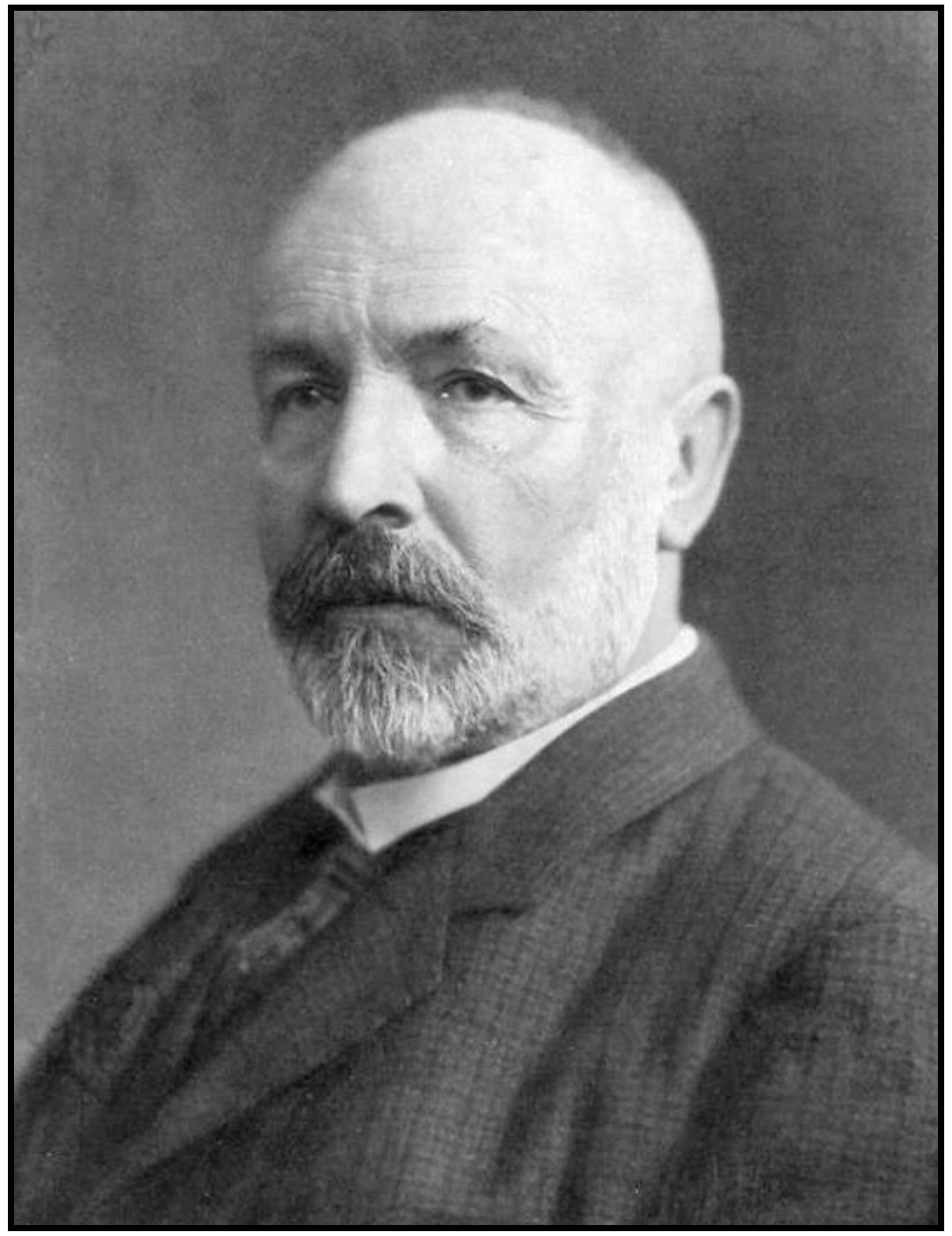
CS251

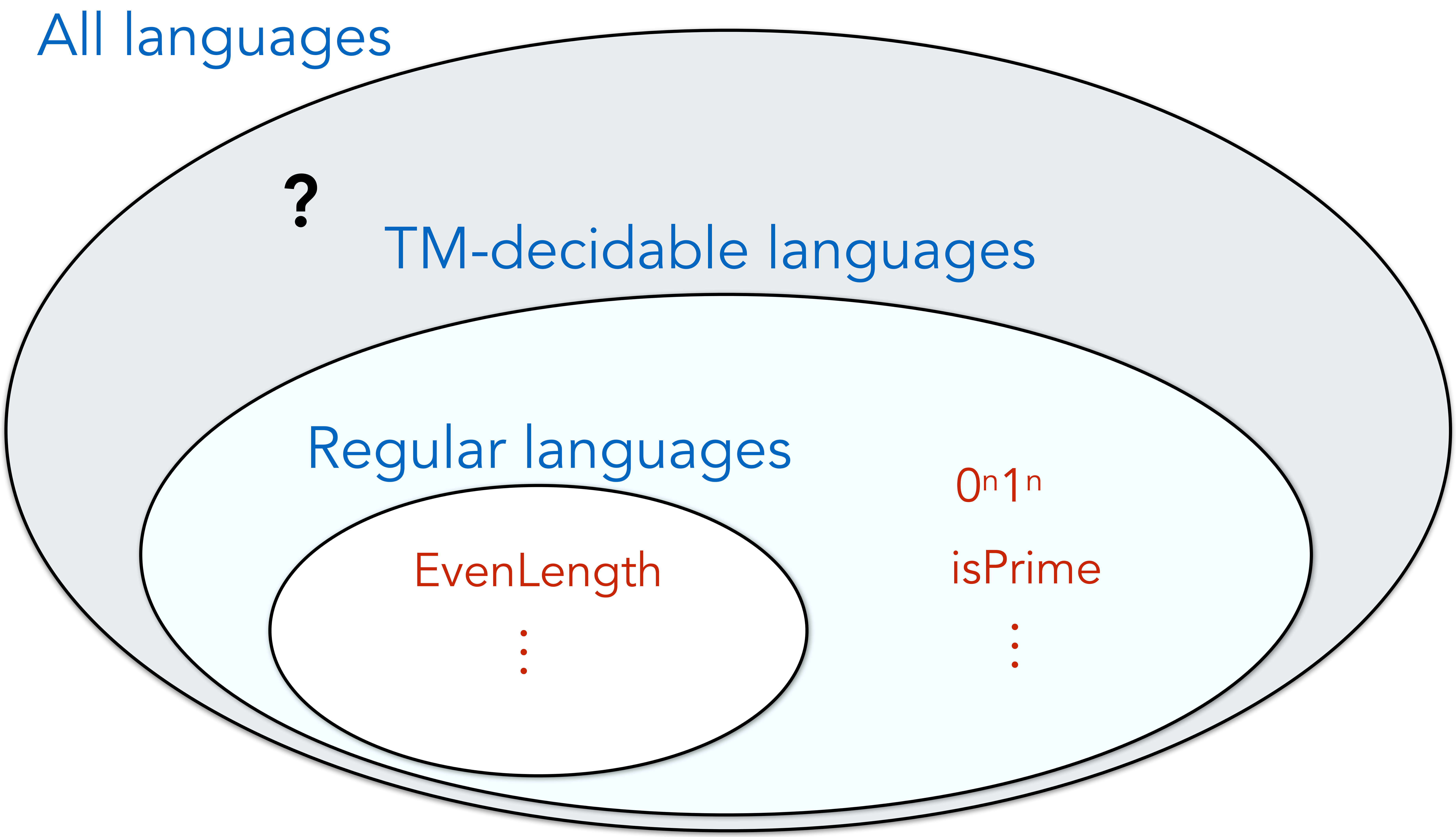
Great Ideas in *Theoretical* Computer Science



Limits of Computation 1: The Finite vs The Infinite

Completed: Formally define computation/algorithm.

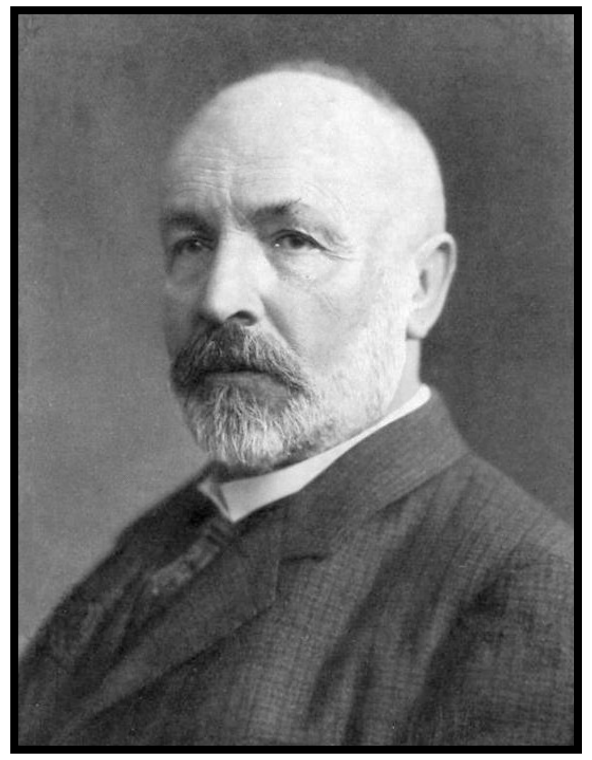
Next: Understand limits of computation and human reasoning.

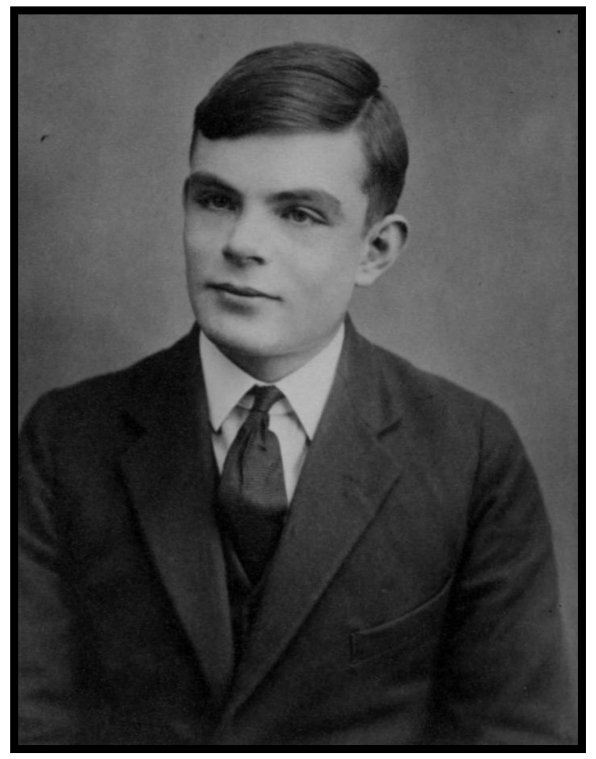


Completed: Formally define computation/algorithm.

Next: Understand limits of computation and human reasoning.

finite vs infinite → limits of computation → limits of human reasoning





The Finite vs The Infinite

Infinity in Mathematics Pre-Cantor:

"Infinity is nothing more than a figure of speech which helps us talk about limits.
The notion of a *completed infinity* doesn't belong in mathematics."

- Carl Friedrich Gauss

Cantor:

Treat infinite sets as first-class citizens!

Reaction to Cantor's ideas at the time

Most of the ideas of Cantorian set theory should be banished from mathematics once and for all!

- Henri Poincaré

Reaction to Cantor's ideas at the time

I don't know what predominates
in Cantor's theory -
philosophy or theology.

- Leopold Kronecker

Reaction to Cantor's ideas at the time

Scientific charlatan.

- Leopold Kronecker

Reaction to Cantor's ideas at the time

Corrupter of youth.

- Leopold Kronecker

Reaction to Cantor's ideas at the time

Wrong.

- Ludwig Wittgenstein

Reaction to Cantor's ideas at the time

Utter non-sense.

- Ludwig Wittgenstein

Reaction to Cantor's ideas at the time

Laughable.

- Ludwig Wittgenstein

Reaction to Cantor's ideas at the time

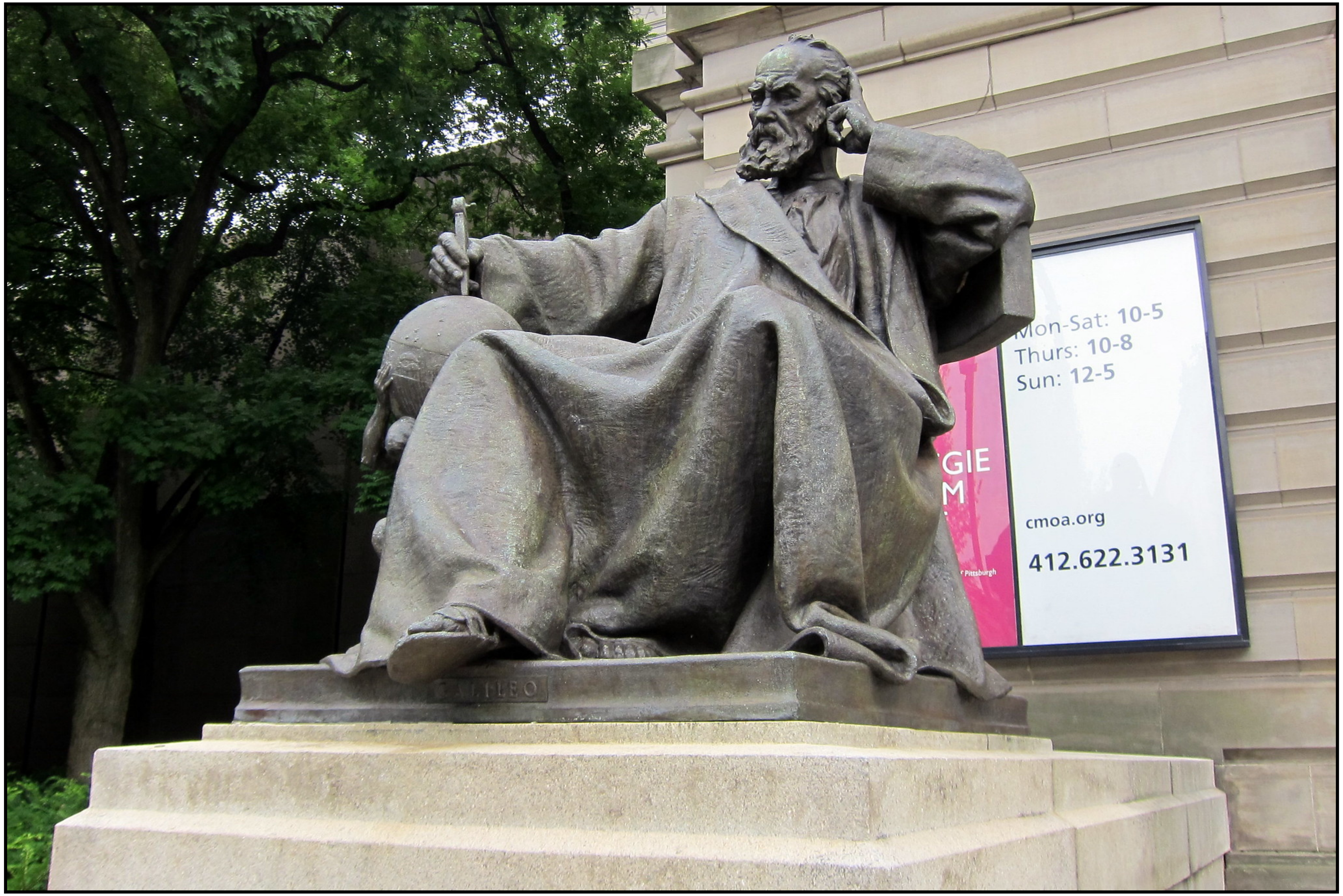
No one should expel us from the Paradise that Cantor has created.

- David Hilbert

Reaction to Cantor's ideas at the time

If one person can see it as a paradise,
why should not another see it as a joke?

- Ludwig Wittgenstein


Mon-Sat: 10-5
Thurs: 10-8
Sun: 12-5
cmoa.org
412.622.3131

Galileo (1564–1642)

Best known publication:

Dialogue Concerning the Two Chief World Systems

His final magnum opus (1638):

Discourses and Mathematical Demonstrations
Relating to Two New Sciences

The three characters

Salviati:

The "smart one". (Obvious Galileo stand-in.)

Named after one of Galileo's friends.

Sagredo:

"Intelligent layperson". He's neutral.

Named after one of Galileo's friends.

Simplicio:

The "idiot".

Modeled after two of Galileo's enemies.

Salviati

Simplicio

I take it for granted that you know which of the numbers are **squares** and which are not.

I am quite aware that a squared number is one which results from the multiplication of another number by itself; thus 4, 9, etc., are squared numbers which come from multiplying 2, 3, etc., by themselves.

Very well. [… defines 'square root' and 'non-square'…]
If I assert that **all numbers**, including both squares and non-squares, **are more than the squares** alone, I shall speak the truth, shall I not?

Most certainly.

$$S = \{0, 1, 4, 9, 16, \dots\}$$

$$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$$

- $|S| < |\mathbb{N}|$

Salviati

Simplicio

If I should ask further **how many squares** there are,
one might reply truly that there are as many as
the corresponding **number of square-roots**,
since every square has its own square-root
and every square-root its own square…

Precisely so.

But if I inquire **how many square-roots** there are,
it cannot be denied that there are **as many as the numbers**
because every number is the square-root of some square.

This being granted, we must say that there are
as many squares as there are numbers because
they are just as numerous as their square-roots,
and all the numbers are square-roots.

Yet at the outset we said that there are
many more numbers than squares.

$$S = \{0,\ 1,\ 4,\ 9,\ 16,\ \ldots\}$$
$$\updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow$$
$$SR = \{0,\ 1,\ 2,\ 3,\ 4,\ \ldots\}$$

$$\mathbb{N} = \{0,\ 1,\ 2,\ 3,\ 4,\ \ldots\}$$

- $|S| < |\mathbb{N}|$
- $|S| = |SR| = |\mathbb{N}|$

Sagredo: What then must one conclude under these circumstances?

Salviati

Cantor

(1845–1918)

Neither is the **number of squares** less than the totality of **all the numbers**, …

Good, good…

… nor the latter greater than the former, …

Good, good…

… and finally, the attributes "equal," "greater," and "less," are not applicable to infinite, but only to finite, quantities.

OOOHHHH! So close!
You were almost there, Galileo!
Why not say that they are indeed equal?

$$S = \{0, 1, 4, 9, 16, \ldots\}$$

$$\updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow$$

$$SR = \{0, 1, 2, 3, 4, \ldots\}$$

$$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$$

- $|S| < |\mathbb{N}|$
- $|S| = |SR| = |\mathbb{N}|$

Great Idea #1:

Use injections/surjections/bijections to compare sets.

Great Idea #2:

Diagonalization proof technique.

Great Idea #1:

Use injections/surjections/bijections to compare sets.

- Part 1: Comparing finite sets.

Comparing sizes of *finite* sets

$X = \{apple, orange, banana, melon\}$

$Y = \{200, 300, 400, 500\}$

What does $|X| = |Y|$ mean?

$$
\begin{array}{lcccc}
apple & \longleftrightarrow & 1 & \longleftrightarrow & 500 \\
orange & \longleftrightarrow & 2 & \longleftrightarrow & 200 \\
banana & \longleftrightarrow & 3 & \longleftrightarrow & 300 \\
melon & \longleftrightarrow & 4 & \longleftrightarrow & 400
\end{array}
$$

Comparing sizes of *finite* sets

$X = \{apple, orange, banana, melon\}$

$Y = \{200, 300, 400, 500\}$

What does $|X| = |Y|$ mean?

$apple \longleftrightarrow 500$

$orange \longleftrightarrow 200$

$banana \longleftrightarrow 300$

$melon \longleftrightarrow 400$

$|X| = |Y|$ iff there is a **1-to-1 correspondence** between X and Y.

Comparing sizes of *finite* sets

$X = \{apple, orange, banana\}$

$Y = \{200, 300, 400, 500\}$

What does $|X| \leq |Y|$ mean?

$$
\begin{array}{lcccc}
apple & \longleftrightarrow & 1 & \longleftrightarrow & 500 \\
orange & \longleftrightarrow & 2 & \longleftrightarrow & 200 \\
banana & \longleftrightarrow & 3 & \longleftrightarrow & 300 \\
 & & 4 & \longleftrightarrow & 400
\end{array}
$$

Comparing sizes of *finite* sets

$X = \{apple, orange, banana\}$

$Y = \{200, 300, 400, 500\}$

What does $|X| \leq |Y|$ mean?

$apple \longrightarrow 500$

$orange \longrightarrow 200$

$banana \longrightarrow 300$

400

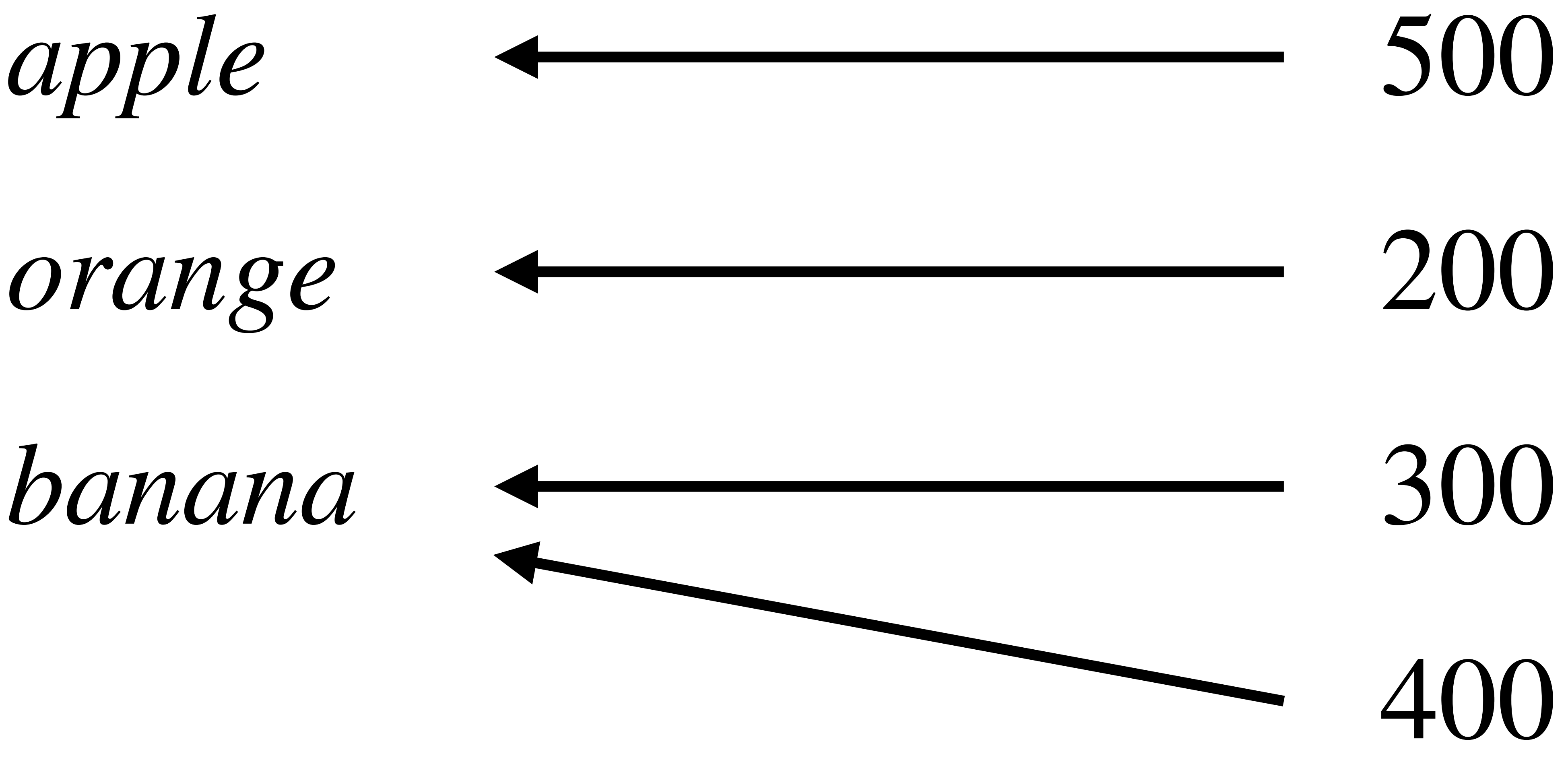
$|X| \leq |Y|$ iff there is an **injection** from X to Y.

Comparing sizes of *finite* sets

$X = \{apple, orange, banana\}$

$Y = \{200, 300, 400, 500\}$

What does $|X| \leq |Y|$ mean?



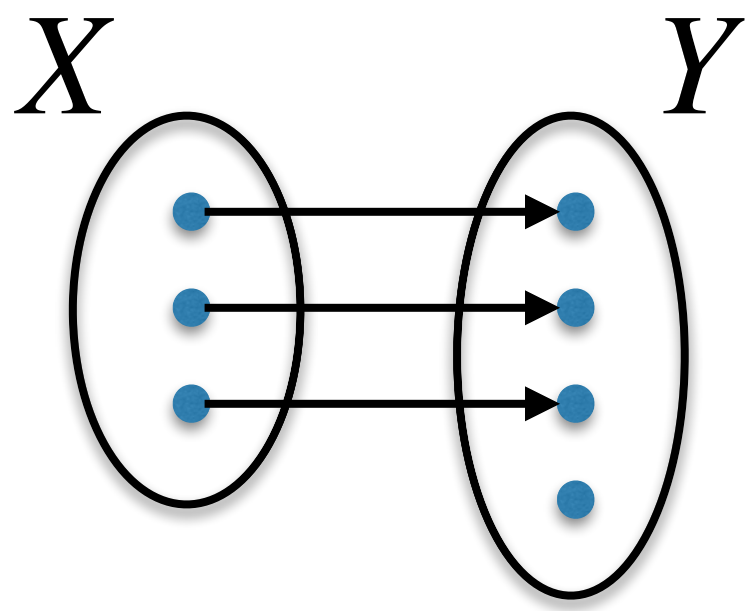
$|X| \leq |Y|$ iff there is a **surjection** from Y to X.

3 types of functions

injective, 1-to-1

$f : X \to Y$ is **injective** if
$x \neq x' \implies f(x) \neq f(x')$.

$X \hookrightarrow Y$

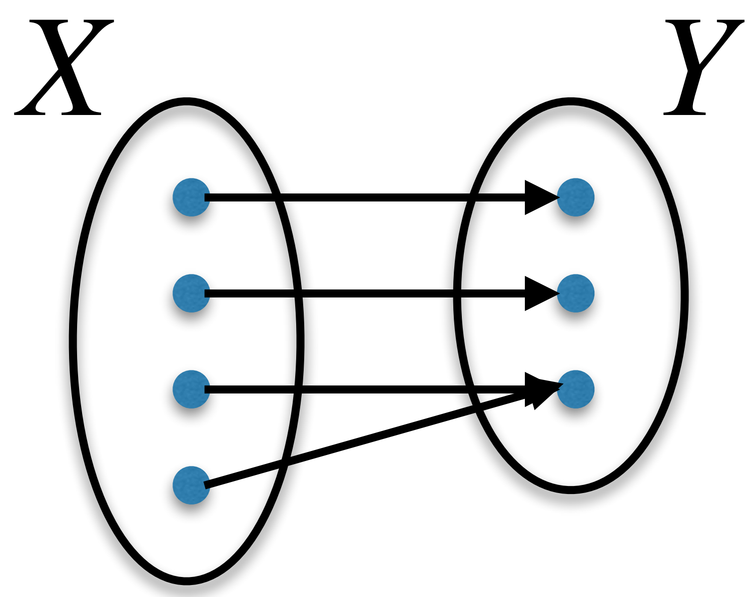


---

surjective, onto

$f : X \to Y$ is **surjective** if
$\forall y \in Y, \exists x \in X$ s.t. $f(x) = y$.

$X \twoheadrightarrow Y$

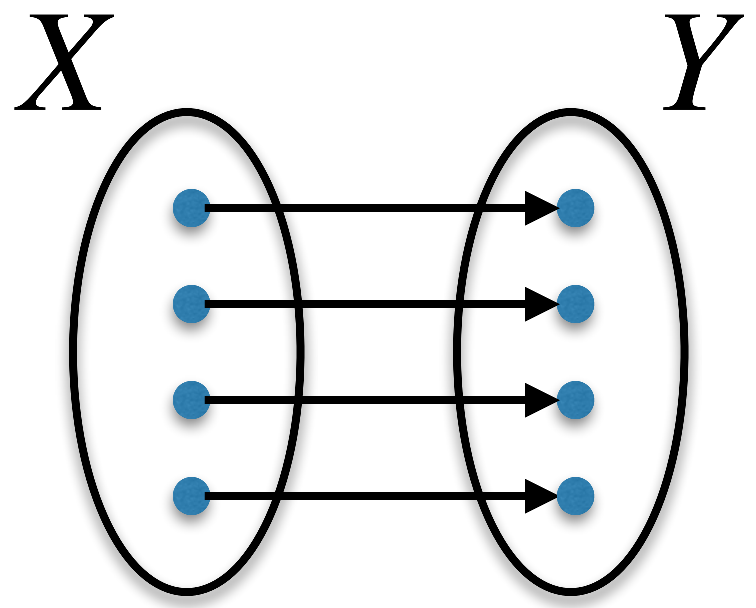


---

bijective, 1-to-1 correspondence

$f : X \to Y$ is **bijective** if
f is injective and surjective.

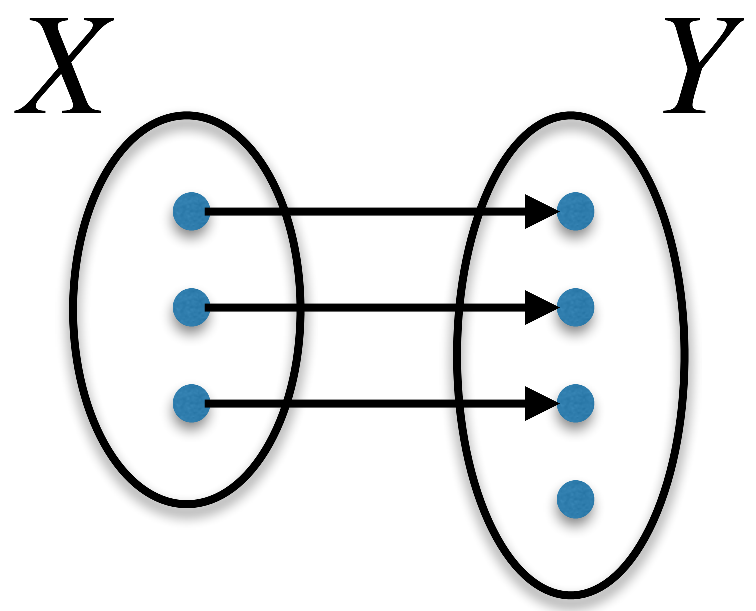
$X \leftrightarrow Y$



3 types of functions

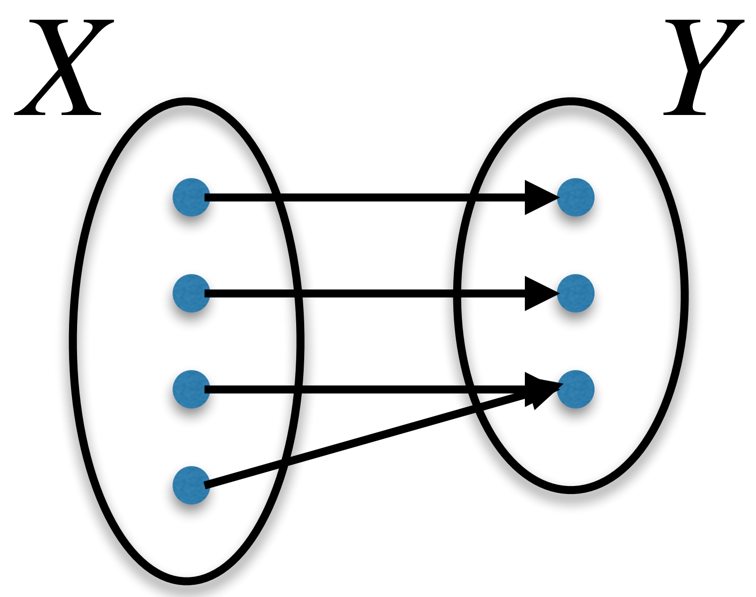
$|X| \leq |Y|$

$X \hookrightarrow Y$



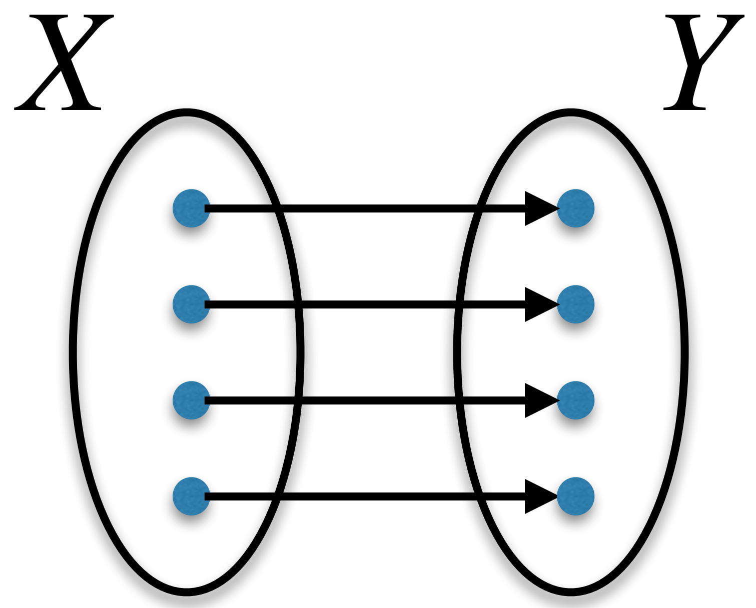
$|X| \geq |Y|$

$X \twoheadrightarrow Y$



$|X| = |Y|$

$X \leftrightarrow Y$



What does $|X| < |Y|$ mean?

not $|X| \geq |Y|$ — there is **no** surjection from X to Y.

there is **no** injection from Y to X.

$|X| \leq |Y|$
but **not** $|X| = |Y|$ — there is an injection from X to Y,
but **no** bijection between X and Y.

Great Idea #1:

Use injections/surjections/bijections to compare sets.

- Part 1: Comparing finite sets.
- Part 2: Comparing **infinite** sets.

The previous definitions
are the "**right**" definitions
for **infinite** sets as well!

Comparing *infinite* sets

$\lvert X\rvert \leq \lvert Y\rvert$	$X \hookrightarrow Y$
$\lvert X\rvert \geq \lvert Y\rvert$	$X \twoheadrightarrow Y$
$\lvert X\rvert = \lvert Y\rvert$	$X \leftrightarrow Y$

Note 1: We are not defining what $\lvert X\rvert$ means.

Note 2: This is just a way to attach meaning to expressions like "$\lvert X\rvert = \lvert Y\rvert$" for infinite sets.

Note 3: Cantor's statements/proofs are just about injections, surjections, bijections.

Sanity checks

- $|X| \leq |Y|$ iff $|Y| \geq |X|$

  $X \hookrightarrow Y$ iff $Y \twoheadrightarrow X$

- $|X| = |Y|$ iff $|X| \leq |Y|$ and $|X| \geq |Y|$

  $X \leftrightarrow Y$ iff $X \hookrightarrow Y$ and $X \twoheadrightarrow Y$

- If $|X| \leq |Y|$ and $|Y| \leq |Z|$, then $|X| \leq |Z|$

  If $X \hookrightarrow Y$ and $Y \hookrightarrow Z$, then $X \hookrightarrow Z$

Examples of bijections

$|\mathbb{N}| = |\mathbb{Z}|$?

$\mathbb{N} = \{0, 1, 2, 3, 4, \ \ldots\}$

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ \ldots\}$

0	1	2	3	4	5	6	7	8	…
↕	↕	↕	↕	↕	↕	↕	↕	↕	
0,	1,	-1,	2,	-2,	3,	-3,	4,	-4,	…

$$f(n) = (-1)^{n+1}\left\lceil \frac{n}{2} \right\rceil$$

Heuristic for showing $|A| = |\mathbb{N}|$

<u>Show A is "listable":</u>

List elements of A such that

every element appears in the list, eventually.

$\mathbb{N}$: 0 1 2 3 4 5 6 …

↕ ↕ ↕ ↕ ↕ ↕ ↕

$\mathbb{Z}$: 0, 1, -1, 2, -2, 3, -3, …

<u>Careful:</u>

$\mathbb{Z}$: ~~0, 1, 2, 3, 4, 5, 6, …~~

Examples of bijections

$|\mathbb{N}| = |\mathbb{S}|$?

$\mathbb{N} = \{0, 1, 2, 3, 4, \ \ldots\}$

$\mathbb{S} = \{0, 1, 4, 9, 16, \ \ldots\}$

<u>listable:</u>

$0, 1, 4, 9, 16, \ \ldots$

$f(n) = n^2$

Examples of bijections

$|\mathbb{N}| = |\mathbb{P}|$?

$\mathbb{N} = \{0, 1, 2, 3, 4, \ \dots\}$

$\mathbb{P} = \{2, 3, 5, 7, 11, \ \dots\}$

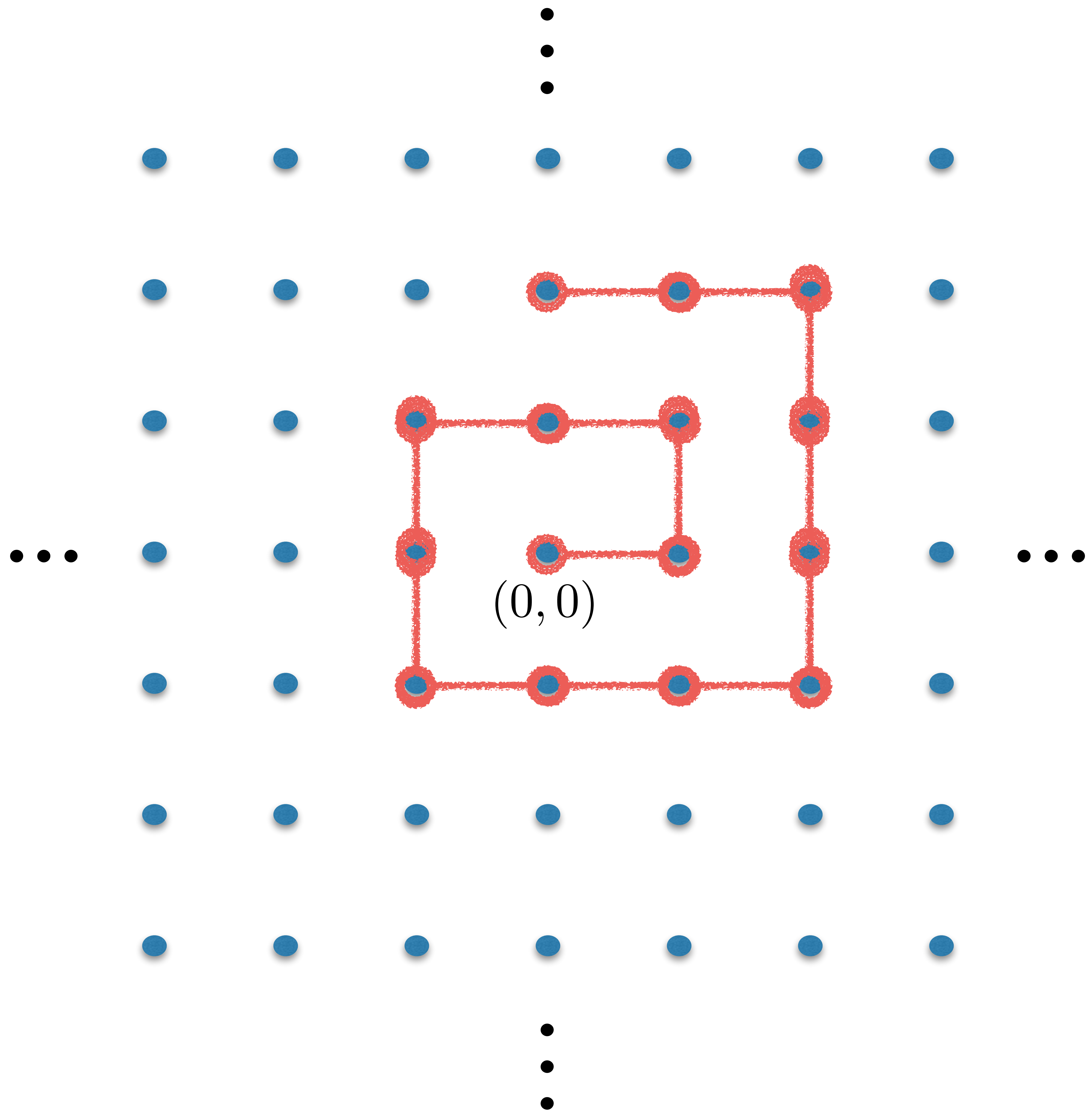
<u>listable:</u>

$2, 3, 5, 7, 11, \ \dots$

$f(n) =$ n'th prime number

Examples of bijections

$|\mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}|$?



<u>listable</u>

$(0,0)$
$(1,0)$
$(1,1)$
$(0,1)$
$(-1,1)$
$(-1,0)$
$(-1,-1)$
$(0,-1)$
$(1,-1)$
$(2,-1)$
$(2,0)$
$(2,1)$
$(2,2)$
$(1,2)$
$(0,2)$
$\vdots$

Examples of bijections

$|\mathbb{N}| = |\{0,1\}^*|$?

$\{0,1\}^*$ = the set of all finite-length binary words.

<u>listable:</u>

ϵ

0, 1

00, 01, 10, 11

000, 001, 010, 011, 100, 101, 110, 111

$\ldots$

Examples of bijections

$|\mathbb{N}| = |\Sigma^*|$?

Σ^* = the set of all finite-length words over Σ.

<u>listable:</u>

length 0 string

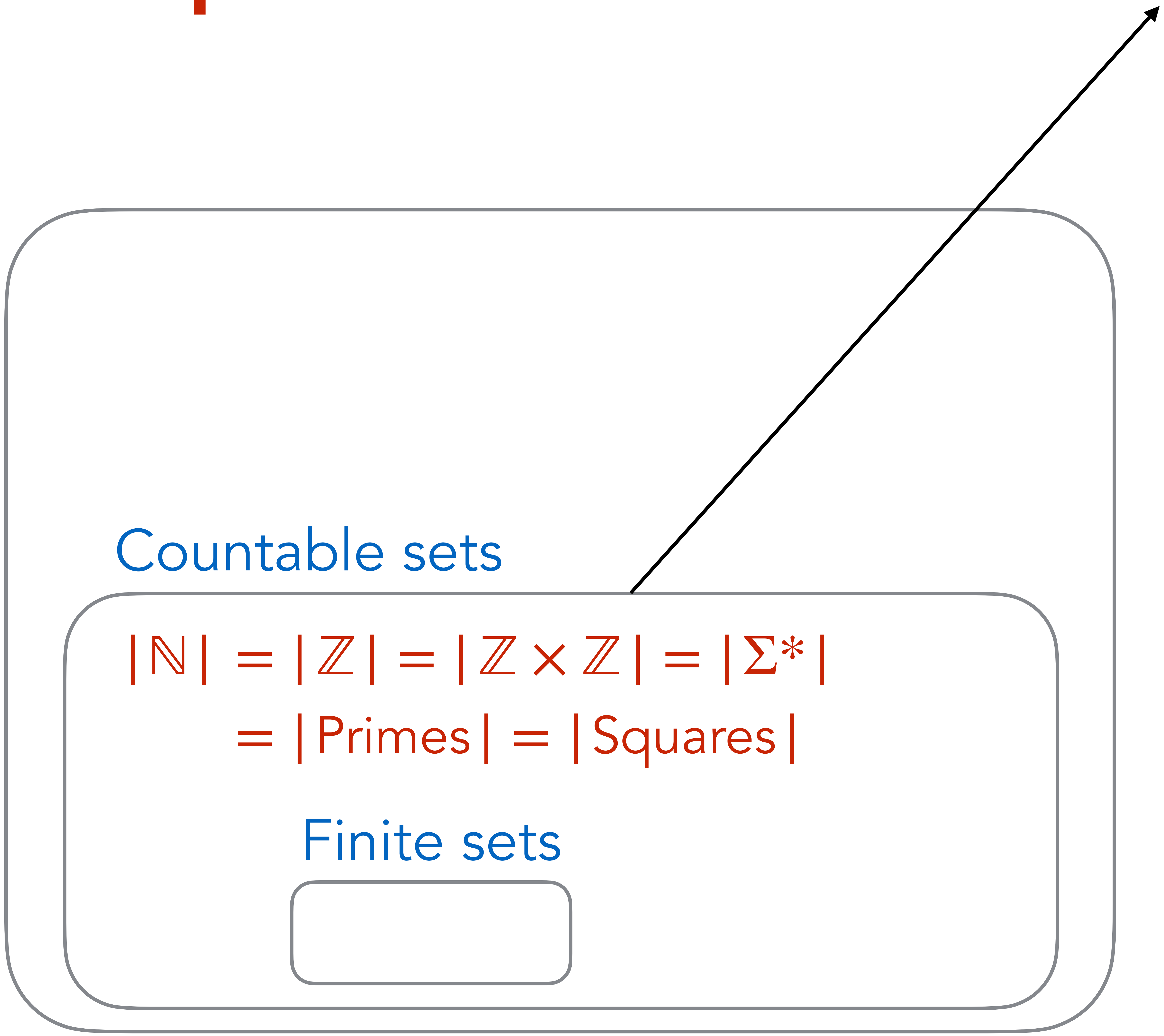
length 1 strings

length 2 strings

length 3 strings

$\vdots$

The picture so far



How should we define this set?

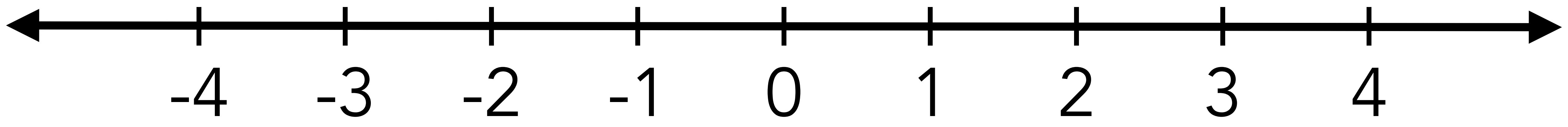
(i) sets S such that $|S| \leq |\mathbb{N}|$.

"listable", "orderable", "countable"

(ii) sets S such that $|S| \leq |\Sigma^*|$.

encodable

Is $\mathbb{Q}$ Countable?



Can we list them in the order they appear on the line? **NO!**

Let $\Sigma = \{0, 1, 2, \ldots, 9, /, - \}$.

Every rational number can be described
by a finite-length string over Σ.

e.g. $-210/251$

So $\mathbb{Q}$ is encodable/countable.

Is $\mathbb{Q}[x]$ Countable?

$\mathbb{Q}[x]$ = the set of polynomials with rational coefficients.

e.g. $$x^3 - \frac{1}{4}x^2 + 6x - \frac{22}{7}$$

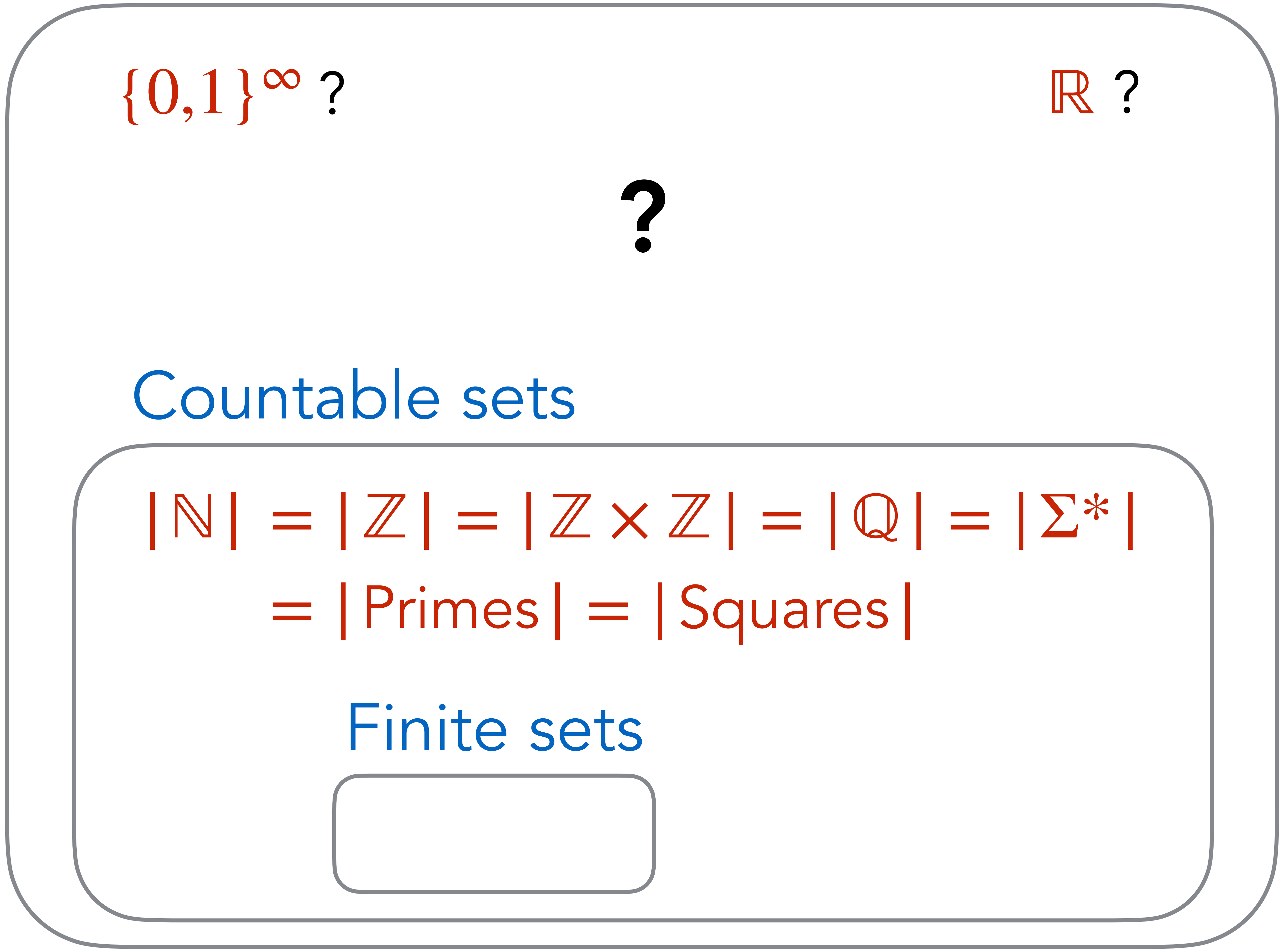
Let $\Sigma = \{0, 1, \ldots, 9, x, +, -, *, /, \hat{}\}$.

Every polynomial can be described by a finite-length string over Σ.

e.g. x^3 – 1/4x^2 + 6x – 22/7

So $\mathbb{Q}[x]$ is encodable/countable.

The picture so far



Great Idea #1:

Use injections/surjections/bijections to compare sets.

Great Idea #2:

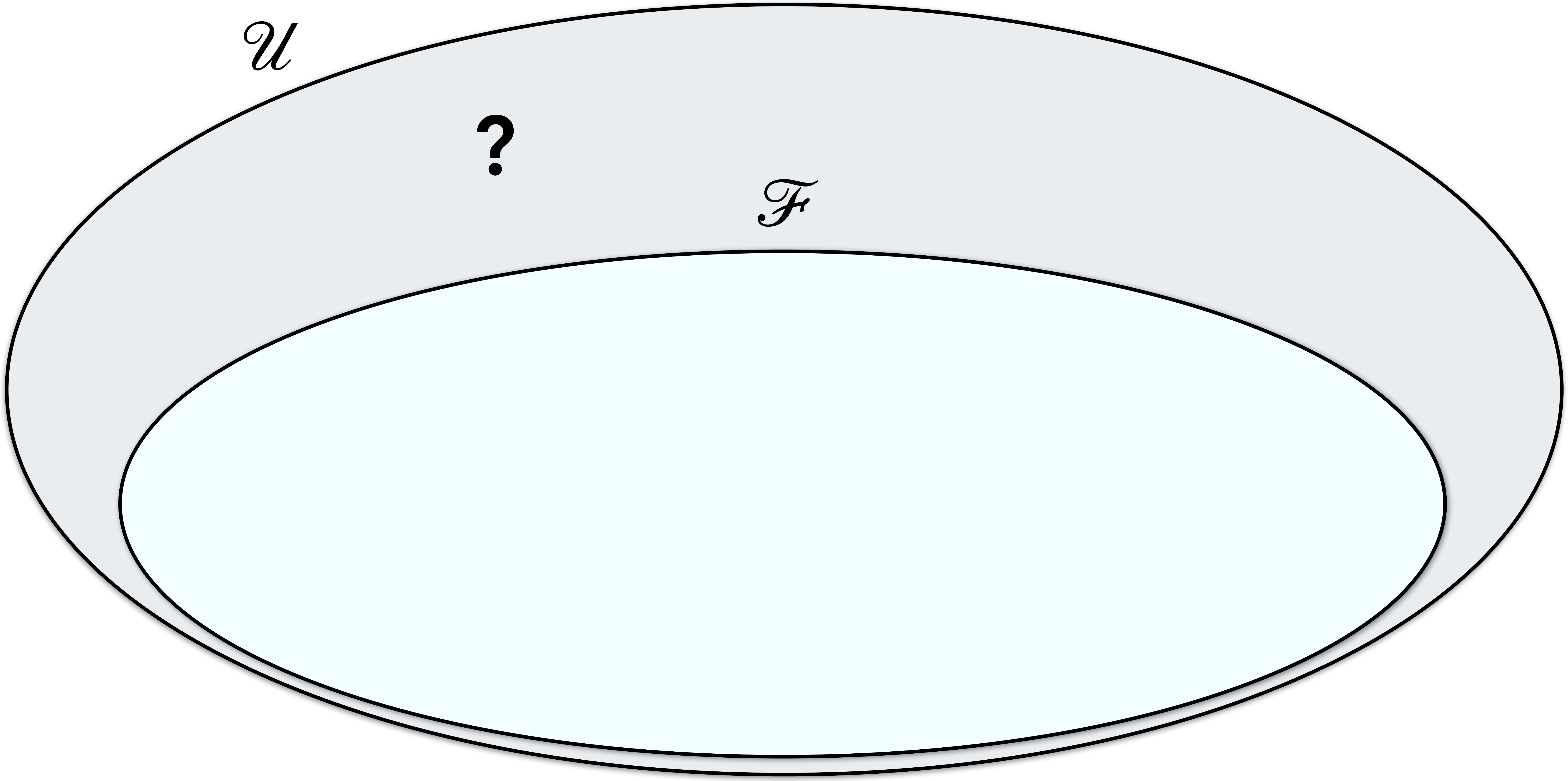
Diagonalization proof technique.

Great Idea #2:

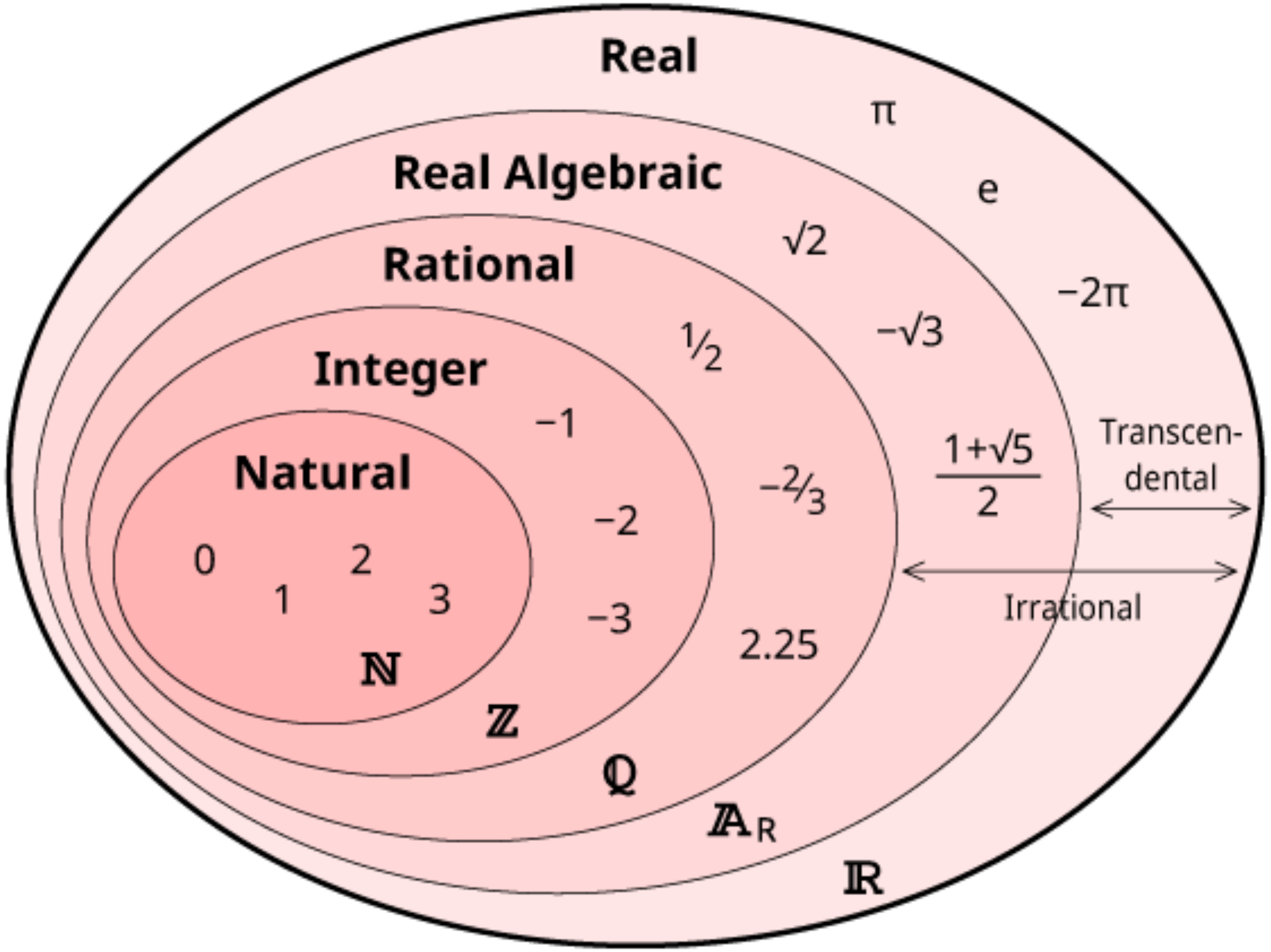
Diagonalization proof technique.

Motivation

Given a set of objects $\mathscr{F}$, can we construct an object not in $\mathscr{F}$?

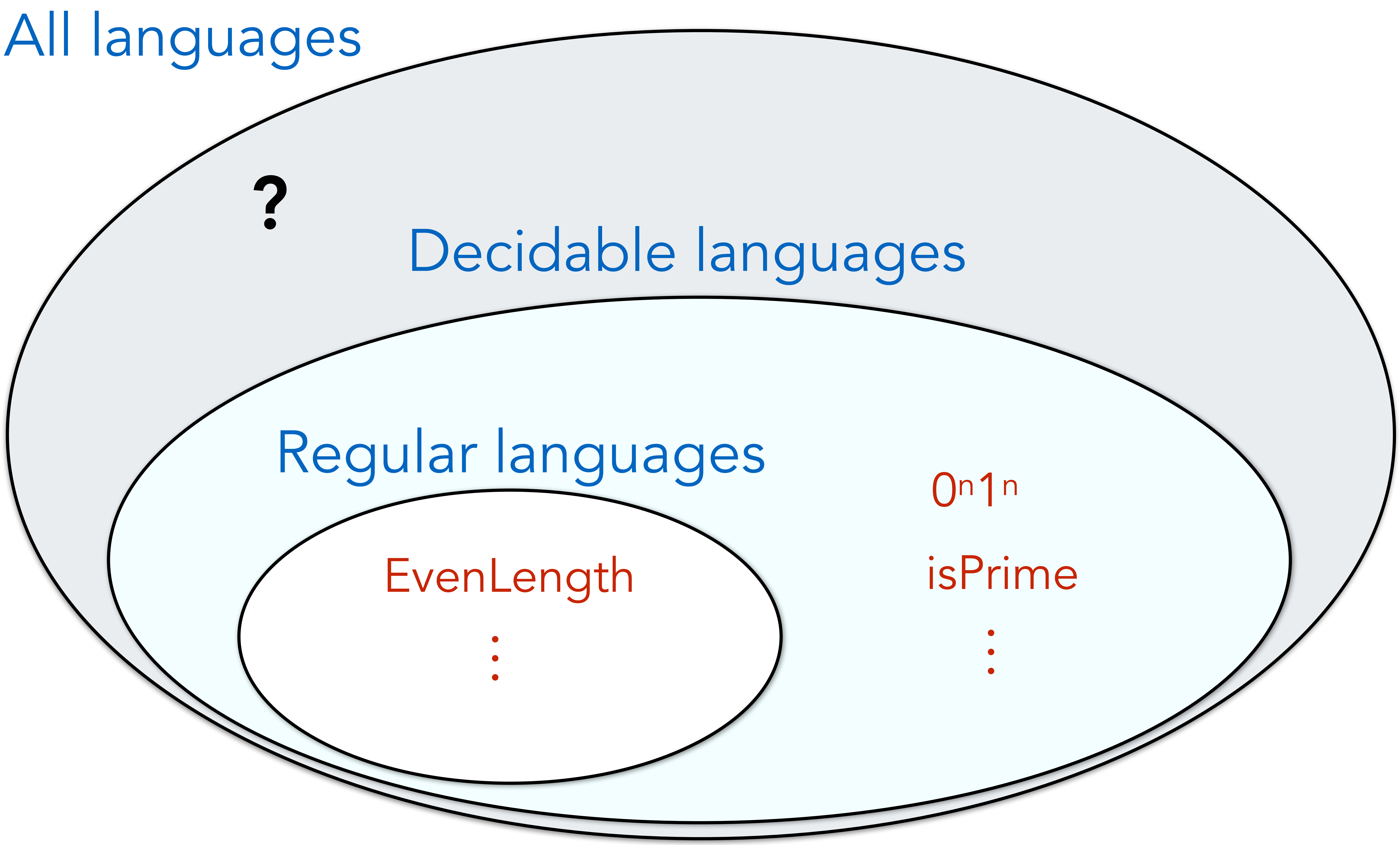


Motivation



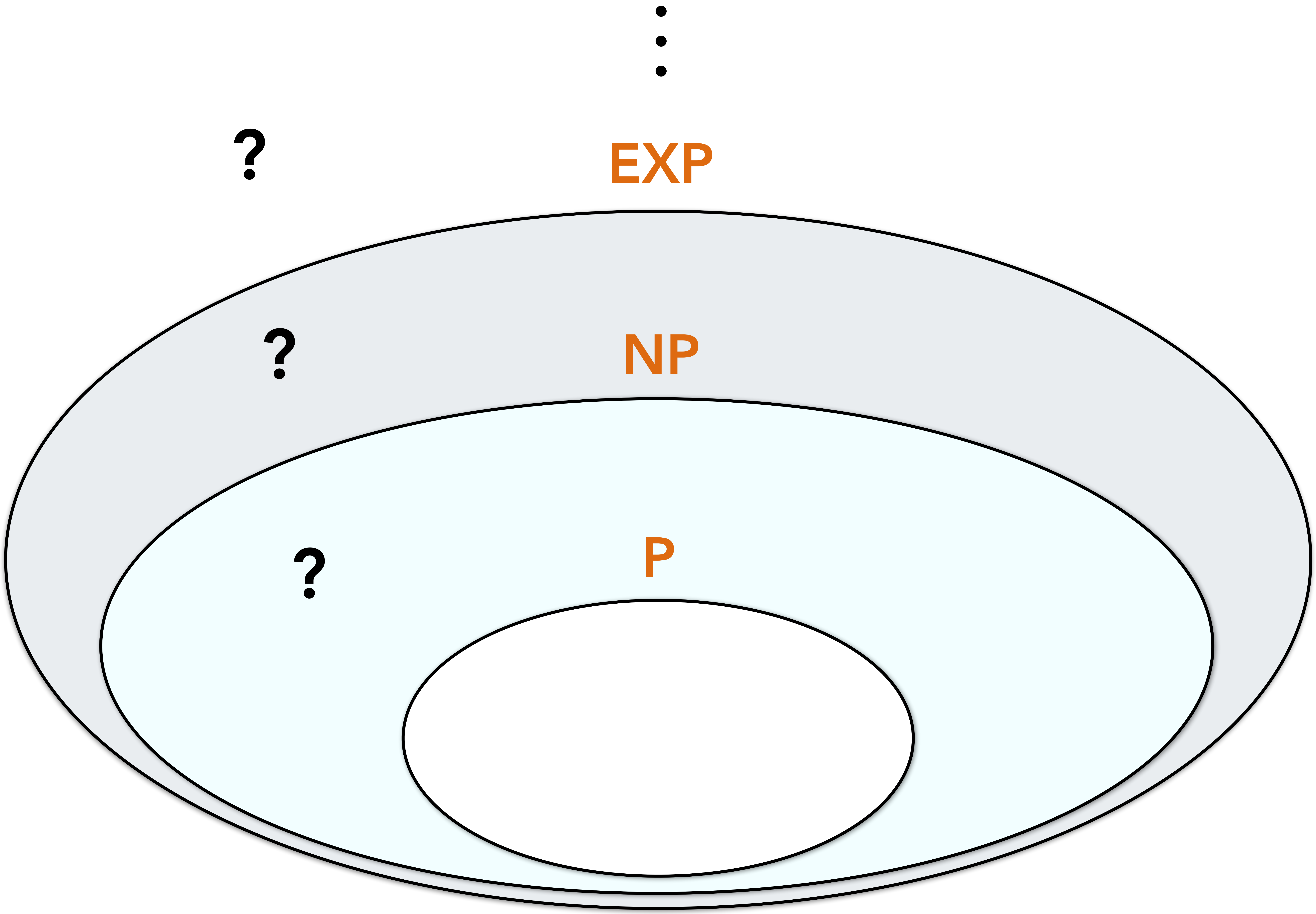
Real
Real Algebraic
Rational
Integer
Natural
π
e
√2
−2π
−√3
½
−1
1+√5
2
Transcen-
dental
−⅔
−2
0
2
1
3
−3
Irrational
2.25
ℕ
ℤ
ℚ
𝔸R
ℝ

Motivation

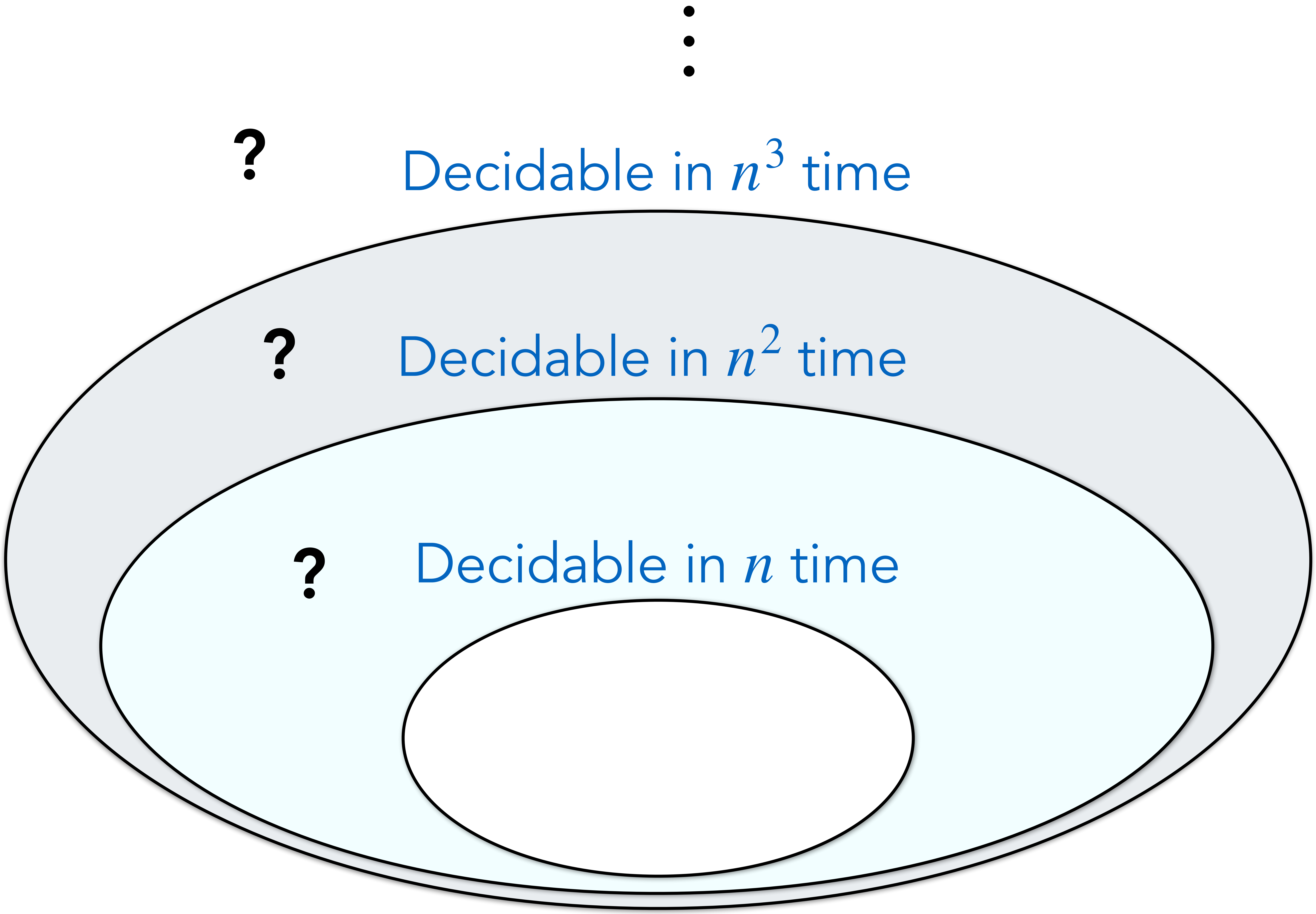


All languages
?
Decidable languages
Regular languages
0n1n
isPrime
EvenLength

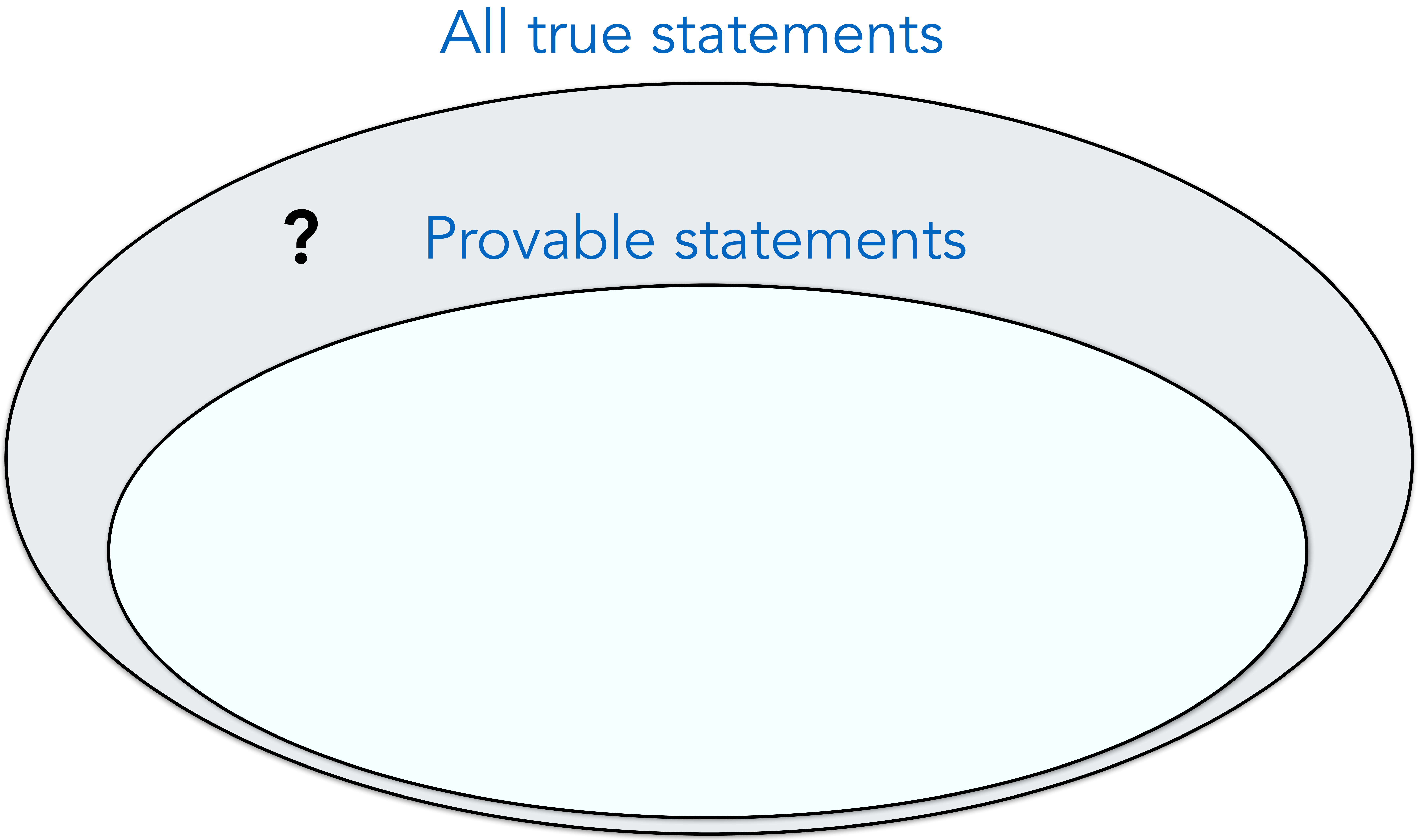
Motivation



Motivation

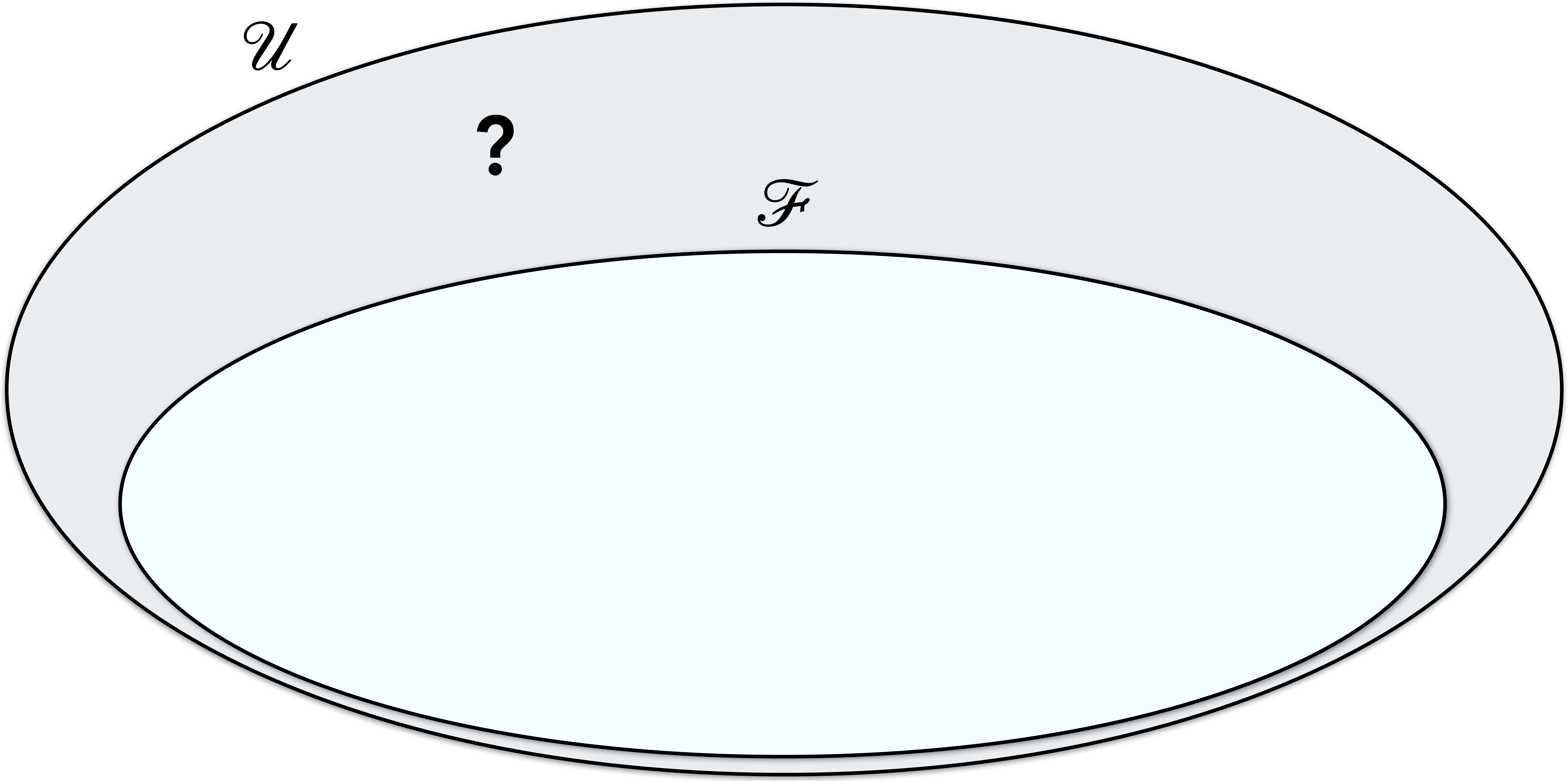

⋮
?
Decidable in n^3 time
?
Decidable in n^2 time
?
Decidable in n time

Motivation



Motivation

? Given a set of objects $\mathscr{F}$, can we construct an object not in $\mathscr{F}$?



Motivation

Given a set of objects $\mathscr{F}$, can we construct an object not in $\mathscr{F}$?

<u>Goal:</u> Find a general technique applicable to various $\mathscr{F}$.

Motivation

? **Given a set of functions $\mathscr{F}$, can we construct a function not in $\mathscr{F}$?**

Goal: Find a general technique applicable to various $\mathscr{F}$.

N Most objects can be conveniently viewed as a function.

N Most objects can be conveniently viewed as a function.

Sets as functions

$$S \subseteq X \quad \longleftrightarrow \quad f_S : X \to \{0, 1\} \qquad f_S(x) = \begin{cases} 1 & \text{if } x \in S \\ 0 & \text{otherwise} \end{cases}$$

e.g. $$\mathbb{P} \subseteq \mathbb{N} \quad \longleftrightarrow \quad f_{\mathbb{P}} : \mathbb{N} \to \{0, 1\} \qquad f_{\mathbb{P}}(n) = \begin{cases} 1 & \text{if } n \text{ is prime} \\ 0 & \text{otherwise} \end{cases}$$

Numbers as functions

$$r \in [0, 1] \quad \longleftrightarrow \quad f_r : \mathbb{N} \to \{0, 1\} \qquad r = 0.\, f(0)\, f(1)\, f(2)\, f(3)\ \ldots$$

e.g. $$r = 0.110110\ldots \quad \longleftrightarrow \quad f_r(0) = 1, \quad f_r(1) = 1, \quad f_r(2) = 0,$$

$$f_r(3) = 1, \quad f_r(4) = 1, \quad f_r(5) = 0, \quad \ldots$$

Great Idea #2:

Diagonalization proof technique.

- Part 1: Diagonalization with finite $\mathscr{F}$.

Let $\mathscr{F}$ be a set of functions $f : X \to \{0,1\}$.

If $|X| \geq |\mathscr{F}|$, can construct $f_D : X \to \{0,1\}$ not in $\mathscr{F}$.

Inputs X

Functions $\mathscr{F}$

	x_1	x_2	x_3	x_4
f_1	[0]	0	1	0
f_2	1	[1]	1	0
f_3	1	0	[0]	0
f_4	1	0	1	[1]
f_D	**1**	**0**	**1**	**0**

Given:

A set $\mathscr{F}$ of functions $f : X \to \{0,1\}$

Goal:

Construct a function f_D different from each $f \in \mathscr{F}$.

How:

$\forall f \in \mathscr{F}$, pick an input $x \in X$, and make $f_D(x) \neq f(x)$.

Careful:

$\forall f \in \mathscr{F}$, pick a different x.

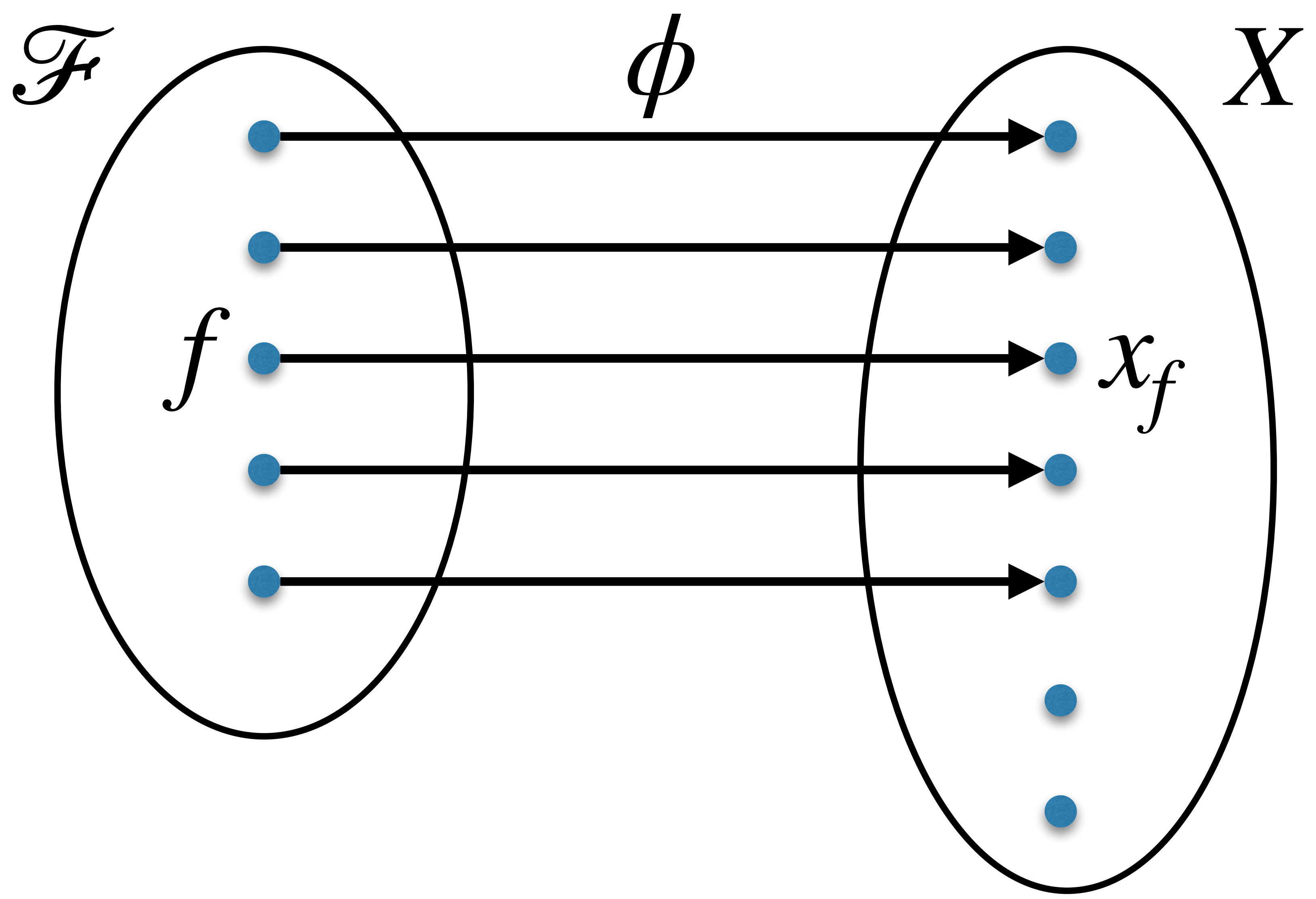
Condition needed:

$|X| \geq |\mathscr{F}|$

Diagonalization Lemma:

Let $\mathscr{F}$ be a set of functions $f : X \to \{0,1\}$.

If $|X| \geq |\mathscr{F}|$, we can construct $f_D : X \to \{0,1\}$ not in $\mathscr{F}$.



$\forall f \in \mathscr{F}$:

- pick a unique $x_f \in X$,
- let $f_D(x_f) \neq f(x_f)$.

Corollary:

Let $\mathscr{F}$ be the set of **all** functions $f : X \to \{0,1\}$.

Then $|X| < |\mathscr{F}| = 2^{|X|}$.

Great Idea #2:

Diagonalization proof technique.

- Part 1: Diagonalization with finite sets.
- Part 2: Diagonalization with **infinite** sets.

Diagonalization Lemma:

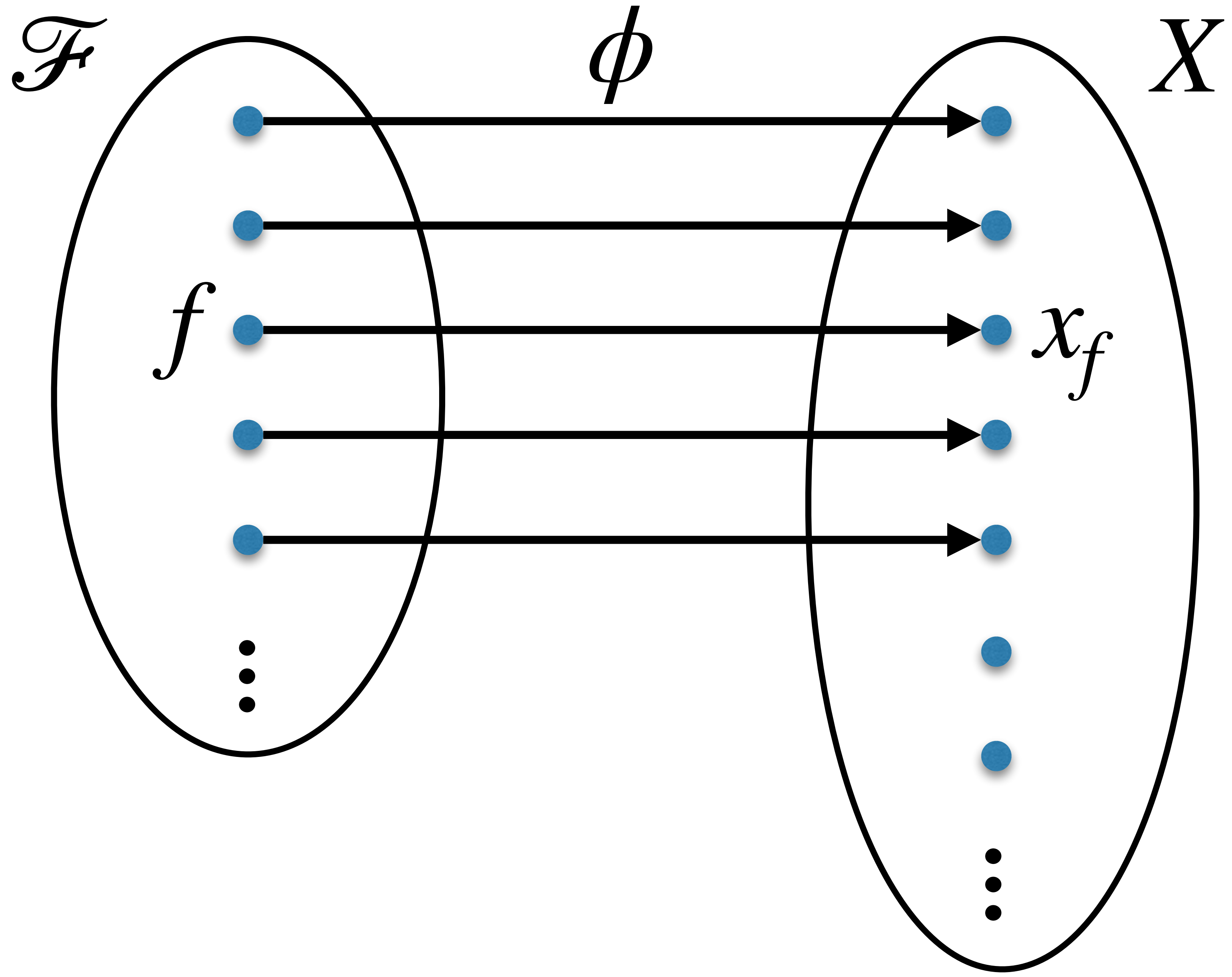
Let $\mathscr{F}$ be a set of functions $f : X \to \{0,1\}$.

If $|X| \geq |\mathscr{F}|$, we can construct $f_D : X \to \{0,1\}$ not in $\mathscr{F}$.

Diagonalization Lemma:

Let X be any set. Let $\mathscr{F}$ be a any set of functions $f : X \to \{0,1\}$.

If $|X| \geq |\mathscr{F}|$, we can construct $f_D : X \to \{0,1\}$ not in $\mathscr{F}$.



$\forall f \in \mathscr{F}$, let $f_D(x_f) \neq f(x_f)$.

Definition: $\mathbf{F}(X)$ = set of **all** functions $f : X \to \{0,1\}$.

Corollary (Cantor's Theorem): For every set X, $|X| < |\mathbf{F}(X)|$.

Cantor's Theorem

$\mathbf{F}(X)$ = set of **all** functions $f : X \to \{0,1\}$

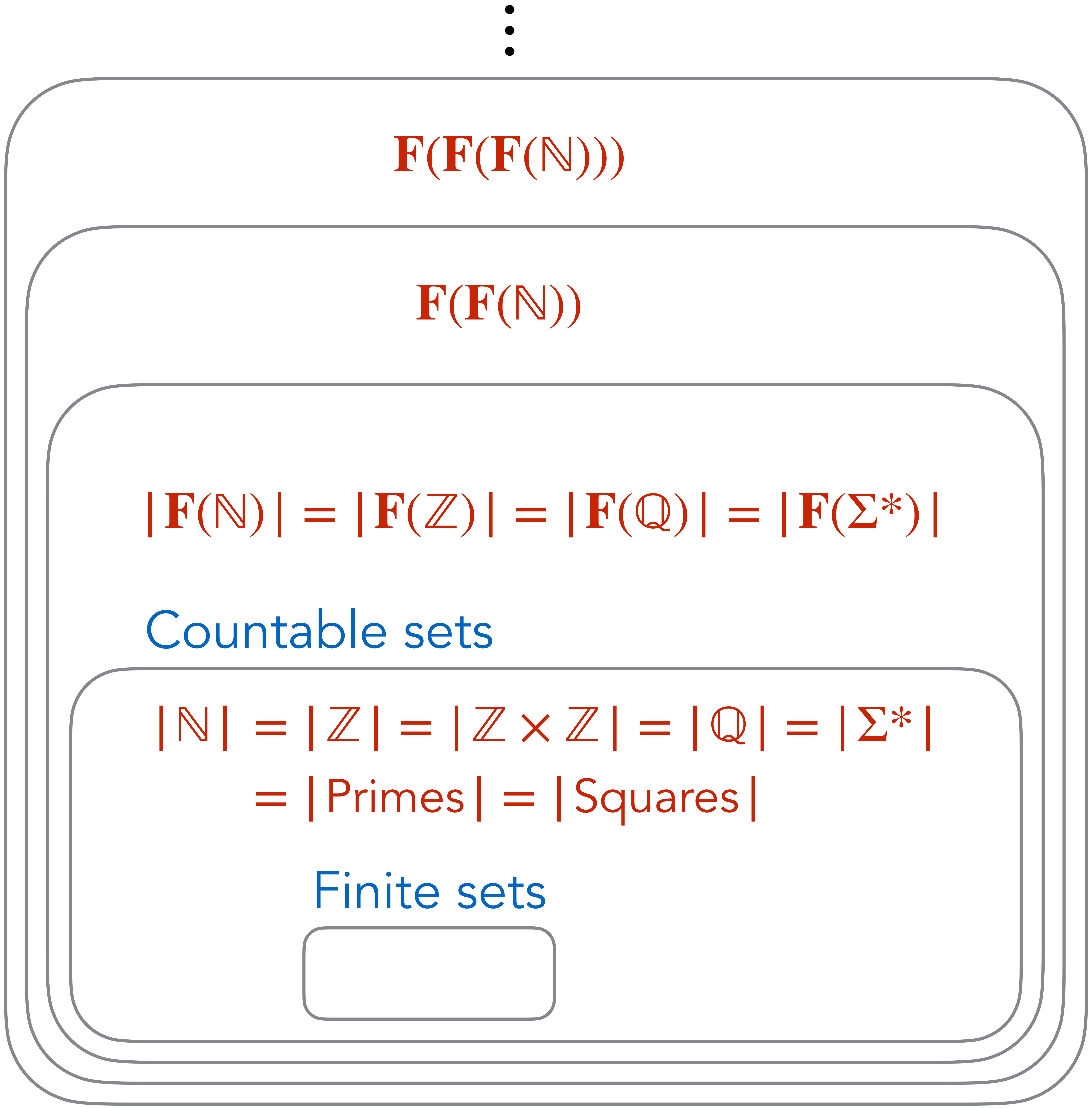
Cantor's Theorem: For every set X, $|X| < |\mathbf{F}(X)|$.

Corollary 1: $|\mathbb{N}| < |\mathbf{F}(\mathbb{N})|$, i.e. $\mathbf{F}(\mathbb{N})$ is uncountable.

Corollary 2: $|\Sigma^*| < |\mathbf{F}(\Sigma^*)|$, i.e. $\mathbf{F}(\Sigma^*)$ is uncountable.

$$|\mathbb{N}| < |\mathbf{F}(\mathbb{N})| < |\mathbf{F}(\mathbf{F}(\mathbb{N}))| < |\mathbf{F}(\mathbf{F}(\mathbf{F}(\mathbb{N})))| < \cdots$$

an infinity of infinities...



⋮
F(F(F(ℕ)))
F(F(ℕ))
|F(ℕ)| = |F(ℤ)| = |F(ℚ)| = |F(Σ*)|
Countable sets
|ℕ| = |ℤ| = |ℤ × ℤ| = |ℚ| = |Σ*|
= |Primes| = |Squares|
Finite sets

An Interesting Question

Is there a set S such that

$|\mathbb{N}| < |S| < |\mathbf{F}(\mathbb{N})|$?

Continuum Hypothesis:
No such set exists.

(Hilbert's 1st problem)

Diagonalization Lemma:

Let X be any set. Let $\mathscr{F}$ be a any set of functions $f : X \to \{0,1\}$.

If $|X| \geq |\mathscr{F}|$, we can construct $f_D : X \to \{0,1\}$ not in $\mathscr{F}$.

N This is called "diagonalization against $\mathscr{F}$".

! Diagonalization produces an explicit f_D outside $\mathscr{F}$.

N You can pretty much view anything as a function.

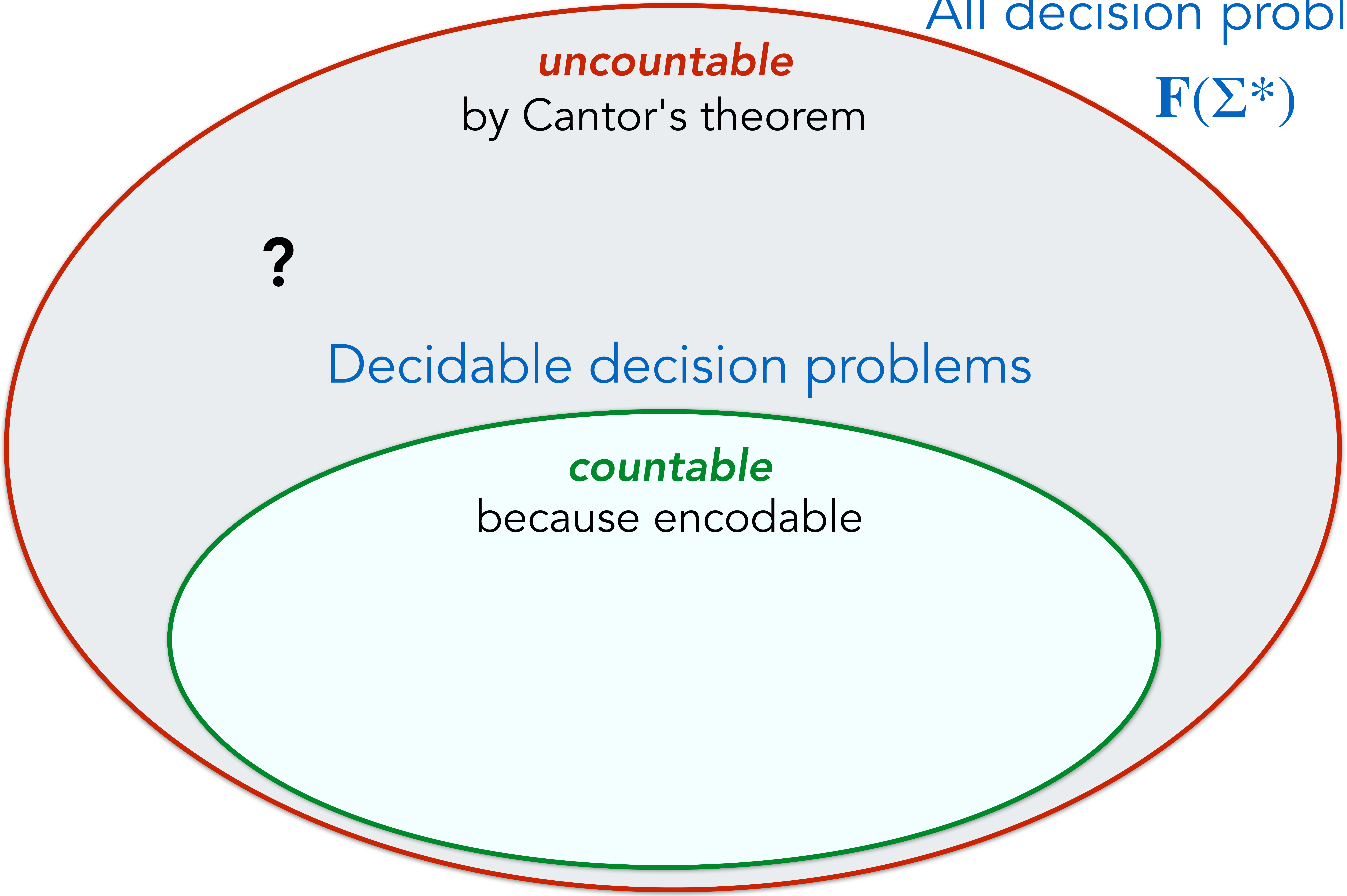
N The range need not be $\{0,1\}$.

Limits of Computation:
The Finite vs The Infinite

Finite		**Countably infinite**		**Uncountable**
finite set	*vs*	infinite set		
		finite descriptions of elements	*vs*	infinite descriptions of elements

All decision problems $f: \Sigma^* \rightarrow \{0,1\}$

$\mathbf{F}(\Sigma^*)$



Encoding of a **decidable** decision problem f: $\langle M \rangle$ (where TM M solves f)

All decision problems $f : \Sigma^* \rightarrow \{0,1\}$

$\mathbf{F}(\Sigma^*)$

Decidable

So are we doomed?

What is an explicit undecidable decision problem?

$\mathcal{F}$ = set of all (semi)-decidable $f : \Sigma^* \to \{0,1\}$.

$|\mathcal{F}| = |\Sigma^*|$.

Diagonalizing against $\mathcal{F}$ spits out undecidable f_D.

Don't forget about me!

The story continues next lecture…