) = 2n}$

$f(k) = 2k$

Countable sets

Definition: A set is **countable** iff it has the same cardinality as some subset of $\mathbb{N}$.

Equivalent: A set $\boldsymbol{S}$ is countable iff there is an onto function $\boldsymbol{g} : \mathbb{N} \to \boldsymbol{S}$



Equivalent: A set $\boldsymbol{S}$ is countable iff we can order the elements $\boldsymbol{S} = \{x_1, x_2, x_3, \ldots\}$

A is countable.

The set $\mathbb{Z}$ of all integers

The set $\mathbb{Z}$ of all integers

$$f(i) = \begin{cases} -\frac{i}{2} & \text{if } i \text{ even} \\ \frac{i+1}{2} & i \text{ odd} \end{cases}$$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	…
0	1	-1	2	-2	3	-3	4	-4	5	-5	6	-6	7	-7	…

The set $\mathbb{Q}$ of rational numbers

We can’t do the same thing we did for the integers.

Between any two rational numbers there are an infinite number of others.

The set of positive rational numbers

1/1	1/2	1/3	1/4	1/5	1/6	1/7	1/8	...
2/1	2/2	2/3	2/4	2/5	2/6	2/7	2/8	...
3/1	3/2	3/3	3/4	3/5	3/6	3/7	3/8	...
4/1	4/2	4/3	4/4	4/5	4/6	4/7	4/8	...
5/1	5/2	5/3	5/4	5/5	5/6	5/7	...	
6/1	6/2	6/3	6/4	6/5	6/6	...		
7/1	7/2	7/3	7/4	7/5	....			
...	...	...	...	...				

The set of positive rational numbers

The set of all positive rational numbers **is countable.**

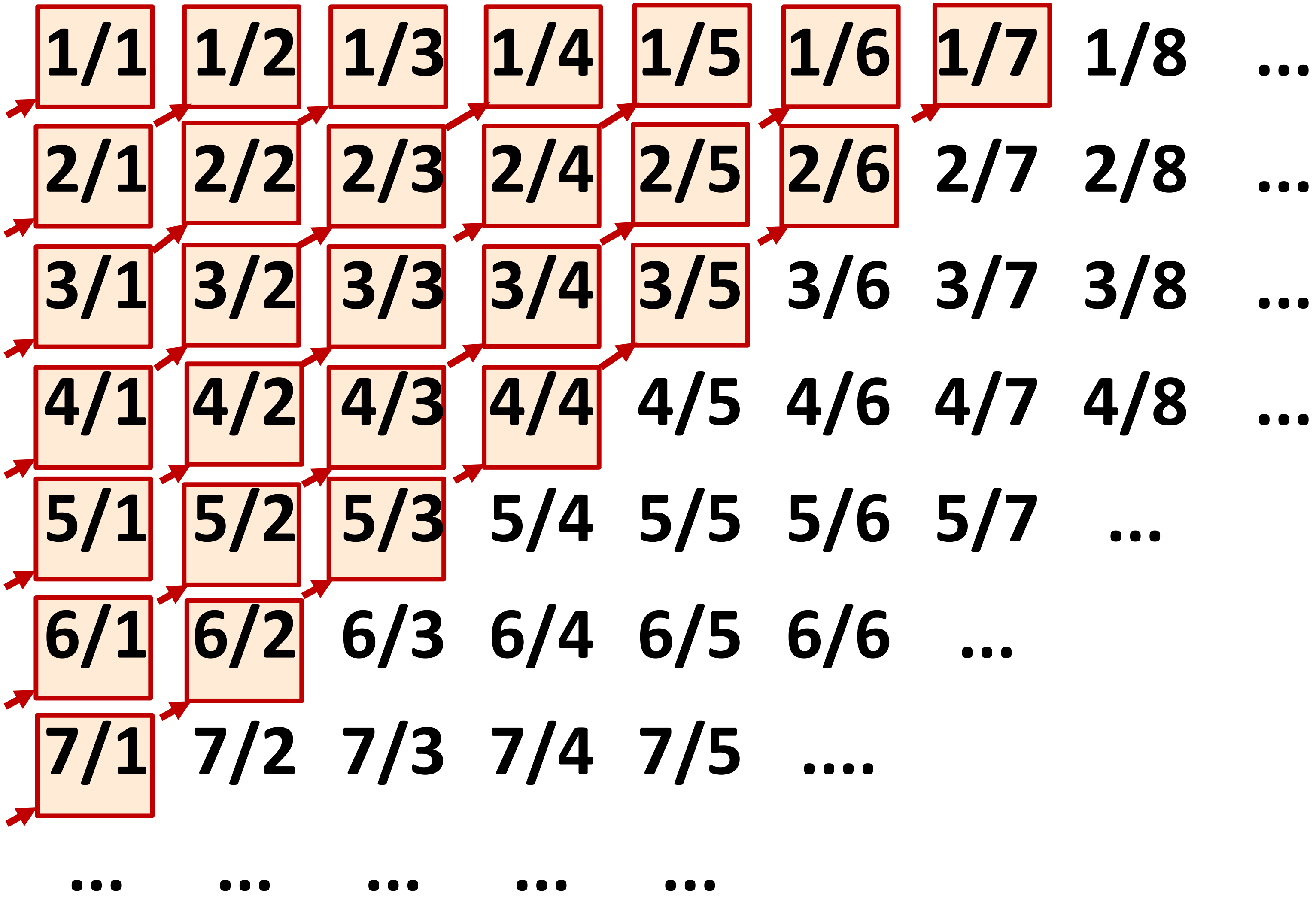
$$\mathbb{Q}^+ = \{\mathbf{1/1, 2/1, 1/2, 3/1, 2/2, 1/3, 4/1, 2/3, 3/2, 1/4, 5/1, 4/2, 3/3, 2/4, 1/5,}\ \ldots\}$$

List elements in order of numerator+denominator, breaking ties according to denominator.

Only $\boldsymbol{k}$ numbers have total of sum of $\boldsymbol{k+1}$, so every positive rational number comes up some point.

The technique is called “**dovetailing**.”

The set of positive rational numbers



1/1	1/2	1/3	1/4	1/5	1/6	1/7	1/8	…
2/1	2/2	2/3	2/4	2/5	2/6	2/7	2/8	…
3/1	3/2	3/3	3/4	3/5	3/6	3/7	3/8	…
4/1	4/2	4/3	4/4	4/5	4/6	4/7	4/8	…
5/1	5/2	5/3	5/4	5/5	5/6	5/7	…	
6/1	6/2	6/3	6/4	6/5	6/6	…		
7/1	7/2	7/3	7/4	7/5	….			
…	…	…	…	…				

The set $\mathbb{Q}$ of rational numbers

Even for positive Rational

Odd for negative

$-\frac{1}{1}$ $-\frac{1}{2}$

$-\frac{2}{1}$ . . .

$\frac{1}{1}$ $\frac{1}{2}$ . . .

$\frac{2}{1}$ . . . .

Claim: Σ^* is countable for every finite Σ

Dictionary/Alphabetical/Lexicographical order is bad

- Never get past the A’s
- A, AA, AAA, AAAA, AAAAA, AAAAAA, ….

Claim: Σ^* is countable for every finite Σ

Dictionary/Alphabetical/Lexicographical order is bad

- – Never get past the A's
- – A, AA, AAA, AAAA, AAAAA, AAAAAA, ….

Instead, use same "dovetailing" idea, except that we first break ties based on length: only $|\Sigma|^k$ strings of length k.

e.g. {0,1}* is countable:

{ε, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111,
… }

The set of all Java programs is countable

Java programs are just strings in Σ^* where Σ is the alphabet of ASCII characters.

Since Σ^* is countable, so is the set of all Java programs.

OK OK… Is Everything Countable ?!!

Are the real numbers countable?

Theorem [Cantor]:
The set of real numbers between 0 and 1 is **not** countable.

Proof will be by contradiction. Using a new method called diagonalization.

Real numbers between 0 and 1: $[0,1)$

Every number between 0 and 1 has an infinite decimal expansion:

$$1/2 = 0.50000000000000000000000...$$

$$1/3 = 0.33333333333333333333333...$$

$$1/7 = 0.14285714285714285714285...$$

$$\pi\text{-}3 = 0.14159265358979323846264...$$

$$1/5 = 0.19999999999999999999999...$$

$$= 0.20000000000000000000000...$$

Representation is unique except for the cases that the decimal expansion ends in all 0's or all 9's.
We will never use the all 9's representation.

Proof that $[0,1)$ is not countable

Suppose, for the sake of contradiction, that there is a list of them:

		1	2	3	4	5	6	7	8	9	...
r_1	0.	5	0	0	0	0	0	0	0	...	...
r_2	0.	3	3	3	3	3	3	3	3	...	...
r_3	0.	1	4	2	8	5	7	1	4	...	...
r_4	0.	1	4	1	5	9	2	6	5	...	...
r_5	0.	1	2	1	2	2	1	2	2	...	...
r_6	0.	2	5	0	0	0	0	0	0	...	...
r_7	0.	7	1	8	2	8	1	8	2	...	...
r_8	0.	6	1	8	0	3	3	9	4	...	...
...	....	...	....	....	...	...	...	...	...	...	

Proof that $[0,1)$ is not countable

Suppose, for the sake of contradiction, that there is a list of them:

		1	2	3	4	5	6	7	8	9	…
r_1	0.	5	0	0	0	0	0	0	0	…	…
r_2	0.	3	3	3	3	3	3	3	3	…	…
r_3	0.	1	4	2	8	5	7	1	4	…	…
r_4	0.	1	4	1	5	9	2	6	5	…	…
r_5	0.	1	2	1	2	2	1	2	2	…	…
r_6	0.	2	5	0	0	0	0	0	0	…	…
r_7	0.	7	1	8	2	8	1	8	2	…	…
r_8	0.	6	1	8	0	3	3	9	4	…	…
…	….	…	….	….	…	…	…	…	…	…	

Proof that $[0,1)$ is not countable

Suppose, for the sake of contradiction, that there is a list of them:

		1	2	3	4						
r_1	0.	5	0	0	0						
r_2	0.	3	3	3	3						
r_3	0.	1	4	2	8	5	7	1	4	…	…
r_4	0.	1	4	1	5	9	2	6	5	…	…
r_5	0.	1	2	1	2	2	1	2	2	…	…
r_6	0.	2	5	0	0	0	0	0	0	…	…
r_7	0.	7	1	8	2	8	1	8	2	…	…
r_8	0.	6	1	8	0	3	3	9	4	…	…
…	….	…	….	….	…	…	…	…	…	…	

Flipping rule:

Only if the other driver deserves it.

Proof that $[0,1)$ is not countable

Suppose, for the sake of contradiction, that there is a list of them:

		1	2	3	4						
r_1	0.	5^{1}	0	0	0						
r_2	0.	3	3^{5}	3	3						
r_3	0.	1	4	2^{5}	8	5	7	1	4	...	...
r_4	0.	1	4	1	5^{1}	9	2	6	5	...	...
r_5	0.	1	2	1	2	2^{5}	1	2	2	...	...
r_6	0.	2	5	0	0	0	0^{5}	0	0	...	...
r_7	0.	7	1	8	2	8	1	8^{5}	2	...	...
r_8	0.	6	1	8	0	3	3	9	4^{5}	...	...
...	....	...	....	....	...	...	...	...	...	...	

Flipping rule:

If digit is 5, make it 1.

If digit is not 5, make it 5.

Proof that $[0,1)$ is not countable

Suppose, for the sake of contradiction, that there is a list of them:

Flipping rule:

If digit is 5, make it 1.

If digit is not 5, make it 5.

		1	2	3	4						
r_1	0.	5^{1}	0	0	0						
r_2	0.	3	3^{5}	3	3						
r_3	0.	1	4	2^{5}	8	5	7	1	4	...	...
r_4	0.	1	4	1	5^{1}	9	2	6	5	...	...
r_5	0.	1	2	1	2	2^{5}	1	2	2	...	...
r_6	0.	2	5	0	0	0	0^{5}	0	0	...	...
r_7	0.	7	1	8	2	8	1	8^{5}	2	...	...

If diagonal element is $\mathbf{0}.\,x_{11}x_{22}x_{33}x_{44}x_{55}\cdots$ then let's call the flipped number $\mathbf{0}.\,\widehat{x}_{11}\widehat{x}_{22}\widehat{x}_{33}\widehat{x}_{44}\widehat{x}_{55}\cdots$

It cannot appear anywhere on the list!

Proof that $[0,1)$ is not countable

Suppose, for the sake of contradiction, that there is a list of them:

		1	2	3	4						
r_1	0.	5^{1}	0	0	0						
r_2	0.	3	3^{5}	3	3						
r_3	0.	1	4	2^{5}	8	5	7	1	4	...	...
r_4	0.	1	4	1	5^{1}	9	2	6	5	...	...
						2^{5}	1	2	2	...	...
						0	0^{5}	0	0	...	...
						8	1	8^{5}	2	...	...

Flipping rule:

If digit is 5, make it 1.

If digit is not 5, make it 5.

For every $n \geq 1$:

$r_n \neq 0.\hat{x}_{11}\hat{x}_{22}\hat{x}_{33}\hat{x}_{44}\hat{x}_{55}\cdots$

because the numbers differ on the n-th digit!

If diagonal element is $0.x_{11}x_{22}x_{33}x_{44}x_{55}\cdots$ then let's call the flipped number $0.\hat{x}_{11}\hat{x}_{22}\hat{x}_{33}\hat{x}_{44}\hat{x}_{55}\cdots$

It cannot appear anywhere on the list!

Proof that $[0,1)$ is not countable

Suppose, for the sake of contradiction, that there is a list of them:

		1	2	3	4						
r_1	0.	5^{1}	0	0	0						
r_2	0.	3	3^{5}	3	3						
r_3	0.	1	4	2^{5}	8	5	7	1	4	…	…
r_4	0.	1	4	1	5^{1}	9	2	6	5	…	…
						2^{5}	1	2	2	…	…
						0	0^{5}	0	0	…	…
						8	1	8^{5}	2	…	…

Flipping rule:

If digit is 5, make it 1.

If digit is not 5, make it 5.

For every $n \geq 1$:

$r_n \neq 0.\hat{x}_{11}\hat{x}_{22}\hat{x}_{33}\hat{x}_{44}\hat{x}_{55}\cdots$

because the numbers differ on the n-th digit!

So the list is incomplete, which is a contradiction.

Thus the real numbers between 0 and 1 are **not countable**: “uncountable”

The set of all functions $f : \mathbb{N} \to \{0, \ldots, 9\}$ is uncountable

Uncomputable functions

We have seen that:

- The set of all (Java) programs is countable
- The set of all functions $f : \mathbb{N} \to \{0, \ldots, 9\}$ is not countable

So: There must be some function $f : \mathbb{N} \to \{0, \ldots, 9\}$ that is not computable by any program!

Interesting… maybe.

Can we come up with an explicit function that is uncomputable?