Goals for this Course

- Explore **mathematical structures** that arise in math and computing.
- Equip you with the **fundamental mathematical tools** to reason about problems that arise in computing.
- Explore the **limits of computing** and what can be computed.

Introduction to Set Theory

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

{ 

, 

, 

, 

}

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

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).

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

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

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

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

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

{ 

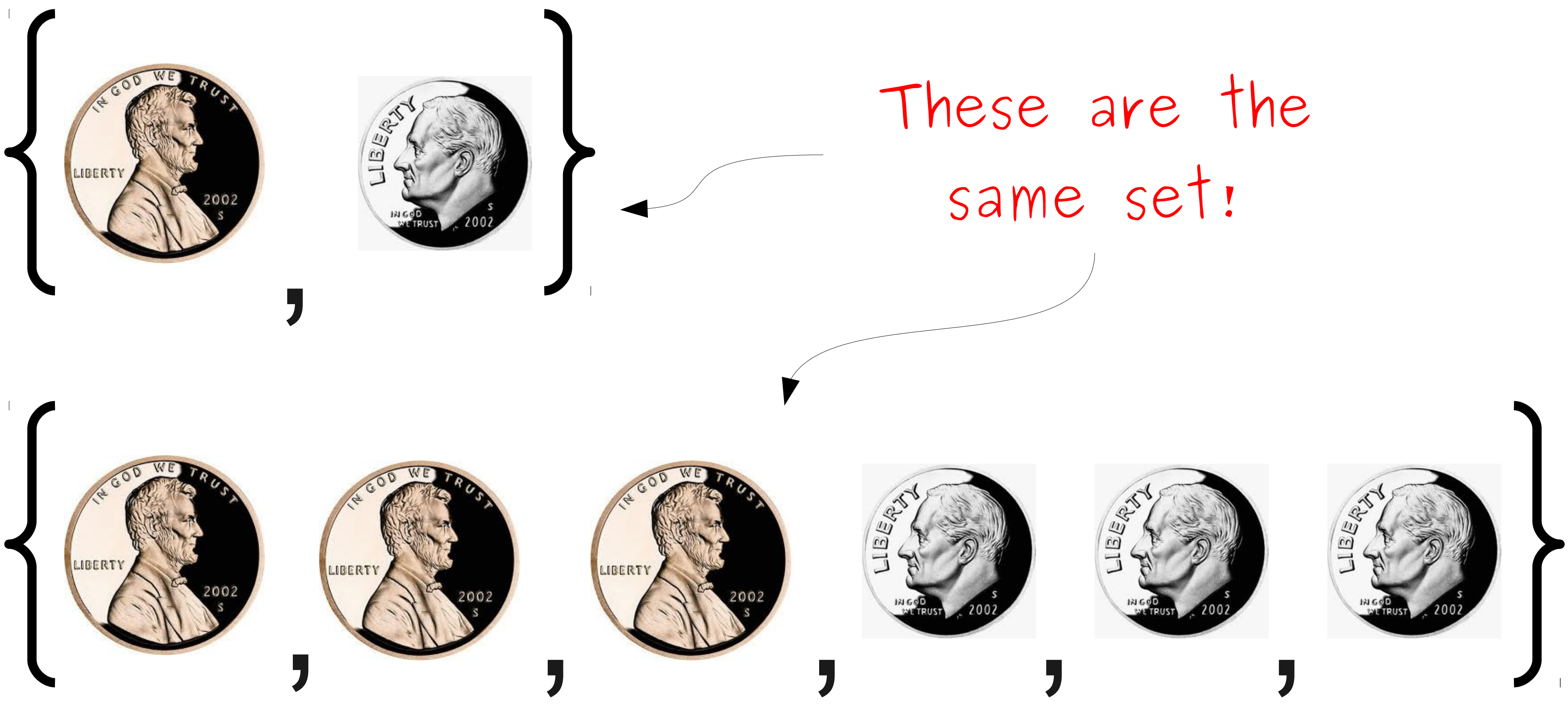
, 

}

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

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

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



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

$$\{\quad\}$$

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

$$\{\ \}$$

The <u>empty set</u>
contains no elements.

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

$\emptyset$

We denote it with this symbol

$\{\ \}$

The <u>empty set</u> contains no elements.

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

$$\emptyset \equiv \{\ \}$$

We denote it with this symbol

The empty set contains no elements.

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

This symbol means "is defined as"

$$\emptyset \equiv \{ \ \}$$

We denote it with this symbol

The **empty set** contains no elements.

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

Membership

Membership

{ 
IN GOD WE TRUST
LIBERTY
2004
S
, 
IN GOD WE TRUST
LIBERTY
2002
S
, 
UNITED STATES OF AMERICA
IN GOD WE TRUST
LIBERTY
S
QUARTER DOLLAR
, 
LIBERTY
IN GOD WE TRUST
S
2002
}

Membership

Is  in this set?

Membership

Is  in this set?

Membership

$\in$ $\{$


,


,


,


$\}$

Is


in this set?

Membership

$\notin$ {

,

,

,

}

Is

in this set?

Set Membership

- Given a set S and an object x, we write

  $$x \in S$$

  if x is contained in S, and

  $$x \notin S$$

  otherwise.
- If $x \in S$, we say that x is an **element** of S.
- Given any object and any set, either that object is in the set or it isn't.

Infinite Sets

- Sets can be infinitely large.
- The **natural numbers**, $\mathbb{N}$: { 0, 1, 2, 3, …}
  - Some authors (including Sipser) don't include zero; in this class, assume that 0 is a natural number.
- The **integers**, $\mathbb{Z}$: { …, -2, -1, 0, 1, 2, … }
  - Z is from German "Zahlen."
- The **real numbers**, $\mathbb{R}$, including rational and irrational numbers.

Constructing Sets from Other Sets

- Consider these English descriptions:

  “All even numbers.”

  “All real numbers less than 137.”

  “All negative integers.”

- We can't list their (infinitely many!) elements.
- How would we rigorously describe them?

The Set of Even Numbers

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

The Set of Even Numbers

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

The set of all x

The Set of Even Numbers

$$\{\ \boldsymbol{x}\ |\ x \in \mathbb{N} \text{ and } x \text{ is even}\ \}$$

The set of all x

where

The Set of Even Numbers

$$\{\, \boldsymbol{x} \mid \boldsymbol{x} \in \mathbb{N} \text{ and } x \text{ is even} \,\}$$

The set of all x

where

x is in the set of natural numbers

The Set of Even Numbers

$$\{\, \boldsymbol{x} \mid \boldsymbol{x} \in \mathbb{N} \text{ and } \boldsymbol{x} \textbf{ is even} \,\}$$

The set of all x

where

x is in the set of
natural numbers

and x is even

Set Builder Notation

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

  $\{ x \mid \textit{some property } x \textit{ satisfies} \}$

- For example:

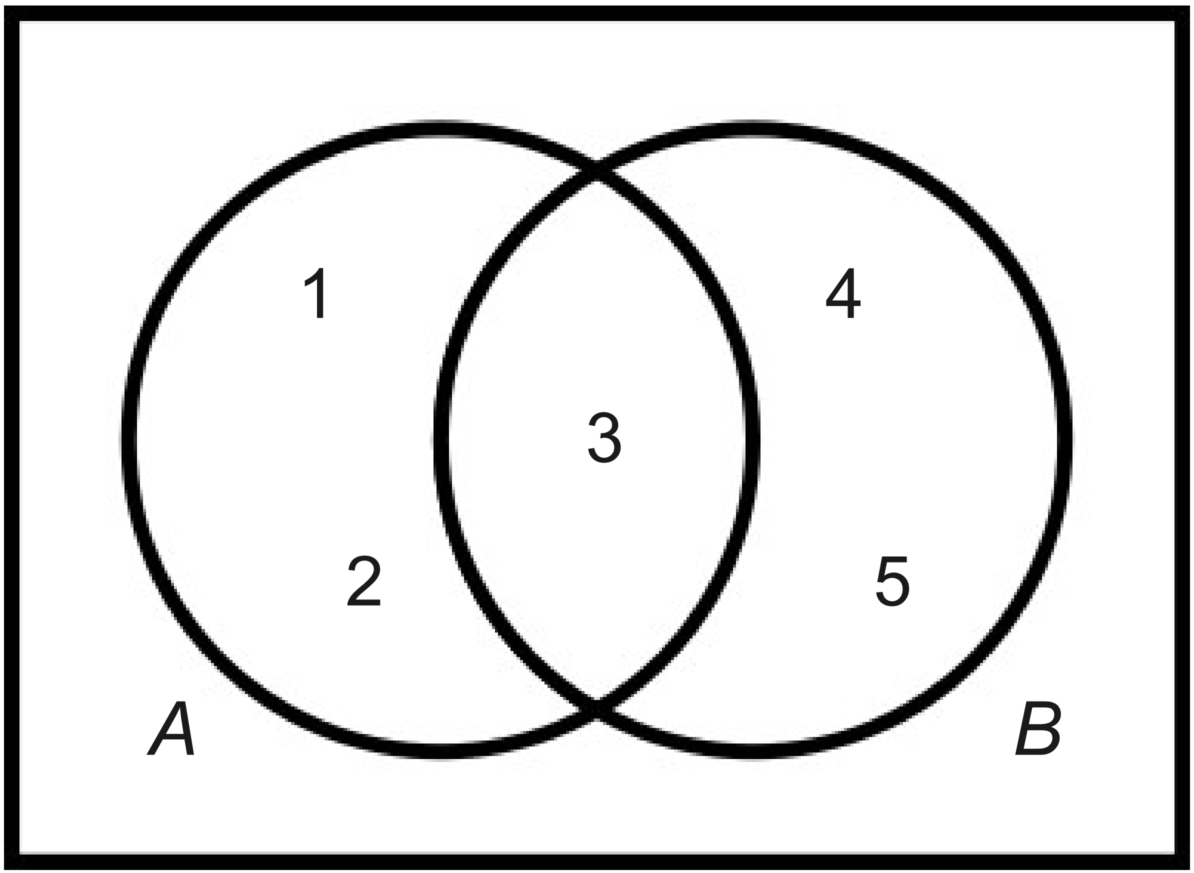
  $\{ r \mid r \in \mathbb{R}, r < 137 \}$

  $\{ n \mid n \text{ is a perfect square} \}$

  $\{ x \mid x \text{ is a set of US currency} \}$

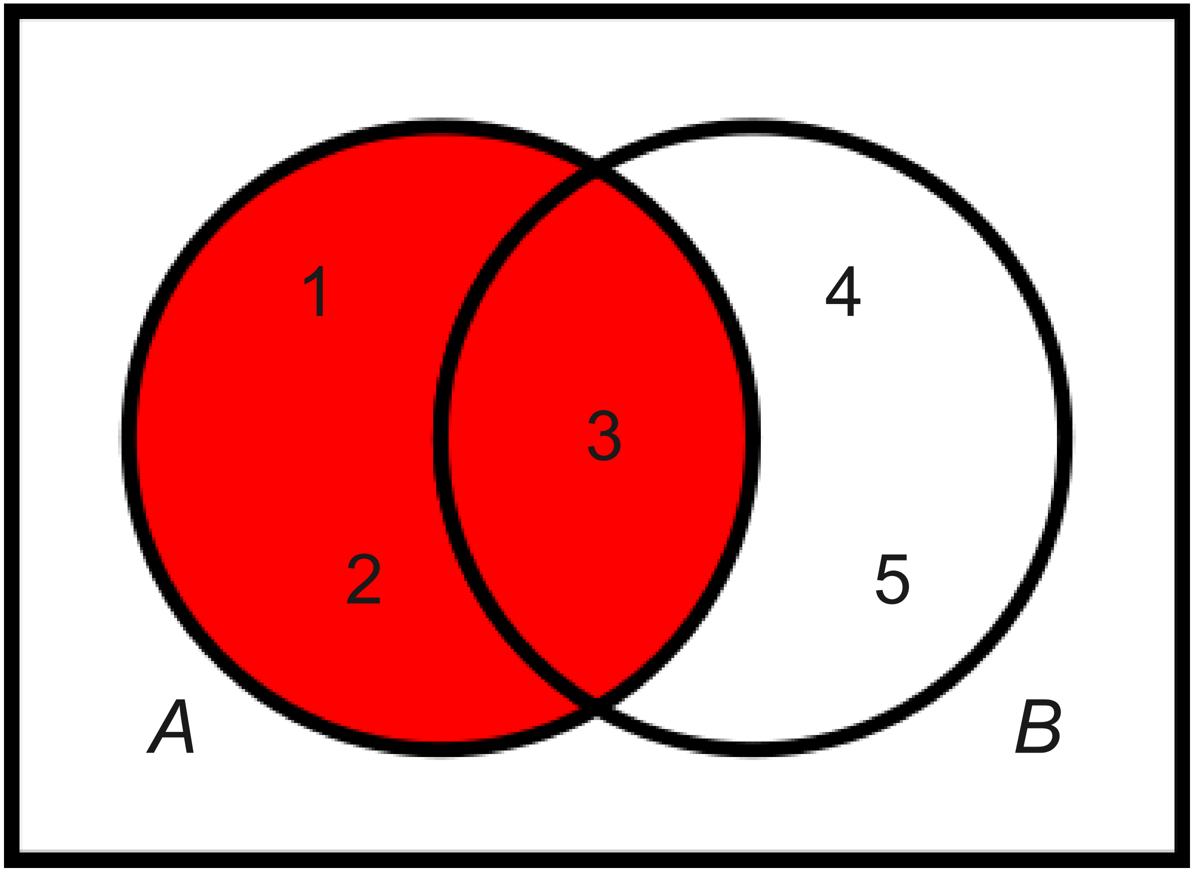
Operations on Sets

Venn Diagrams



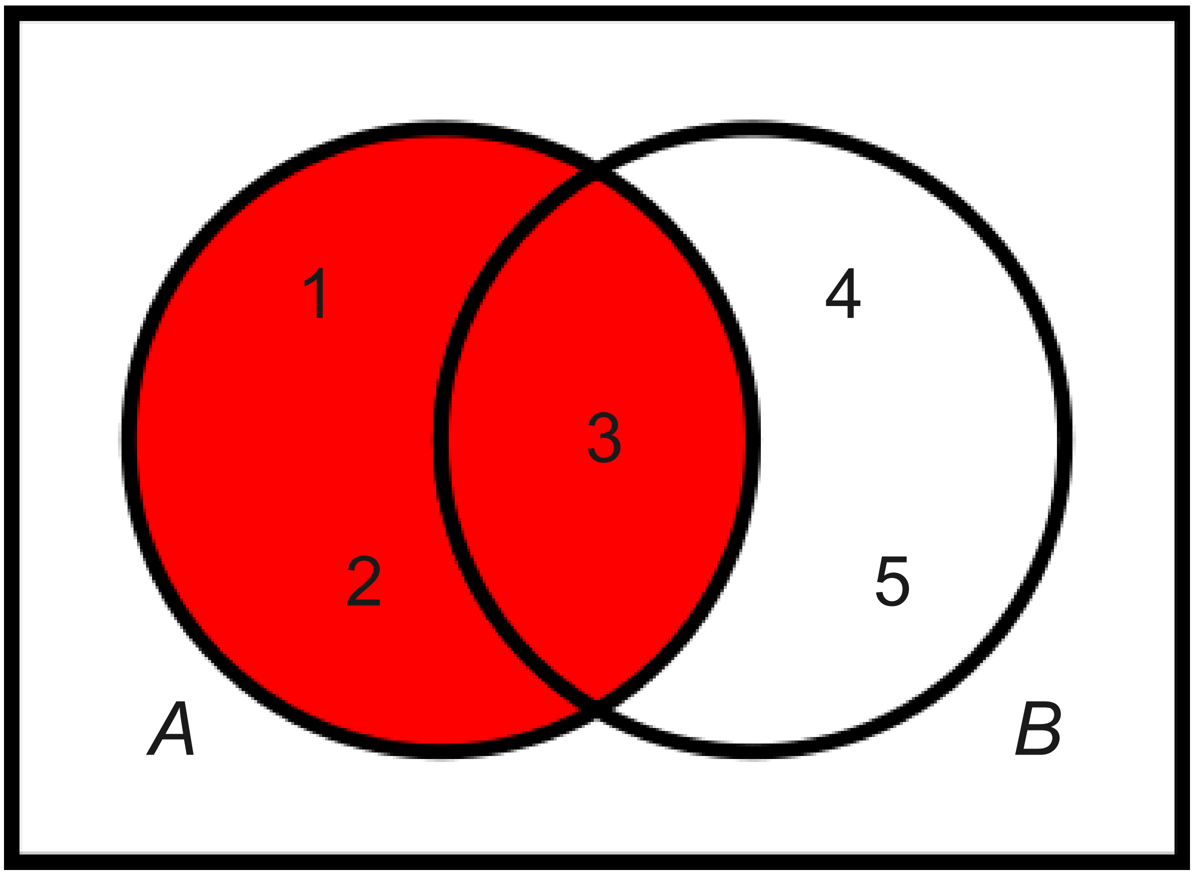
$A = \{ 1, 2, 3 \}$
$B = \{ 3, 4, 5 \}$

Venn Diagrams



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

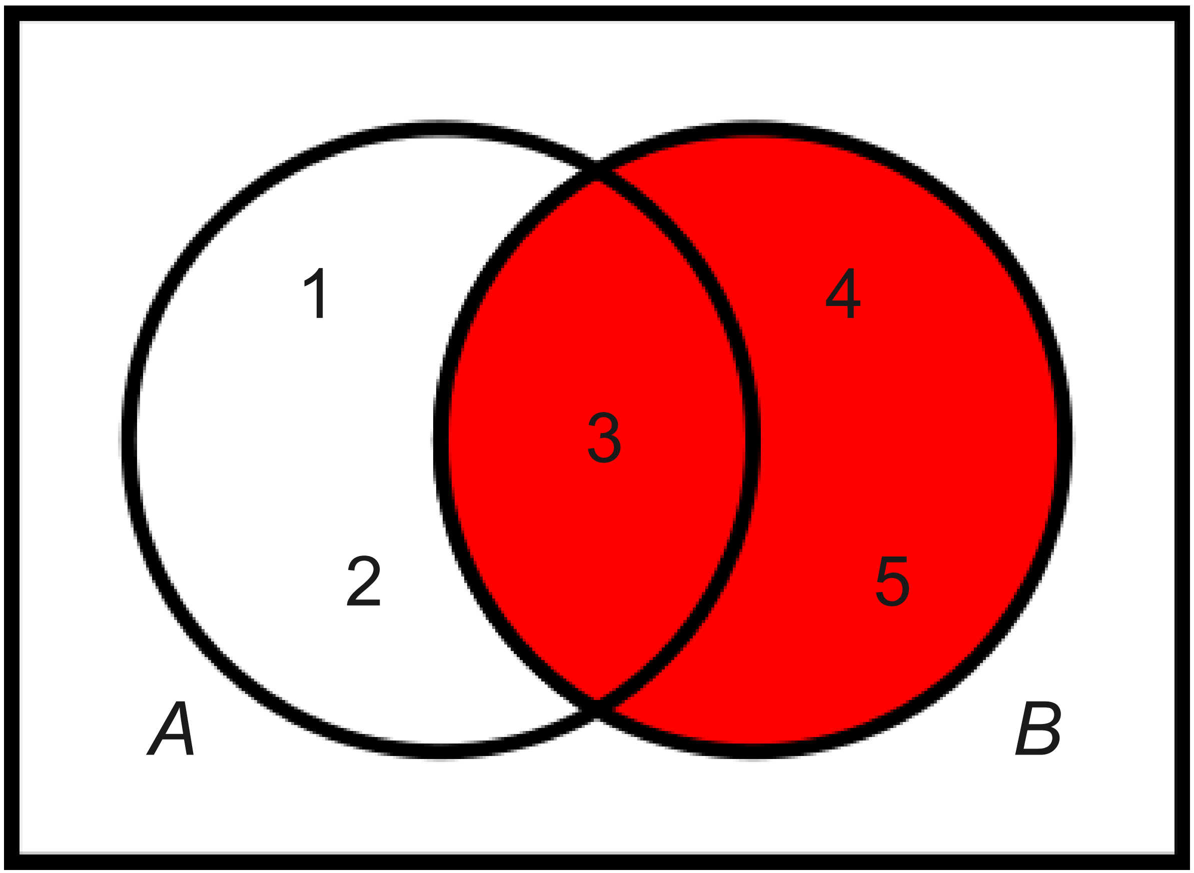
Venn Diagrams



A

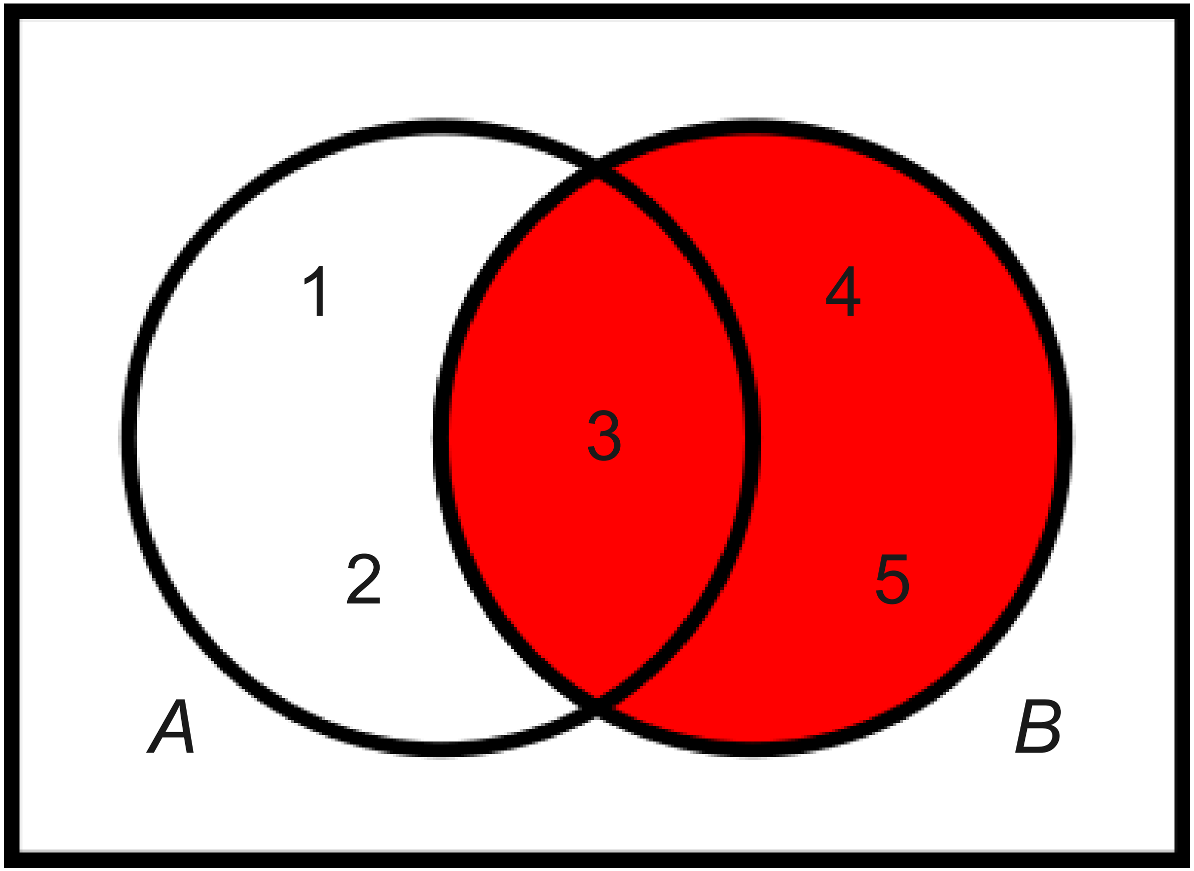
$A = \{ 1, 2, 3 \}$
$B = \{ 3, 4, 5 \}$

Venn Diagrams



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

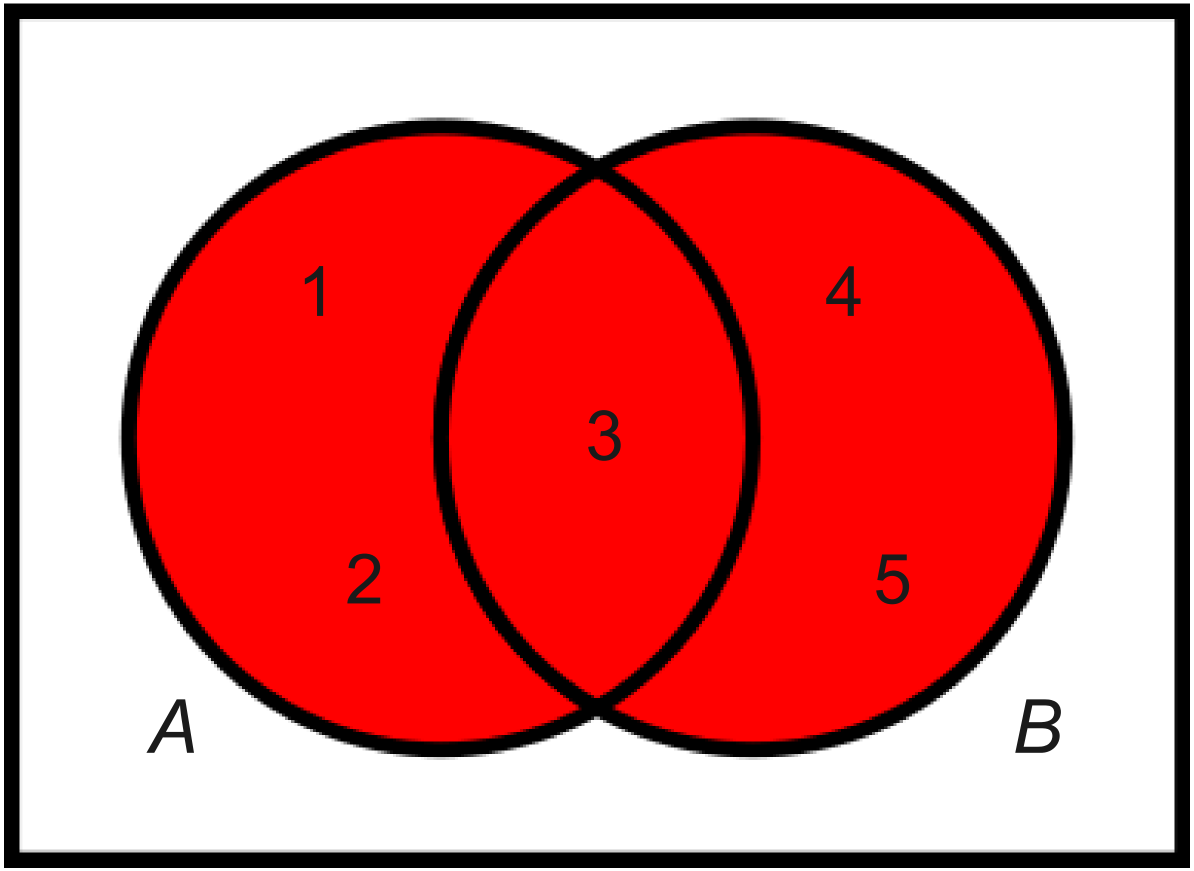
Venn Diagrams



B

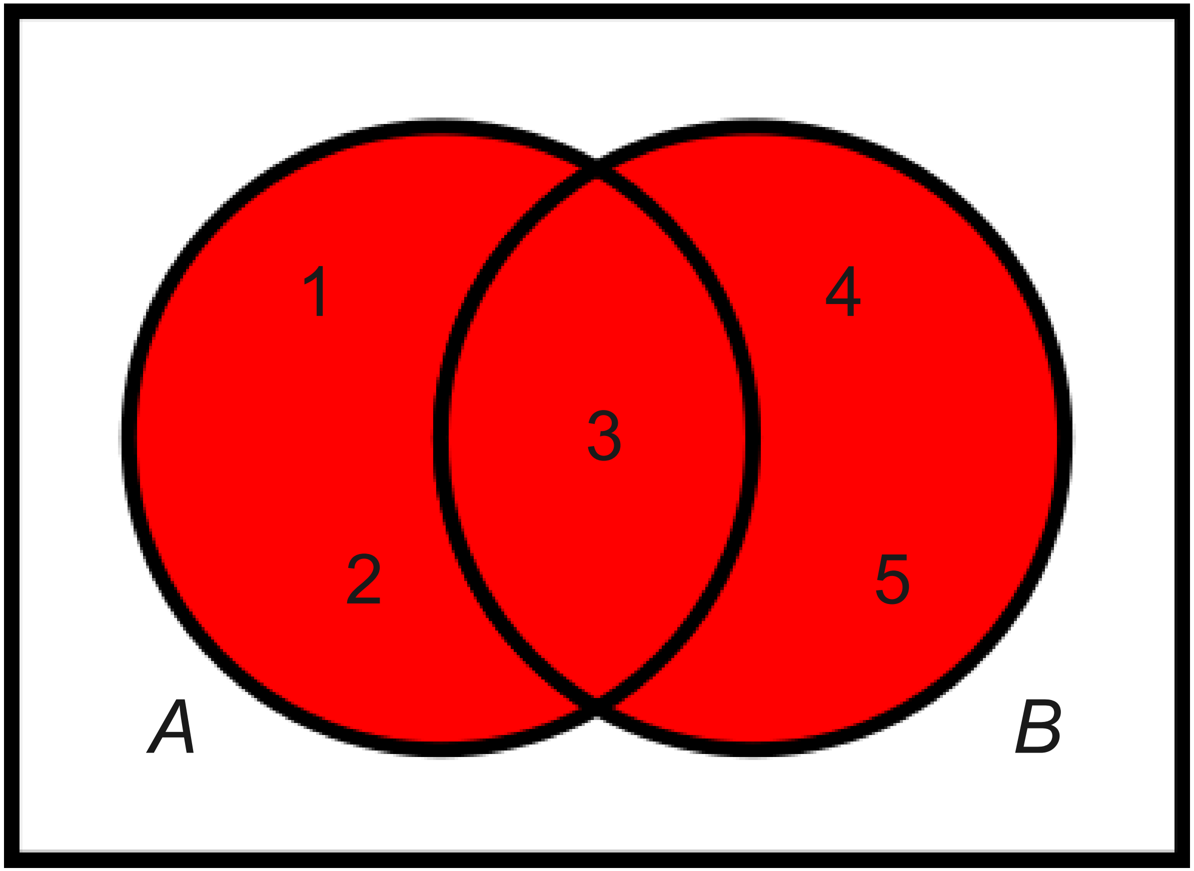
$A = \{ 1, 2, 3 \}$
$B = \{ 3, 4, 5 \}$

Venn Diagrams



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

Venn Diagrams



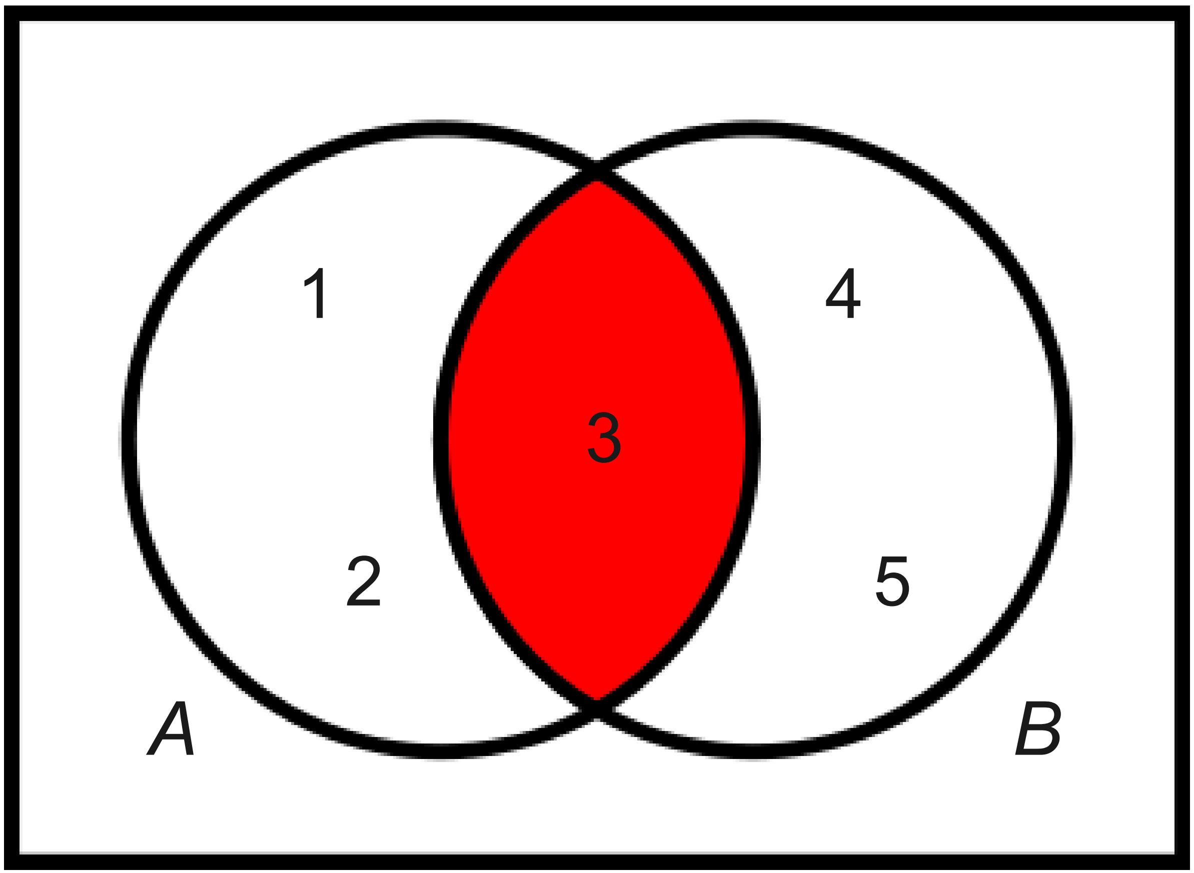
Union

$A \cup B$

$\{ 1, 2, 3, 4, 5 \}$

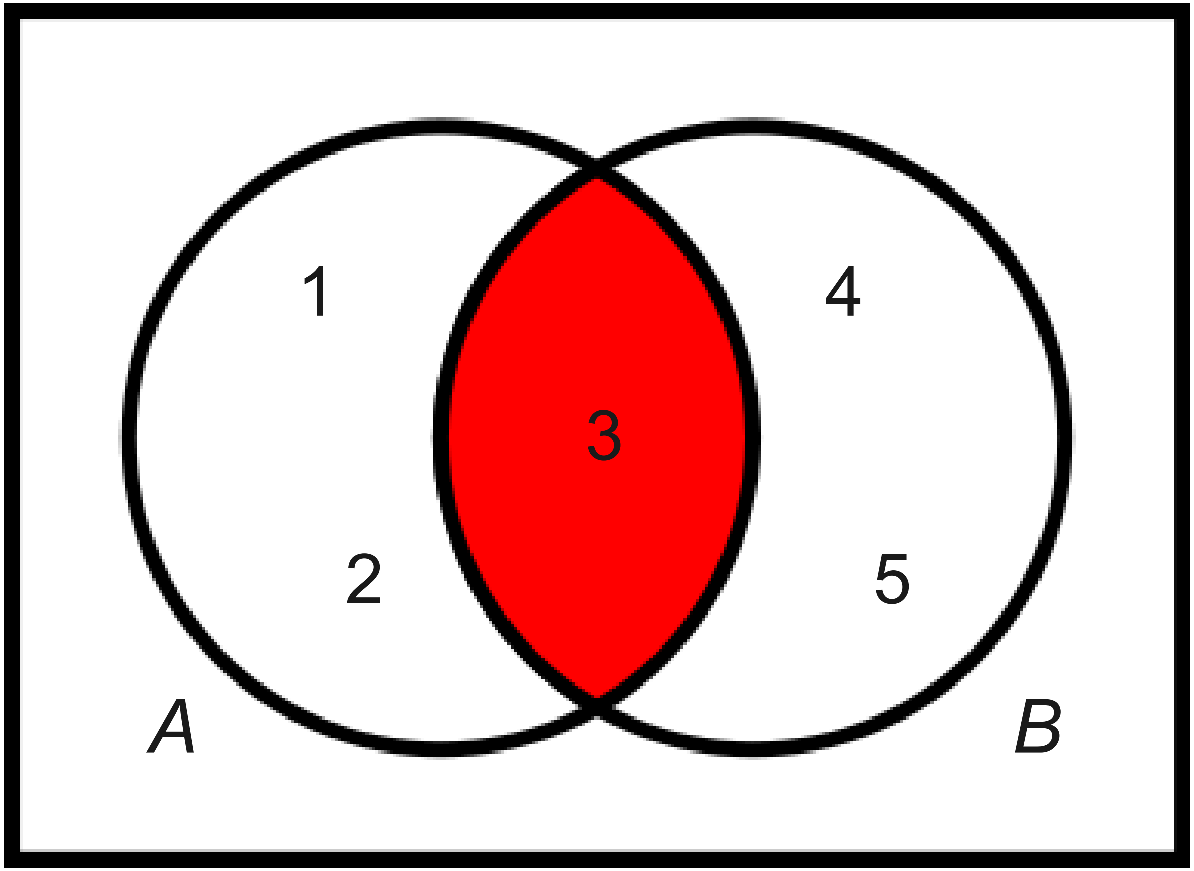
$A = \{ 1, 2, 3 \}$
$B = \{ 3, 4, 5 \}$

Venn Diagrams



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

Venn Diagrams



Intersection

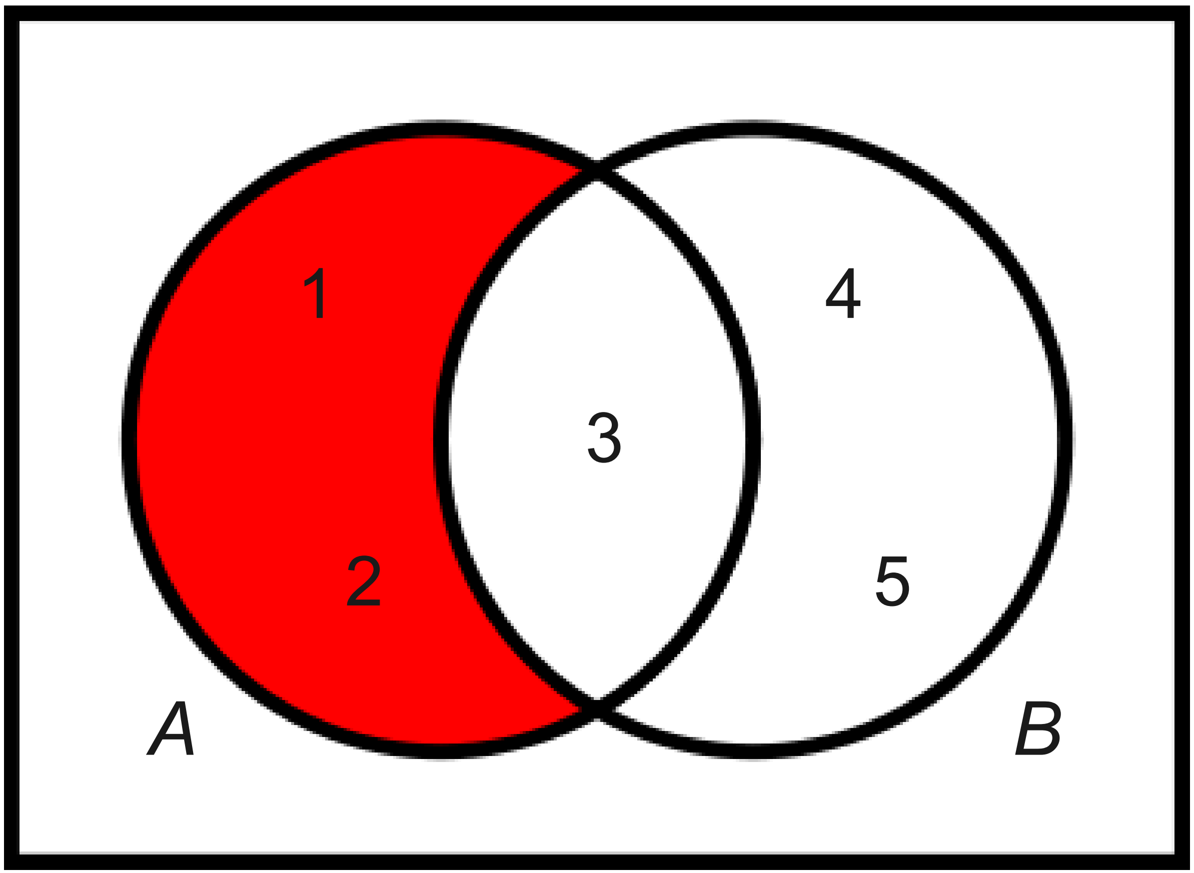
$A \cap B$

$\{ 3 \}$

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

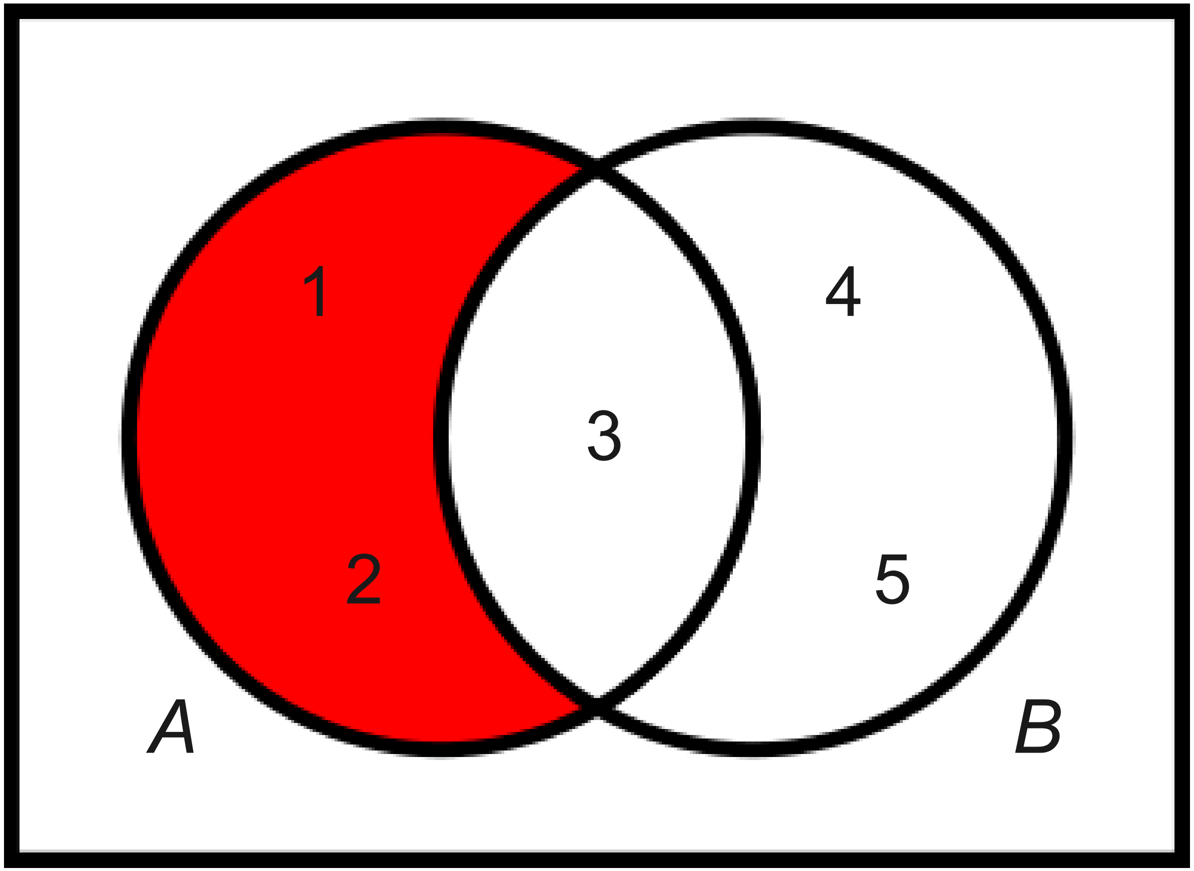
$B = \{ 3, 4, 5 \}$

Venn Diagrams



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

Venn Diagrams



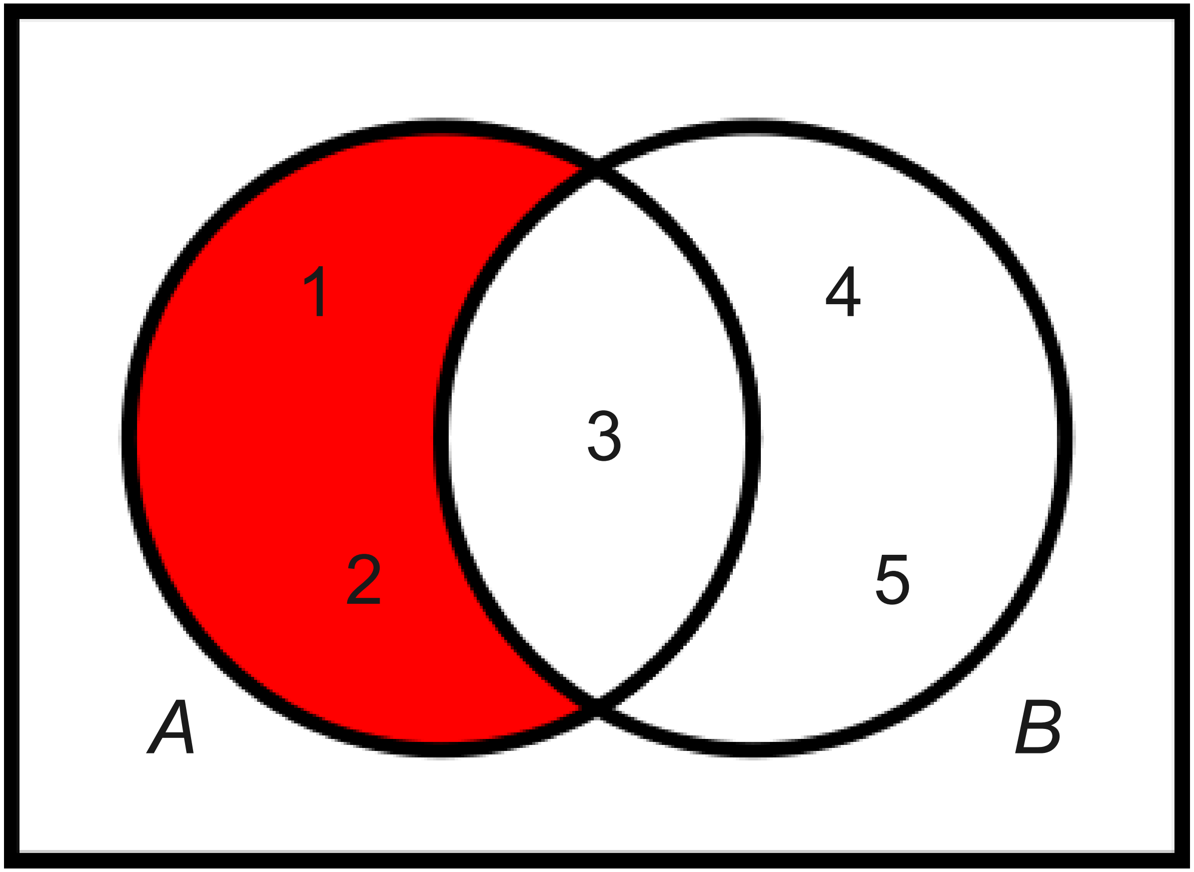
Difference

$A - B$

$\{ 1, 2 \}$

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

Venn Diagrams



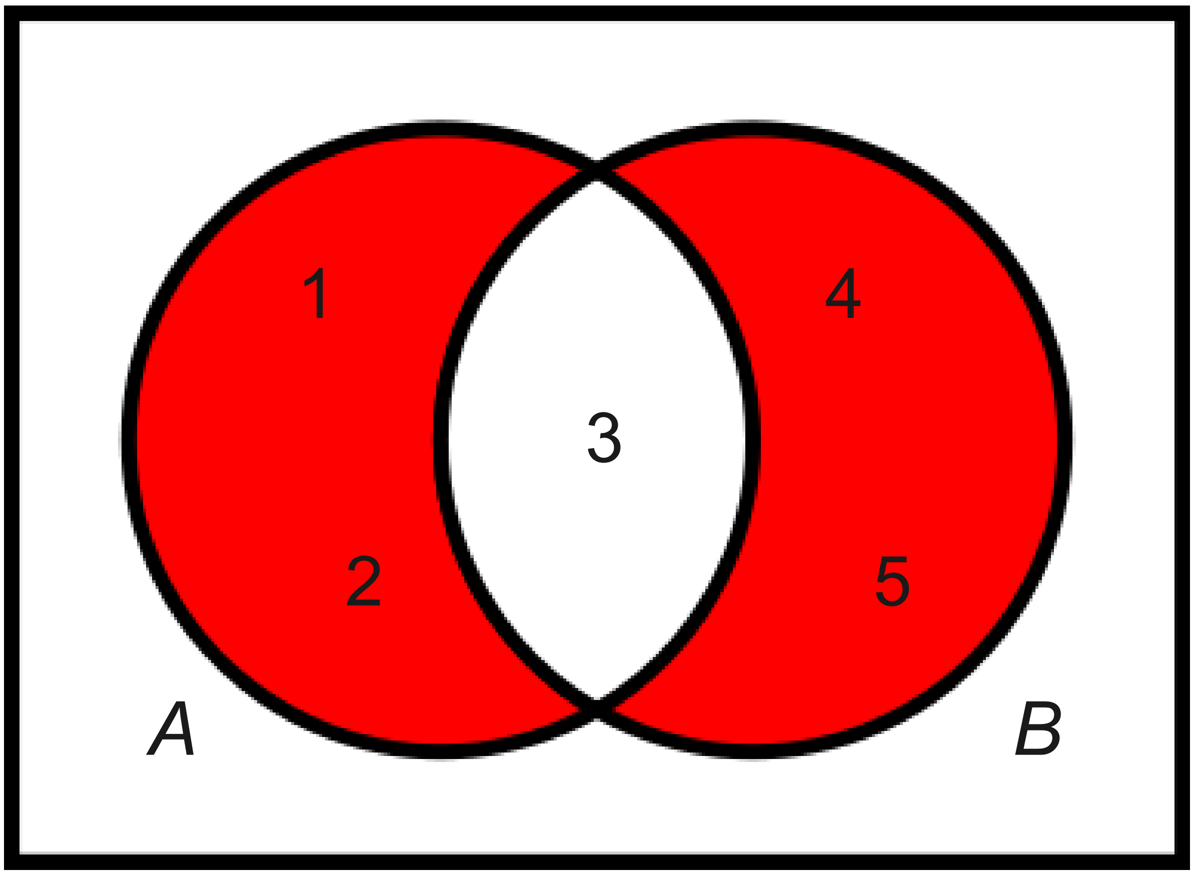
Difference

$A \setminus B$

$\{ 1, 2 \}$

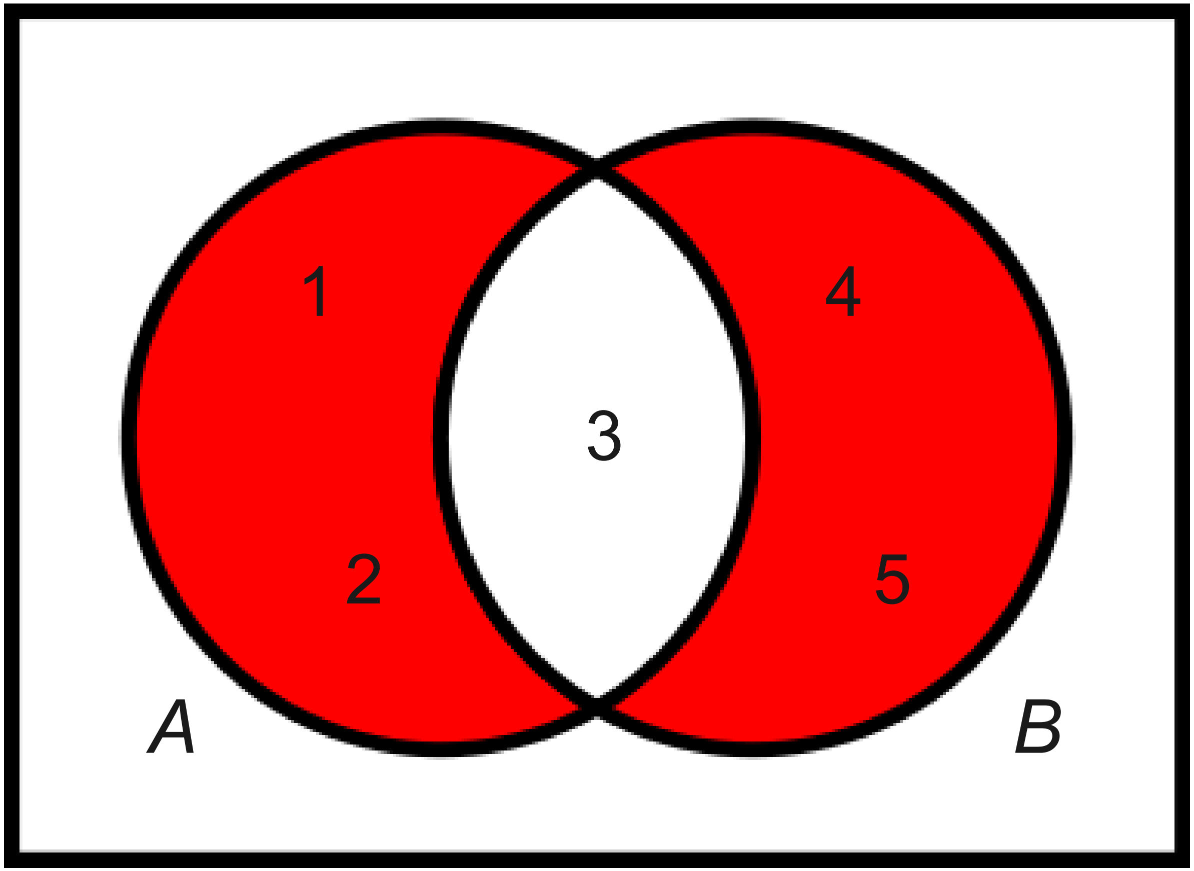
$A = \{ 1, 2, 3 \}$
$B = \{ 3, 4, 5 \}$

Venn Diagrams



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

Venn Diagrams



Symmetric Difference

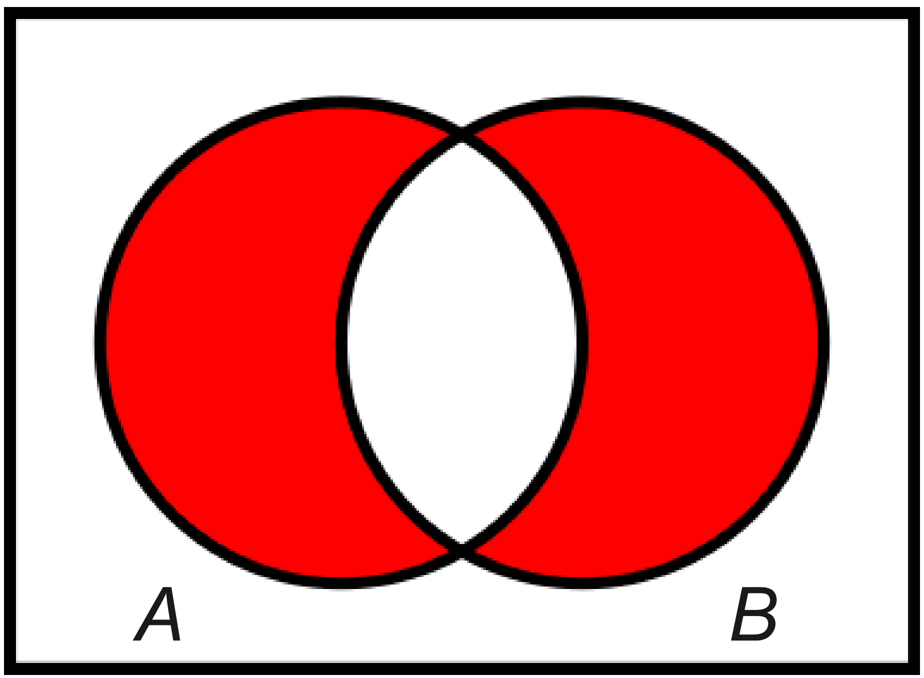
$A \,\Delta\, B$

{ 1, 2, 4, 5 }

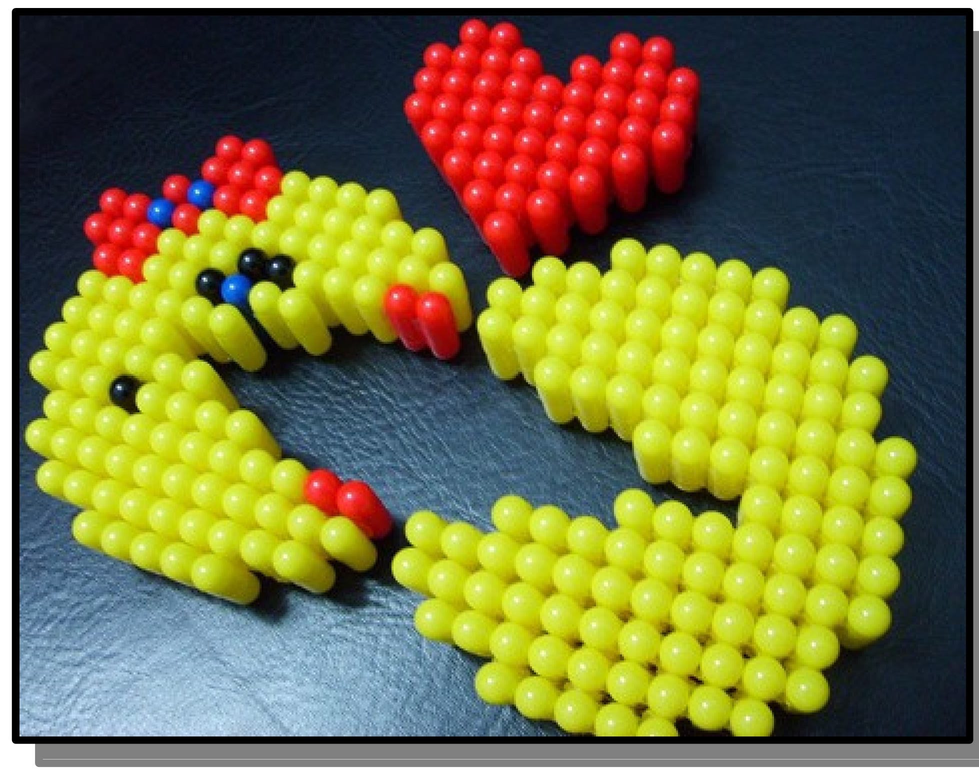
A = { 1, 2, 3 }

B = { 3, 4, 5 }

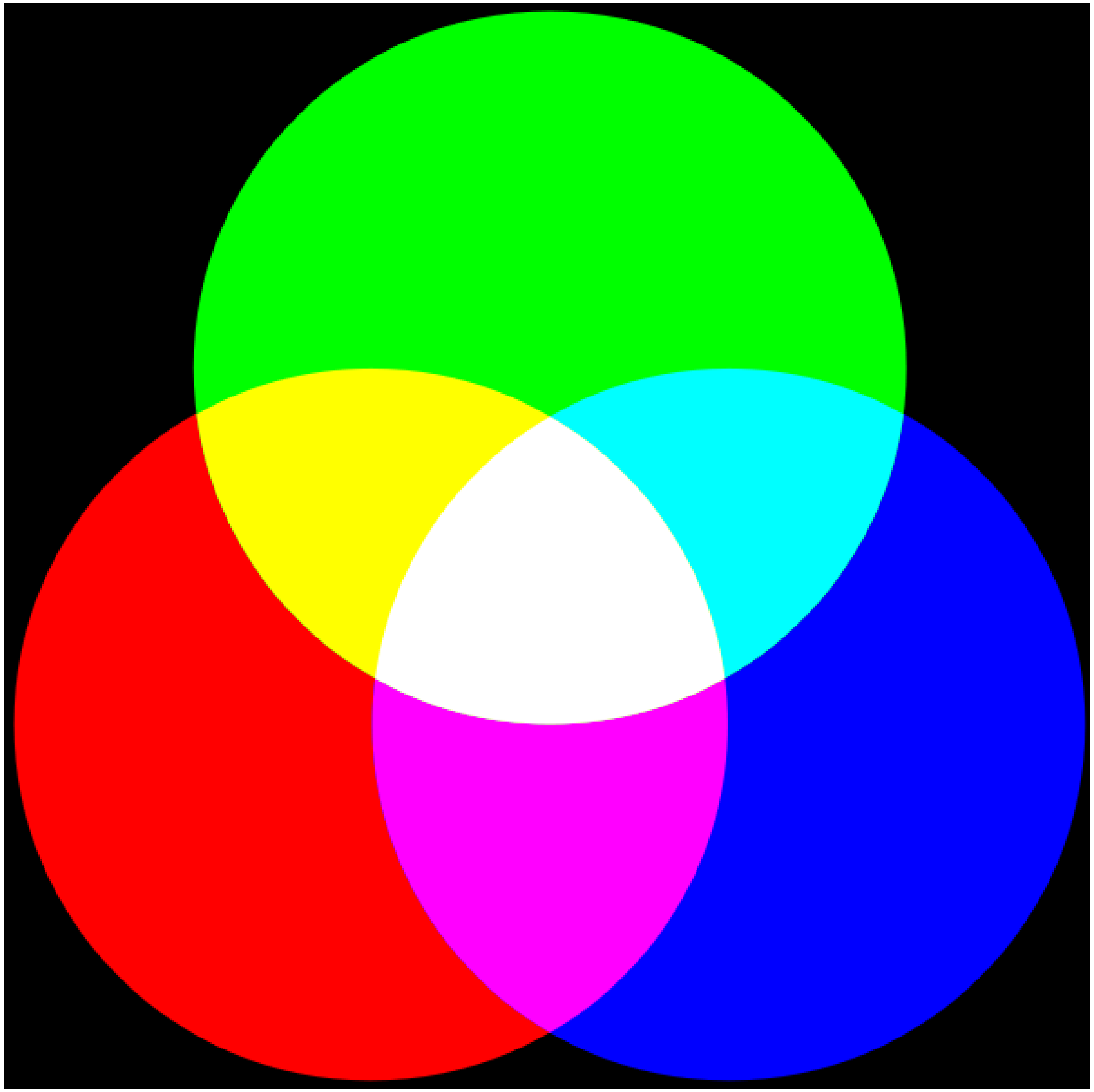
Venn Diagrams



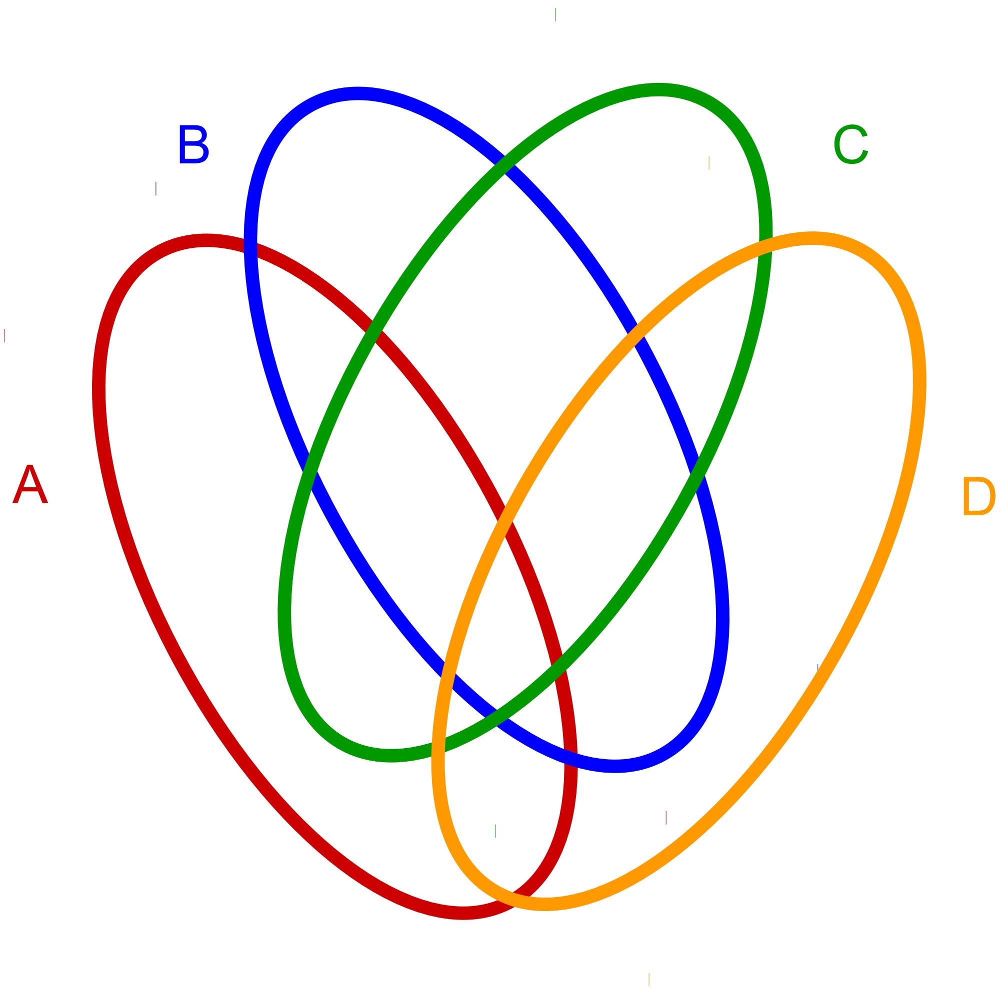
$A \, \Delta \, B$



Venn Diagrams for Three Sets

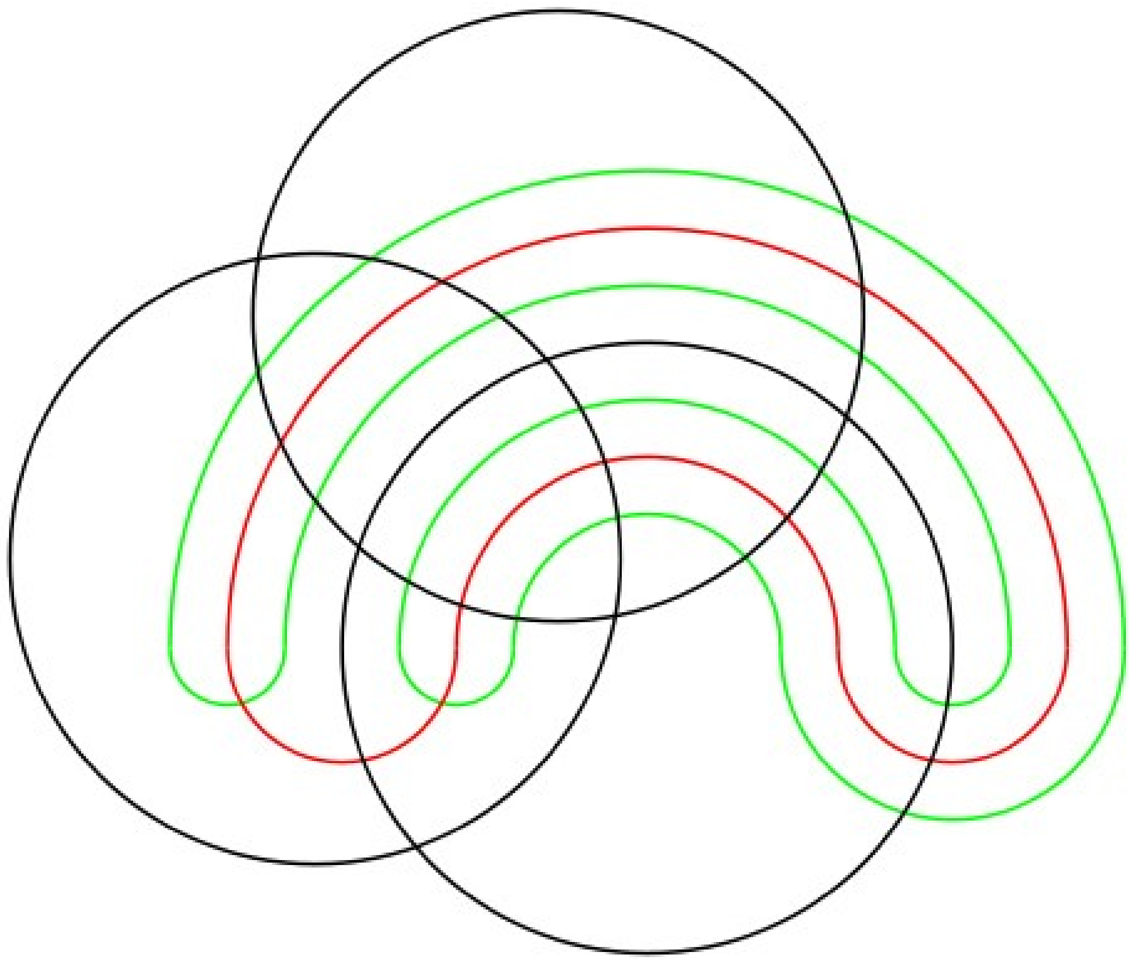


Venn Diagrams for Four Sets

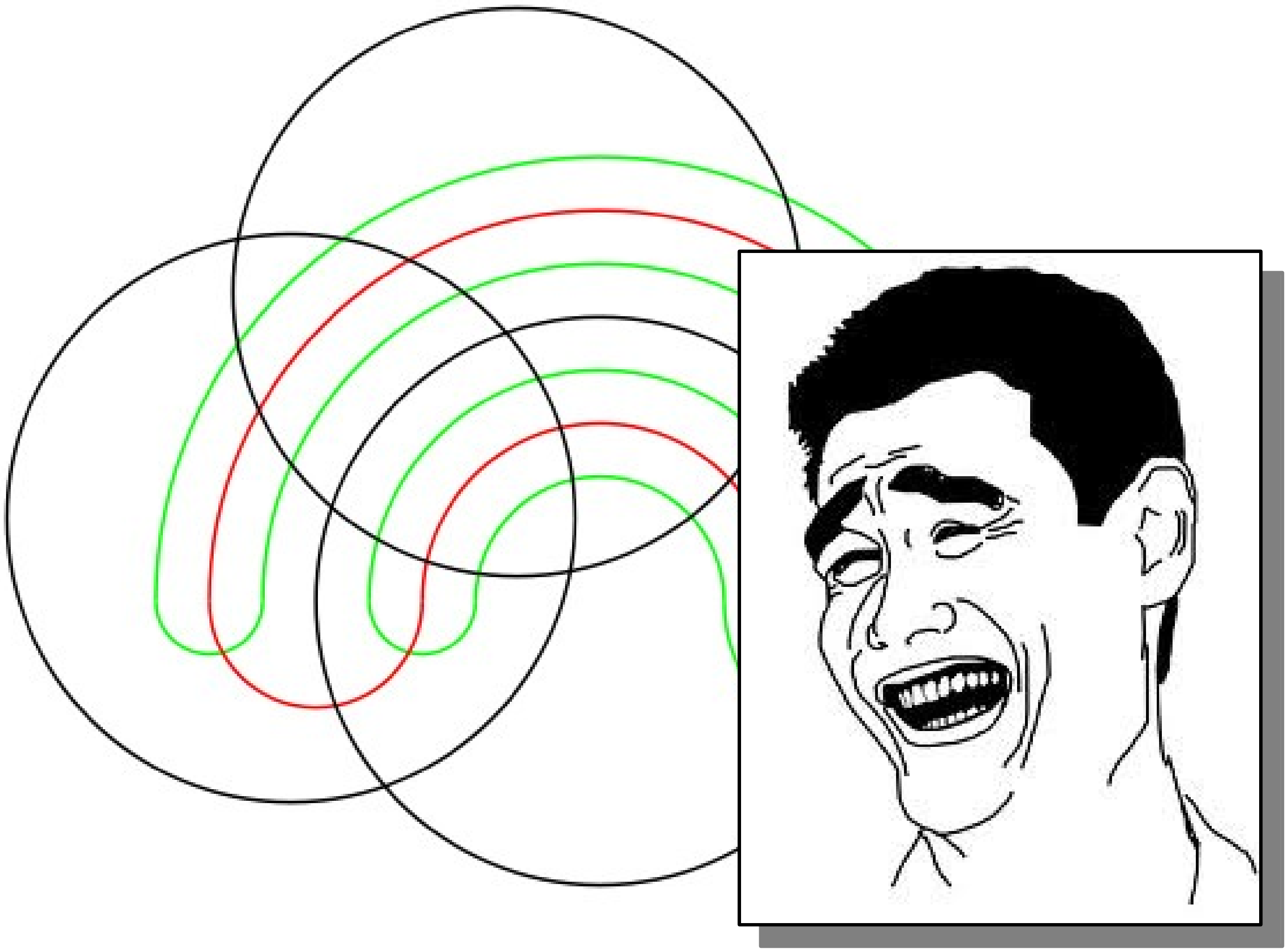


Venn Diagrams for Five Sets

Venn Diagrams for Five Sets

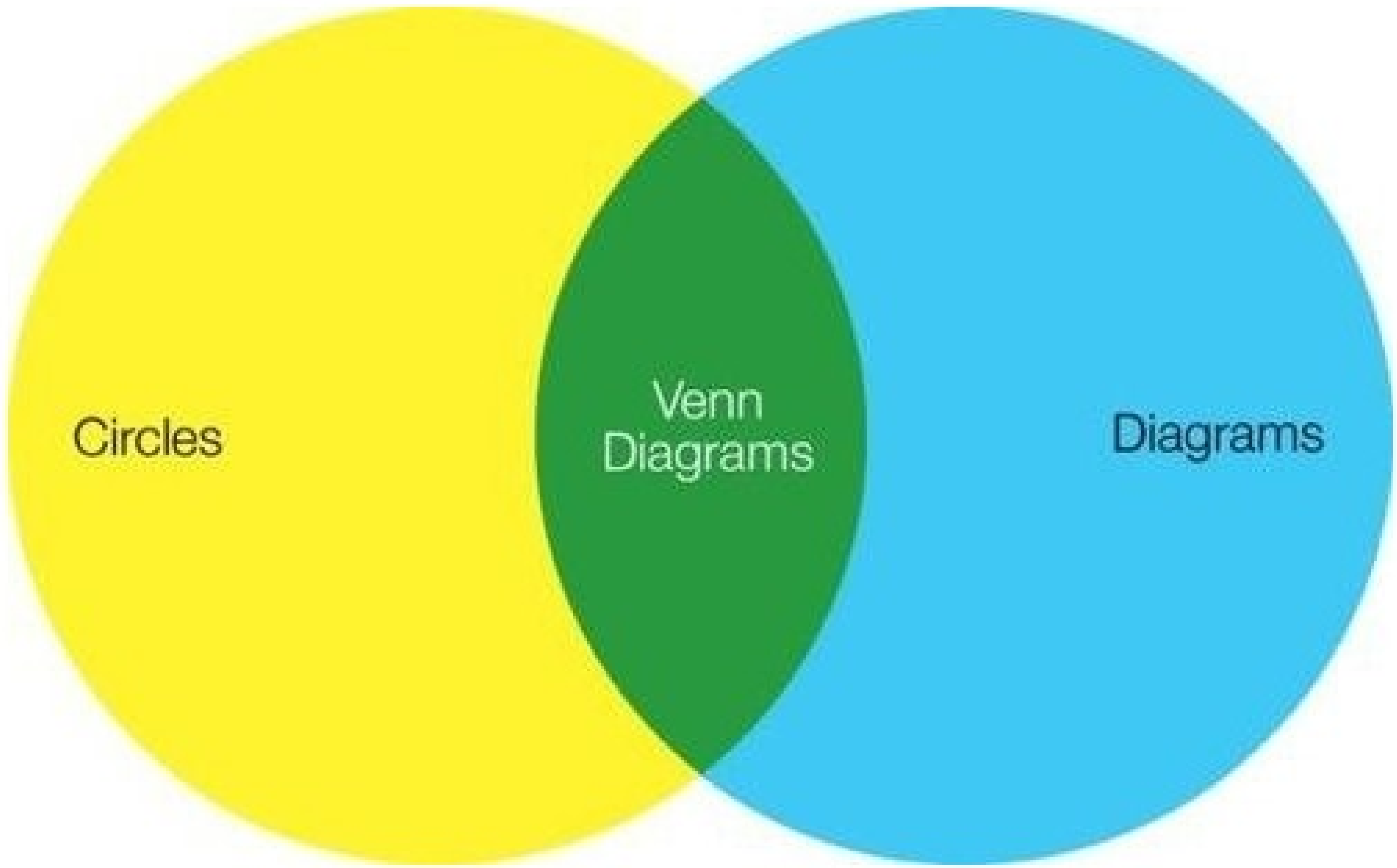


Venn Diagrams for Five Sets

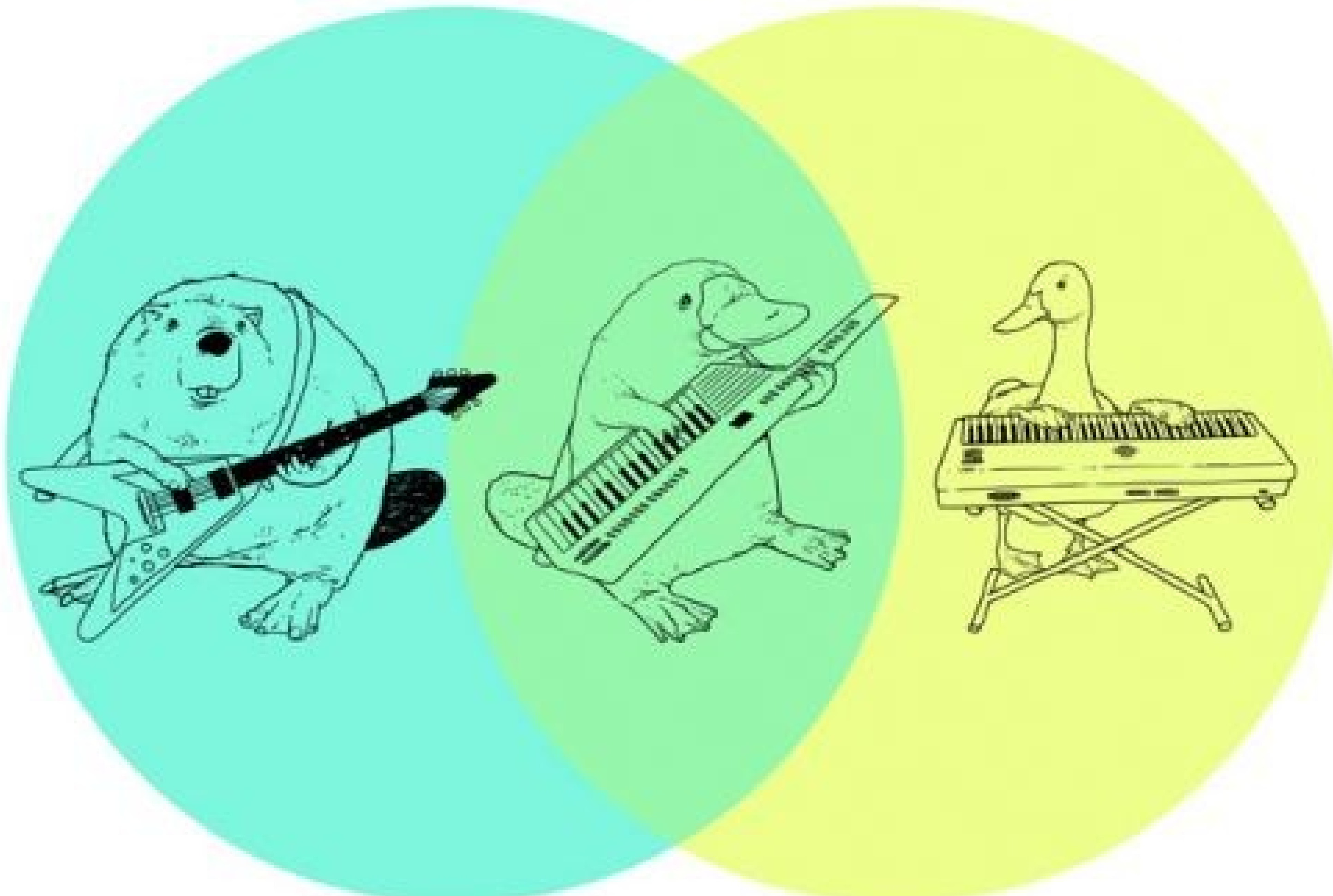


Meta Venn Diagram

Meta Venn Diagram



Animals with Instruments



Subsets and Power Sets

Subsets

- A set S is a **subset** of some set T if every element of S is also an element in T:

$$\text{For all } x \in S,\ x \in T.$$

- We denote this as $\boldsymbol{S \subseteq T}$.
- Examples:
  - $\{ 1, 2, 3 \} \subseteq \{ 1, 2, 3, 4 \}$
  - $\mathbb{N} \subseteq \mathbb{Z}$
  - $\mathbb{Z} \subseteq \mathbb{R}$

What About the Empty Set?

- A set S is a **subset** of some set T if every element of S is also an element in T:

$$\text{For all } x \in S,\ x \in T.$$

- Is $\emptyset \subseteq S$ for any set S?

What About the Empty Set?

- A set S is a **subset** of some set T if every element of S is also an element in T:

$$\text{For all } x \in S,\ x \in T.$$

- Is $\varnothing \subseteq S$ for any set S?
- **Yes**: The above statement is always true.
- **Vacuous truth**: A statement that is true because it does not apply to anything.
  - "All unicorns are blue."
  - "All unicorns are pink."
  - "Every prime number divisible by 3 and 5 is divisible by 7."

Proper Subsets

- By definition, any set is a subset of itself. *(Why?)*
- A **proper subset** of a set S is a set T such that
  - $T \subseteq S$
  - $T \neq S$
- There are multiple notations for this; they all mean the same thing:
  - $T \subsetneq S$
  - $T \subset S$

$S = \{$ 

, 

$\}$

S = {  ,  }

∅ {  } {  } {  ,  }

$S = \{$ ,  $\}$

$\{\emptyset,\{$  $\},\{$  $\},\{$ ,  $\}\}$

$S = \{$  ,  $\}$

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

$S = \{$  ,  $\}$

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

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

Cardinalities

Cardinality

- The **cardinality** of a set is the number of elements it contains.
- Denoted $|S|$.
- Examples:
  - $|\{ 1, 2, 3, 3, 3, 3, 3 \}| = 3$
  - $|\{ \{ a, b \}, \{ c, d, e, f, g \}, \{ h \} \}| = 3$
  - $|\{ x \mid x \in \mathbb{N}, x \geq 0, x < 137 \}| = 137$

What is the cardinality of $\mathbb{N}$?

- There are infinitely many natural numbers!
- The cardinality of $\mathbb{N}$ is not any natural number, since it's infinitely large.
- We need to introduce a new term.

What is the cardinality of ℕ?

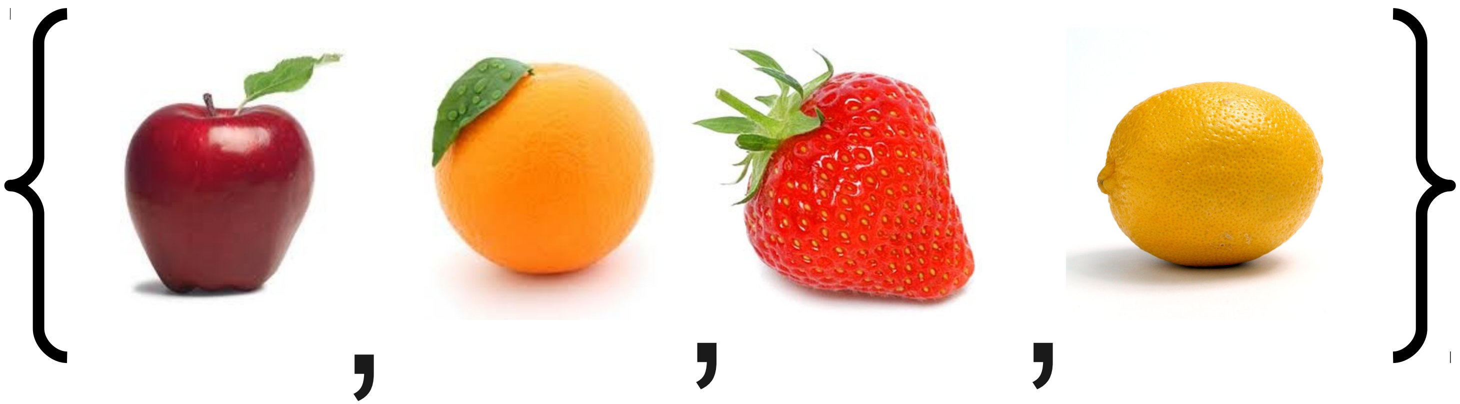
- There are infinitely many natural numbers!
- The cardinality of ℕ is not any natural number, since it's infinitely large.
- We need to introduce a new term.
- Definition: $|\mathbb{N}| = \aleph_0$
  - Pronounced “Aleph-Zero” or “Aleph-Null”

Consider the set

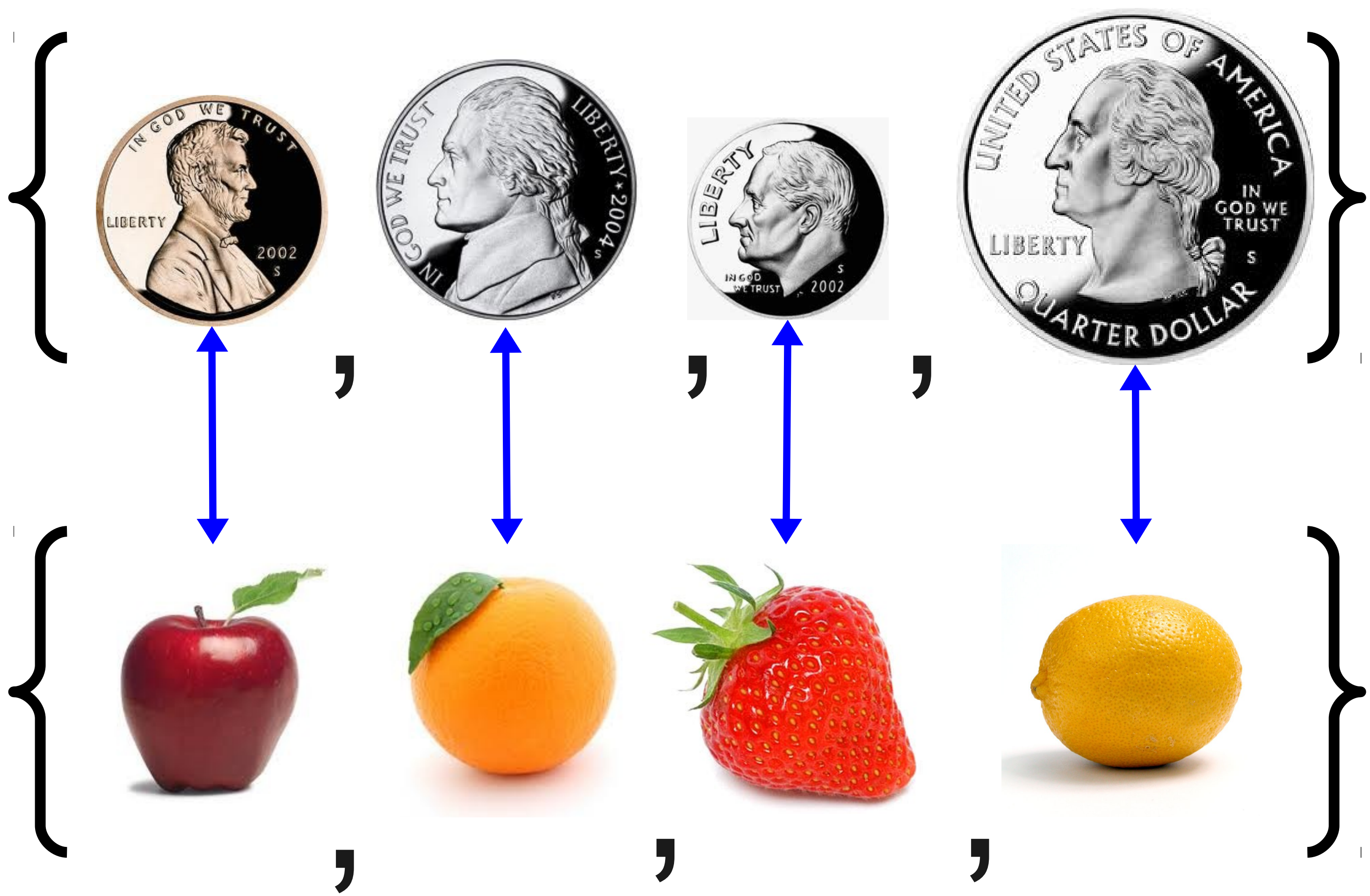
$S = \{ x \mid x \in \mathbb{N} \text{ and x is even } \}$

What is $|S|$?

How Big Are These Sets?

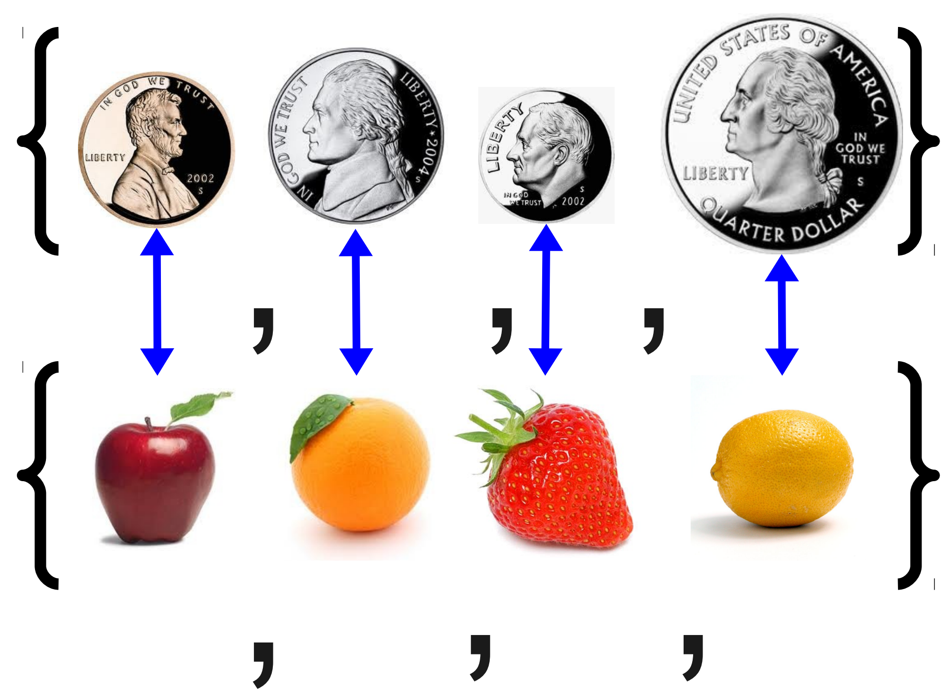


How Big Are These Sets?



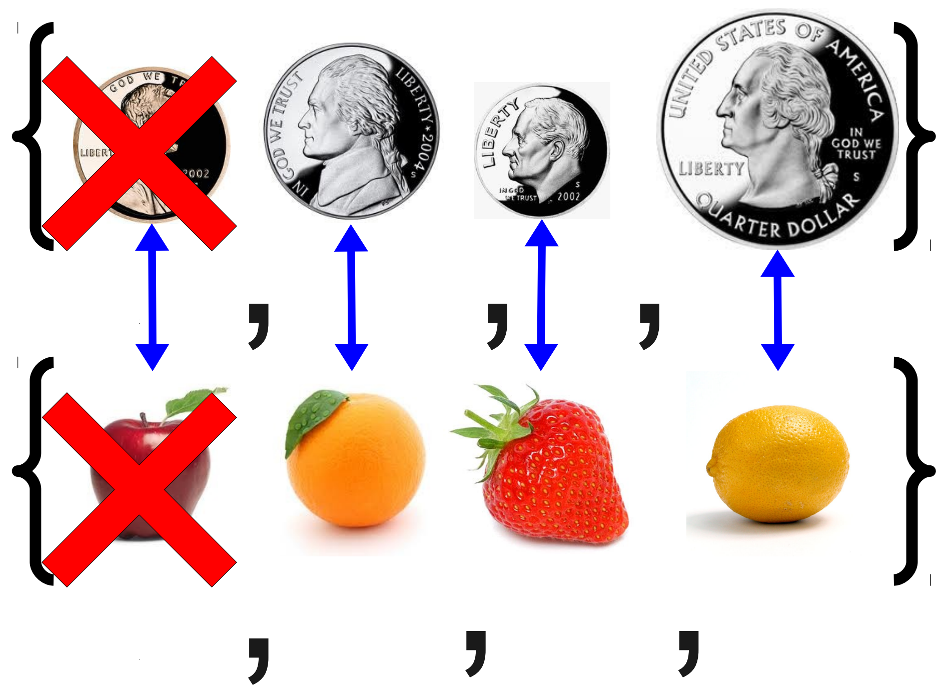
Comparing Cardinalities

- Two sets have the same cardinality if their elements can be put into a one-to-one correspondence with one another.
- The intuition:



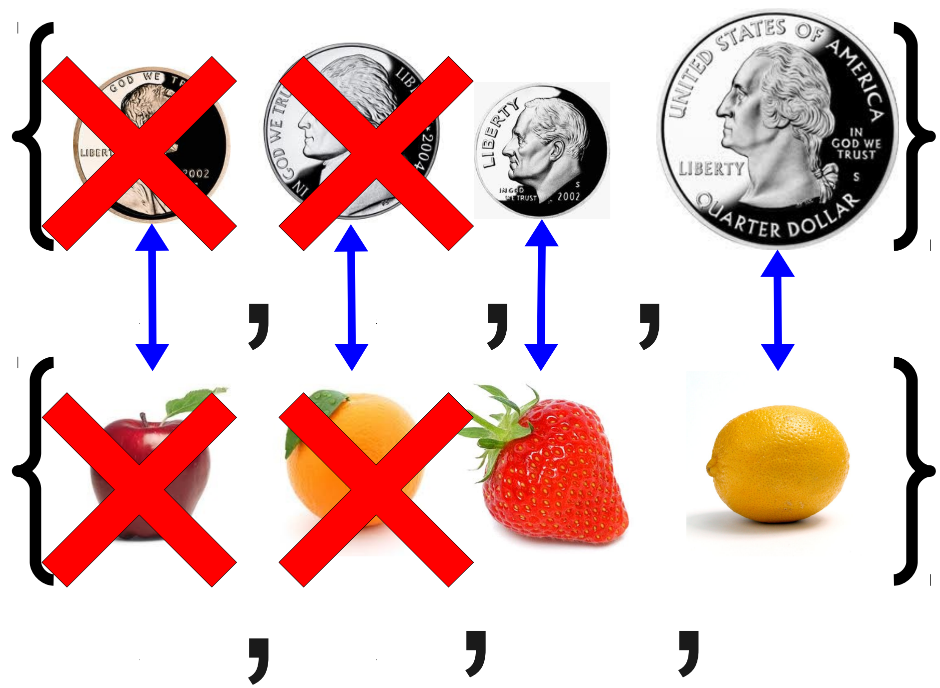
Comparing Cardinalities

- Two sets have the same cardinality if their elements can be put into a one-to-one correspondence with one another.
- The intuition:



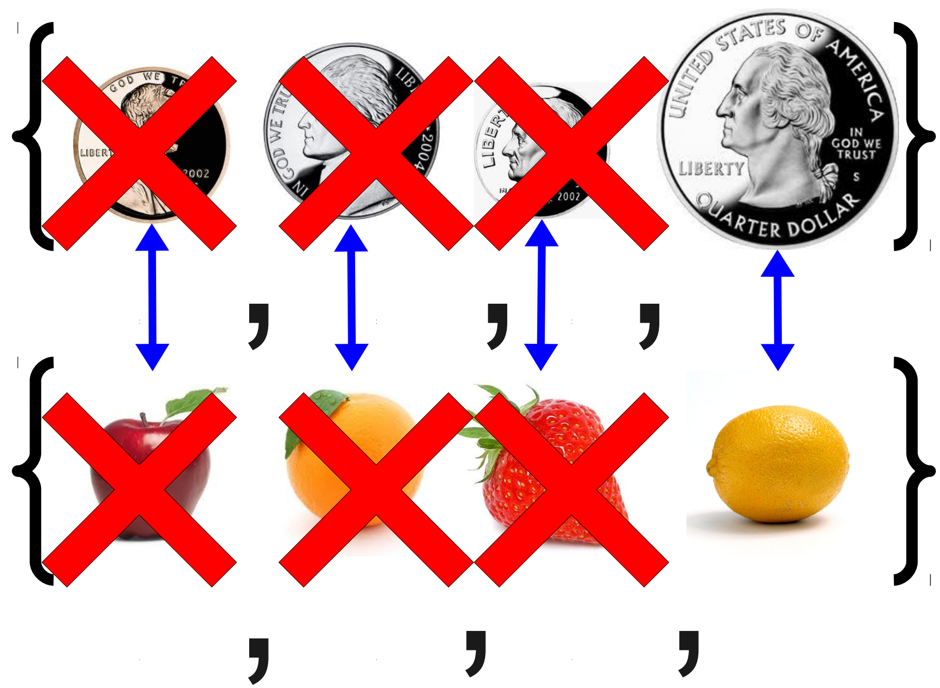
Comparing Cardinalities

- Two sets have the same cardinality if their elements can be put into a one-to-one correspondence with one another.
- The intuition:



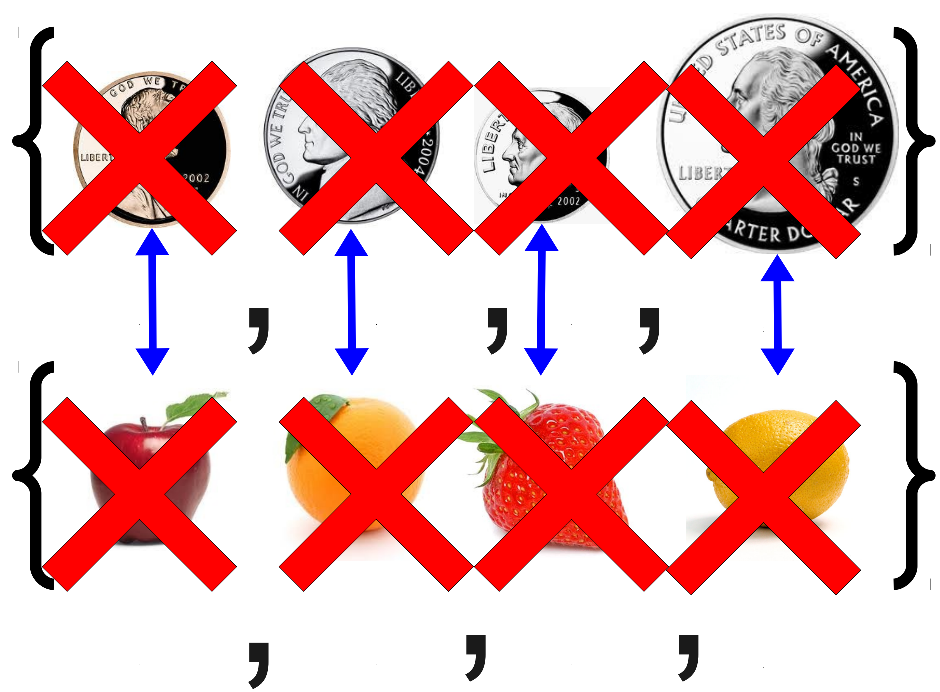
Comparing Cardinalities

- Two sets have the same cardinality if their elements can be put into a one-to-one correspondence with one another.
- The intuition:



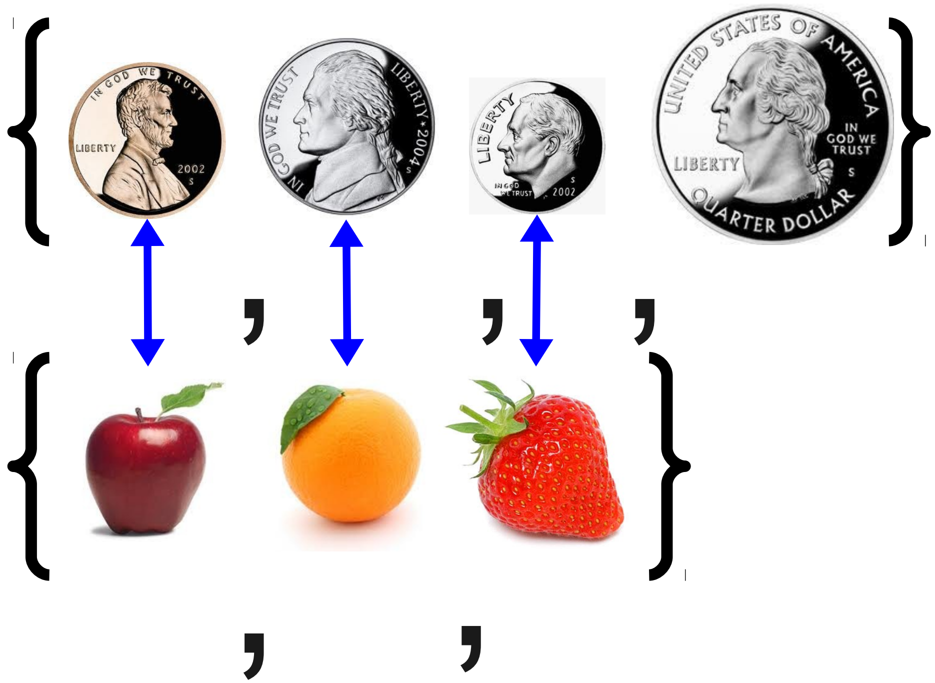
Comparing Cardinalities

- Two sets have the same cardinality if their elements can be put into a one-to-one correspondence with one another.
- The intuition:



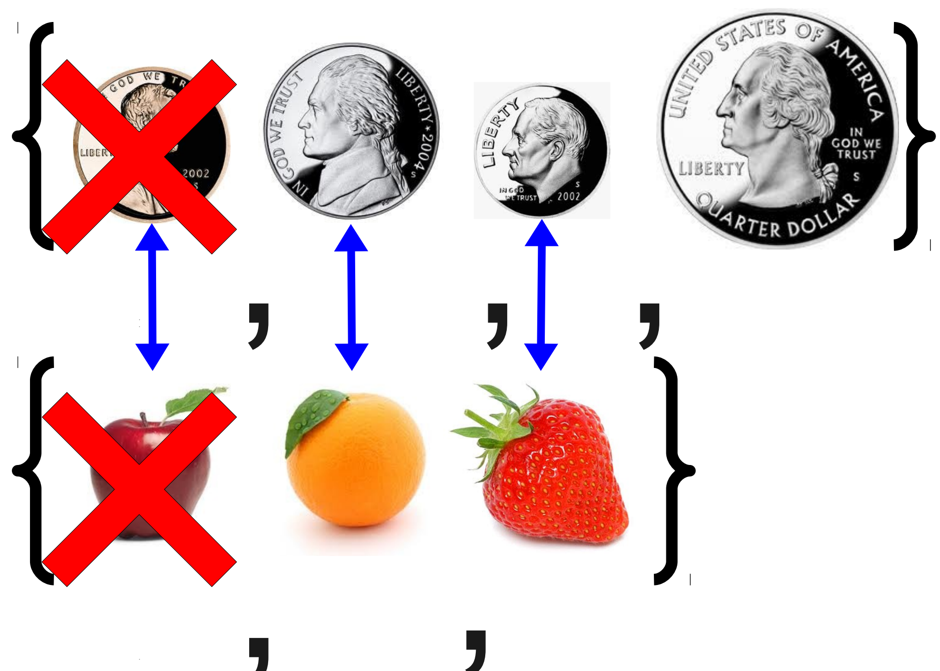
Comparing Cardinalities

- Two sets have the same cardinality if their elements can be put into a one-to-one correspondence with one another.
- The intuition:



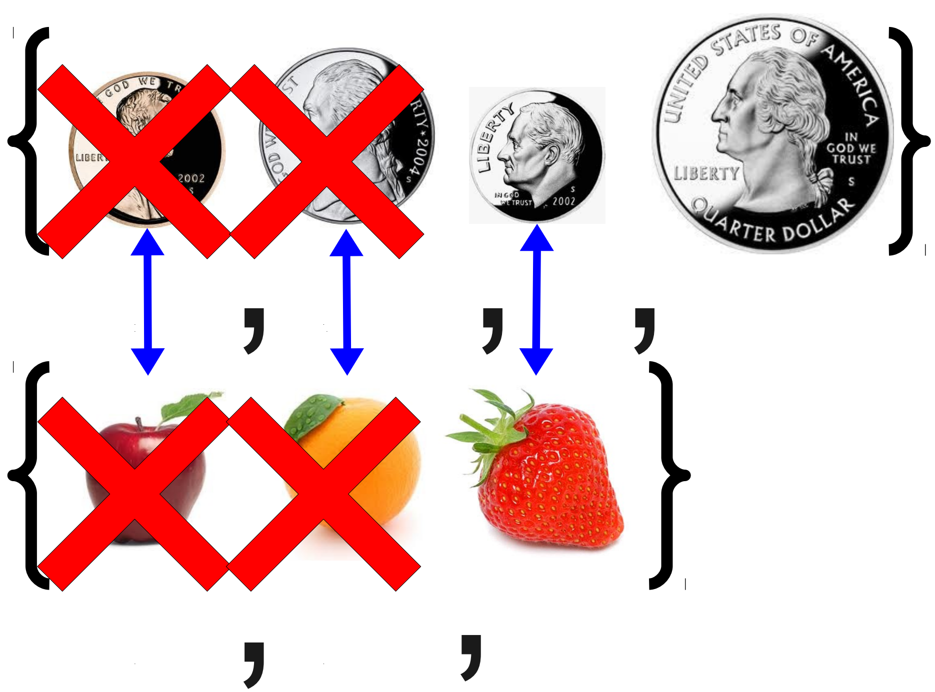
Comparing Cardinalities

- Two sets have the same cardinality if their elements can be put into a one-to-one correspondence with one another.
- The intuition:



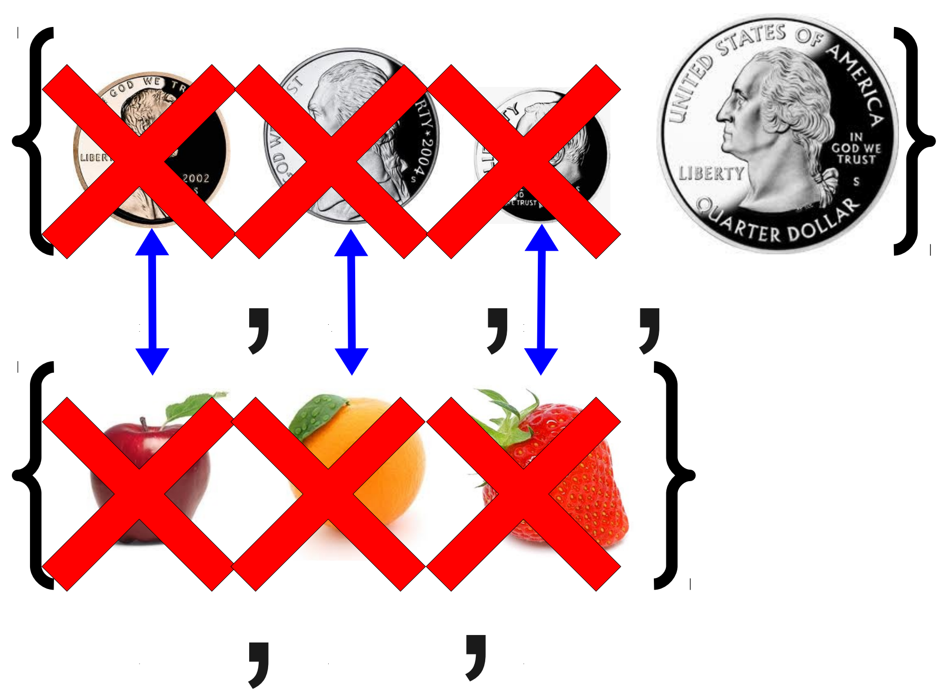
Comparing Cardinalities

- Two sets have the same cardinality if their elements can be put into a one-to-one correspondence with one another.
- The intuition:



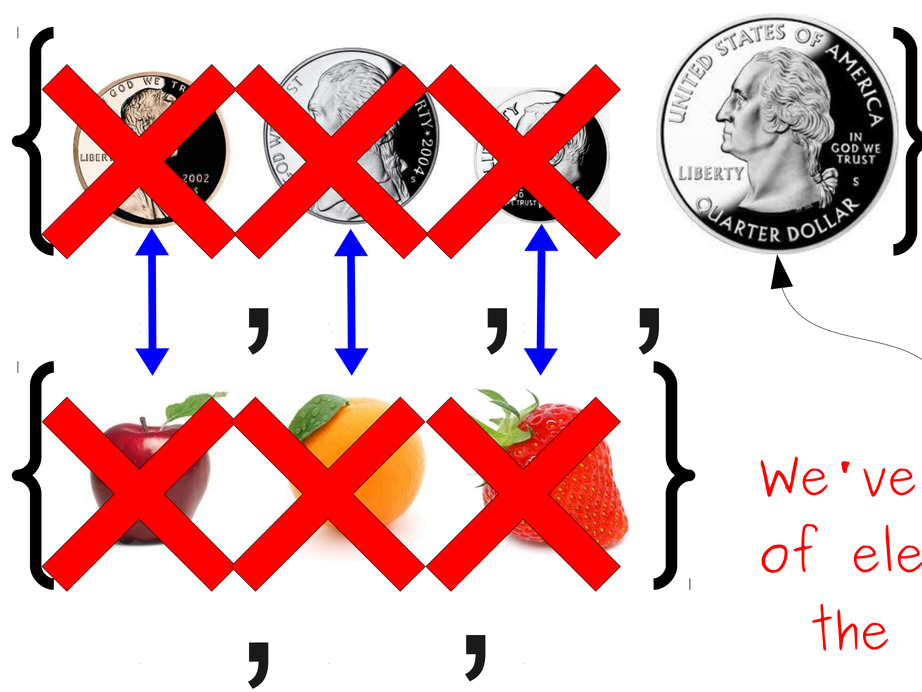
Comparing Cardinalities

- Two sets have the same cardinality if their elements can be put into a one-to-one correspondence with one another.
- The intuition:



Comparing Cardinalities

- Two sets have the same cardinality if their elements can be put into a one-to-one correspondence with one another.
- The intuition:



We've run out of elements in the second set!

Infinite Cardinalities

0	1	2	3	4	5	6	7	8	...
0	2	4	6	8	10	12	14	16	...

Infinite Cardinalities

0	1	2	3	4	5	6	7	8	...
0	2	4	6	8	10	12	14	16	...

$$n \leftrightarrow 2n$$

Infinite Cardinalities

0	1	2	3	4	5	6	7	8	...
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	
0	2	4	6	8	10	12	14	16	...

$$n \leftrightarrow 2n$$

Infinite Cardinalities

$$
\begin{array}{cccccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \ldots \\
\updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\
0 & 2 & 4 & 6 & 8 & 10 & 12 & 14 & 16 & \ldots
\end{array}
$$

$$n \leftrightarrow 2n$$

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

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

Infinite Cardinalities

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	...
$\mathbb{Z}$	...	-3	-2	-1	0	1	2	3	4	...

Infinite Cardinalities

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	...
$\mathbb{Z}$	0	1	-1	2	-2	3	-3	4	-4	...

Infinite Cardinalities

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	...
$\mathbb{Z}$	0	1	-1	2	-2	3	-3	4	-4	...

$n \leftrightarrow$ if n is even, then $-n/2$
if n is odd, then $(n + 1) / 2$

Infinite Cardinalities

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	...
	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	
$\mathbb{Z}$	0	1	-1	2	-2	3	-3	4	-4	...

$n \leftrightarrow$ if n is even, then $-n/2$
if n is odd, then $(n + 1) / 2$

Infinite Cardinalities

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	...
	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	
$\mathbb{Z}$	0	1	-1	2	-2	3	-3	4	-4	...

$n \leftrightarrow$ if n is even, then $-n/2$
if n is odd, then $(n + 1) / 2$

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

The Limits of Computation

Properties

- Given a set S, a **property of S** is a yes/no question that may be asked of any element of S.
- Examples:
  - A property of $\mathbb{N}$ is "is n even?"
  - A property of $\mathbb{R}$ is "is x rational?"
  - A property of the set of strings is "is s a legal Java program?"

Properties as Sets

- Any property of *S* can be described by the subset of *S* of elements with that property.
- The property "is *x* even?":
  - { 0, 2, 4, 6, 8, … }
- The property "is *x* a palindrome?":
  - { "", "a", "b", "aa", "bb", "aaa", "aba", ... }

Counting Properties

- Each subset of S defines some property and vice-versa.
- The set of properties is therefore $\wp(S)$.
- How does $|S|$ relate to $|\wp(S)|$?
- The result is known as **Cantor's Theorem**.

Prepare for one of the most beautiful (and surprising!) proofs in mathematics...

Suppose that $|S| = |\wp(S)|$.

This would mean that there is a one-to-one correspondence between elements of S and sets of elements of S.

What might this look like?

x_0

x_1

x_2

x_3

x_4

x_5

...

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

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

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

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

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

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

$$\ldots$$

x_0	x_1	x_2	x_3	x_4	x_5	…

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

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

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

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

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

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

…

	x_0	x_1	x_2	x_3	x_4	x_5	…
$x_0 \leftrightarrow$	**Y**	**N**	**Y**	**N**	**Y**	**N**	…

$x_1 \leftrightarrow \{ x_0, x_3, x_4, \ldots \}$

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

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

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

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

…

	x_0	x_1	x_2	x_3	x_4	x_5	…
$x_0 \leftrightarrow$	**Y**	**N**	**Y**	**N**	**Y**	**N**	…

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

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

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

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

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

…

This string of Ys and Ns is called a <u>characteristic vector</u>. Every characteristic vector defines a set, and vice-versa.

	x_0	x_1	x_2	x_3	x_4	x_5	…
$x_0 \longleftrightarrow$	**Y**	**N**	**Y**	**N**	**Y**	**N**	…
$x_1 \longleftrightarrow$	**Y**	**N**	**N**	**Y**	**Y**	**N**	…

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

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

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

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

…

	x_0	x_1	x_2	x_3	x_4	x_5	…
$x_0 \longleftrightarrow$	**Y**	**N**	**Y**	**N**	**Y**	**N**	…
$x_1 \longleftrightarrow$	**Y**	**N**	**N**	**Y**	**Y**	**N**	…
$x_2 \longleftrightarrow$	**N**	**N**	**N**	**N**	**Y**	**N**	…

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

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

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

…

	x_0	x_1	x_2	x_3	x_4	x_5	…
$x_0 \leftrightarrow$	**Y**	**N**	**Y**	**N**	**Y**	**N**	…
$x_1 \leftrightarrow$	**Y**	**N**	**N**	**Y**	**Y**	**N**	…
$x_2 \leftrightarrow$	**N**	**N**	**N**	**N**	**Y**	**N**	…
$x_3 \leftrightarrow$	**N**	**Y**	**N**	**N**	**Y**	**N**	…

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

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

…

	x_0	x_1	x_2	x_3	x_4	x_5	…
$x_0 \leftrightarrow$	**Y**	**N**	**Y**	**N**	**Y**	**N**	…
$x_1 \leftrightarrow$	**Y**	**N**	**N**	**Y**	**Y**	**N**	…
$x_2 \leftrightarrow$	**N**	**N**	**N**	**N**	**Y**	**N**	…
$x_3 \leftrightarrow$	**N**	**Y**	**N**	**N**	**Y**	**N**	…
$x_4 \leftrightarrow$	**Y**	**N**	**N**	**N**	**N**	**Y**	…

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

…

	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	**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**	…
…	…	…	…	…	…	…	…

	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_3	**Y**	**N**	**N**	**N**	**N**	**Y**	…
X_4	**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_3	Y	N	N	N	N	Y	...
X_4	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_3	Y	N	N	N	N	Y	...
X_4	Y	Y	Y	Y	Y	Y	...
...	...	...	...	...	...	...	...

Y	N	N	N	N	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_3	**Y**	**N**	**N**	**N**	**N**	**Y**	...
X_4	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	...
...	...	...	...	...	...	...	...

Y	**N**	**N**	**N**	**N**	**Y**	...

Which row in the table has this characteristic vector?

	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_3	**Y**	**N**	**N**	**N**	**N**	**Y**	…
x_4	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	…
…	…	…	…	…	…	…	…

Y	**N**	**N**	**N**	**N**	**Y**	…

Which row in the table has this characteristic vector?

	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_3	**Y**	**N**	**N**	**N**	**N**	**Y**	...
X_4	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	...
...	...	...	...	...	...	...	...

Y	**N**	**N**	**N**	**N**	**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_3	**Y**	**N**	**N**	**N**	**N**	**Y**	…
X_4	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	…
…	…	…	…	…	…	…	…

N	**Y**	**Y**	**Y**	**Y**	**N**	…

	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_3	**Y**	**N**	**N**	**N**	**N**	**Y**	...
X_4	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	...
...	...	...	...	...	...	...	...

Flip all Y's to N's and vice-versa to get a new characteristic vector.

N	**Y**	**Y**	**Y**	**Y**	**N**	...

	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_3	**Y**	**N**	**N**	**N**	**N**	**Y**	...
X_4	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	...
...	...	...	...	...	...	...	...

N	**Y**	**Y**	**Y**	**Y**	**N**	...

	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_3	**Y**	**N**	**N**	**N**	**N**	**Y**	...
X_4	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	...
...	...	...	...	...	...	...	...

N	**Y**	**Y**	**Y**	**Y**	**N**	...

Which row in the table has this characteristic vector?

	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_3	**Y**	**N**	**N**	**N**	**N**	**Y**	...
X_4	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	...
...	...	...	...	...	...	...	...

N	**Y**	**Y**	**Y**	**Y**	**N**	...

Which row in the table has this characteristic vector?

	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_3	**Y**	**N**	**N**	**N**	**N**	**Y**	...
x_4	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	...
...	...	...	...	...	...	...	...

Which row in the table has this characteristic vector?

N	**Y**	**Y**	**Y**	**Y**	**N**	...

	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_3	**Y**	**N**	**N**	**N**	**N**	**Y**	...
X_4	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	...
...	...	...	...	...	...	...	...

N	**Y**	**Y**	**Y**	**Y**	**N**	...

Which row in the table has this characteristic vector?

	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_3	Y	N	N	N	N	Y	...
X_4	Y	Y	Y	Y	Y	Y	...
...	...	...	...	...	...	...	...

N	Y	Y	Y	Y	N	...

Which row in the table has this characteristic vector?

	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_3	**Y**	**N**	**N**	**N**	**N**	**Y**	…
x_4	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	…
…	…	…	…	…	…	…	…

N	**Y**	**Y**	**Y**	**Y**	**N**	…

Which row in the table has this characteristic vector?

	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_3	**Y**	**N**	**N**	**N**	**N**	**Y**	...
X_4	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	...
...	...	...	...	...	...	...	...

N	**Y**	**Y**	**Y**	**Y**	**N**	...

Which row in the table has this characteristic vector?

	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_3	**Y**	**N**	**N**	**N**	**N**	**Y**	...
X_4	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	...
...	...	...	...	...	...	...	...

N	**Y**	**Y**	**Y**	**Y**	**N**	...

Which row in the table has this characteristic vector?

	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_3	**Y**	**N**	**N**	**N**	**N**	**Y**	…
X_4	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	…
…	…	…	…	…	…	…	…

N	**Y**	**Y**	**Y**	**Y**	**N**	…

Which row in the table has this characteristic vector?

	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_3	**Y**	**N**	**N**	**N**	**N**	**Y**	…
x_4	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	…
…	…	…	…	…	…	…	…

N	**Y**	**Y**	**Y**	**Y**	**N**	…

Which row in the table has this characteristic vector?

The Diagonalization Proof

- The **complemented diagonal** cannot appear anywhere in the table.
  - In row *n*, the *n*th element must be wrong.
- No matter how we try to assign subsets of *S* to elements of *S*, there will always be at least one subset left over.
- **Cantor's Theorem**: $|S| < |\wp(S)|$
  - Every set, even an infinite set, is smaller than its power set.
- This is called a **diagonalization proof**; we will see many of these over the course of the quarter.

What does this have to do with computation?

Strings and Programs

- Consider the set Σ^* of all strings.
  - Σ^* = { “”, “a”, “b”, “aa”, “ab”, “ba”, “bb”, “aaa”, … }
- Given some property *P* of strings, consider the following problem:

Write a program that accepts as input a string, then prints out whether or not that string has property *P*.

- The number of problems to solve is at least as large as the number of properties of strings.

Every computer program is a string.

Every computer program is a string.

So, there can't be any more programs than strings.

Every computer program is a string.

So, there can't be any more programs than strings.

There are fewer strings than problems.

Every computer program is a string.

So, there can't be any more programs than strings.

There are fewer strings than problems.

So, there are fewer programs than problems.

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

It Gets Worse

- Because there are more properties of strings than strings, we can't even *describe* some of the problems that we can't solve.
- Using more advanced set theory, we can show that there are *infinitely more* properties of strings than there are strings.
- In fact, if you pick a totally random property, the probability that you can solve it is *zero*.

But then it gets better...

Where We're Going

- **Given this hard theoretical limit, what *can* we compute?**
  - What are the hardest problems we *can* solve?
  - How powerful of a computer do we need to solve these problems?
  - Of what we can compute, what can we compute *efficiently*?
- **What tools do we need to reason about this?**
  - How do we build a mathematical model of computation?
  - How can we reason about this model?

Next Time

- **Mathematical Proof**
  - What is a mathematical proof?
  - How can we prove things with certainty?