Key Questions in Theory of Computation

- What problems can you solve with a computer?
  - Computability Theory
- Why are some problems harder to solve than others?
  - Complexity Theory
- How can we be certain in our answers to these questions?
  - Discrete Mathematics

Introduction to Set Theory

“CS103 students”

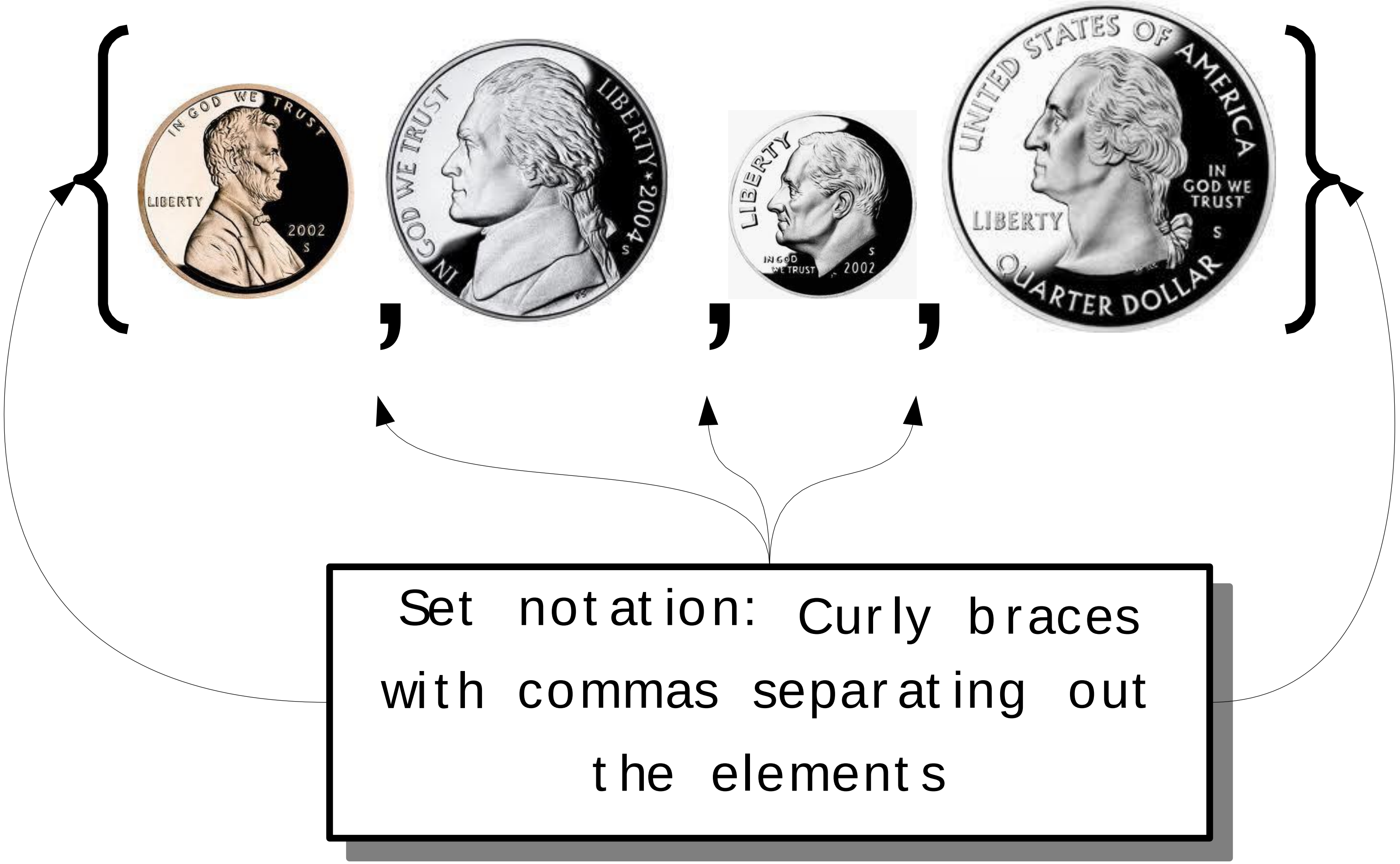
“All the computers on the Stanford network”

“Cool people”

“The chemical elements”

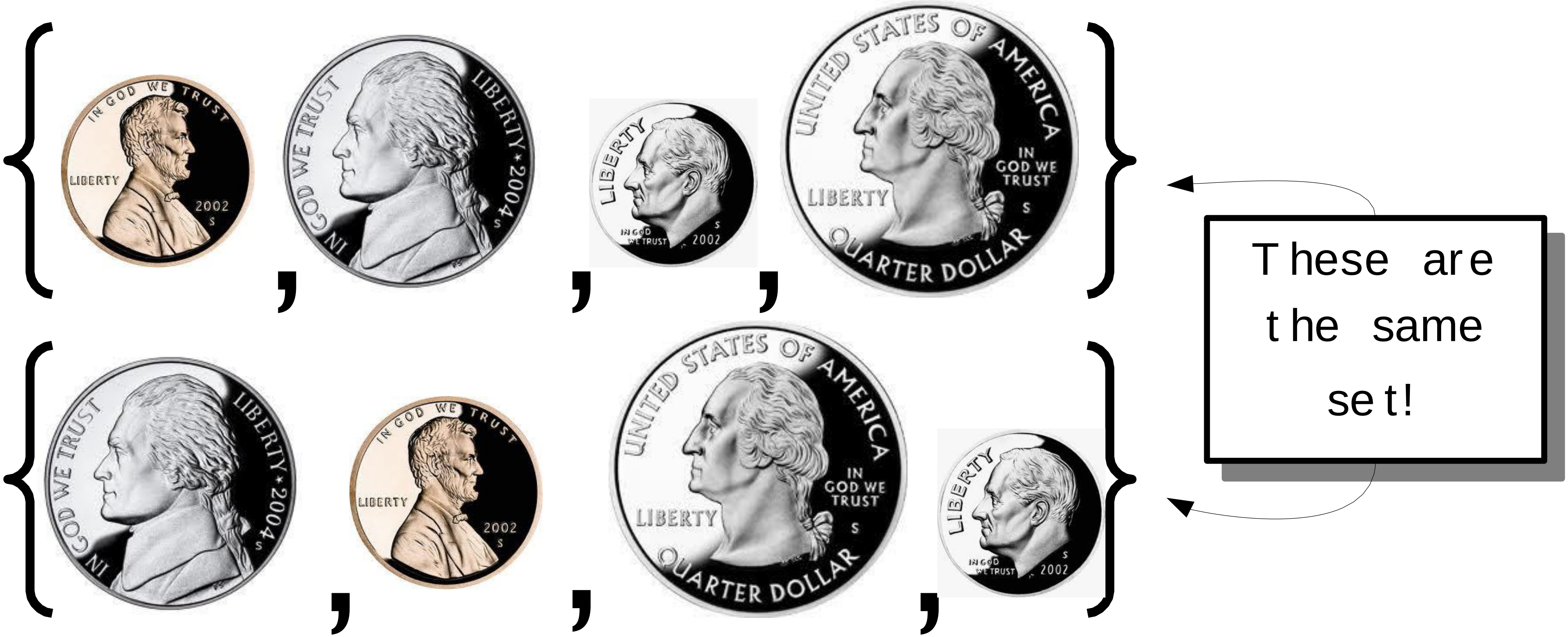
“Cute animals”

“US coins”



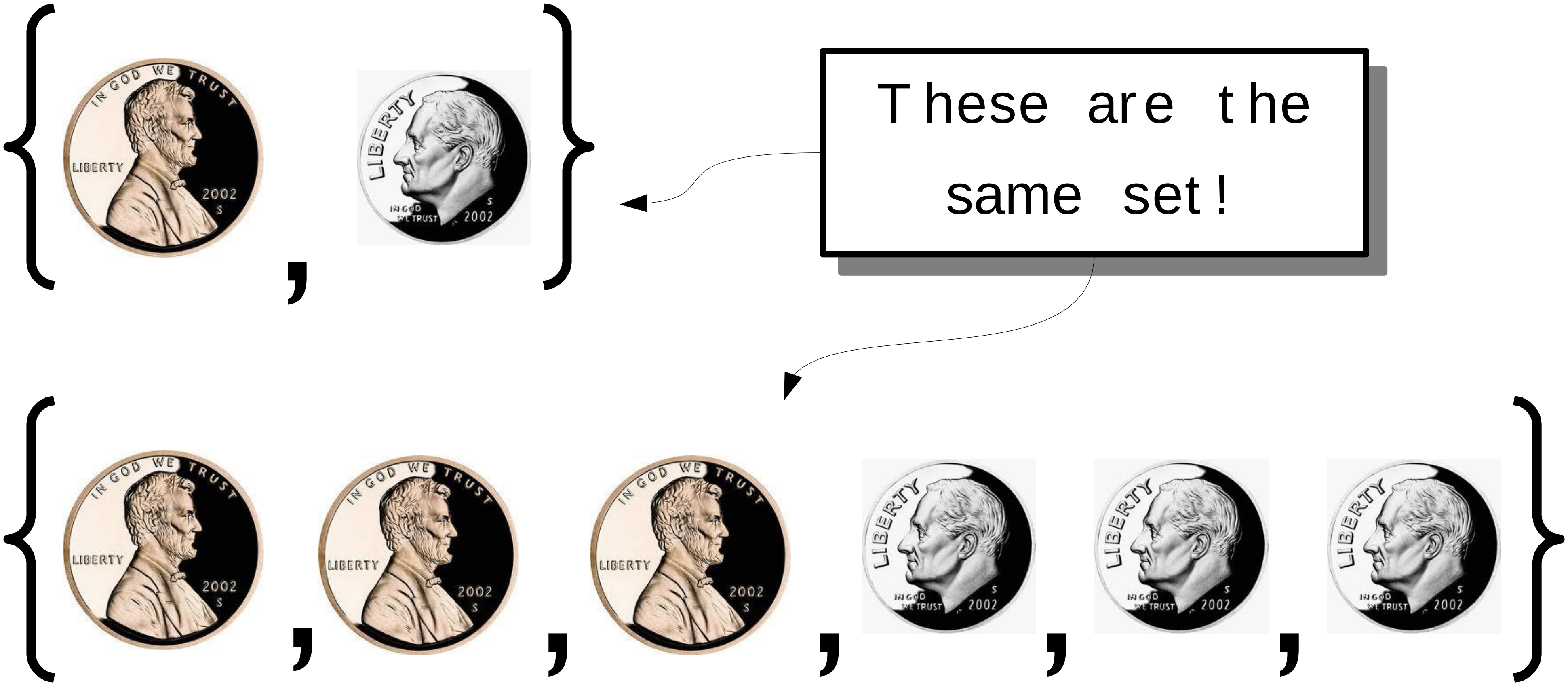
Set notation: Curly braces with commas separating out the elements

A ***set*** is an unordered collection of distinct objects, which may be anything (including other sets).



These are the same set!

A ***set*** is an unordered collection of distinct objects, which may be anything (including other sets).



These are the same set!

A ***set*** is an unordered collection of distinct objects, which may be anything (including other sets).

$$\{ \quad \} \quad = \quad \emptyset$$

The **empty set** contains no elements.

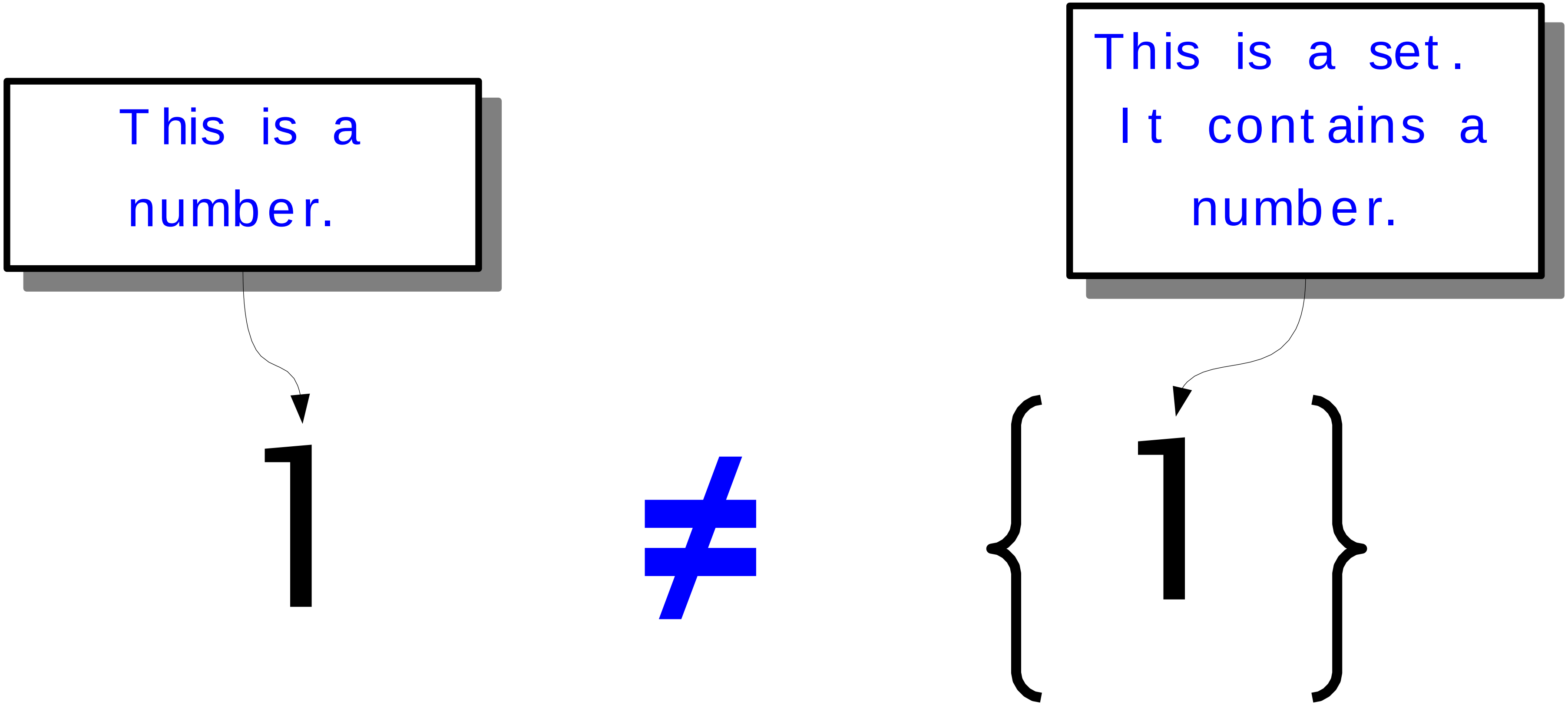
We use this symbol to denote the empty set.

A ***set*** is an unordered collection of distinct objects, which may be anything (including other sets).

This set has one element, which happens to be the empty set.

$$\emptyset \neq \{\emptyset\}$$

Are these equal to one another?



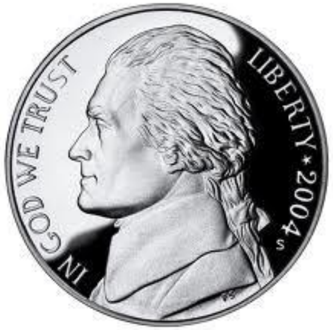
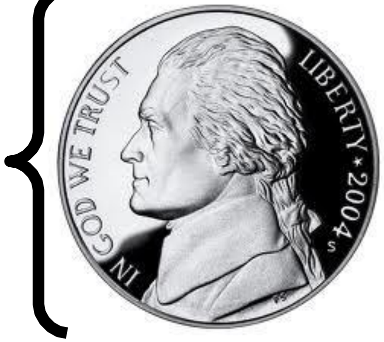
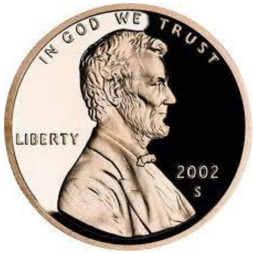
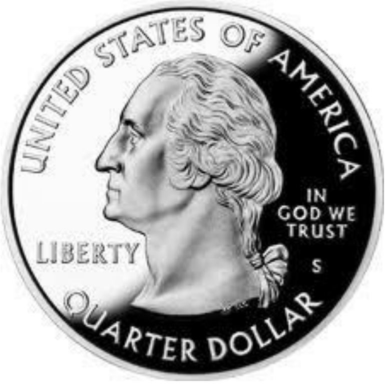
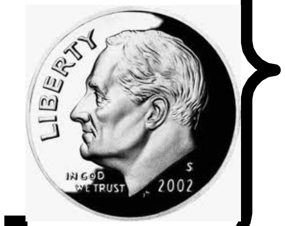
This is a number.

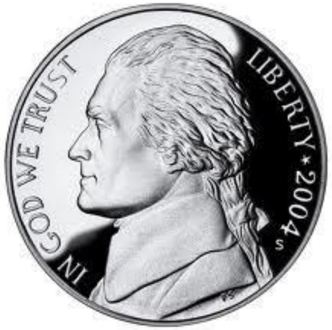
This is a set. It contains a number.

$$1 \neq \{1\}$$

Are these equal to one another?

Set Membership

 $\in$ $\{$ , , ,  $\}$

Is  in this set?

Set Membership

$\notin \{$, , , $\}$

Is in this set?

Set Membership

- Given a set S and an object x, we write
  $$\boldsymbol{x \in S}$$
  if x is contained in S, and
  $$\boldsymbol{x \notin S}$$
  otherwise.
- If $x \in S$, we say that x is an ***element*** of S.
- Given any object x and any set S, either $x \in S$ or $x \notin S$.

Infinite Sets

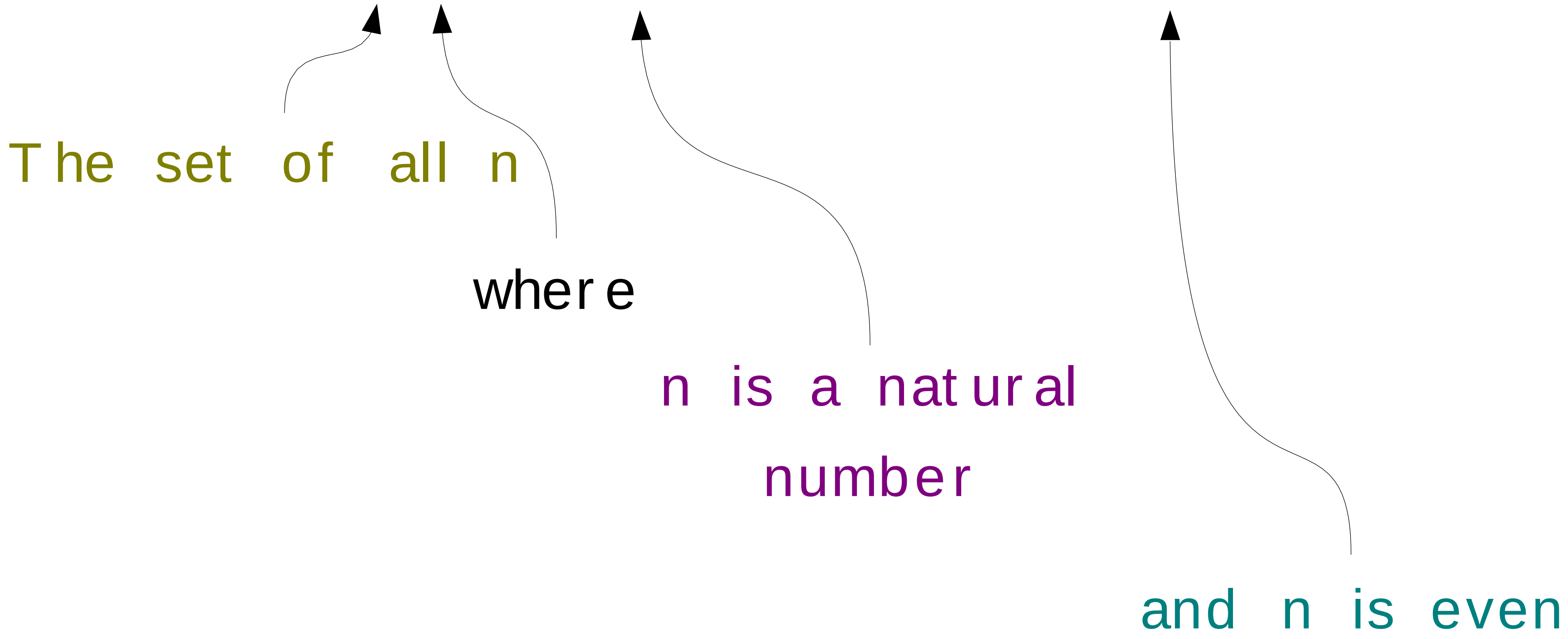
- Some sets contain *infinitely many* elements!
- The set $\mathbb{N} = \{ 0, 1, 2, 3, \ldots \}$
  - the set of all the ***natural numbers***.
  - Some mathematicians don't include zero; in this class, assume that 0 is a natural number.
- The set $\mathbb{Z} = \{ \ldots, -2, -1, 0, 1, 2, \ldots \}$
  - the set of all the ***integers***.
  - Z is from German "Zahlen."
- The set $\mathbb{R} = \{2.712, 3.1415\ldots, 4, -10\}$
  - the set of all ***real numbers***

Describing Complex Sets

- Some English descriptions of infinite sets:
  - “The set of all even numbers.”
  - “The set of all real numbers less than 137.”
  - “The set of all negative integers.”
- To describe complex sets like these mathematically, we'll use ***set-builder notation***.

Even Natural Numbers

$$\{\ n \mid n \in \mathbb{N} \text{ and } n \text{ is even } \}$$



The set of all n

where

n is a natural number

and n is even

$$\{\ 0, 2, 4, 6, 8, 10, 12, 14, 16, \ldots\ \}$$

Set Builder Notation

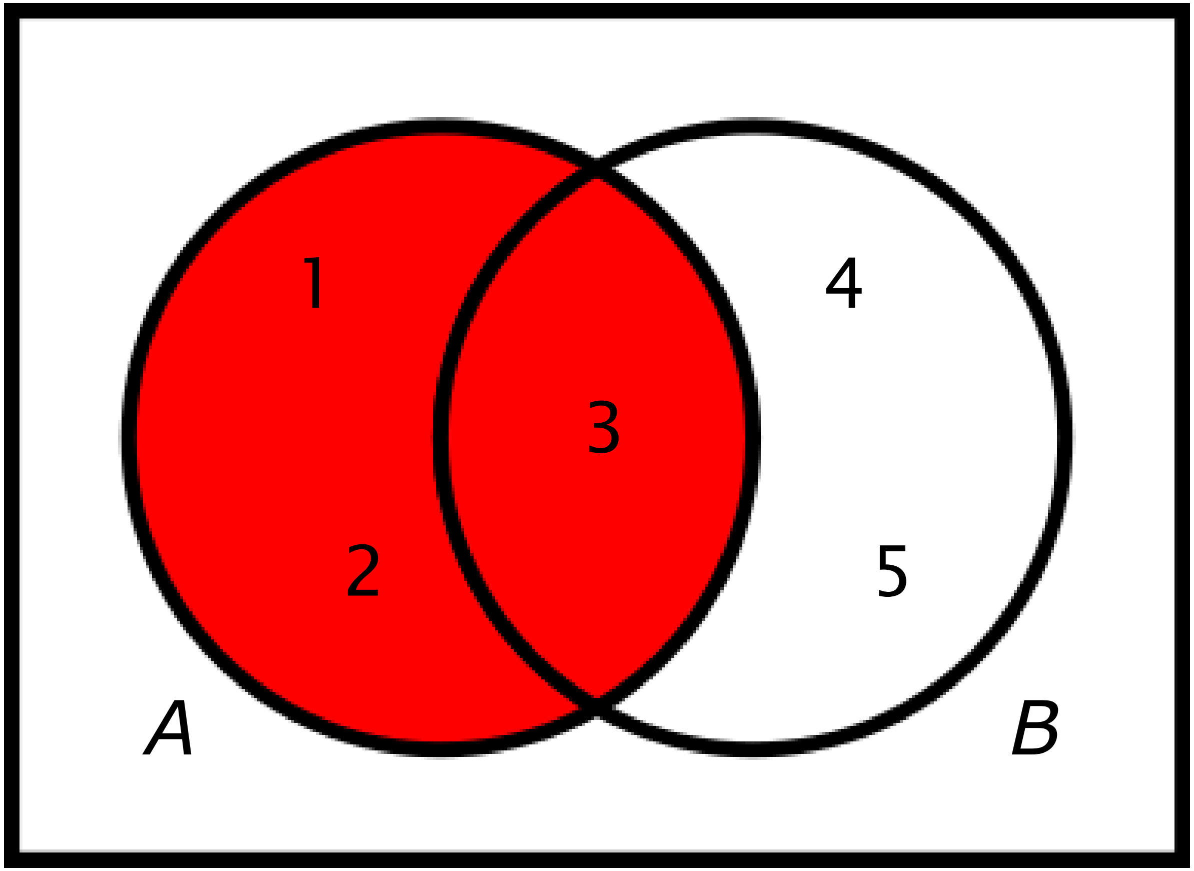
- A set may be specified in ***set-builder notation***:

  { x | *some property x satisfies* }

- For example:
  - { $r \mid r \in \mathbb{R}$ and $r < 137$ }
  - { n | n is an even natural number }
  - { S | S is a set of US currency }
  - { a | a is cute animal }

Combining Sets

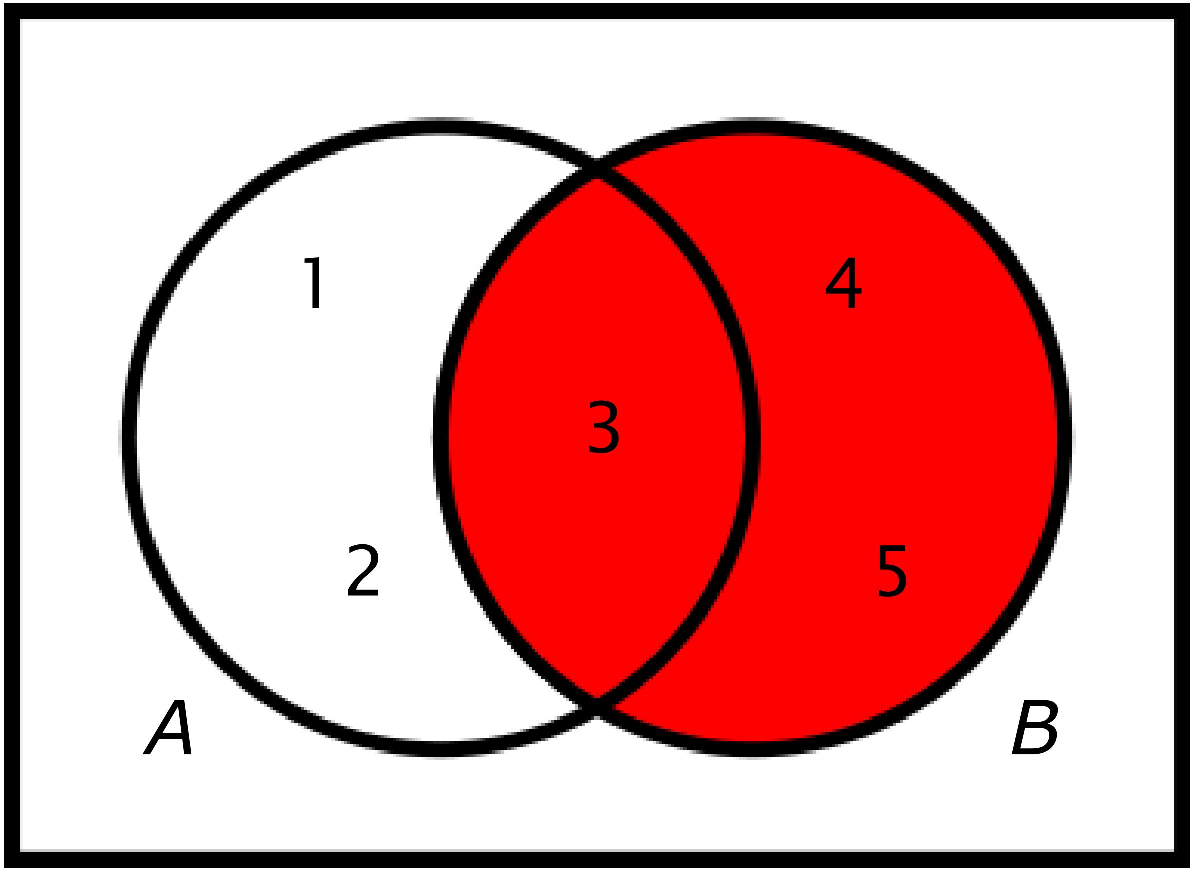
Venn Diagrams



A

A = { 1, 2, 3 }
B = { 3, 4, 5 }

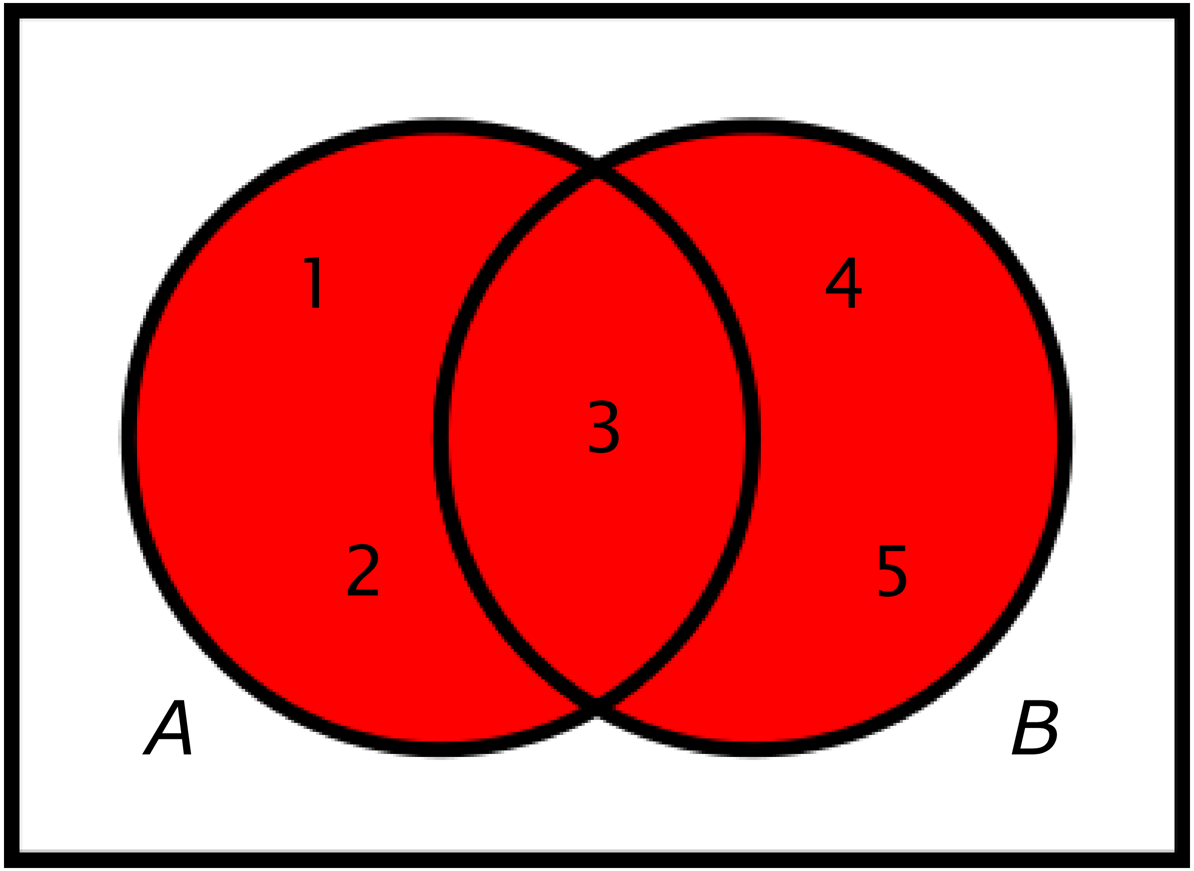
Venn Diagrams



B

$A = \{\ 1, 2, 3\ \}$
$B = \{\ 3, 4, 5\ \}$

Venn Diagrams



Union

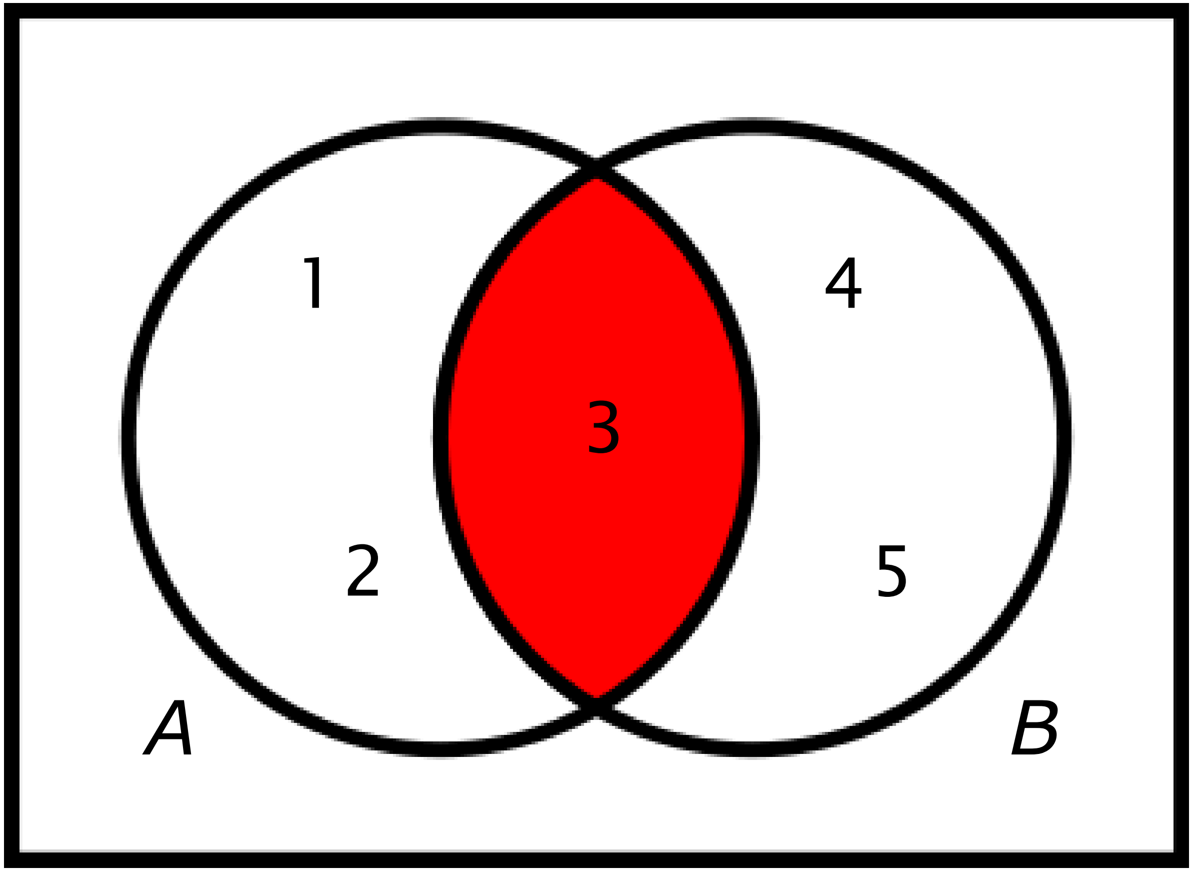
$A \cup B$

{ 1, 2, 3, 4, 5 }

$A = \{ 1, 2, 3 \}$

$B = \{ 3, 4, 5 \}$

Venn Diagrams



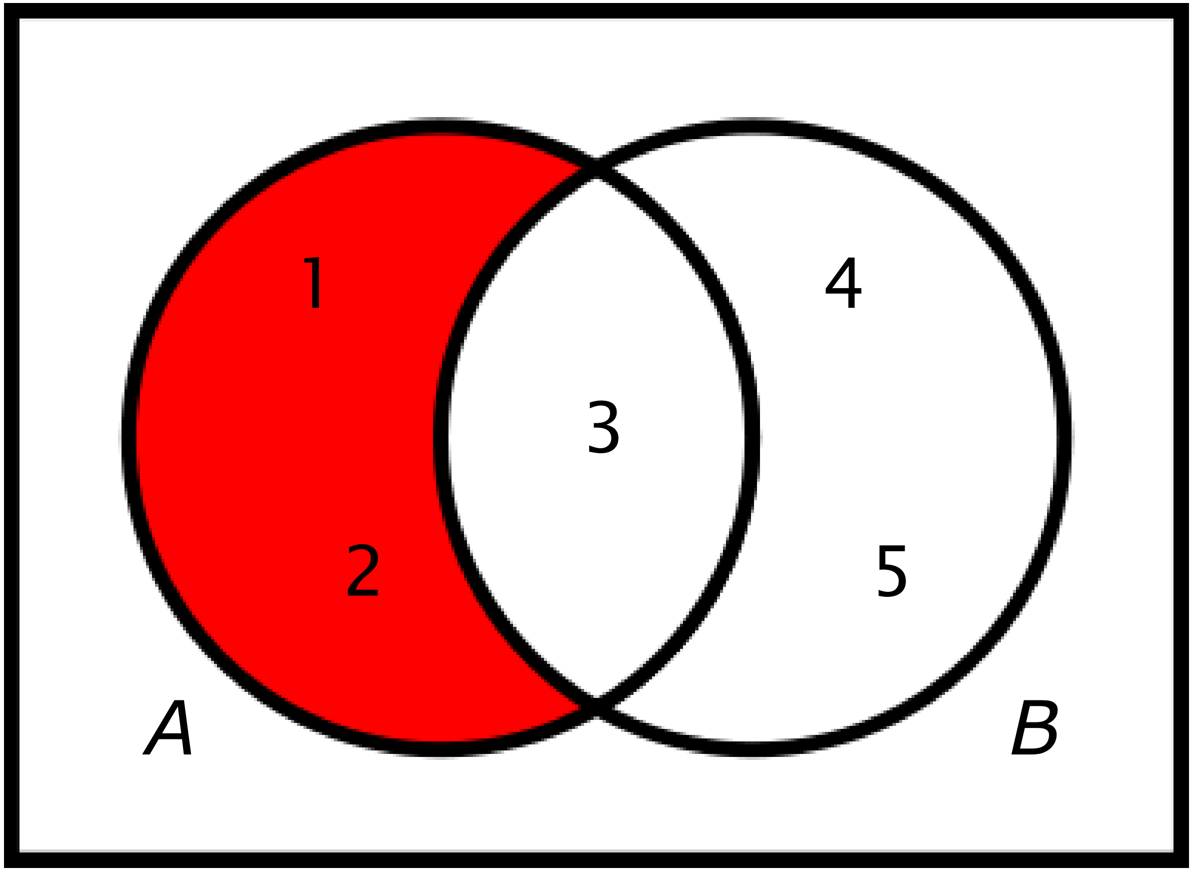
Intersection

$A \cap B$

{ 3 }

$A = \{\ 1, 2, 3\ \}$
$B = \{\ 3, 4, 5\ \}$

Venn Diagrams



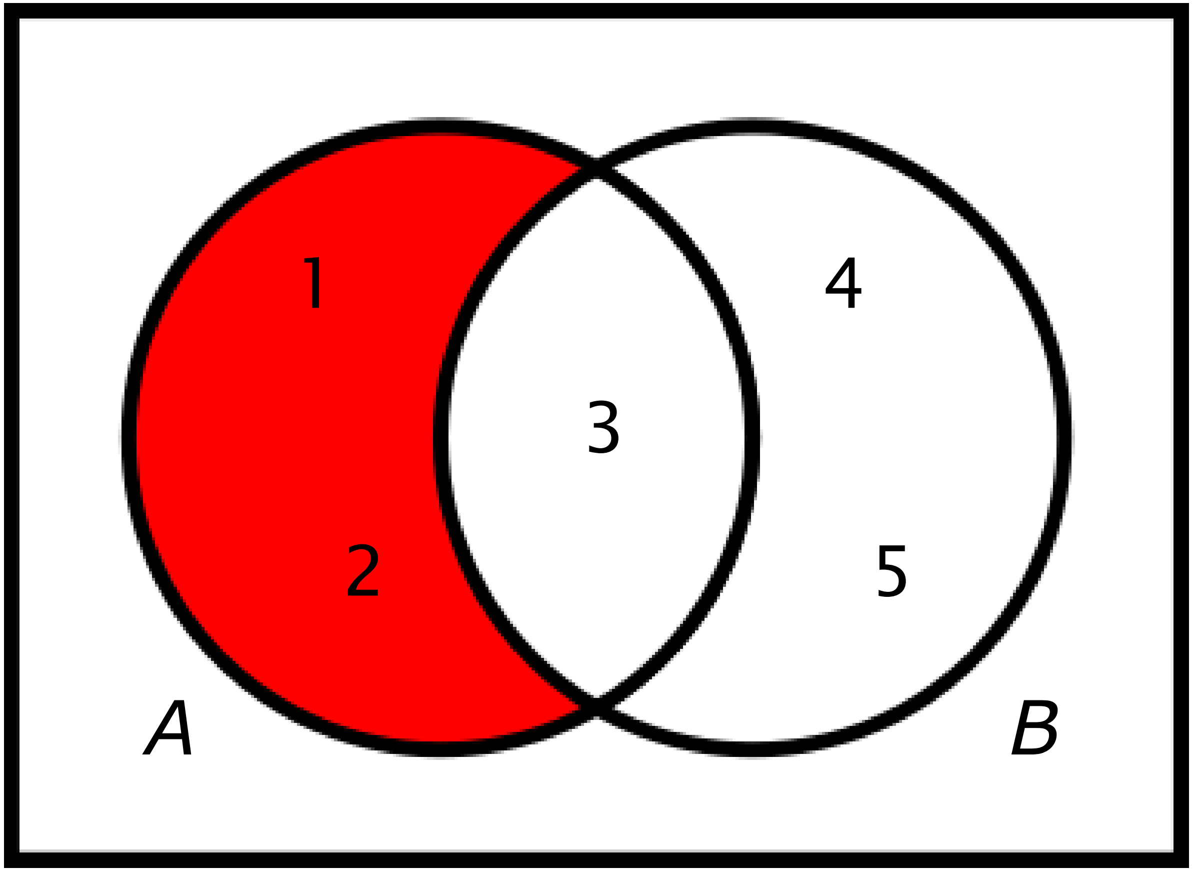
Difference

$A - B$

$\{\ 1, 2\ \}$

$A = \{\ 1, 2, 3\ \}$
$B = \{\ 3, 4, 5\ \}$

Venn Diagrams



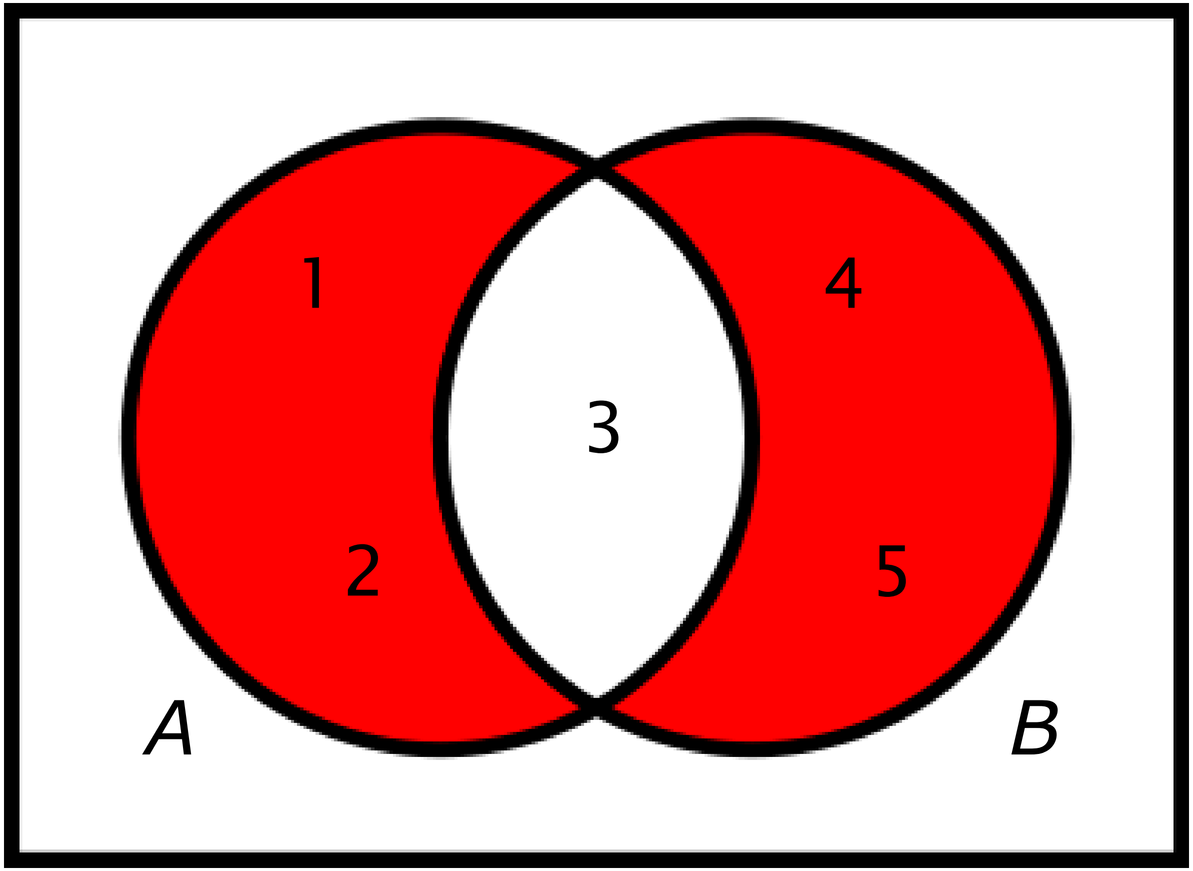
Difference

A ₩ *B*

{ 1, 2 }

A = { 1, 2, 3 }
B = { 3, 4, 5 }

Venn Diagrams



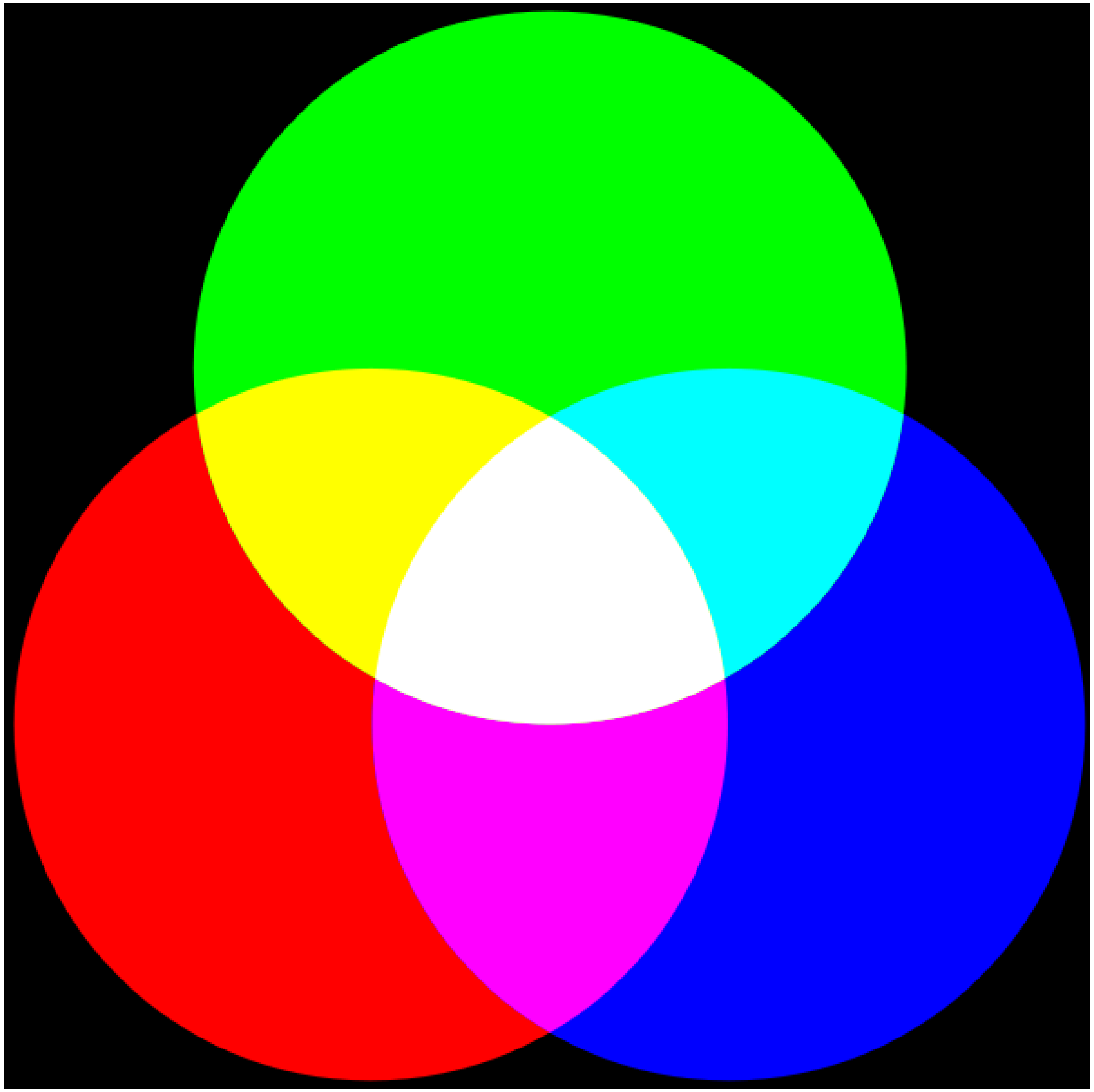
Symmetric Difference

$A \Delta B$

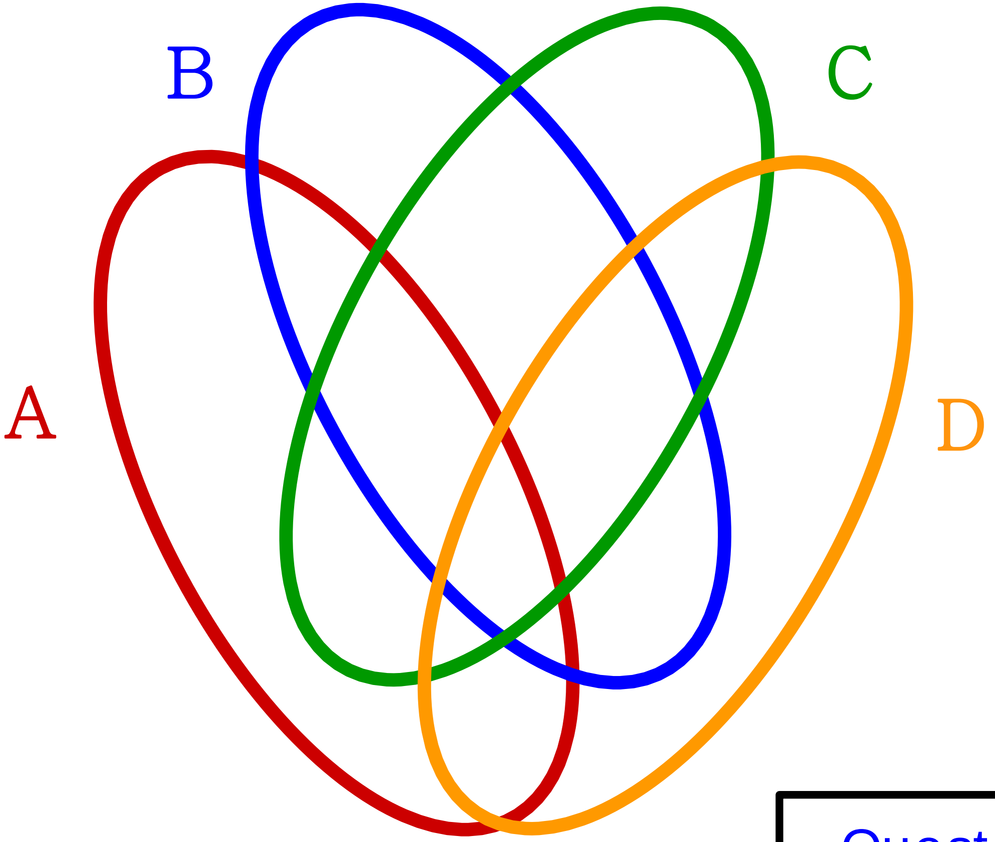
{ 1, 2, 4, 5 }

A = { 1, 2, 3 }
B = { 3, 4, 5 }

Venn Diagrams for Three Sets

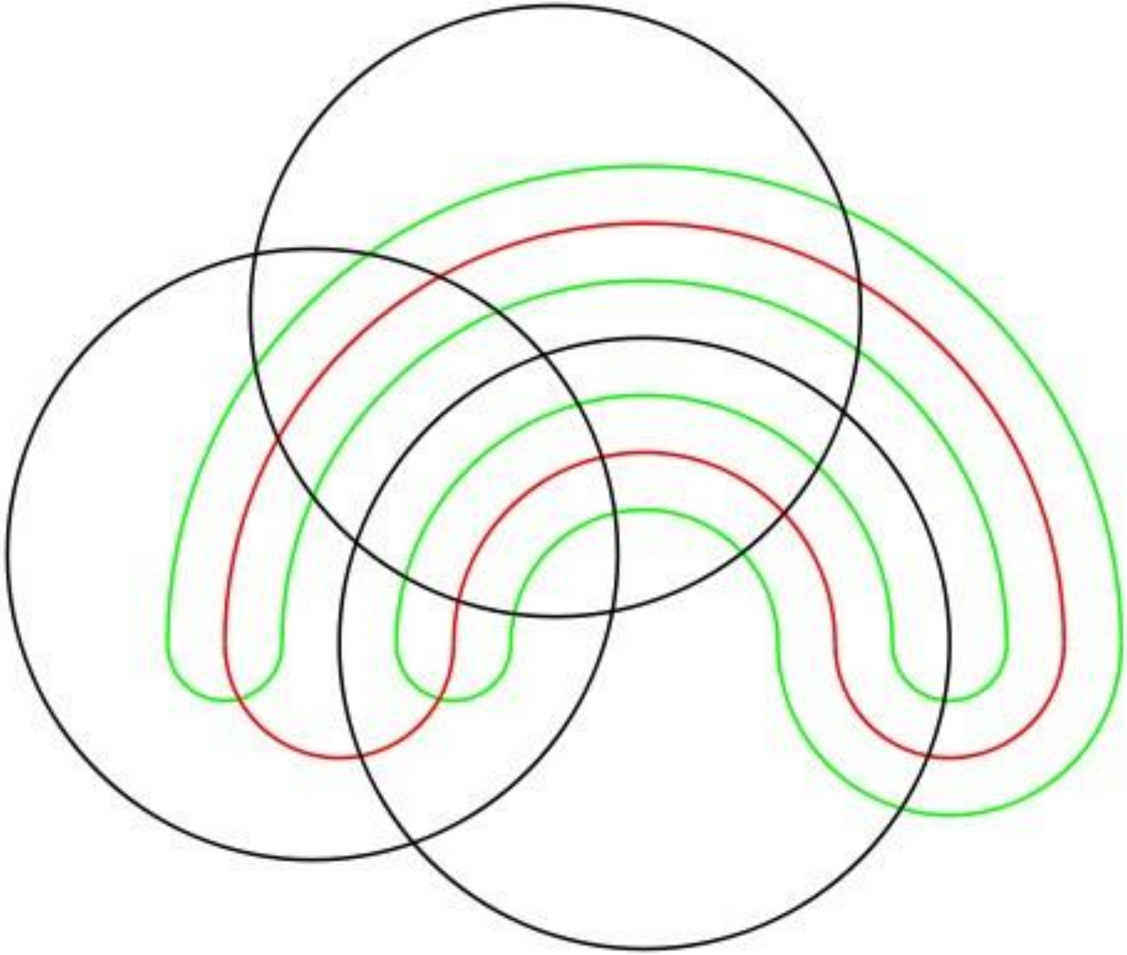


Venn Diagrams for Four Sets



Question to ponder: why can't we just draw four circles?

Venn Diagrams for Five Sets



Venn Diagrams for Seven Sets

http://moebio.com/research/sevensets/

Subsets and Power Sets

Subsets

A set *S* is a subset of a set *T* (denoted $\boldsymbol{S} \subseteq \boldsymbol{T}$) if all elements of *S* are also elements of *T*.

Examples:

- $\{1, 2, 3\} \subseteq \{1, 2, 3, 4\}$
- $\mathbb{N} \subseteq \mathbb{Z}$ (*every natural number is an integer*)
- $\mathbb{Z} \subseteq \mathbb{R}$ (*every integer is a real number*)

THEREFORE, $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{R}$

What About the Empty Set?

- A set *S* is a subset of a set *T* (denoted $S \subseteq T$) if all elements of *S* are also elements of *T*.
- Are there any sets *S* where $\emptyset \subseteq S$?
- Equivalently, is there a set *S* where the following statement is true?
  - "All elements of Ø are also elements of ***S***"
- Yes! In fact, this statement is true for every choi ce of *S*!

Vacuous Truth

- A statement of the form "All objects of type ***P*** are also of type ***Q***" is called ***vacuously true*** if there are no objects of type *P*.

- Vacuously true statements are true *by definition*.

  This is a convention used throughout mathematics.

- Some examples:

  - All unicorns are pink. (For all x, unicorn(x) => pink(x))
  - All unicorns are blue.
  - Every element of Ø is also an element of *S*.

$S = \{$, $\}$

$\wp(S) = \{ \varnothing ,$ $\{$ $\}$, $\{$ $\}$, $\{$, $\}$ $\}$

$\wp(S)$ is the ***power set*** of S
(the set of all subsets of S)

Formally, $\wp(S) = \{ \; T \mid T \subseteq S \; \}$

What is $\wp(\varnothing)$?

Answer: $\{ \varnothing\}$

Remember that $\varnothing \neq \{\varnothing\}$*!*

Cardinality

Cardinality

- The ***cardinality*** of a set is the number of elements it contains.
- If S is a set, we denote its cardinality by writing $|S|$.
- Examples:
  - $|\{a, b, c, d, e\}| = 5$
  - $|\{\{a, b\}, \{c, d, e, f, g\}, \{h\}\}| = 3$
  - $|\{1, 2, 3, 3, 3, 3, 3\}| = 3$
  - $|\{n \in \mathbb{N} \mid n < 137\}| = 137$

The Cardinality of $\mathbb{N}$

- What is $|\mathbb{N}|$?
  - There are infinitely many natural numbers.
  - $|\mathbb{N}|$ can't be a natural number, since it's infinitely large.

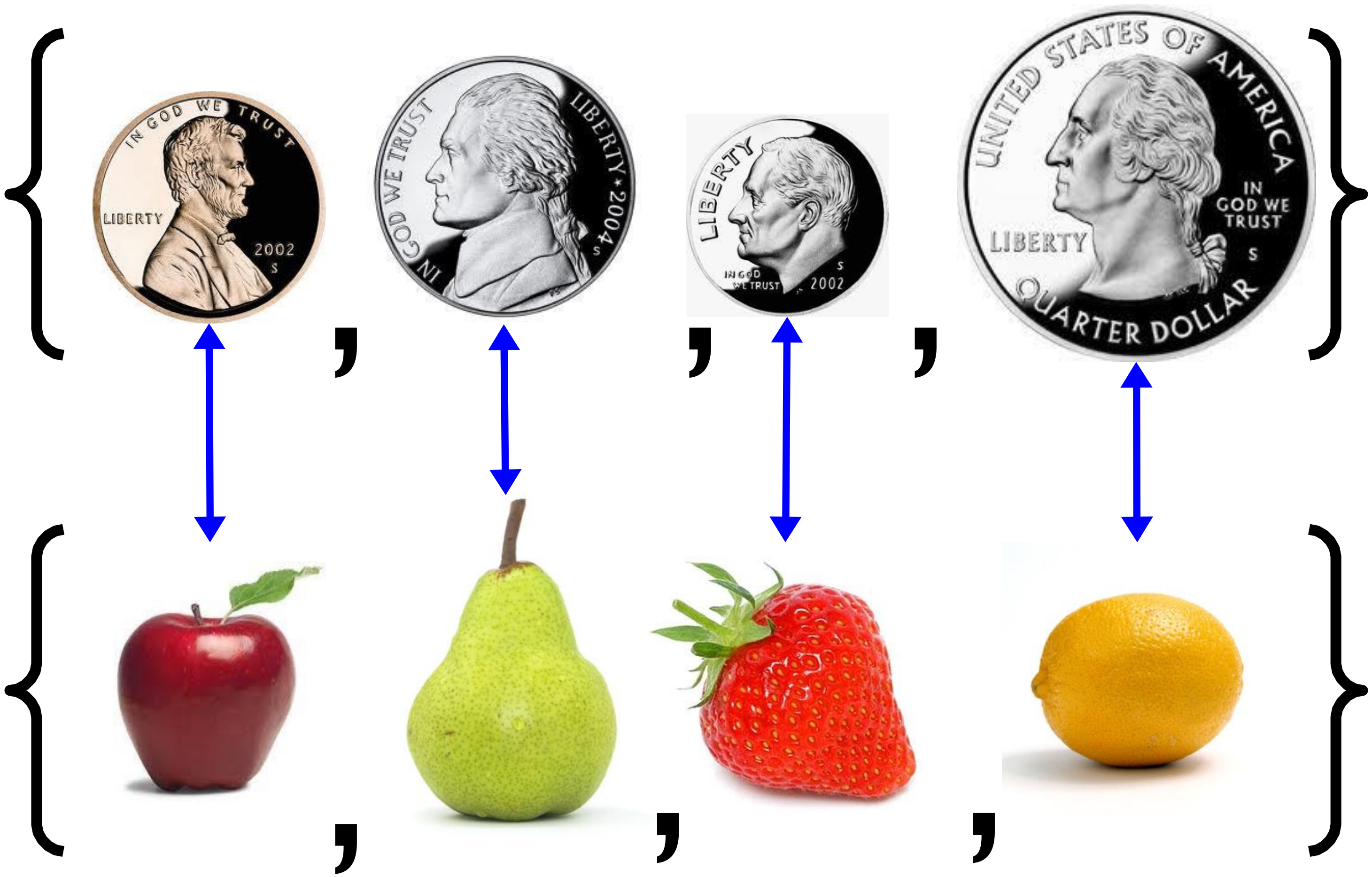
- We need to introduce a new term.
- Let's define $\aleph_0 = |\mathbb{N}|$.
  - ℵ is pronounced "aleph-zero," "aleph-nought," or "aleph-null."

Consider the set

$$S = \{\ n \mid n \in \mathbb{N} \text{ and } n \text{ is even } \}$$

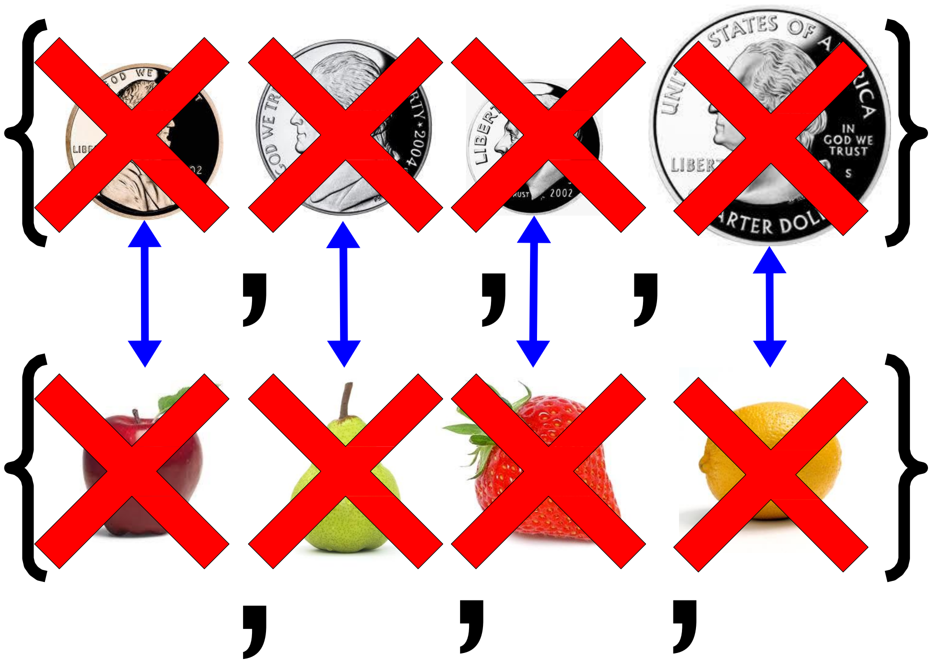
What is $|S|$?

How Big Are These Sets?



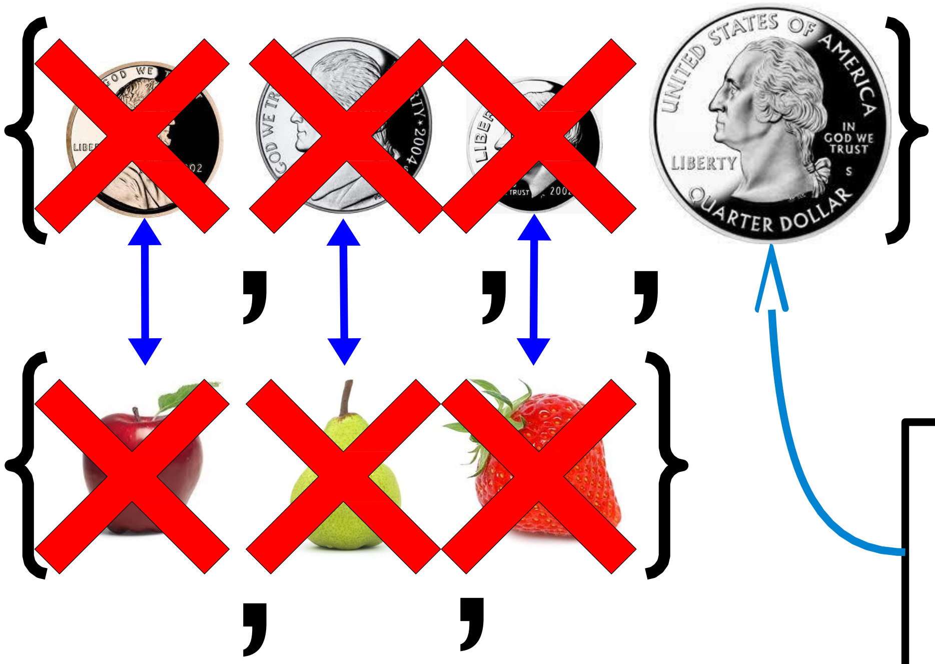
Comparing Cardinalities

- *By definition*, two sets have the same size if their elements can be paired off with no elements remaining.
- The intuition:



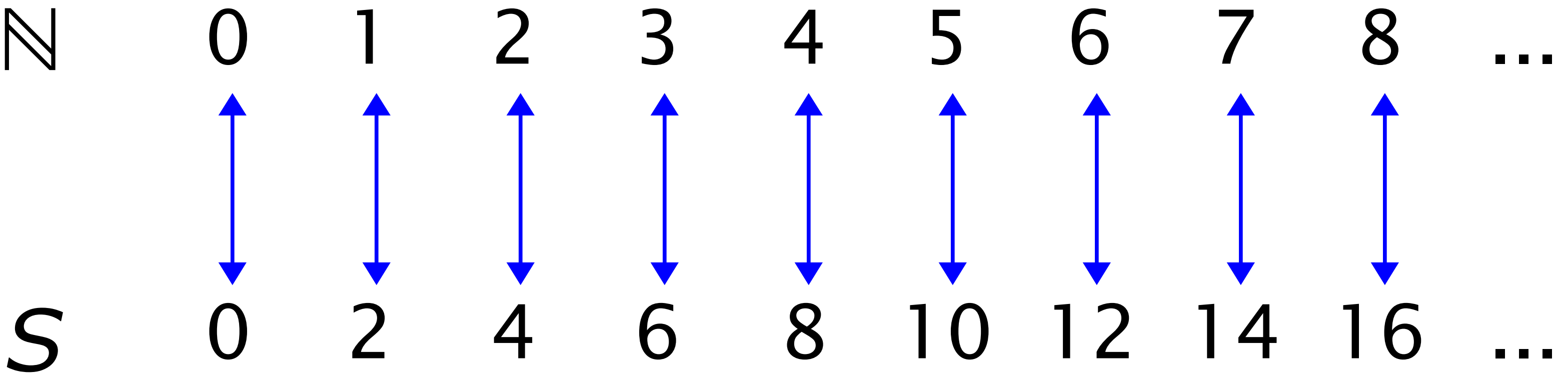
Comparing Cardinalities

- *By definition*, two sets have the same size if their elements can be paired off with no elements remaining.
- The intuition:



Everything has been paired up, and this one is all alone.

Infinite Cardinalities



$\mathbb{N}$ 0 1 2 3 4 5 6 7 8 …

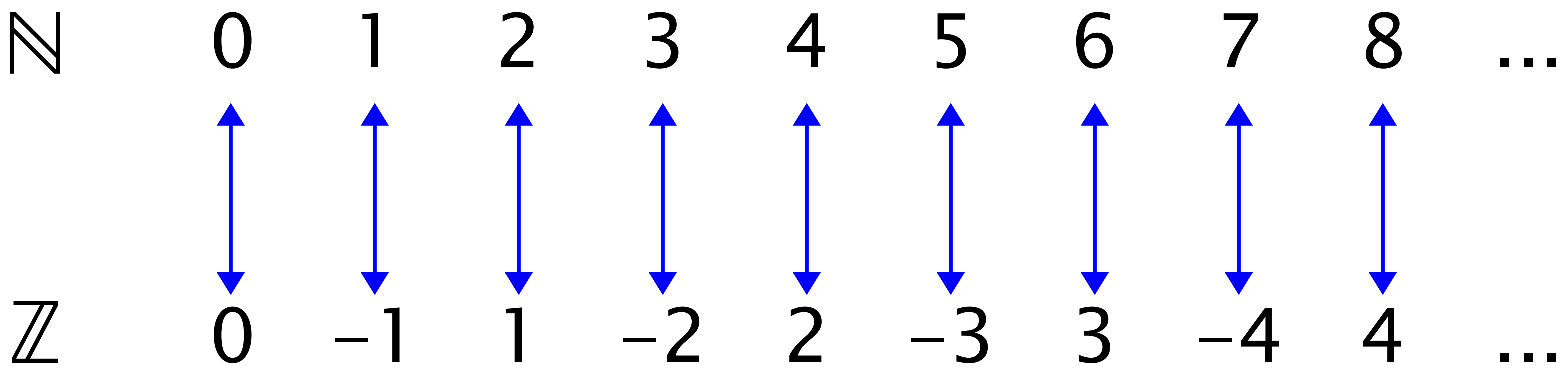
S 0 2 4 6 8 10 12 14 16 …

$$n \leftrightarrow 2n$$

$$S = \{\ n \mid n \in \mathbb{N} \text{ and } n \text{ is even } \}$$

$$|S| = |\mathbb{N}| = \aleph_0$$

Infinite Cardinalities



$\mathbb{N}$ 0 1 2 3 4 5 6 7 8 …

$\mathbb{Z}$ 0 –1 1 –2 2 –3 3 –4 4 …

$$|\mathbb{N}| = |\mathbb{Z}| = \aleph_0$$

- Pair nonnegative integers with even natural numbers.
- Pair negative integers with odd natural numbers.

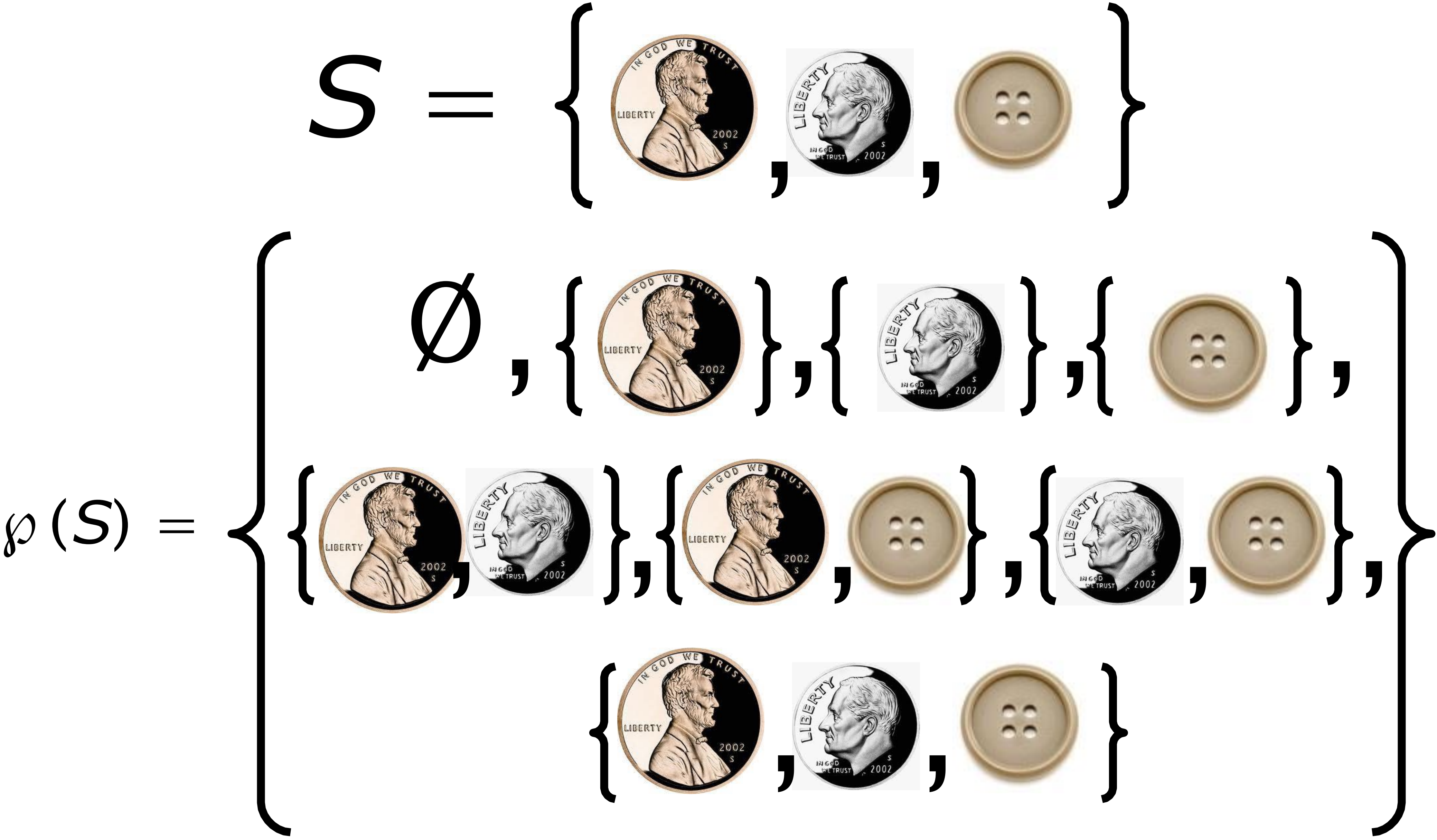
Important Question

Do all infinite sets have the same cardinality?

$S = \{$, $\}$

$\wp(S) = \{ \emptyset, \{$ $\}, \{$ $\}, \{$, $\} \}$

$|S| < |\wp(S)|$



$|S| < |\wp(S)|$

$$S = \{ a, b, c, d \}$$

$$\wp(S) = \{$$

$$\varnothing,$$

$$\{ a \}, \{ b \}, \{ c \}, \{ d \},$$

$$\{ a, b \}, \{ a, c \}, \{ a, d \}, \{ b, c \}, \{ b, d \}, \{ c, d \}$$

$$\{ a, b, c \}, \{ a, b, d \}, \{ a, c, d \}, \{ b, c, d \},$$

$$\{ a, b, c, d \}$$

$$\}$$

$$|S| < |\wp(S)|$$

If S is infinite, what is the relation between $|S|$ and $|\wp(S)|$?

Does $|S| = |\wp(S)|$?

Cantor's Diagonalization Argument

If $|S| = |\wp(S)|$, we can pair up the elements of S and the subsets of S without leaving anything out.

What would that look like?

$x_0 \longleftrightarrow \{\ x_0, x_2, x_4, \dots\ \}$

$x_1 \longleftrightarrow \{\ x_0, x_3, x_4, \dots\ \}$

$x_2 \longleftrightarrow \{\ x_4, \dots\ \}$

$x_3 \longleftrightarrow \{\ x_1, x_4, \dots\ \}$

$x_4 \longleftrightarrow \{\ x_0, x_5, \dots\ \}$

$x_5 \longleftrightarrow \{\ x_0, x_1, x_2, x_3, x_4, x_5, \dots\ \}$

…

$x_0 \quad x_1 \quad x_2 \quad x_3 \quad x_4 \quad x_5 \quad \dots$

$x_0 \longleftrightarrow \{ \; x_0, x_2, x_4, \dots \}$

$x_1 \longleftrightarrow \{ \; x_0, x_3, x_4, \dots \}$

$x_2 \longleftrightarrow \{ \; x_4, \dots \}$

$x_3 \longleftrightarrow \{ \; x_1, x_4, \dots \}$

$x_4 \longleftrightarrow \{ \; x_0, x_5, \dots \}$

$x_5 \longleftrightarrow \{ \; x_0, x_1, x_2, x_3, x_4, x_5, \dots \}$

$\dots$

	x_0	x_1	x_2	x_3	x_4	x_5	$\cdots$
$x_0 \longleftrightarrow$	Y	N	Y	N	Y	N	$\cdots$

$x_1 \longleftrightarrow \{\ x_0, x_3, x_4, \ldots$

$x_2 \longleftrightarrow \{\ x_4, \ldots\ \}$

$x_3 \longleftrightarrow \{\ x_1, x_4, \ldots\ \}$

$x_4 \longleftrightarrow \{\ x_0, x_5, \ldots\ \}$

$x_5 \longleftrightarrow \{\ x_0, x_1, x_2, x_3, x_4, x_5, \ldots\ \}$

$\ldots$

	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0 ↔	Y	N	Y	N	Y	N	…
x_1 ↔	Y	N	N	Y	Y	N	…

x_2 ↔ $\{ \quad x_4, \dots \}$

x_3 ↔ $\{ \quad x_1, x_4, \dots \}$

x_4 ↔ $\{ \quad x_0, x_5, \dots \}$

x_5 ↔ $\{ \quad x_0, x_1, x_2, x_3, x_4, x_5, \dots \}$

…

	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	Y	N	Y	N	Y	N	…
x_1	Y	N	N	Y	Y	N	…
x_2	N	N	N	N	Y	N	…
x_3	N	Y	N	N	Y	N	…
x_4	Y	N	N	N	N	Y	…
x_5	Y	Y	Y	Y	Y	Y	…
…	…	…	…	…	…	…	…

	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	Y	N	Y	N	Y	N	…
x_1	Y	N	N	Y	Y	N	…
x_2	N	N	N	N	Y	N	…
x_3	N	Y	N	N	Y	N	…
x_4	Y	N	N	N	N	Y	…
x_5	Y	Y	Y	Y	Y	Y	…
…	…	…	…	…	…	…	…

Y	N	N	N	N	Y	…

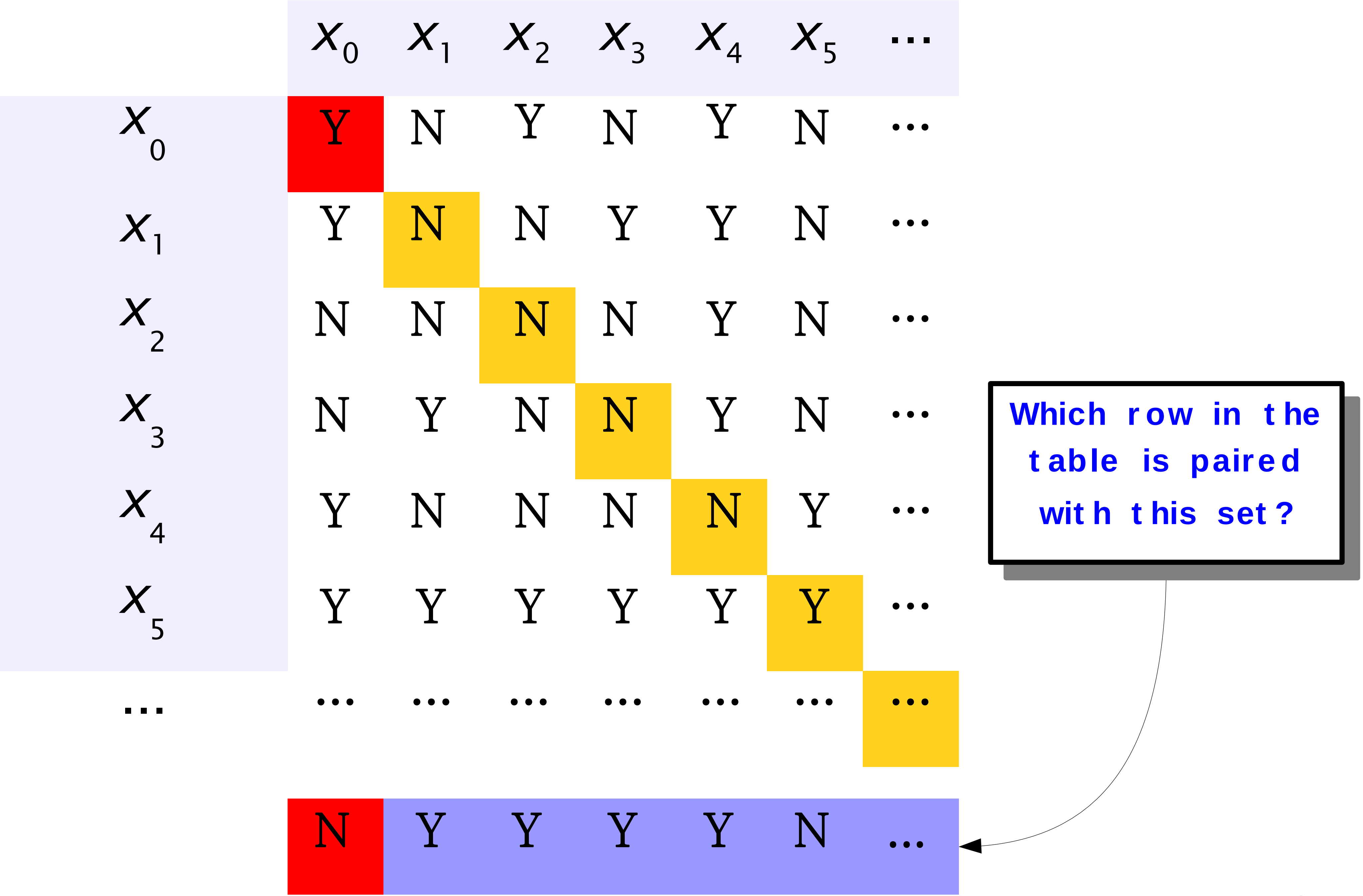
Which row in the table is paired with this set?

	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	Y	N	Y	N	Y	N	…
x_1	Y	N	N	Y	Y	N	…
x_2	N	N	N	N	Y	N	…
x_3	N	Y	N	N	Y	N	…
x_4	Y	N	N	N	N	Y	…
x_5	Y	Y	Y	Y	Y	Y	…
…	…	…	…	…	…	…	…
	N	Y	Y	Y	Y	N	…

Flip all Y's to N's and vice-versa to get a new set

	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	Y	N	Y	N	Y	N	…
x_1	Y	N	N	Y	Y	N	…
x_2	N	N	N	N	Y	N	…
x_3	N	Y	N	N	Y	N	…
x_4	Y	N	N	N	N	Y	…
x_5	Y	Y	Y	Y	Y	Y	…
…	…	…	…	…	…	…	…
	N	Y	Y	Y	Y	N	…

Which row in the table is paired with this set?



	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	Y	N	Y	N	Y	N	…
x_1	Y	N	N	Y	Y	N	…
x_2	N	N	N	N	Y	N	…
x_3	N	Y	N	N	Y	N	…
x_4	Y	N	N	N	N	Y	…
x_5	Y	Y	Y	Y	Y	Y	…
…	…	…	…	…	…	…	…
	N	Y	Y	Y	Y	N	…

Which row in the table is paired with this set?

	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	Y	N	Y	N	Y	N	…
x_1	Y	N	N	Y	Y	N	…
x_2	N	N	N	N	Y	N	…
x_3	N	Y	N	N	Y	N	…
x_4	Y	N	N	N	N	Y	…
x_5	Y	Y	Y	Y	Y	Y	…
…	…	…	…	…	…	…	…

N	Y	Y	Y	Y	N	…

Which row in the table is paired with this set?

	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	Y	N	0 Y	N	. Y	N	…
x_1	Y	N	N	Y	Y	N	…
x_2	N	N	N	N	Y	N	…
x_3	N	Y	N	N	Y	N	…
x_4	Y	N	N	N	N	Y	…
x_5	Y	Y	Y	Y	Y	Y	…
…	…	…	…	…	…	…	…
	N	Y	Y	Y	Y	N	…

Which row in the table is paired with this set?

	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	Y	N	Y	N	Y	N	…
x_1	Y	N	N	Y	Y	N	…
x_2	N	N	N	N	Y	N	…
x_3	N	Y	N	N	Y	N	…
x_4	Y	N	N	N	N	Y	…
x_5	Y	Y	Y	Y	Y	Y	…
…	…	…	…	…	…	…	…

N	Y	Y	Y	Y	N	…

Which row in the table is paired with this set?

	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	Y	N	Y	N	Y	N	…
x_1	Y	N	N	Y	Y	N	…
x_2	N	N	N	N	Y	N	…
x_3	N	Y	N	N	Y	N	…
x_4	Y	N	N	N	N	Y	…
x_5	Y	Y	Y	Y	Y	Y	…
…	…	…	…	…	…	…	…
	N	Y	Y	Y	Y	N	…

Which row in the table is paired with this set?

	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	Y	N	Y	N	Y	N	…
x_1	Y	N	N	Y	Y	N	…
x_2	N	N	N	N	Y	N	…
x_3	N	Y	N	N	Y	N	…
x_4	Y	N	N	N	N	Y	…
x_5	Y	Y	Y	Y	Y	Y	…
…	…	…	…	…	…	…	…
	N	Y	Y	Y	Y	N	…

Which row in the table is paired with this set?

	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	Y	N	Y	N	Y	N	…
x_1	Y	N	N	Y	Y	N	…
x_2	N	N	N	N	Y	N	…
x_3	N	Y	N	N	Y	N	…
x_4	Y	N	N	N	N	Y	…
x_5	Y	Y	Y	Y	Y	Y	…
…	…	…	…	…	…	…	…

N	Y	Y	Y	Y	N	…

Which row in the table is paired with this set?

The Diagonalization Proof

- No matter how we pair up elements of *S* and subsets of *S*, the complemented diagonal won't appear in the table.
  - In row *n*, the *n*th element must be wrong.

- No matter how we pair up elements of *S* and subsets of *S*, there is *always* at least one subset left over.

- This result is ***Cantor's theorem***: Every set is strictly smaller than its power set:
  - If S is a set, then $|S| < |\wp(S)|$.

Infinite Cardinalities

- By Cantor's Theorem:

$$|\mathbb{N}| < |\wp(\mathbb{N})|$$

$$|\wp(\mathbb{N})| < |\wp(\wp(\mathbb{N}))|$$

$$|\wp(\wp(\mathbb{N}))| < |\wp(\wp(\wp(\mathbb{N})))|$$

$$|\wp(\wp(\wp(\mathbb{N})))| < |\wp(\wp(\wp(\wp(\mathbb{N}))))|$$

$$\dots$$

- ***Not all infinite sets have the same size!***
- ***There is no biggest infinity!***
- ***There are infinitely many infinities!***

What does this have to do with computation?

“The set of all computer programs”

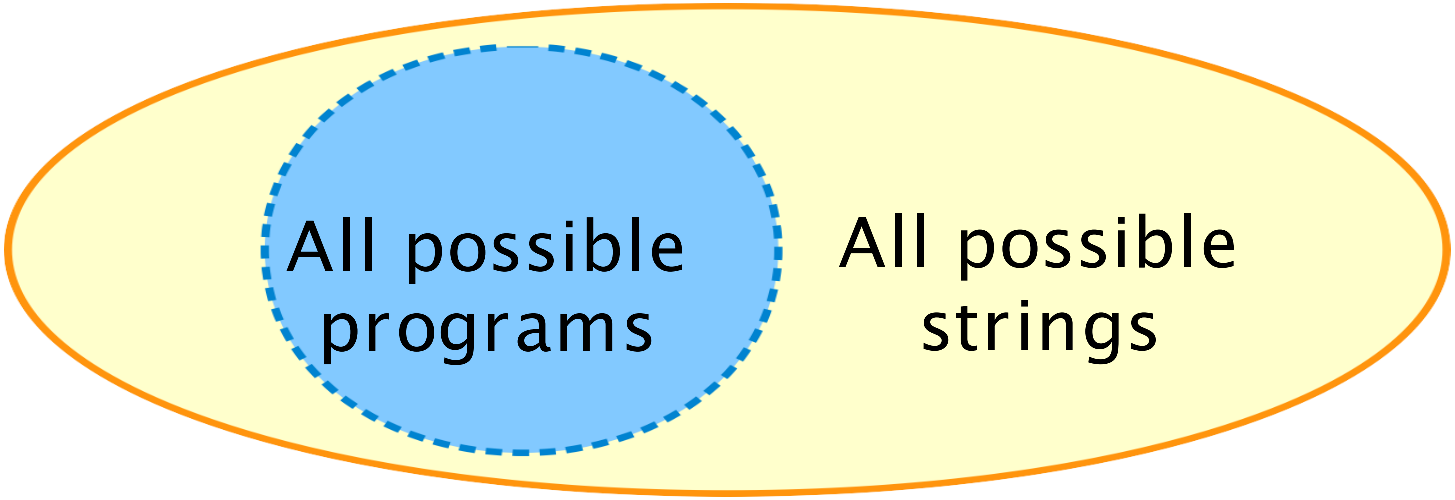
“The set of all problems to solve”

Where We're Going

- A ***string*** is a sequence of characters.
- We're going to prove the following results:
  - There are ***at most*** as many programs as there are strings.
  - There are ***at least*** as many problems as there are sets of strings.
- This leads to some *incredible* results – we'll see why in a minute!

Strings and Programs

- The source code of a computer program is just a (long, structured, well-commented) string of text.
- All programs are strings, but not all strings are necessarily programs.



$$|\text{Programs}| \leq |\text{Strings}|$$

Strings and Problems

- There is a connection between the number of sets of strings and the number of problems to solve.
- Let *S* be any set of strings. This set *S* gives rise to a p roblem to solve:
  - Given a string ***w***, determine whether ***w*** $\in$***S*** .

Strings and Problems

- Given a string ***w***, determine whether ***w*** $\in$ ***S***.
- Suppose that *S* is the set
  - $S = \{$ "*a*", "*b*", "*c*", … "*z*" $\}$
- From this set *S*, we get this problem:

Given a string ***w***, determine whether
w is a single lower-case English letter.

Strings and Problems

Given a string $\boldsymbol{w}$, determine whether $\boldsymbol{w} \in \boldsymbol{S}$.

- Suppose that S is the set

$$S = \{ \text{"0"}, \text{"1"}, \text{"2"}, \dots, \text{"9"}, \text{"10"}, \text{"11"}, \dots \}$$

- From this set S, we get this problem:

Given a string $\boldsymbol{w}$, determine whether $\boldsymbol{w}$ represents a natural number.

Strings and Problems

Given a string ***w***, determine whether ***w*** $\in$ ***S***.

- Suppose that *S* is the set

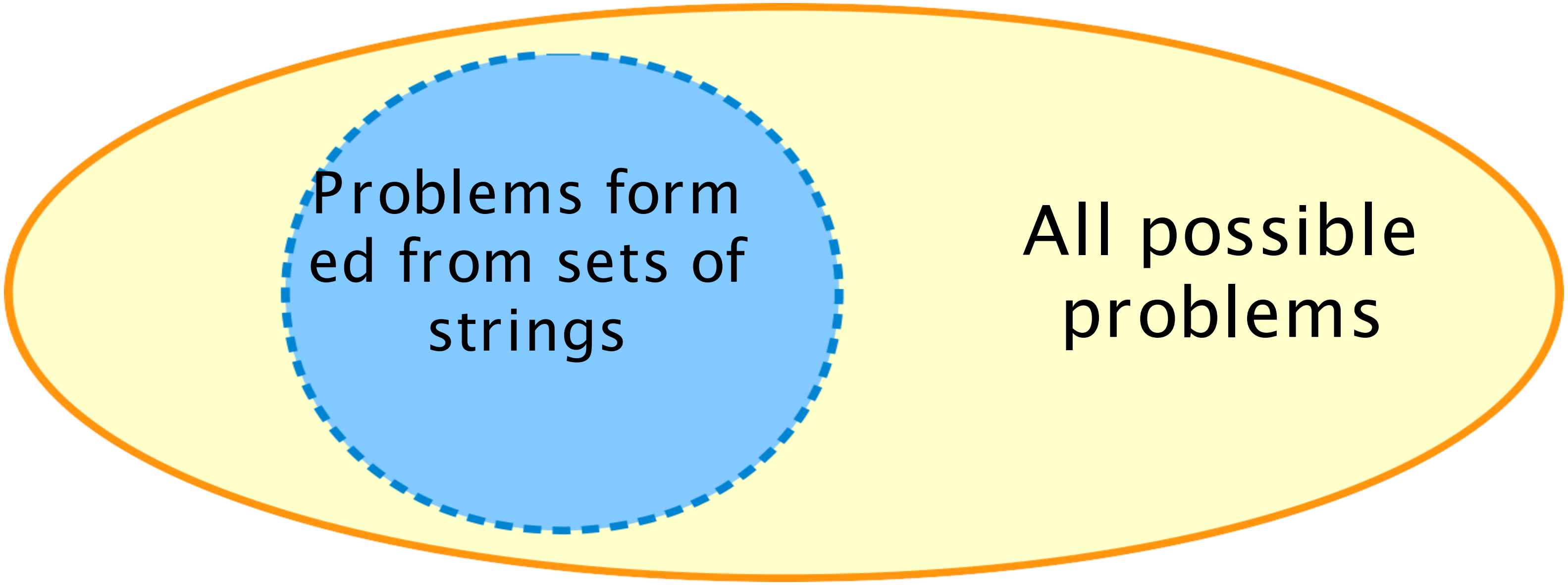
$$S = \{\ p \mid p \text{ is a legal Java program } \}$$

- From this set *S*, we get this problem:

Given a string ***w***, determine whether ***w*** is a legal Java program.

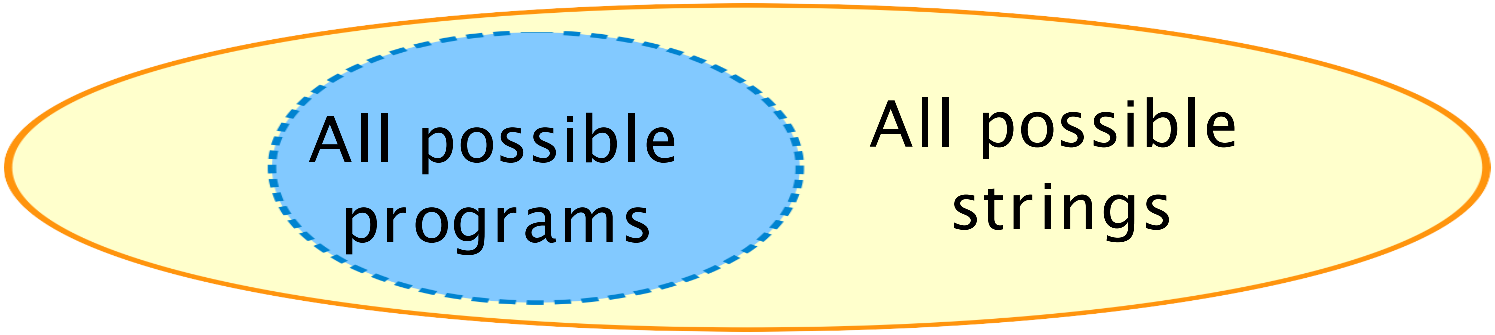
Strings and Problems

- Every set of strings gives rise to a unique problem to solve.
- Other problems exist as well.

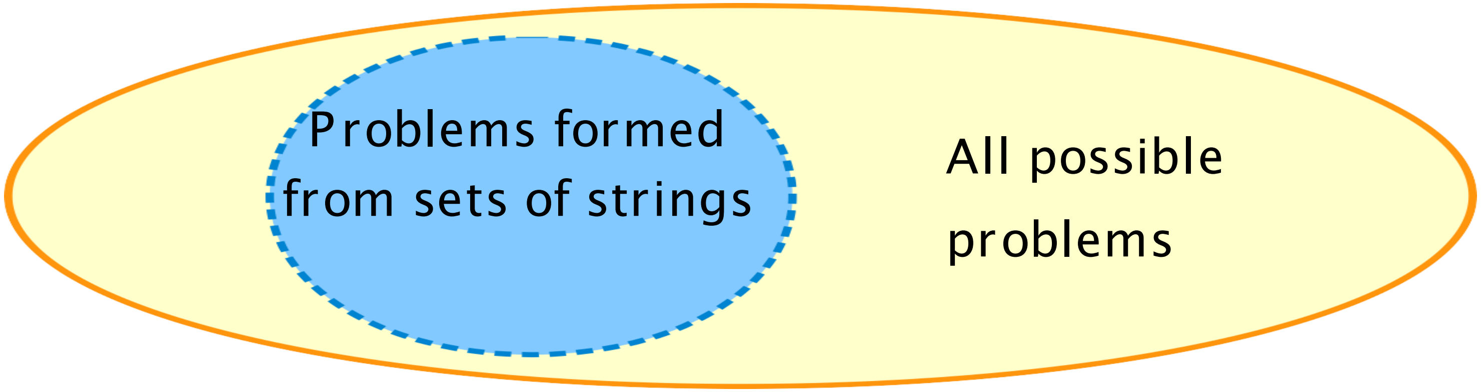


$$|\text{Sets of Strings}| \leq |\text{Problems}|$$

We saw the followings!



|Programs| ≤ |Strings|



|Sets of Strings| ≤ |Problems|

Where We're Going

- A ***string*** is a sequence of characters.
- We're going to prove the following results:

  - There are ***at most*** as many programs as there are strings. ✓
  - There are ***at least*** as many problems as there are sets of strings. ✓

- This leads to some *incredible* results – we'll see why in a minute!

Every computer program is a string.

So, the number of programs is at most the number of strings.

From Cantor's Theorem, we know that there are more sets of strings than strings.

There are at least as many problems as there are sets of strings.

$$|\text{Programs}| \le |\text{Strings}| < |\text{Sets of Strings}| \le |\text{Problems}|$$

There are more problems to solve than there are programs to solve them.

$$|\text{Programs}| < |\text{Problems}|$$

It Gets Worse

- Using more advanced set theory, we can show that there are *infinitely more* problems than solutions.
- In fact, if you pick a totally random problem, the probability that you can solve it is *zero*.
- More troubling fact: We've just shown that *some* problems are impossible to solve, but we don't know *which* problems are impossible!

We need to develop a more nuanced understanding of computation.

- What makes a problem impossible to solve with computers?
  - Is there a deep reason why certain problems can't be solved with computers, or is it completely arbitrary?
  - How do you know when you're looking at an impossible problem?
  - Are these real-world problems, or are they highly contrived?

Problems that cannot be solved by a computer are existing!