CSE 311: Foundations of Computing

Lecture 26: Cardinality, Uncomputability

Course Evaluation Online

- Fill this out by Sunday night!
  - Your ability to fill it out will disappear at 11:59 p.m. on Sunday.
  - It will be worth your while to do so!

Last time: Showing that L is not regular

1. "Suppose for contradiction that some DFA M recognizes L."
2. Consider an **INFINITE** set S of "partial 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 s_a and s_b in **S** for $s_a \neq s_b$ that end up at the same state of **M**."
4. Consider appending the (correct) completion t to each of the two strings.
5. "Since s_a and s_b both end up at the same state of **M**, and we appended the same string t, both $s_a t$ and $s_b t$ end at the same state q of **M**. Since $s_a t \in L$ and $s_b t \notin L$, **M** does not recognize L."
6. "Thus, no DFA recognizes L."

Last time: Showing that L is not regular

Core of Proof: find a set S $\subseteq \Sigma^*$ such that

1. S is infinite

2. $\forall x,y \in S\ ((x \neq y) \rightarrow \exists z \in \Sigma^*\ (x \bullet z \in L \nleftrightarrow y \bullet z \in L))$

If you can find such an S, then the language is irregular.
Fill out the template for a complete proof.

– if S is not infinite, this still proves any correct DFA must have at least as many states as S has elements

Important Notes

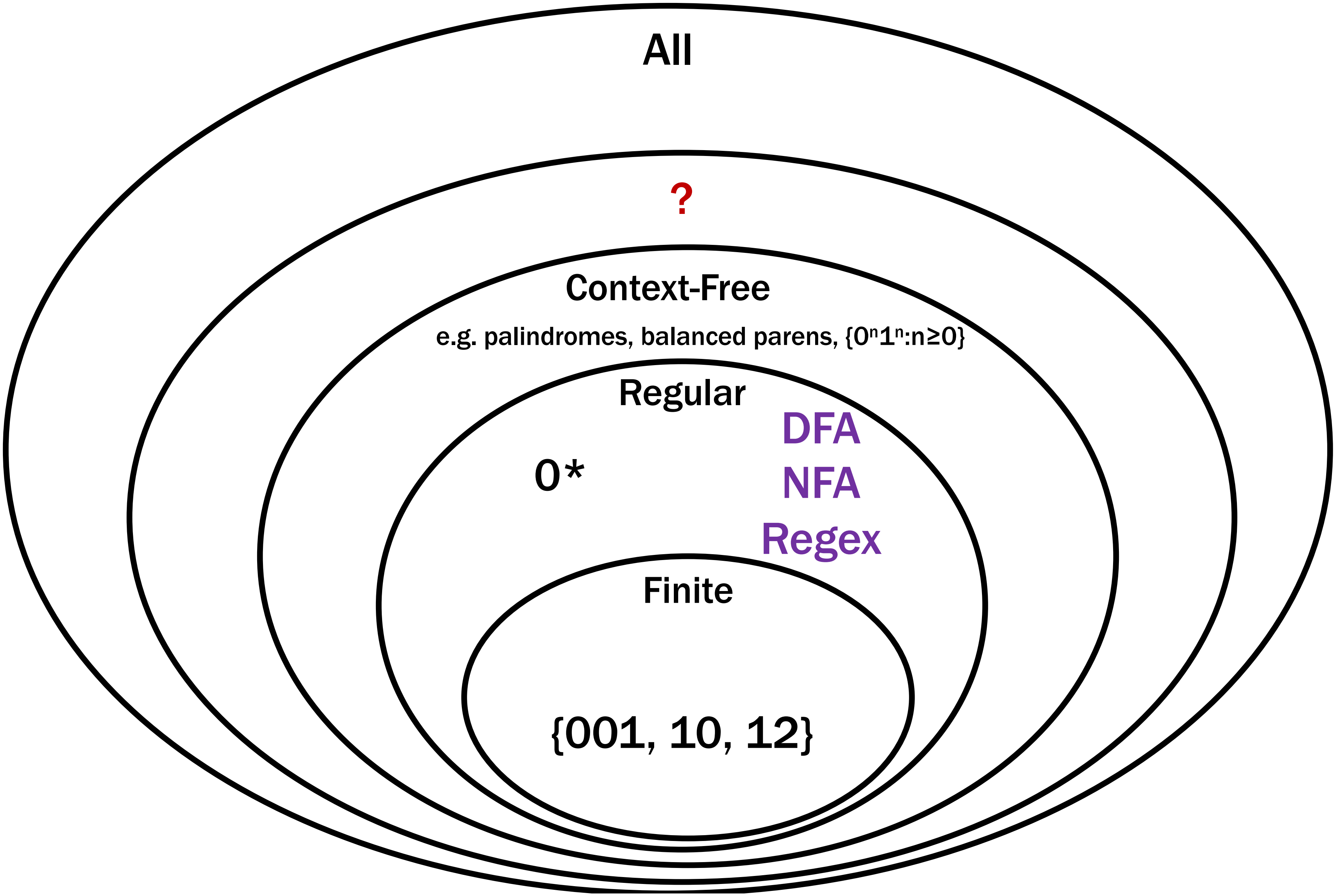
- It is not necessary for our strings $x \bullet z$ with $x \in L$ to produce any string in the language
  - we only need to find a small "core" set of strings that must be distinguished by the machine

- It is **not true** that, if L is irregular and $L \subseteq U$, then U is irregular!
  - we always have $L \subseteq \Sigma^*$ and Σ^* is regular!
  - our argument needs different answers: $x \bullet z \in L \not\leftrightarrow y \bullet z \in L$

    for Σ^*, both strings are always in the language

Do not claim in your proof that, because $L \subseteq U$, U is also irregular

Last time: Languages and Representations



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 initially 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.

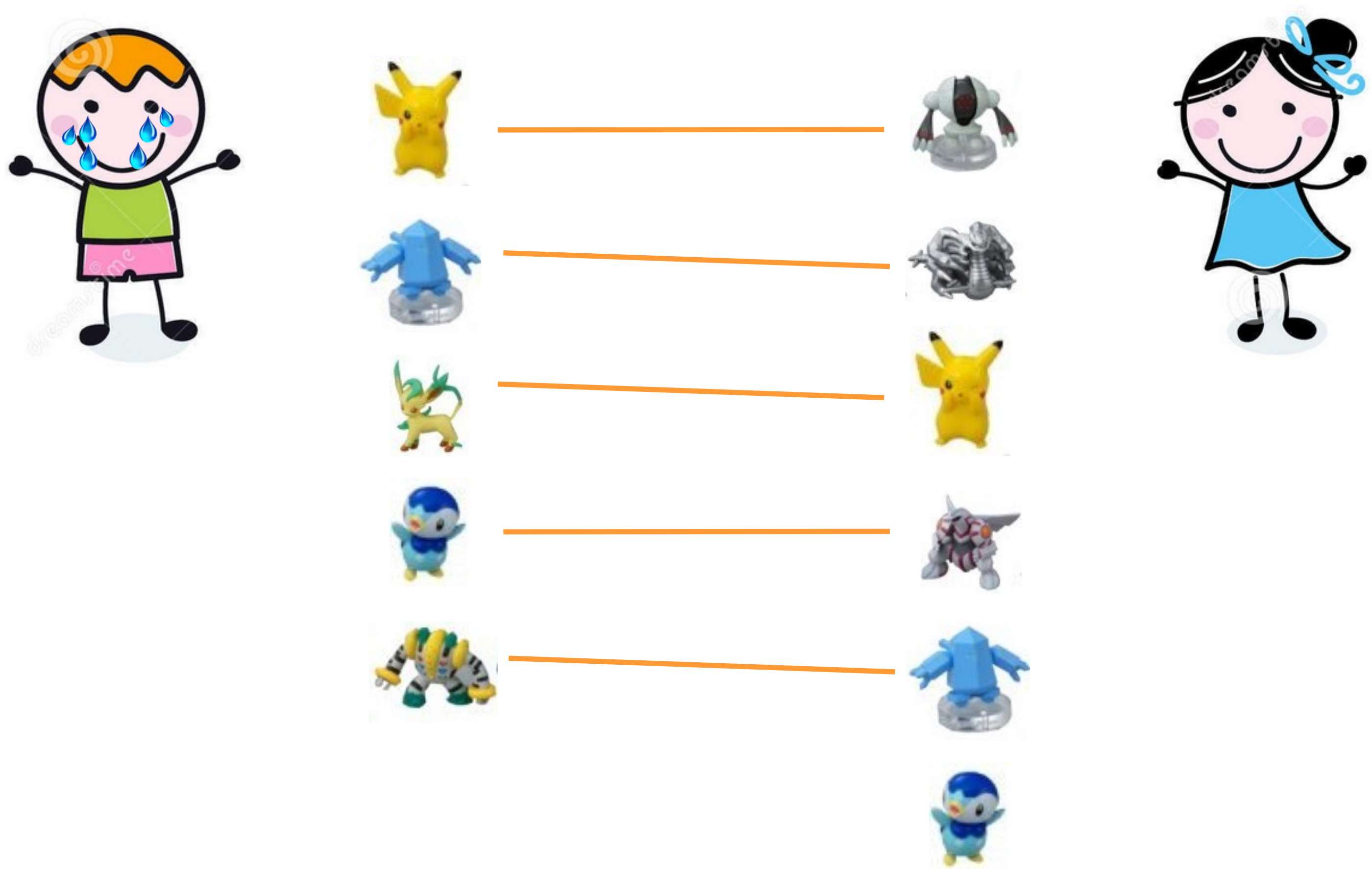
Full employment for mathematicians
and computer scientists!!

Cardinality

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

Cardinality

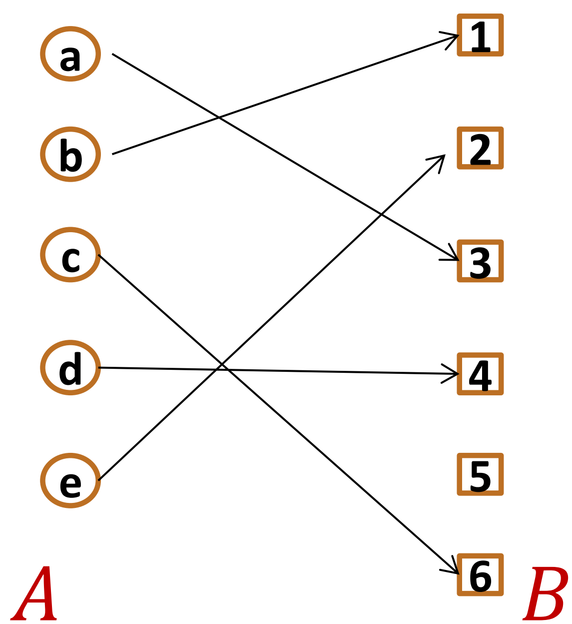
What does it mean that two sets have the same size?



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 $x, x' \in A$.

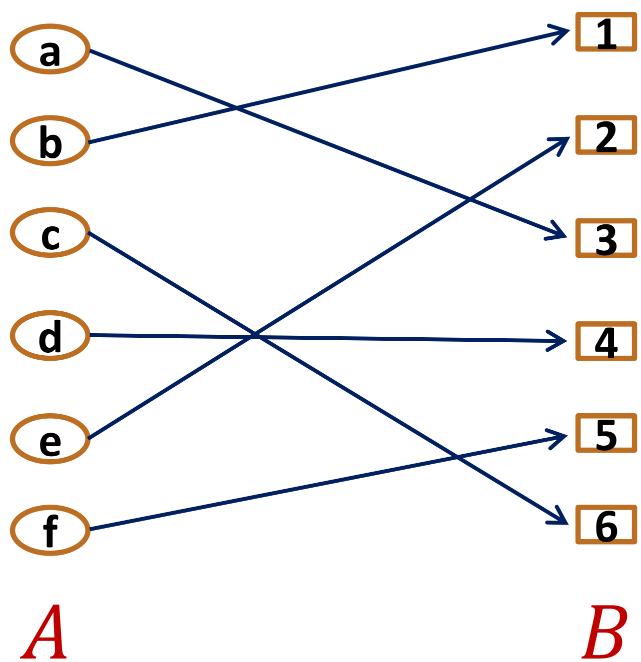
A **function** $f : A \to B$ is **onto** if every output gets hit;
i.e. for every $y \in B$, there exists $x \in A$ such that $f(x) = y$.



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 $f : A \rightarrow B$.



1-1 proves ≤
onto proves ≥

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	…

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

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 $\boldsymbol{S} = \{\boldsymbol{x_1}, \boldsymbol{x_2}, \boldsymbol{x_3}, \dots\}$

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

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

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**."

More generally:

- Put all elements into *finite* groups
- Order the groups
- List elements in order by group (arbitrary order within each group)

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

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 group 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.

More generally, any subset of a countable set is countable: it has same cardinality as an (even smaller) subset of $\mathbb{N}$

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.
Uses 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...

π-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 a contradiction, that there is a list of them:

r_1	**0.50000000…**
r_2	**0.33333333…**
r_3	**0.14285714…**
r_4	**0.14159265…**
r_5	**0.12122122…**
r_6	**0.25000000…**
r_7	**0.71828182…**
r_8	**0.61803394…**
…	…

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

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

Flipping rule:

Only if the other driver deserves it.

		1	2	3	4						
r_1	0.	5	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 a 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 a 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	...	...

Flipping rule:

If digit is 5, make it 1.

If digit is not 5, make it 5.

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

It cannot appear anywhere on the list!

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

Suppose, for a 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 a 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

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

Supposed listing of all the functions:

	1	2	3	4	5	6	7	8	9	...
f_1	5	0	0	0	0	0	0	0	...	...
f_2	3	3	3	3	3	3	3	3	...	...
f_3	1	4	2	8	5	7	1	4	...	...
f_4	1	4	1	5	9	2	6	5	...	...
f_5	1	2	1	2	2	1	2	2	...	...
f_6	2	5	0	0	0	0	0	0	...	...
f_7	7	1	8	2	8	1	8	2	...	...
f_8	6	1	8	0	3	3	9	4	...	...
...	...	....	....	...	...	...	...	...	...	

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

Supposed listing of all the functions:

	1	2	3	4						
f_1	5^{1}	0	0	0						
f_2	3	3^{5}	3	3						
f_3	1	4	2^{5}	8	5	7	1	4	...	...
f_4	1	4	1	5^{1}	9	2	6	5	...	...
f_5	1	2	1	2	2^{5}	1	2	2	...	...
f_6	2	5	0	0	0	0^{5}	0	0	...	...
f_7	7	1	8	2	8	1	8^{5}	2	...	...
f_8	6	1	8	0	3	3	9	4^{5}	...	...
...	...	....	....	...	...	...	...	...	...	

Flipping rule:

If $f_n(n) = 5$, set $D(n) = 1$

If $f_n(n) \neq 5$, set $D(n) = 5$

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

Supposed listing of all the functions:

	1	2	3	4						
f_1	5^{1}	0	0	0						
f_2	3	3^{5}	3	3						
f_3	1	4	2^{5}	8	5	7	1	4	…	…
f_4	1	4	1	5^{1}	9	2	6	5	…	…
f_5	1	2	1	2	2^{5}	1	2	2	…	…
f_6	2	5	0	0	0	0^{5}	0	0	…	…
f_7	7	1	8	2	8	1	8^{5}	2	…	…

Flipping rule:

If $f_n(n) = 5$, set $D(n) = 1$

If $f_n(n) \neq 5$, set $D(n) = 5$

For all n, we have $D(n) \neq f_n(n)$. Therefore $D \neq f_n$ for any n and the list is incomplete! $\Rightarrow$ $\{f \mid f: \mathbb{N} \to \{0,1, \ldots, 9\}\}$ is **not** countable

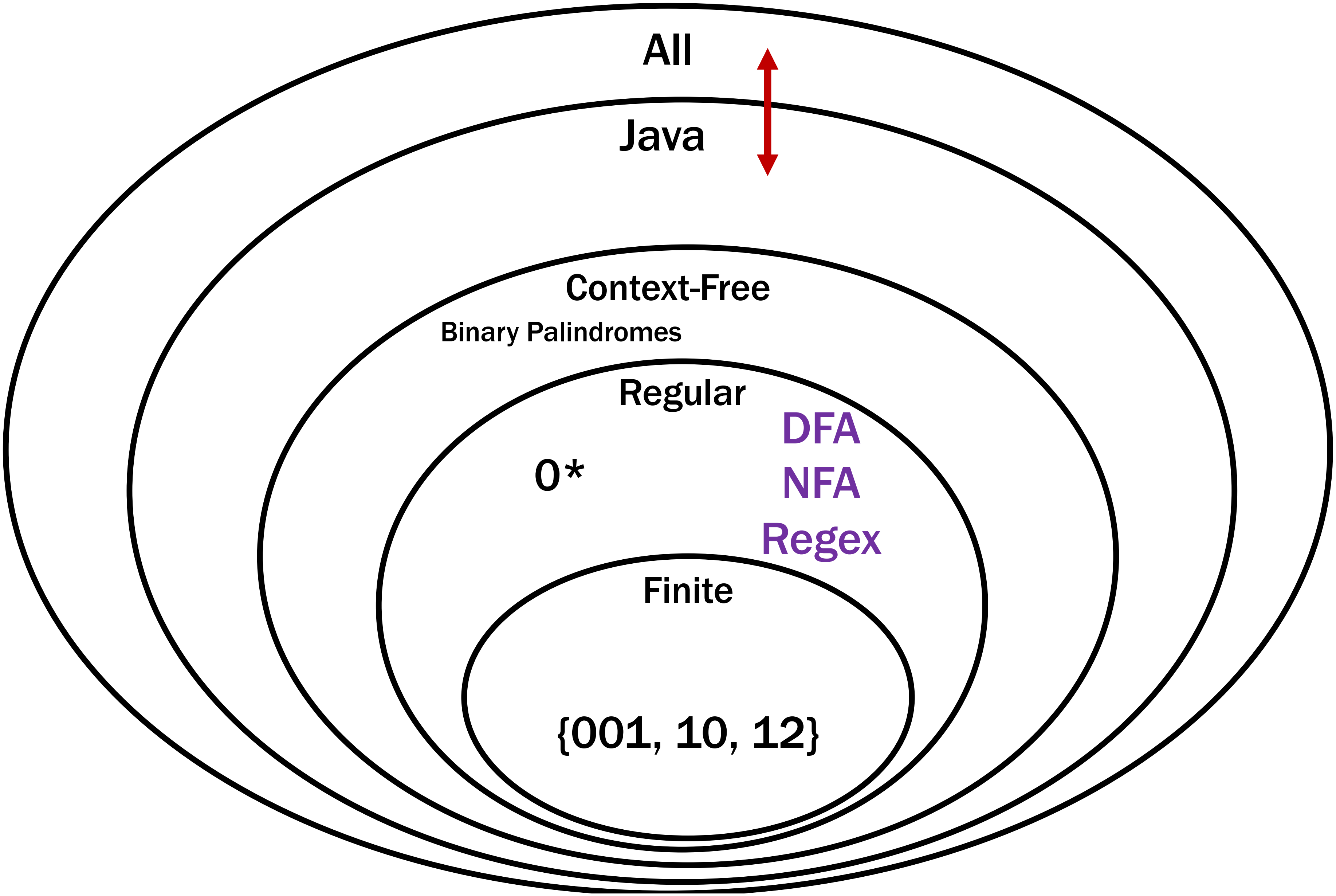
Uncomputable functions

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!

Recall our language picture



Uncomputable functions

Interesting… maybe.

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