Welcome to T35A

- Three Handouts
- Today:
  - Course Overview
  - Introduction to Set Theory
  - The Limits of Computation

The Course Website

Course Mailing :
teoriacomputacional@uaslp.edu.mx
http://carlosgi.work/tc/

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.
- Explore the **inherent complexity** of problems and why some problems are harder than others.

Introduction to Set Theory

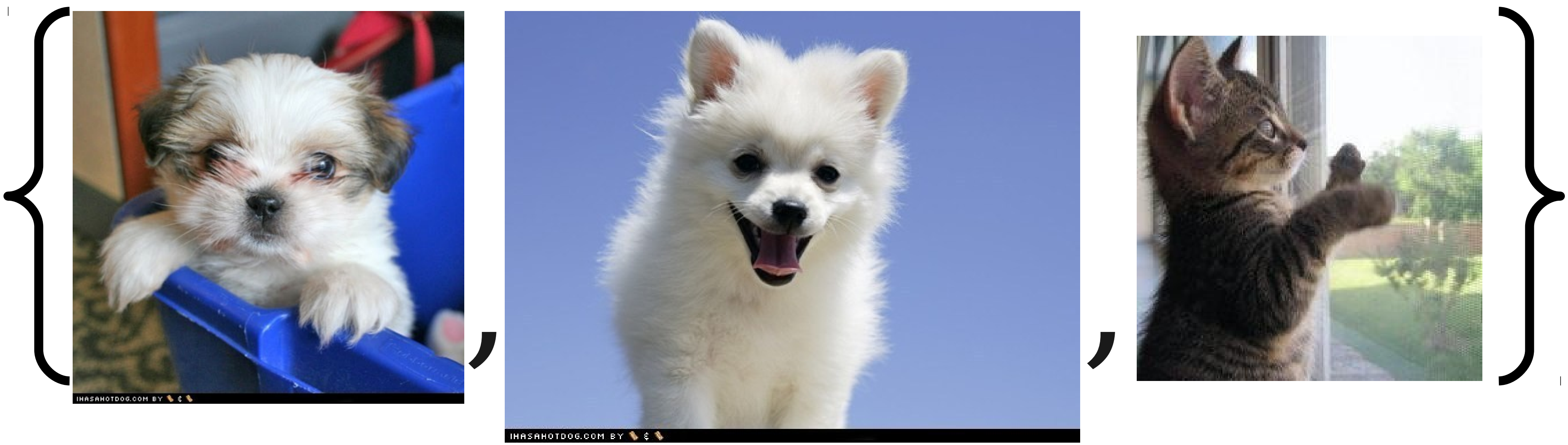
“Cool people”

“The chemical elements”

“Cute animals”

“US coins.”

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).

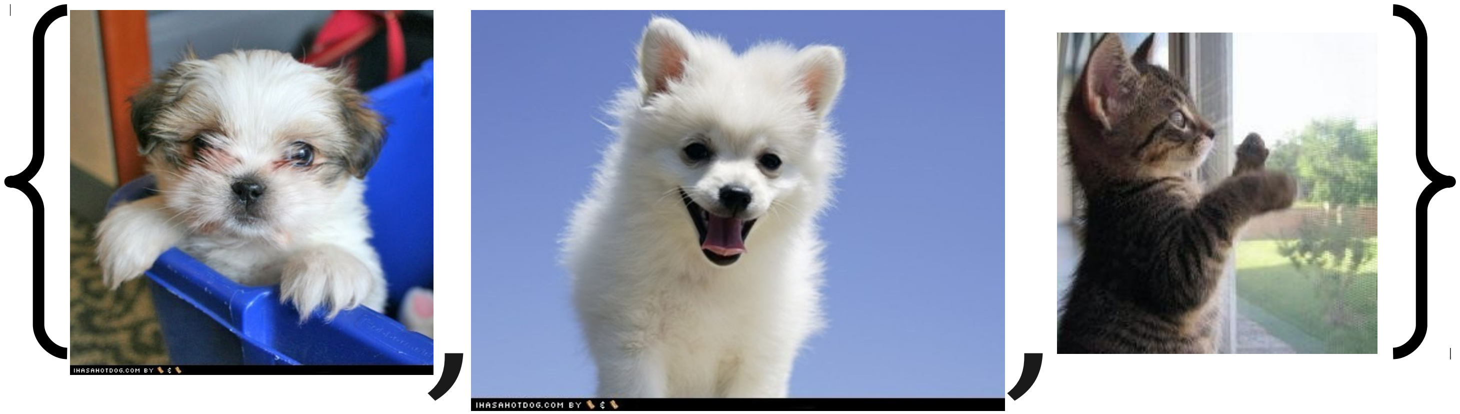
Set notation: Curly braces with commas separating out the elements

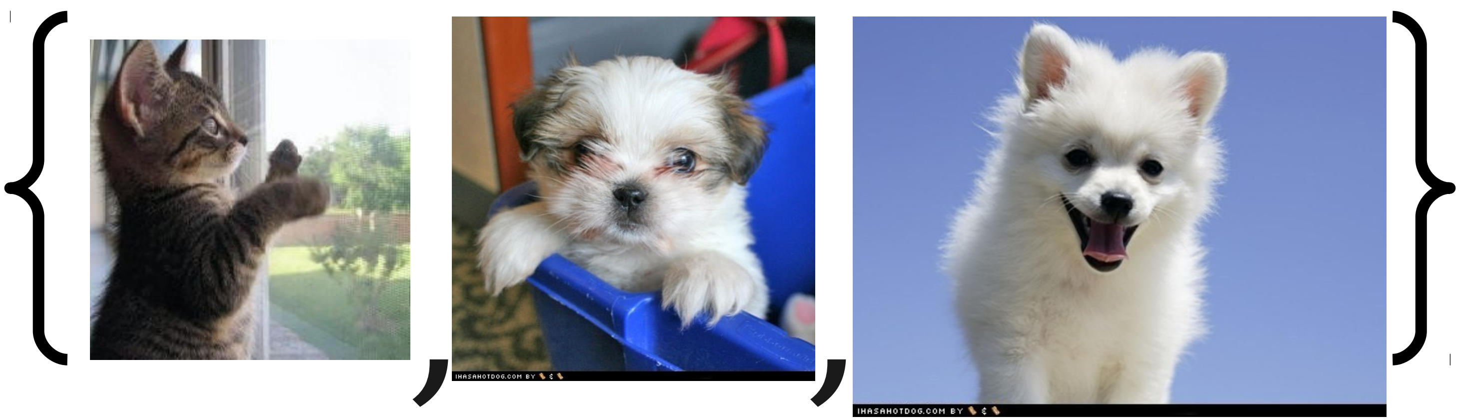
A **set** is an unordered collection of distinct objects, which may be anything (including other sets).

{ , ,  }

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).





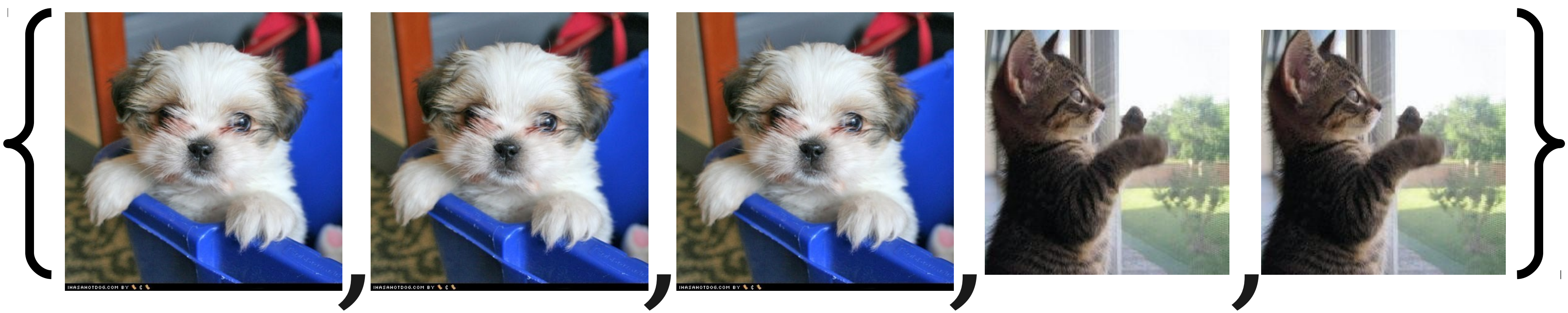
A **set** is an **unordered** collection of distinct objects, which may be anything (including other sets).

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

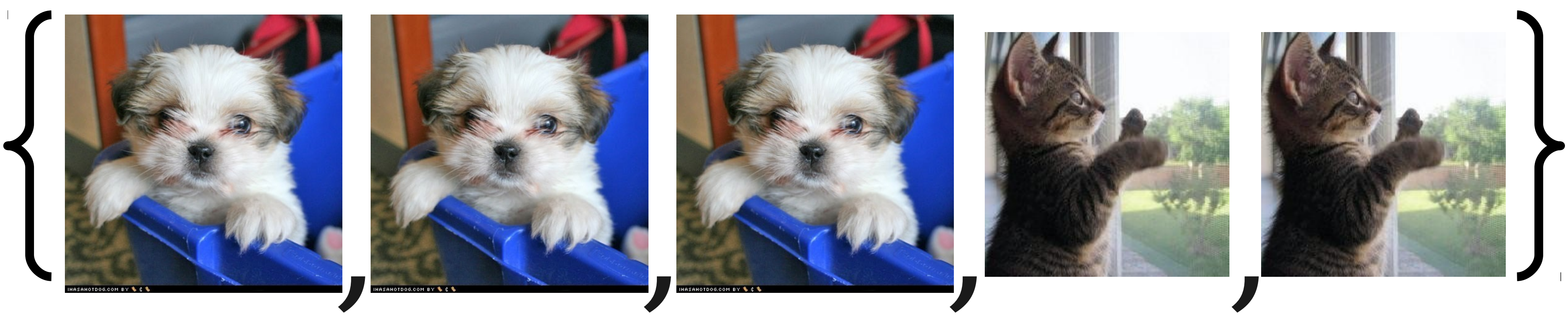
A **set** is an unordered collection of distinct objects, which may be anything (including other sets).

{ ,  }

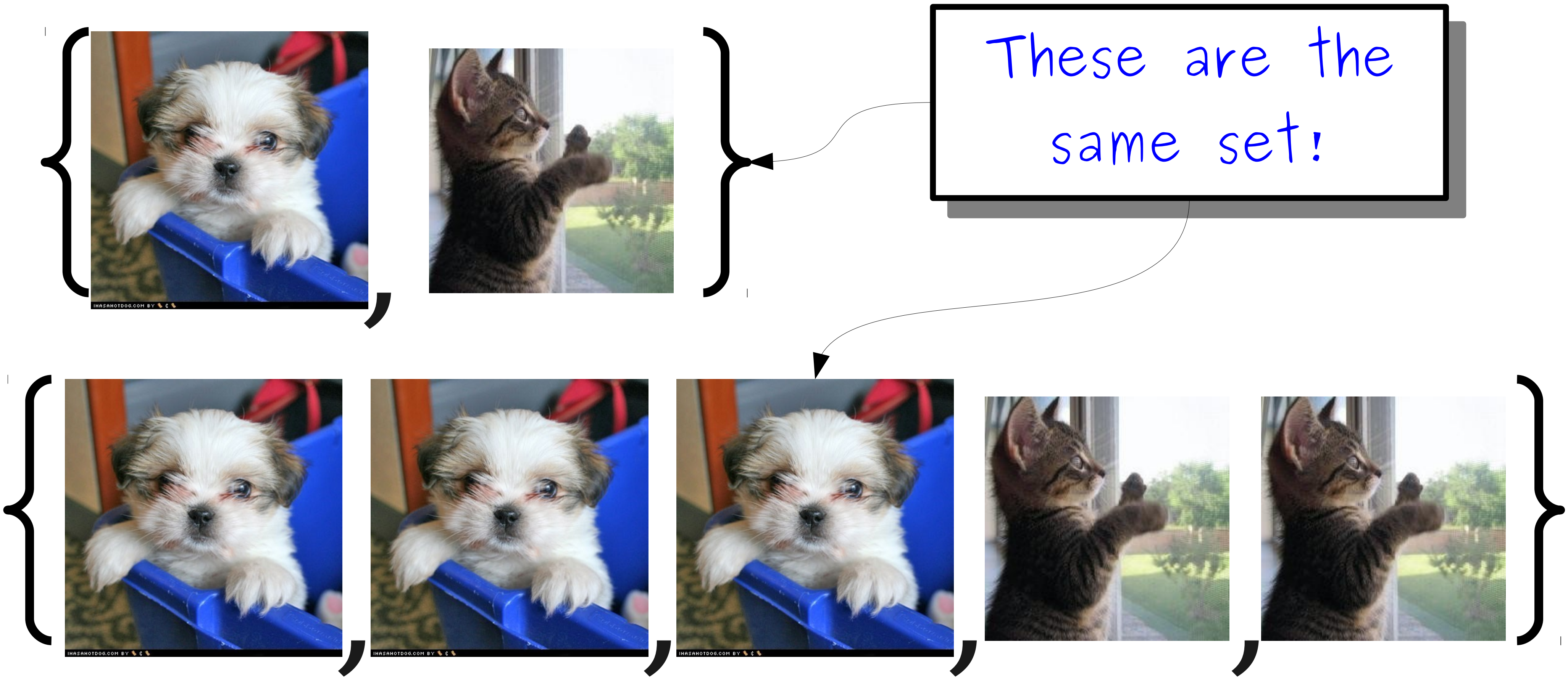
A **set** is an unordered collection of distinct objects, which may be anything (including other sets).



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).

$$\left\{ \quad \right\}$$

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).

$$\emptyset \qquad\qquad \{\ \}$$

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).

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

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).

This symbol means "is defined as"

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

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).

Membership

Membership

IN GOD WE TRUST
LIBERTY
2004
IN GOD WE TRUST
LIBERTY
2002
UNITED STATES OF AMERICA
IN GOD WE TRUST
LIBERTY
QUARTER DOLLAR
LIBERTY
IN GOD WE TRUST
2002

Membership

Is 

in this set?

Membership

 $\in$ {  ,  ,  ,  }

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

  $$\boldsymbol{x \in S}$$

  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 and any set, either that object is in the set or it isn't.

Infinite Sets

- Sets can be infinitely large.
- The **natural numbers**, 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**, ℤ: { …, -2, -1, 0, 1, 2, … }
  - Z is from German “Zahlen.”
- The **real numbers**, 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

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

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:

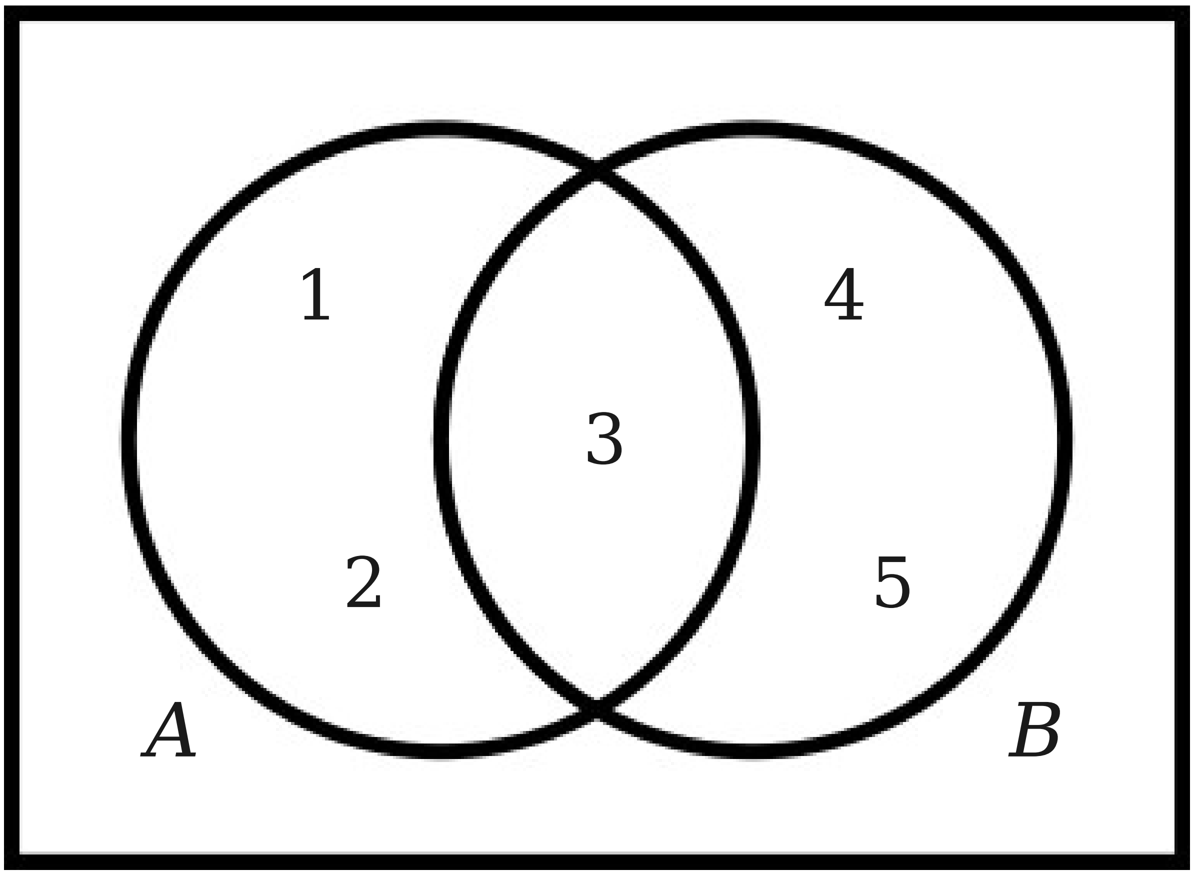
$$\{ \; r \mid r \in \mathbb{R}, r < 137 \; \}$$

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

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

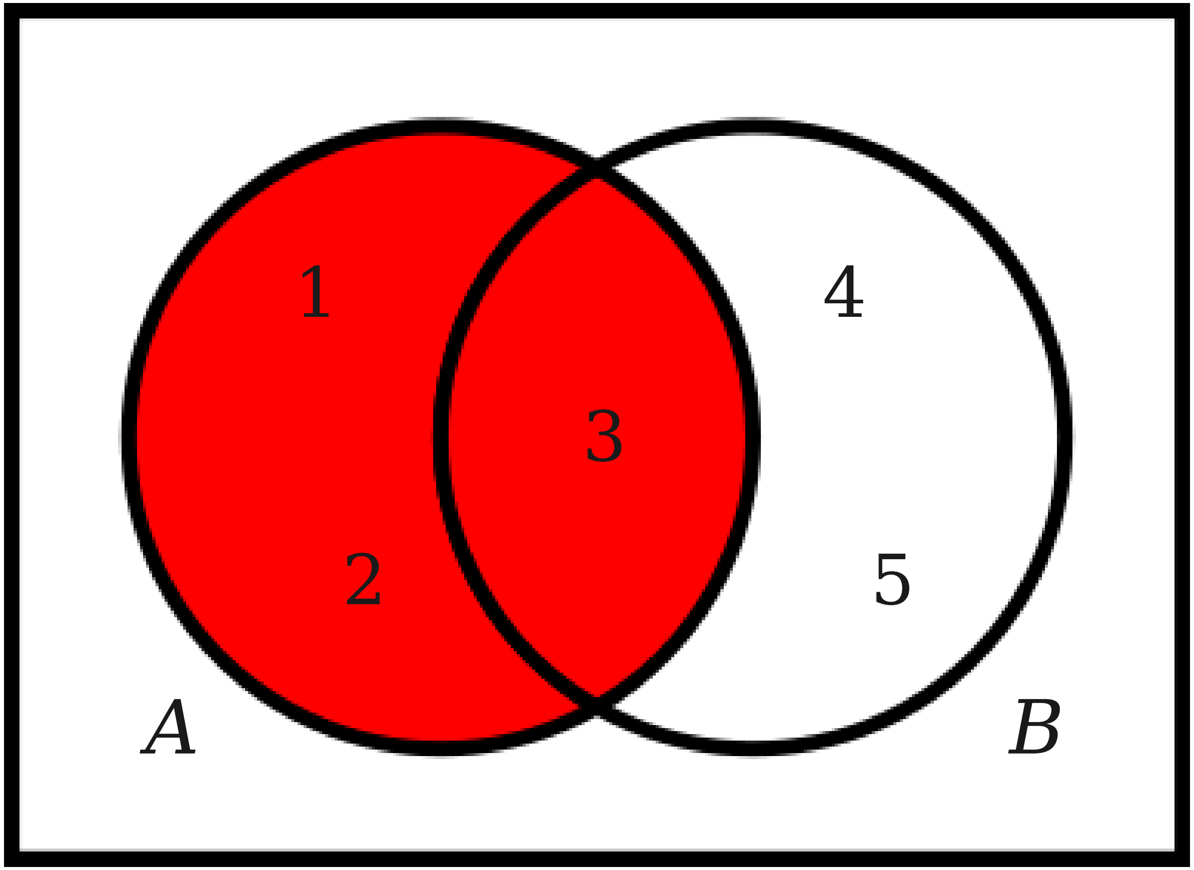
Combining Sets

Venn Diagrams



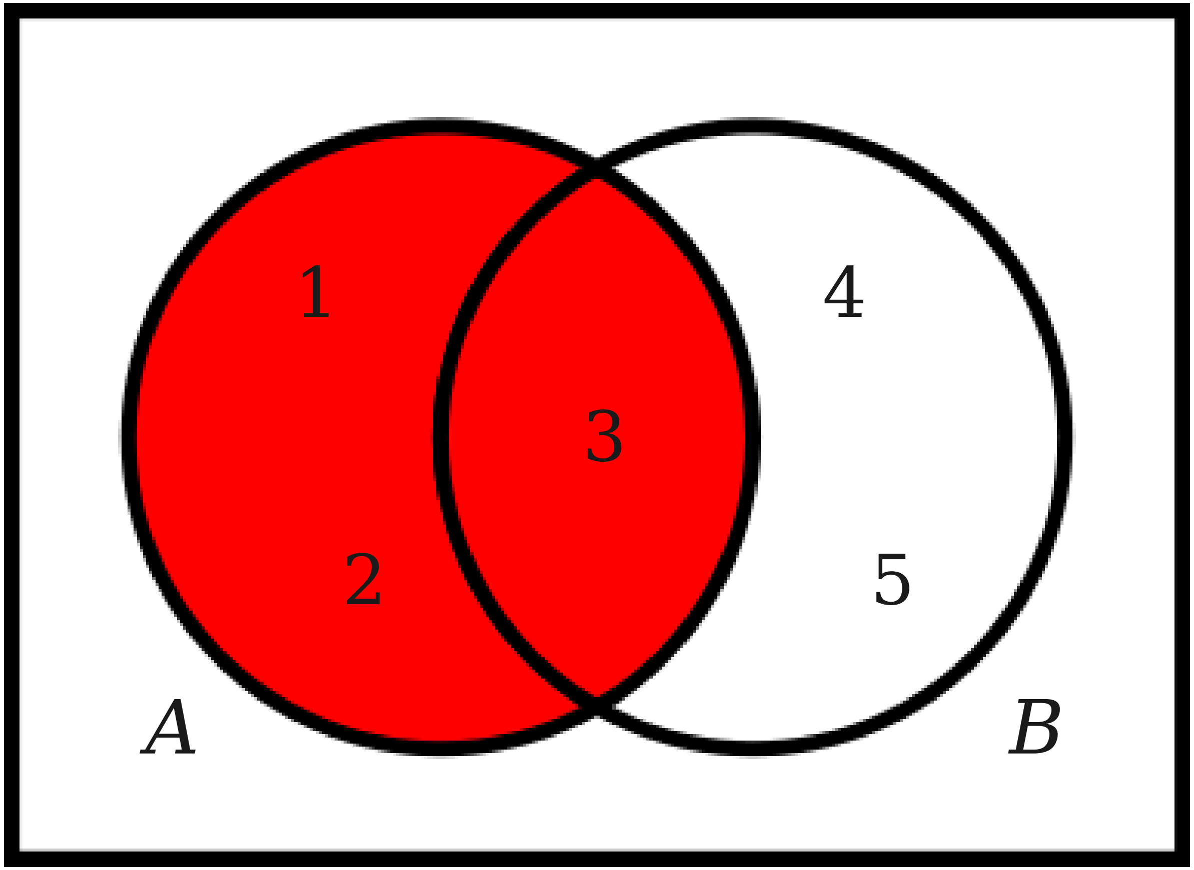
$A = \{ 1, 2, 3 \}$
$B = \{ 3, 4, 5 \}$

Venn Diagrams



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

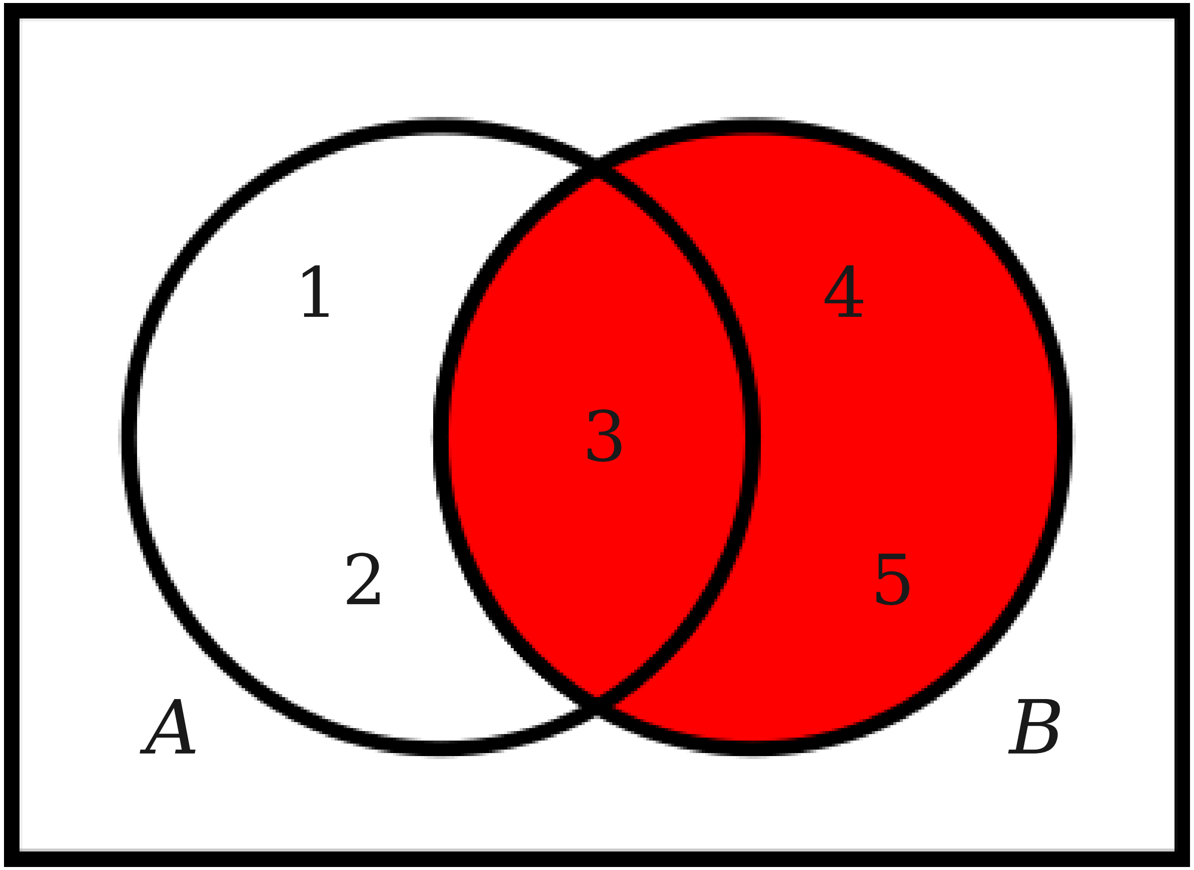
Venn Diagrams



A

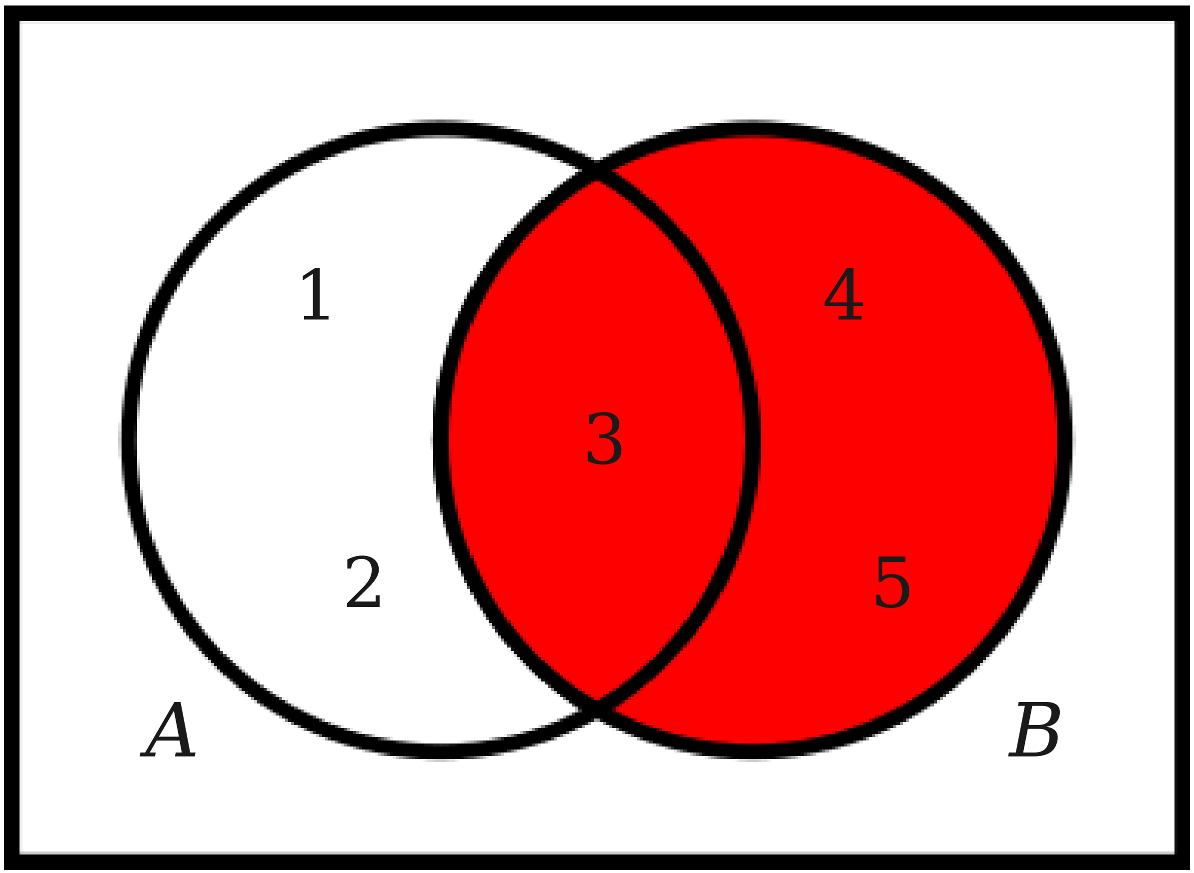
$A = \{ 1, 2, 3 \}$
$B = \{ 3, 4, 5 \}$

Venn Diagrams



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

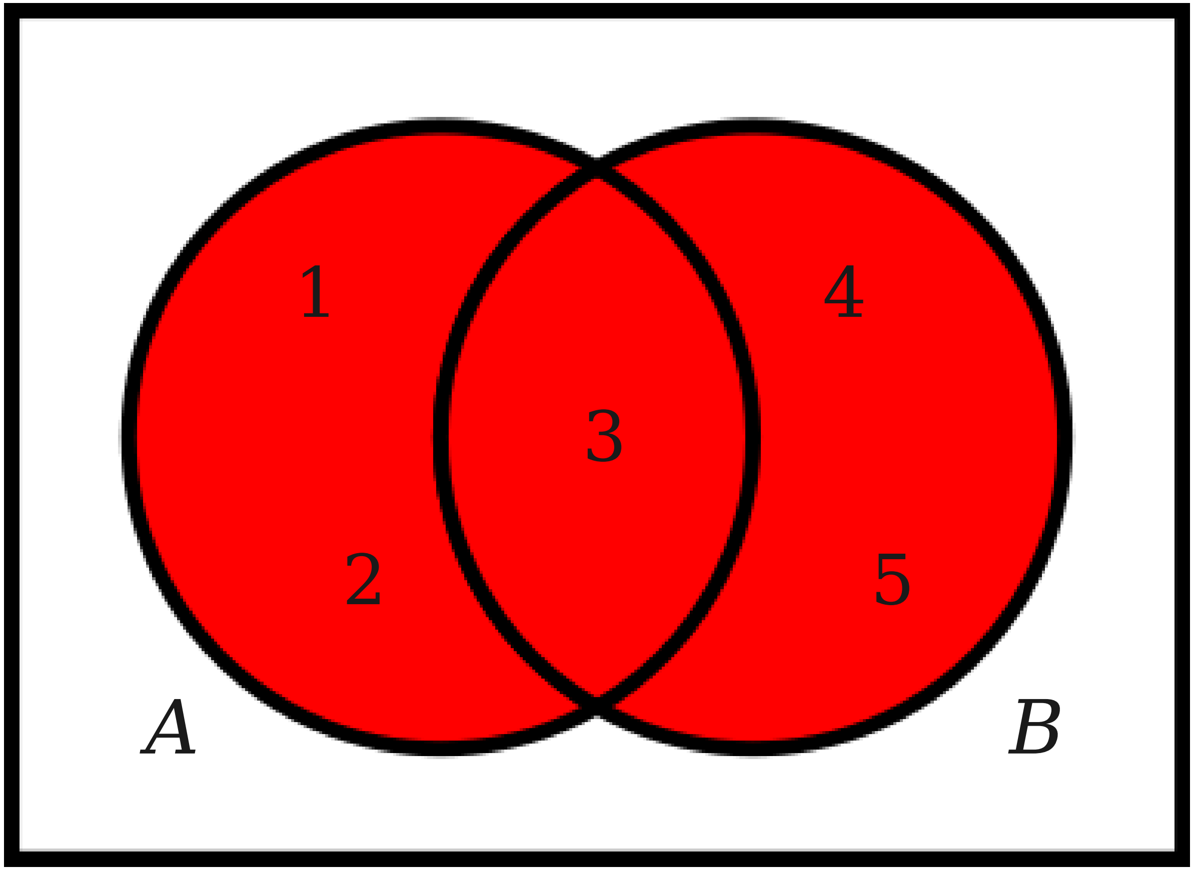
Venn Diagrams



B

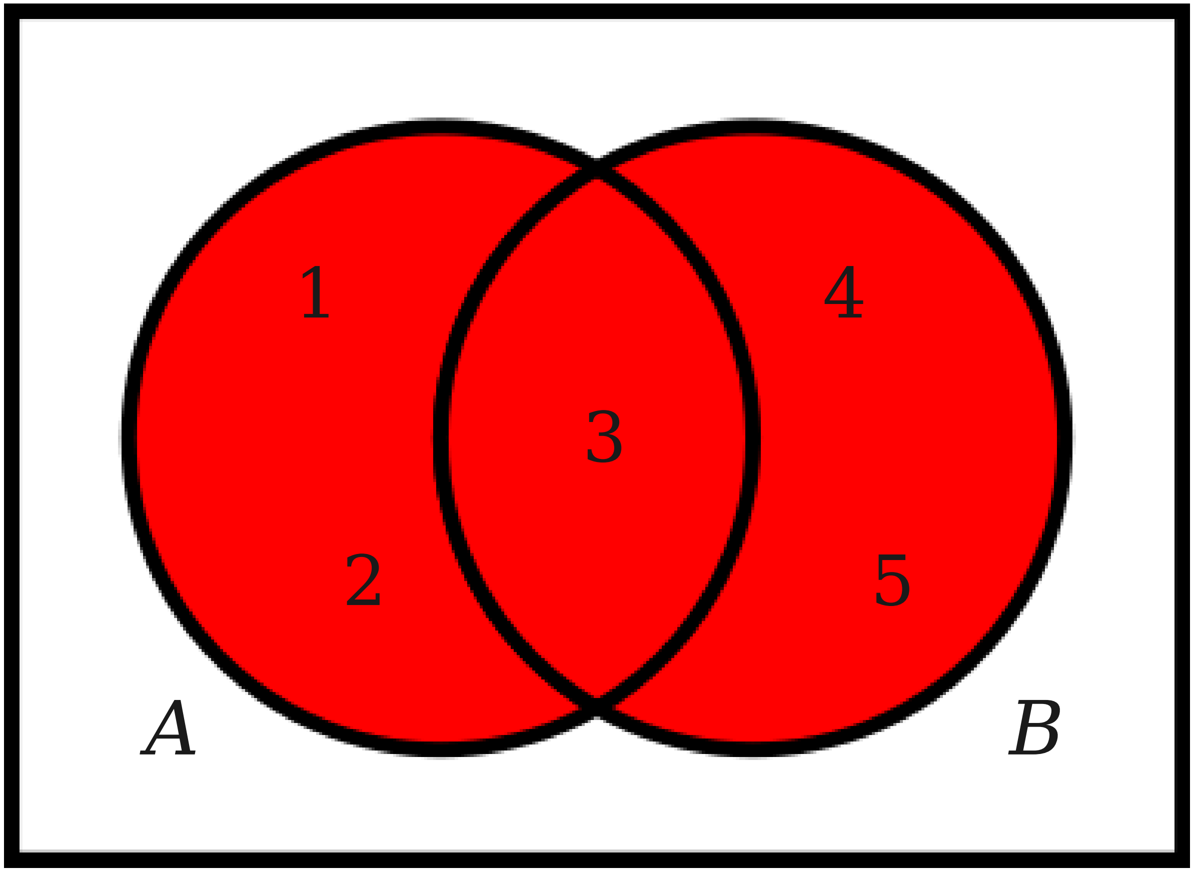
$A = \{ 1, 2, 3 \}$
$B = \{ 3, 4, 5 \}$

Venn Diagrams



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

Venn Diagrams



Union

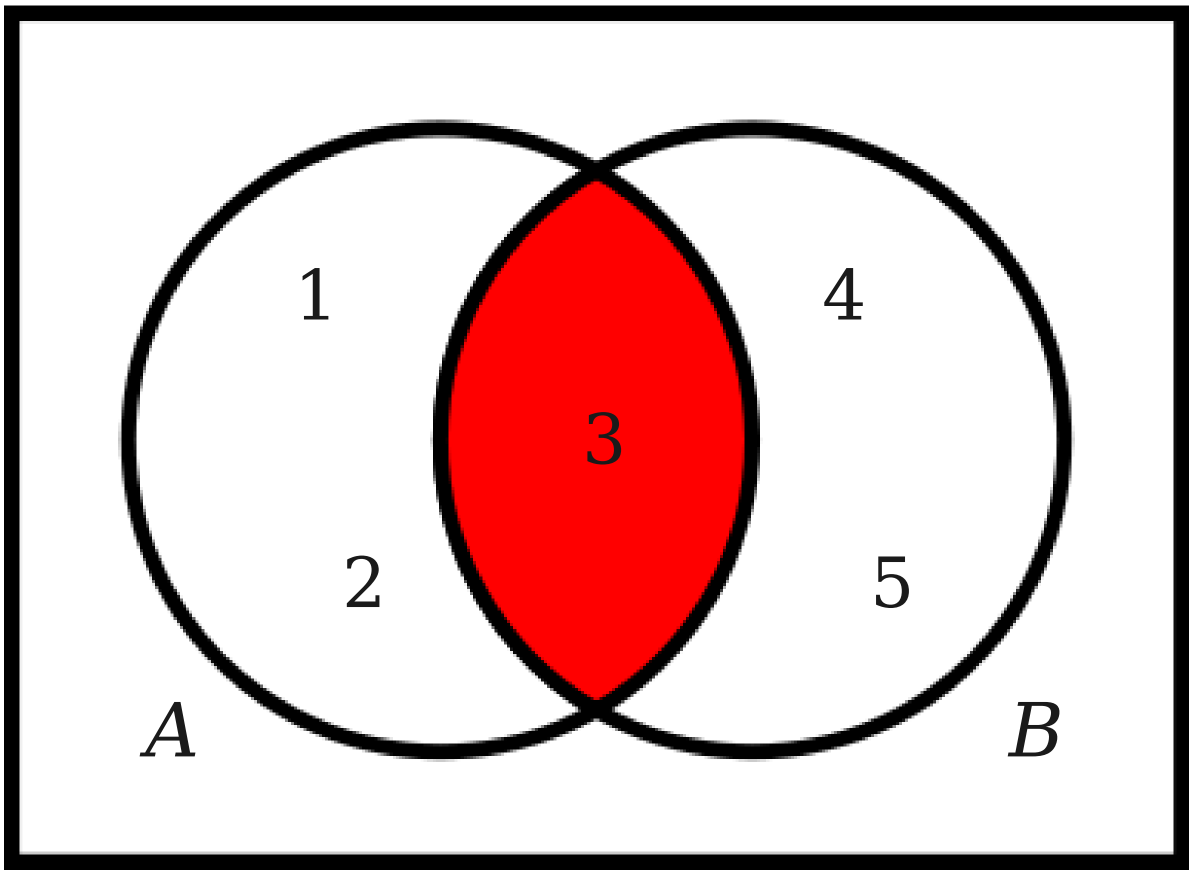
$A \cup B$

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

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

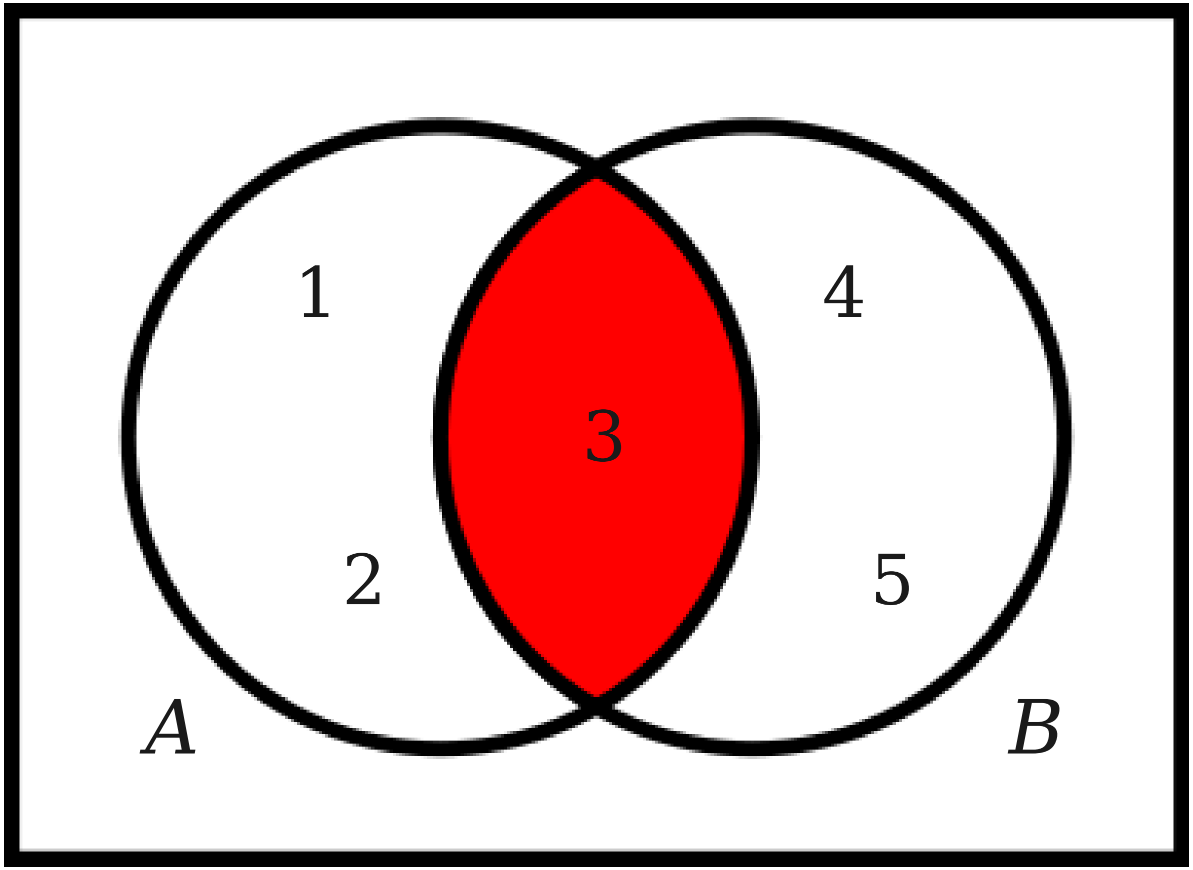
$B = \{ 3, 4, 5 \}$

Venn Diagrams



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

Venn Diagrams



Intersection

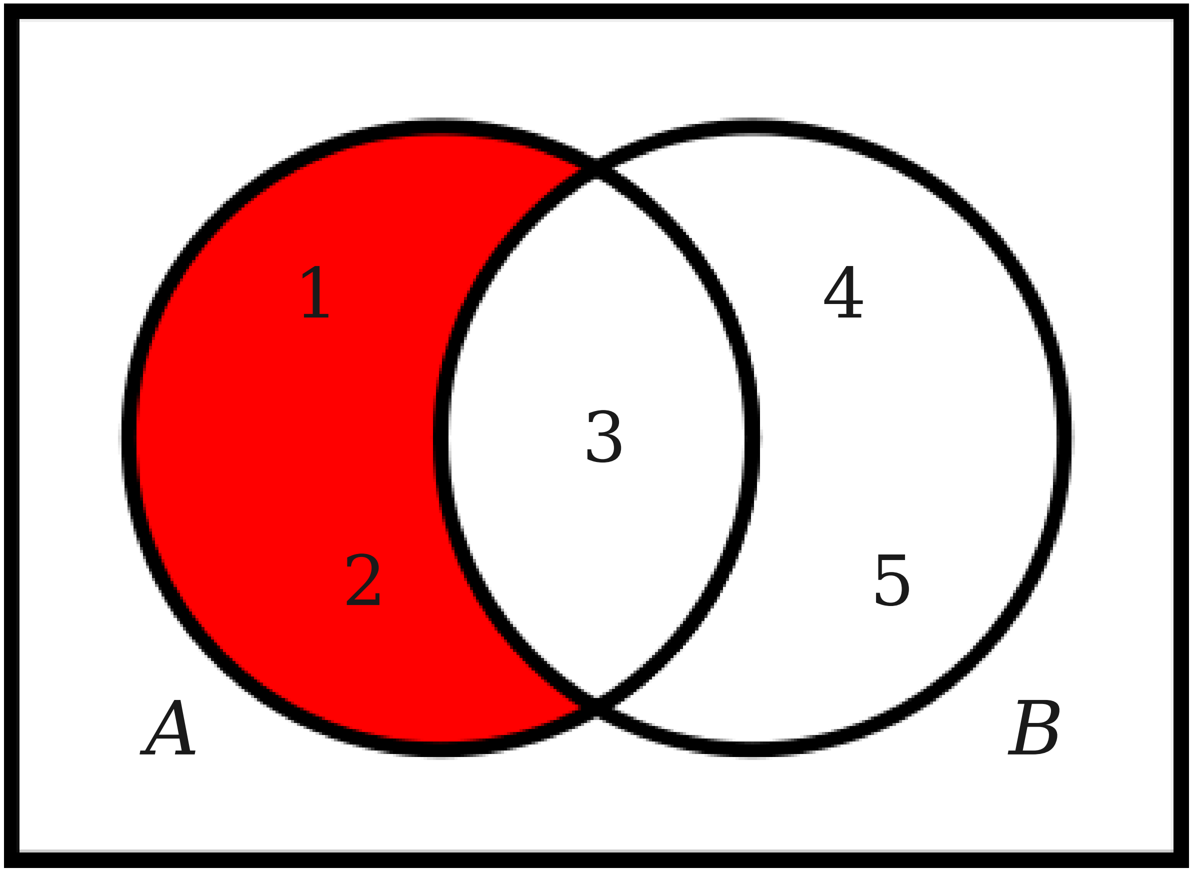
$A \cap B$

$\{ 3 \}$

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

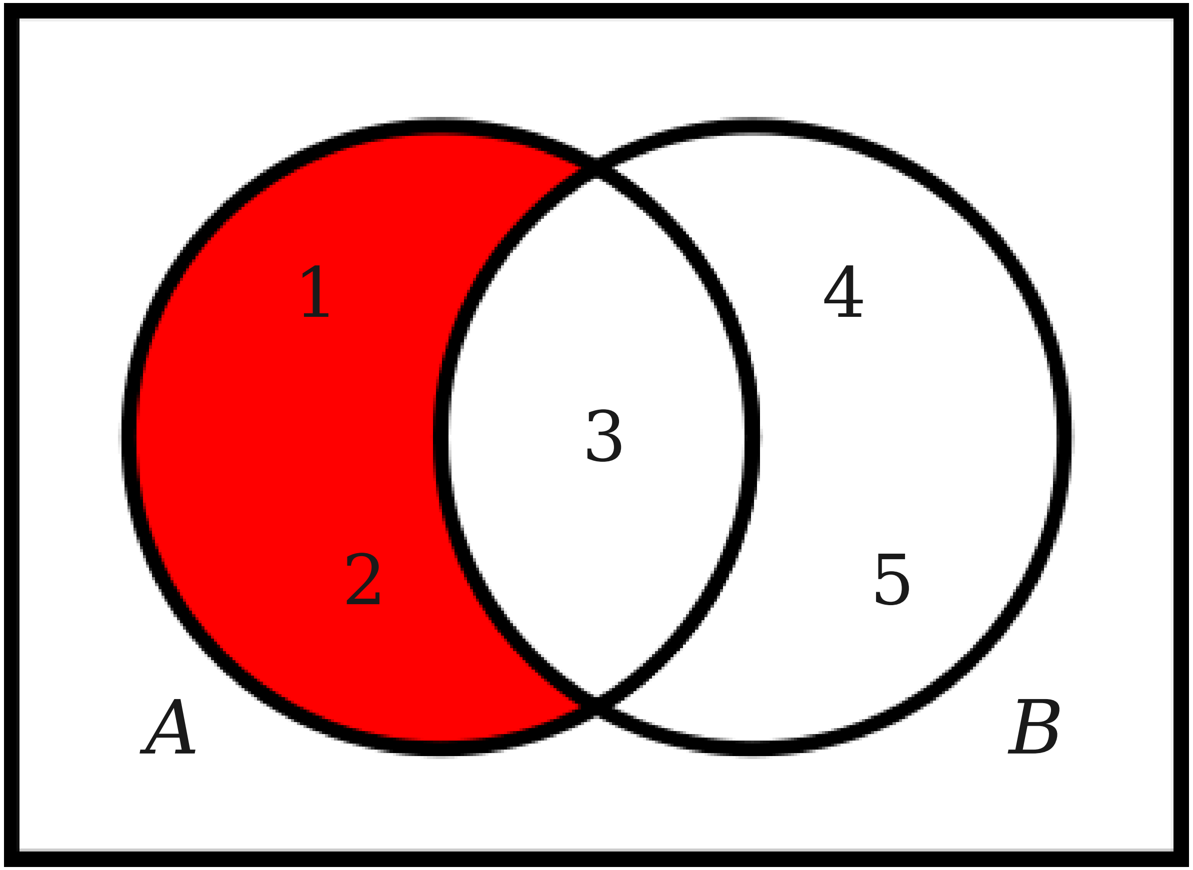
$B = \{ 3, 4, 5 \}$

Venn Diagrams



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

Venn Diagrams



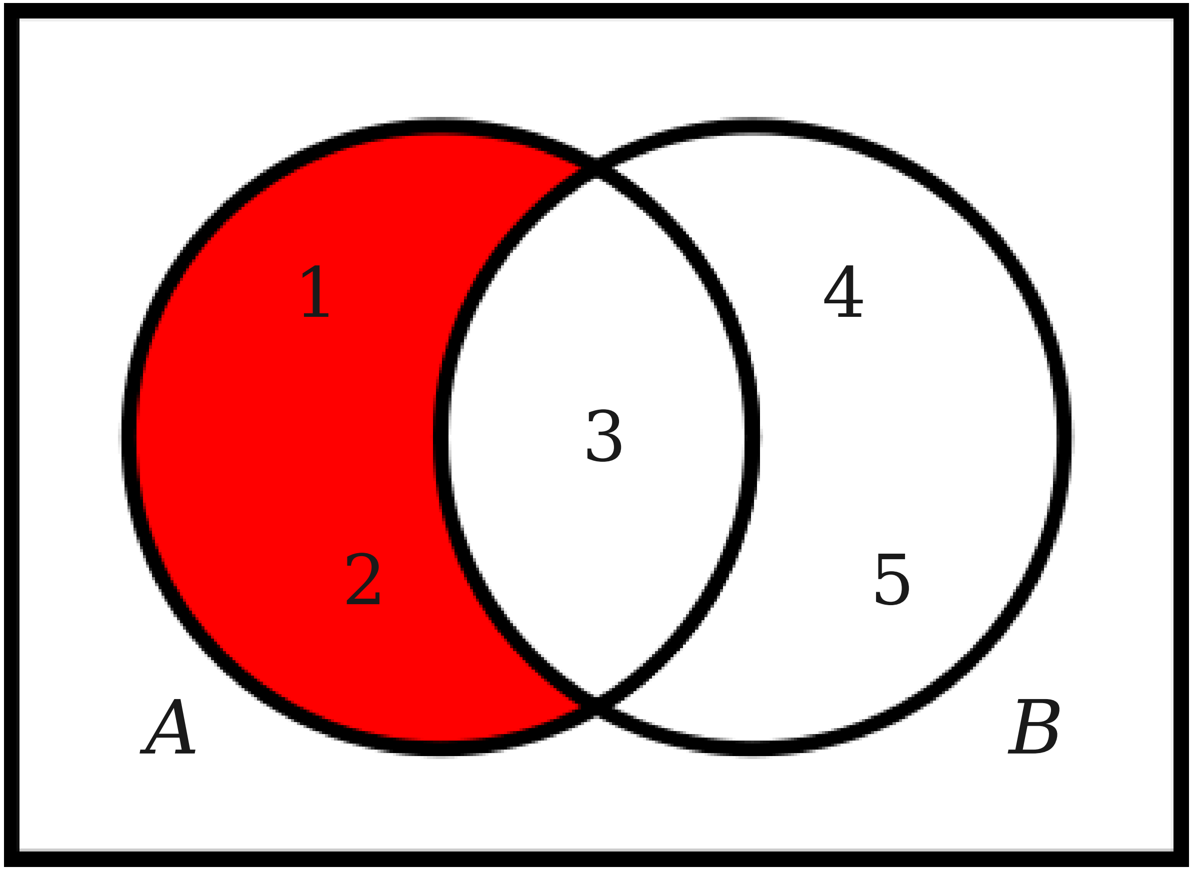
Difference

$A - B$

$\{ 1, 2 \}$

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

Venn Diagrams



Difference

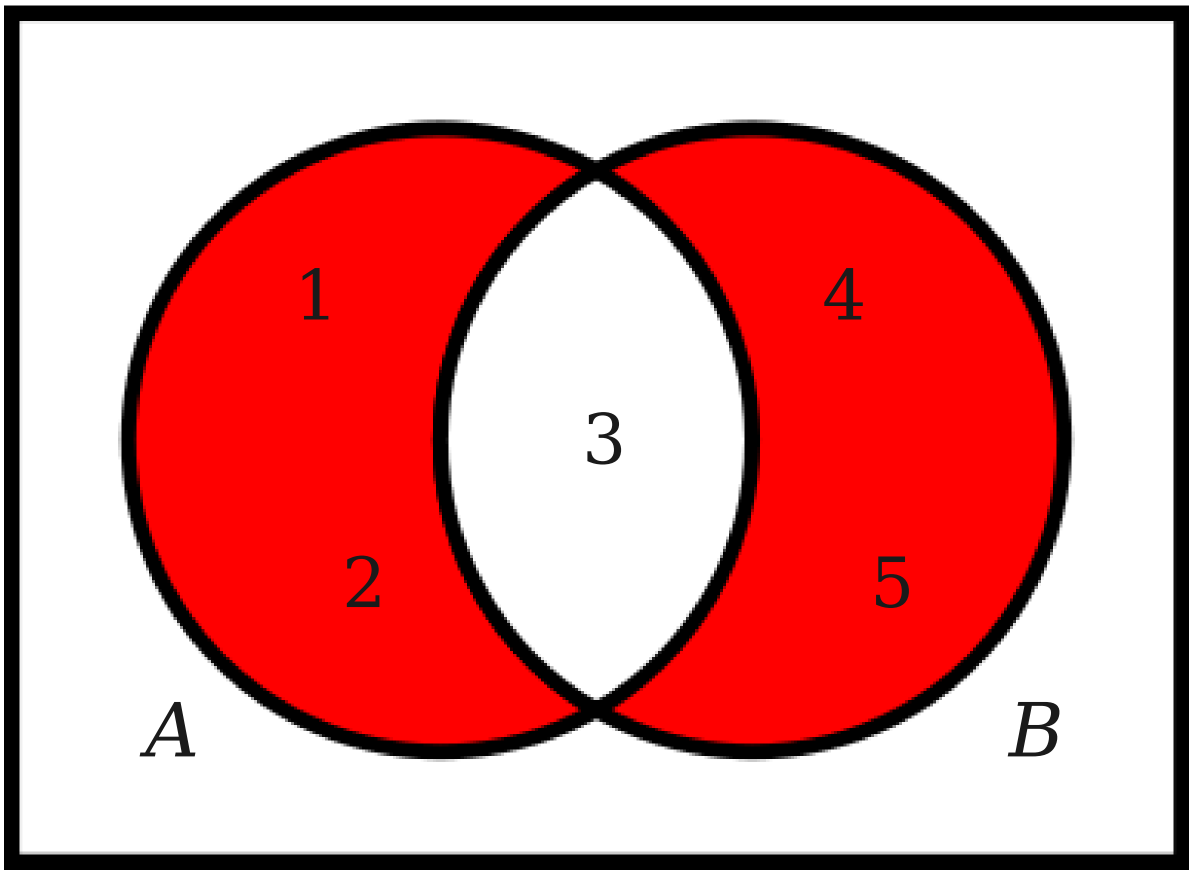
$A \setminus B$

$\{ 1, 2 \}$

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

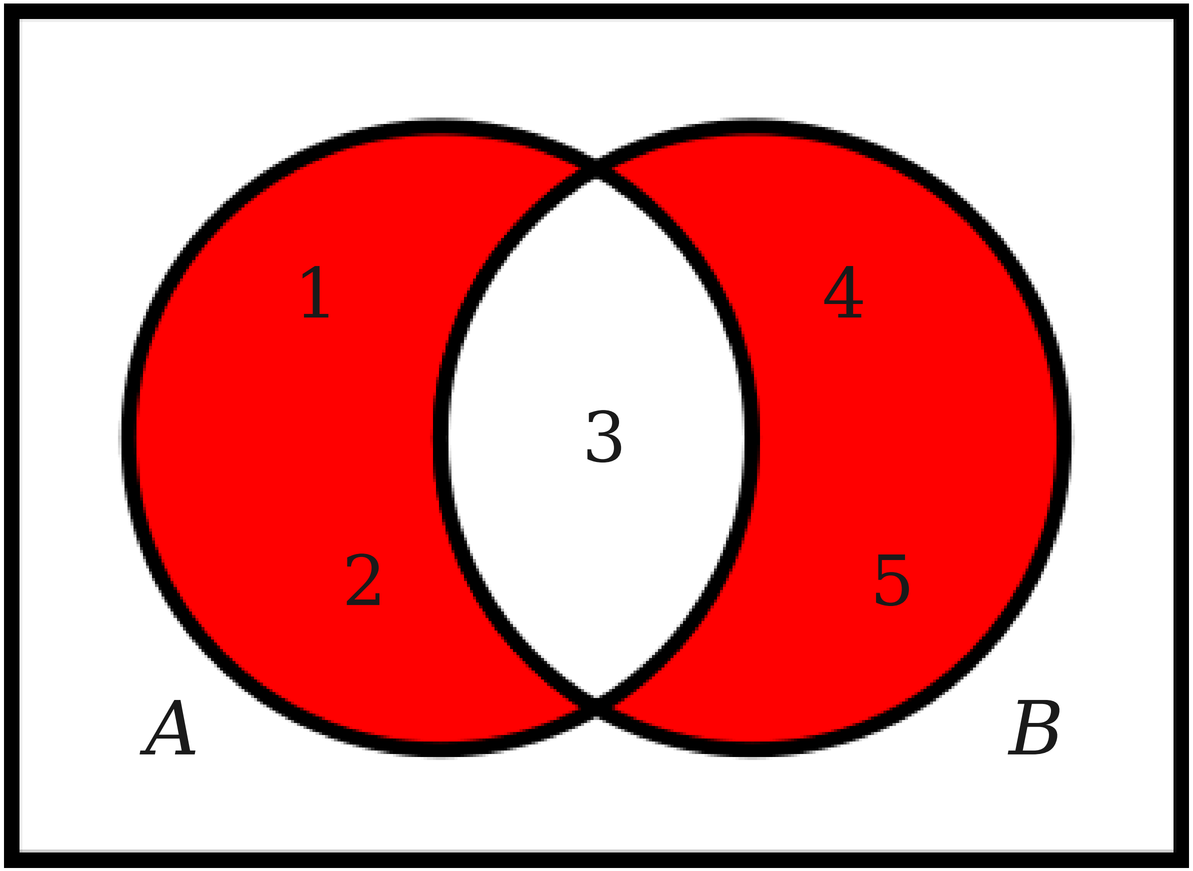
$B = \{ 3, 4, 5 \}$

Venn Diagrams



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

Venn Diagrams



Symmetric Difference

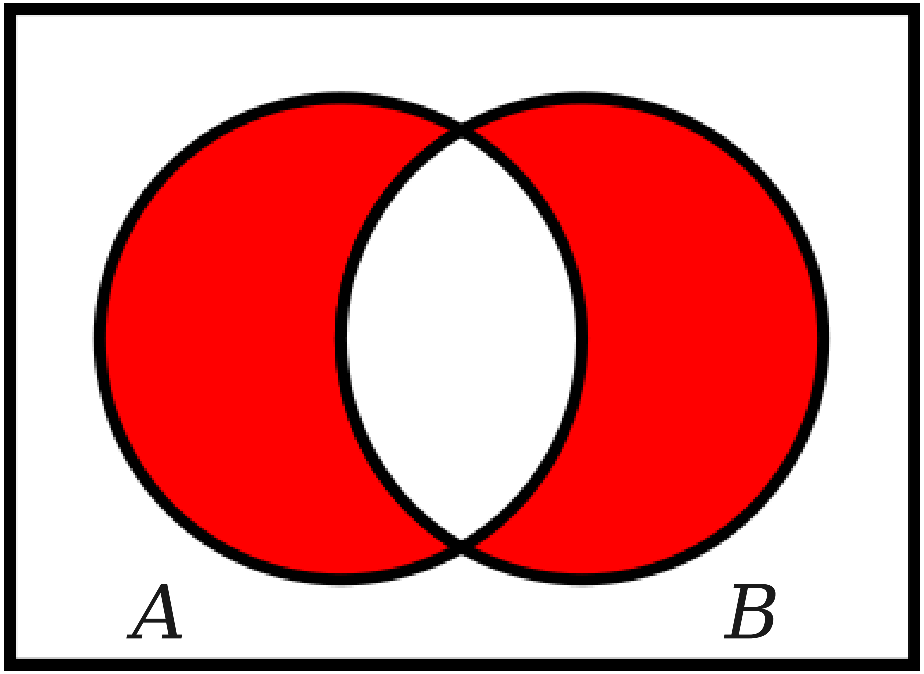
$A \,\Delta\, B$

{ 1, 2, 4, 5 }

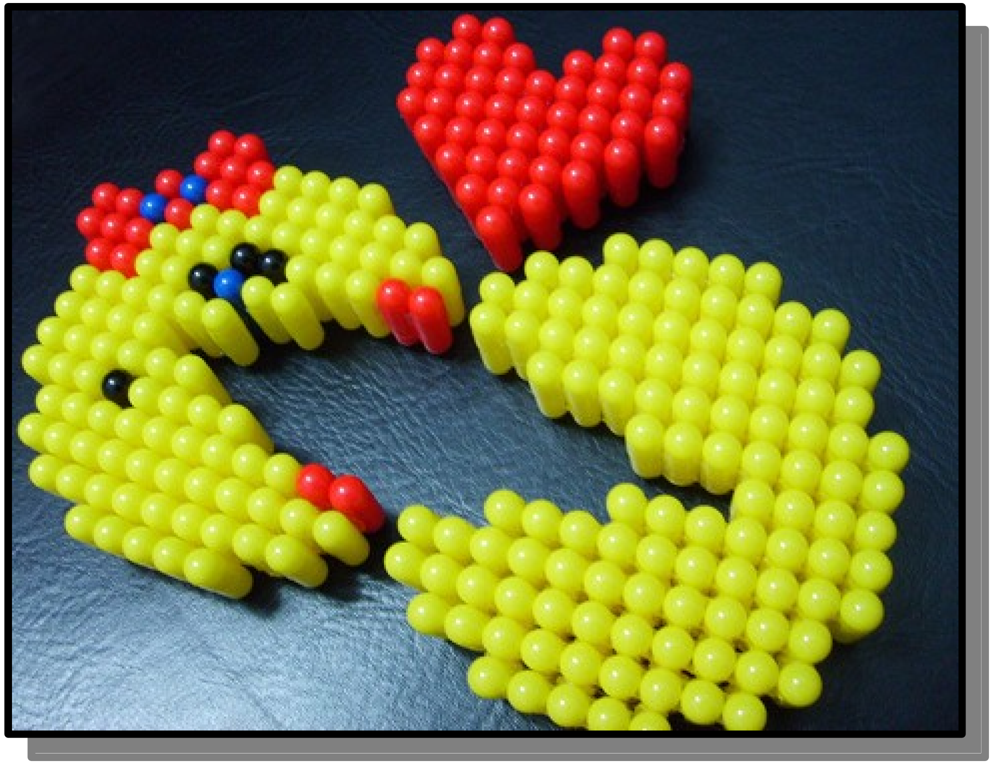
$A = \{ 1, 2, 3 \}$

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

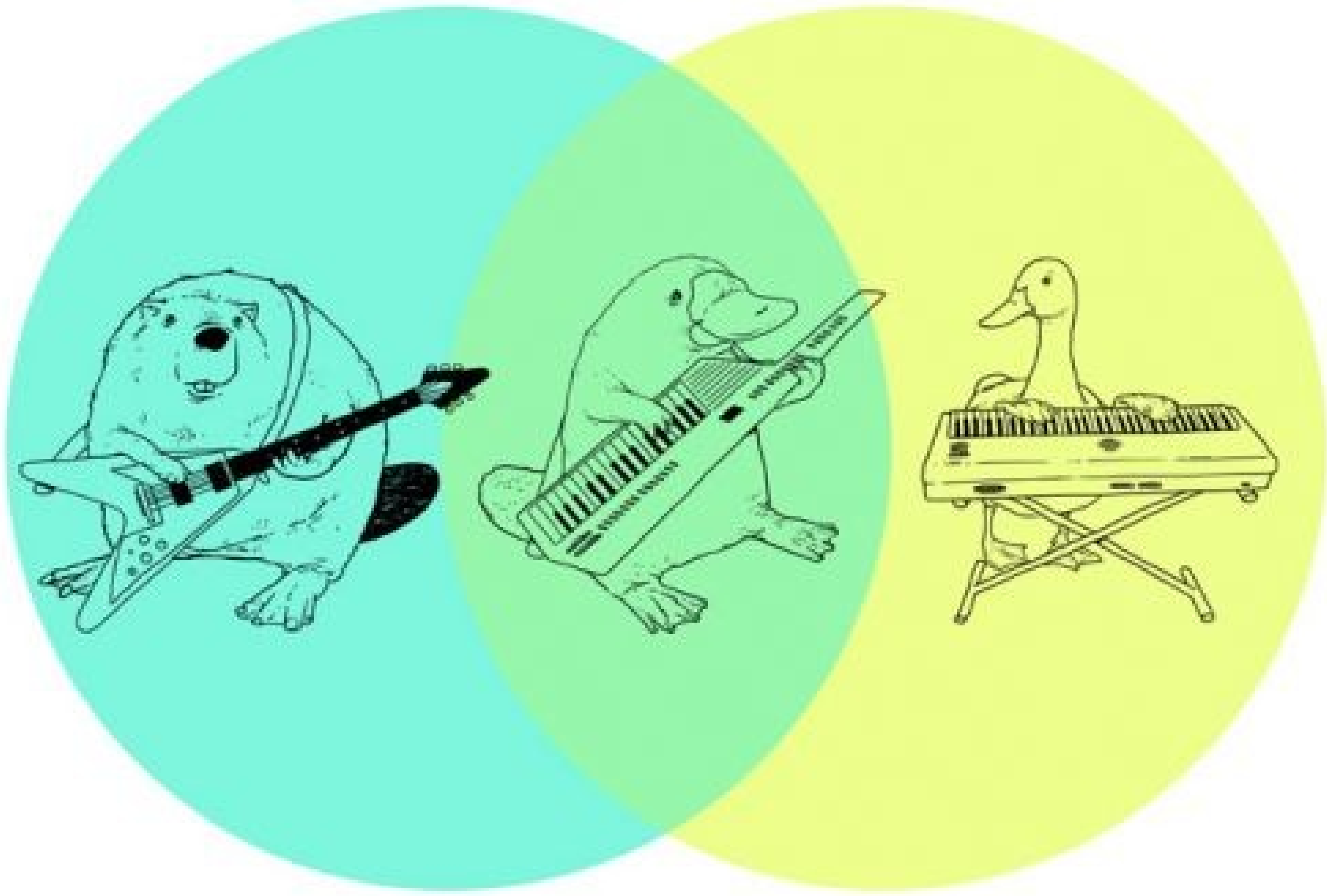
Venn Diagrams



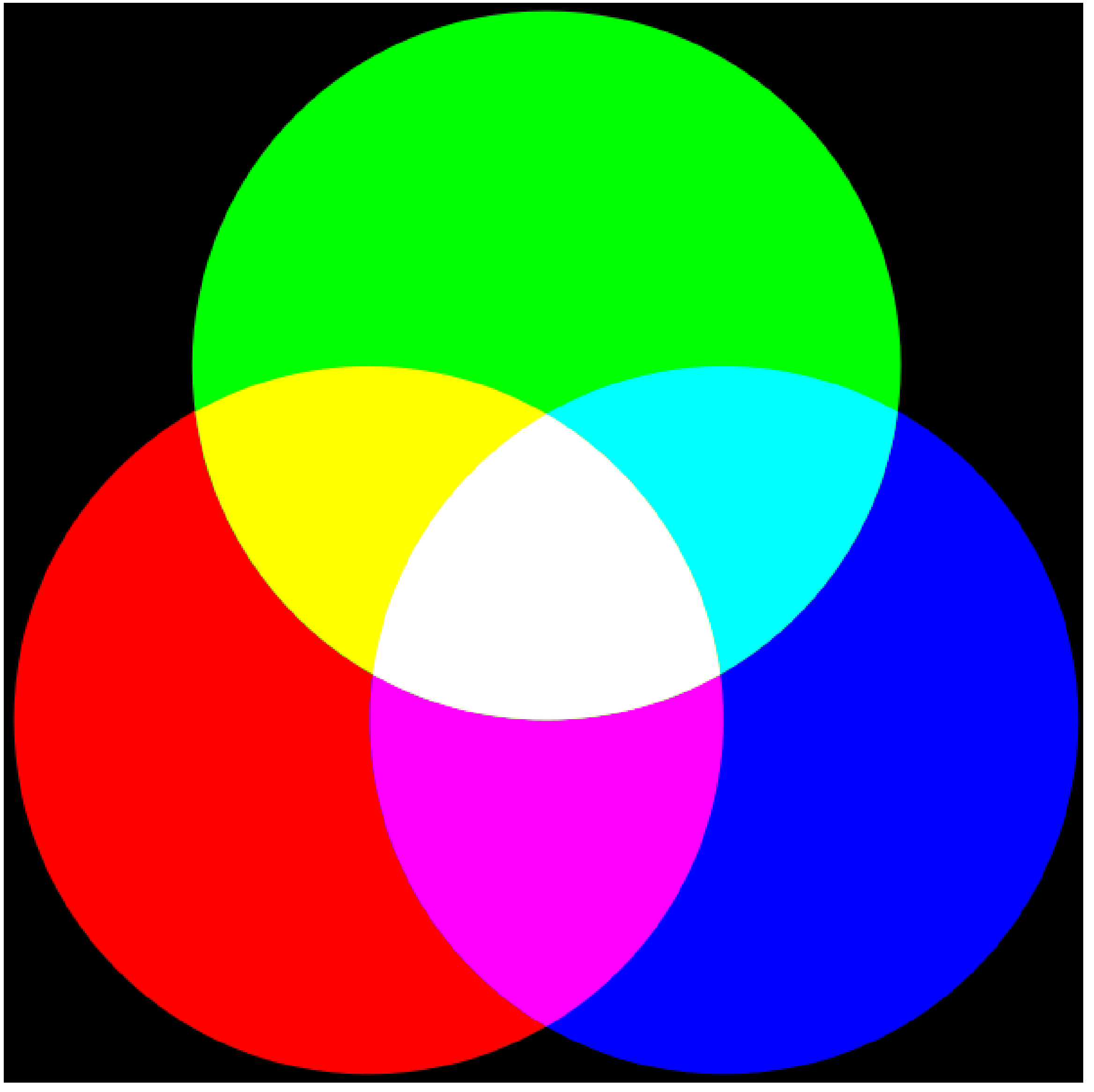
$A \Delta B$



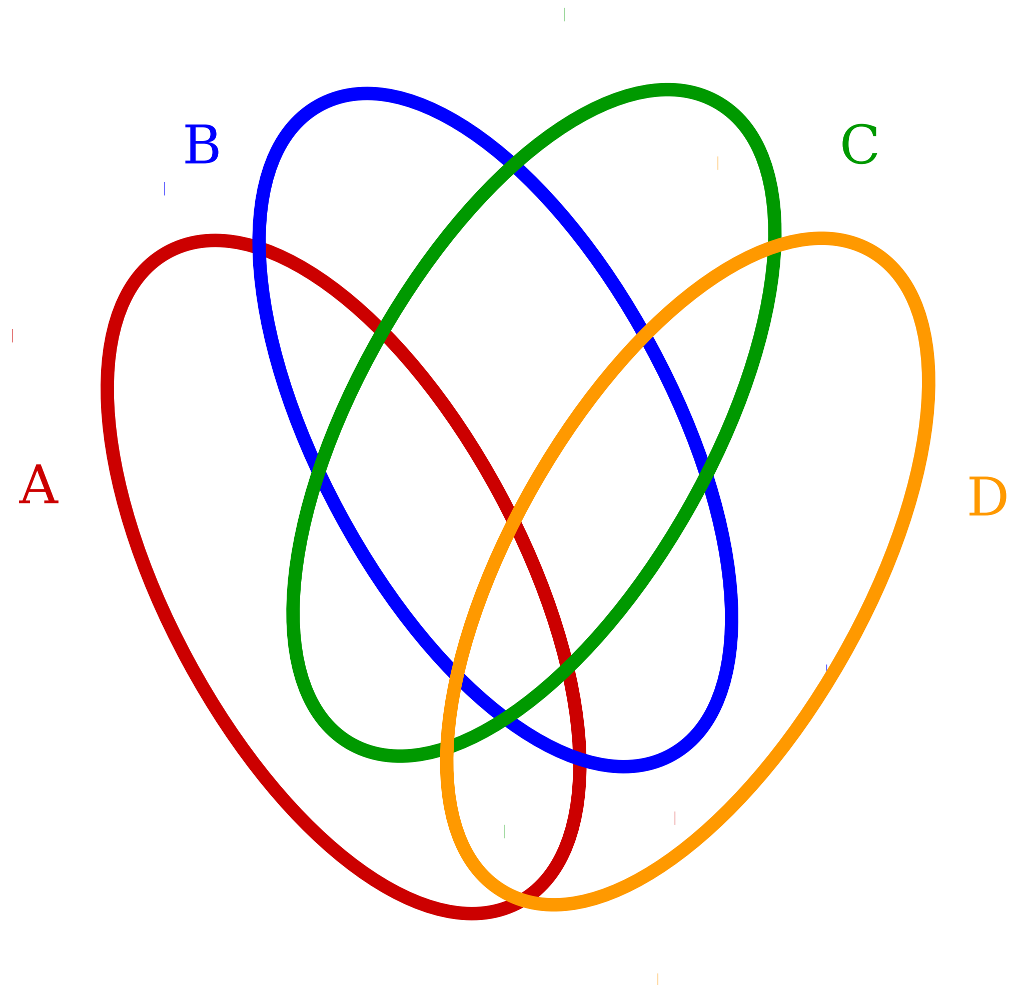
Venn Diagrams



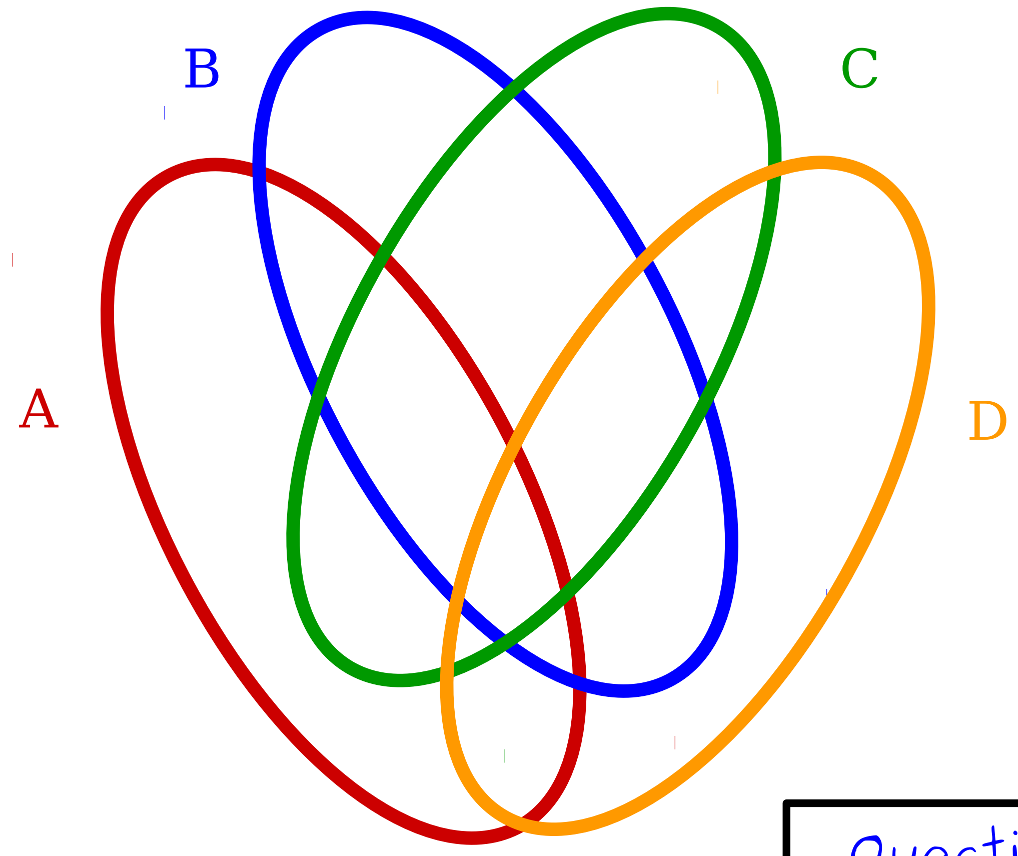
Venn Diagrams for Three Sets



Venn Diagrams for Four Sets



Venn Diagrams for Four Sets



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

A Fun Website:
Venn Diagrams for Seven Sets

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

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:

$$\textbf{If } \boldsymbol{x \in S}\textbf{, then } \boldsymbol{x \in T}\textbf{.}$$

- We denote this as $\boldsymbol{S \subseteq T}$.
- 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*)

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:

  If $x \in S$, then $x \in T$.

- Is $\emptyset \subseteq S$ for any set S?
- **Yes**: The above statement is true.
- **Vacuous truth**: A statement that is true because it does not apply to anything.
  - "All unicorns are blue."
  - "All unicorns are pink."

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:
  - $T \subsetneq S$
  - $T \subset S$

$S = \{$ 

, 

$\}$

$S = \{$ 
IN GOD WE TRUST
LIBERTY
2002
S
, 
LIBERTY
IN GOD WE TRUST
S
2002
$\}$

$\emptyset$ $\{$ 
LIBERTY
IN GOD WE TRUST
S
2002
$\}$ $\{$ 
IN GOD WE TRUST
LIBERTY
2002
S
$\}$ $\{$ 
IN GOD WE TRUST
LIBERTY
2002
S
, 
LIBERTY
IN GOD WE TRUST
S
2002
$\}$

$S = \{$ 

, 

$\}$

$\{\varnothing, \{$ 

$\}, \{$ 

$\}, \{$ 

, 

$\}\}$

$S = \{$ 

, 

$\}$

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

$\}$, $\{$ 

$\}$, $\{$ 

, 

$\}\}$

$S = \{$  ,  $\}$

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

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

Cardinalities

Cardinalities

Cardinality

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

Cardinality

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

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.

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.
- Definition: $|\mathbb{N}| = \aleph_0$
  - Pronounced “Aleph-Zero,” “Aleph-Nought,” or “Aleph-Null”

Consider the set

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

What is $|S|$?

How Big Are These Sets?

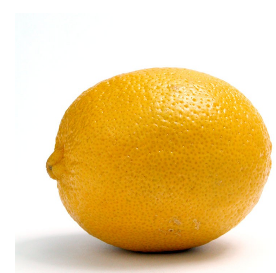
$\{$ 

, 

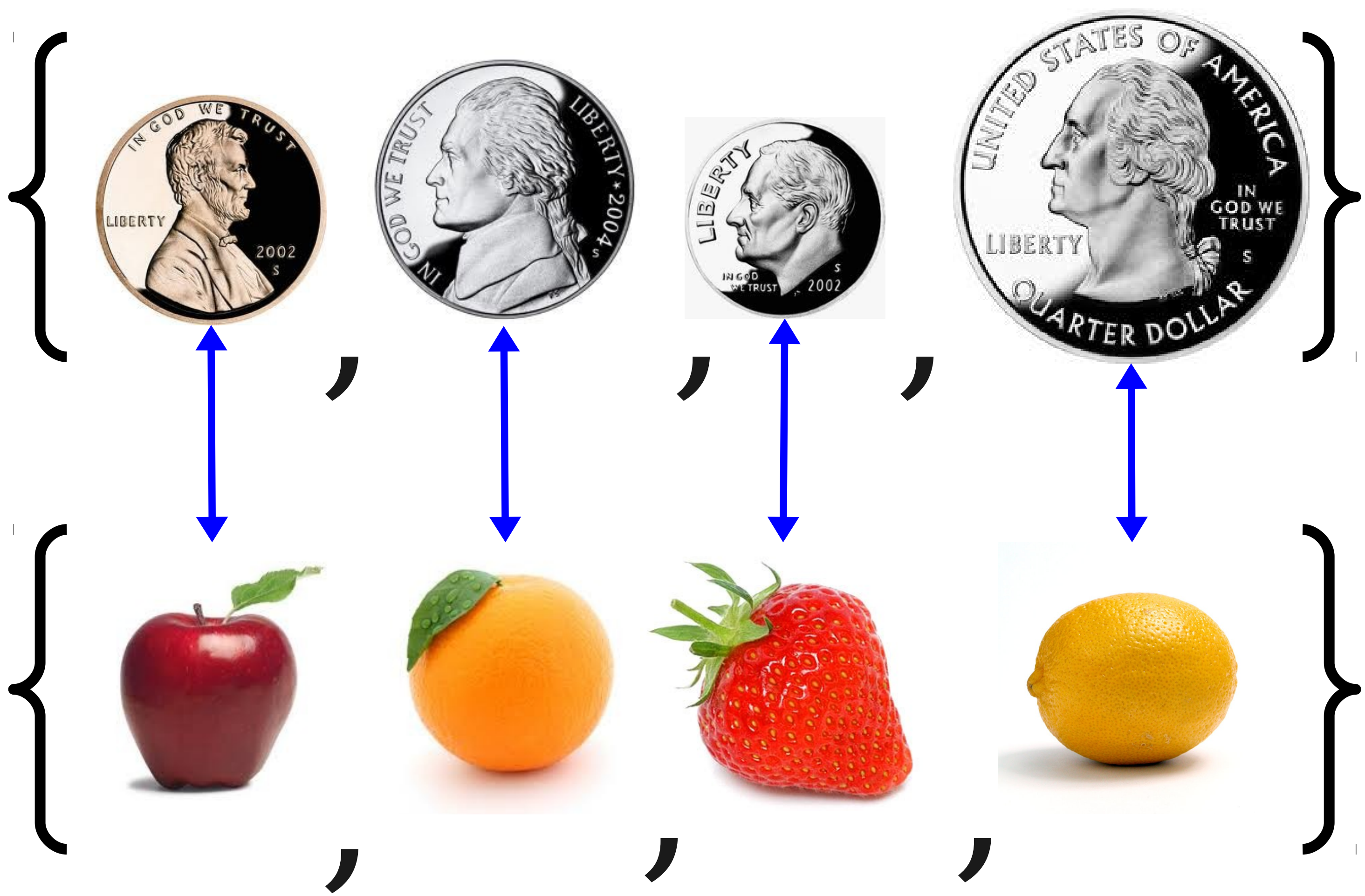
, 

, 

$\}$

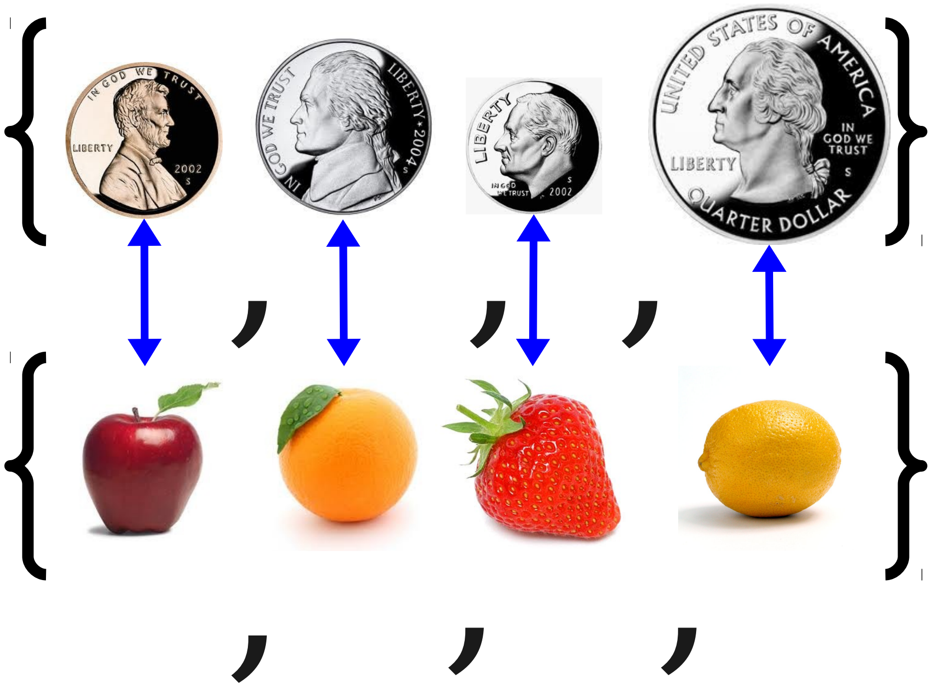
$\{$  ,  ,  ,  $\}$

How Big Are These Sets?



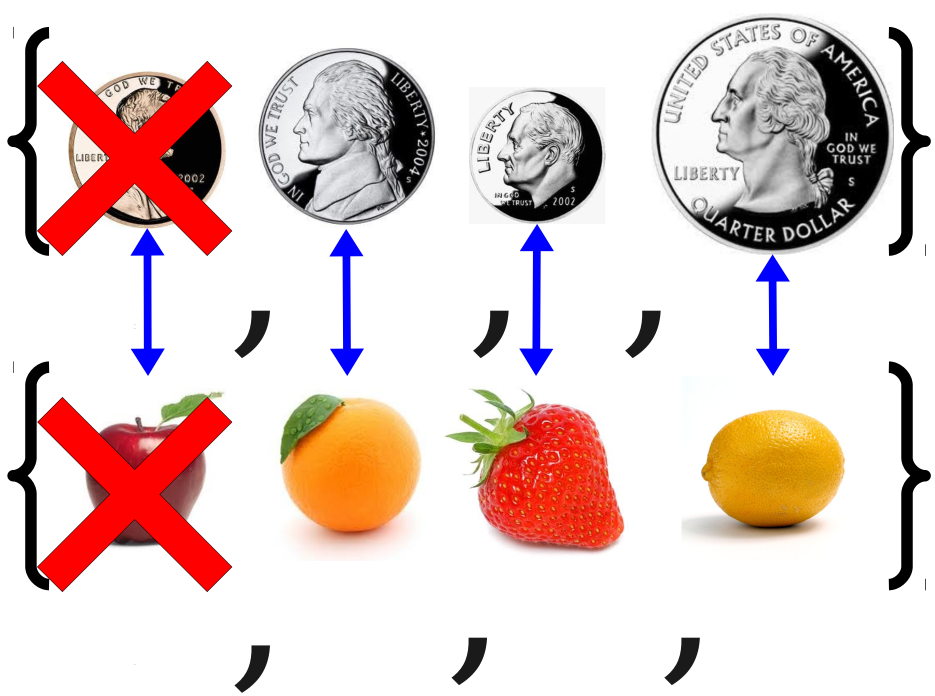
Comparing Cardinalities

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



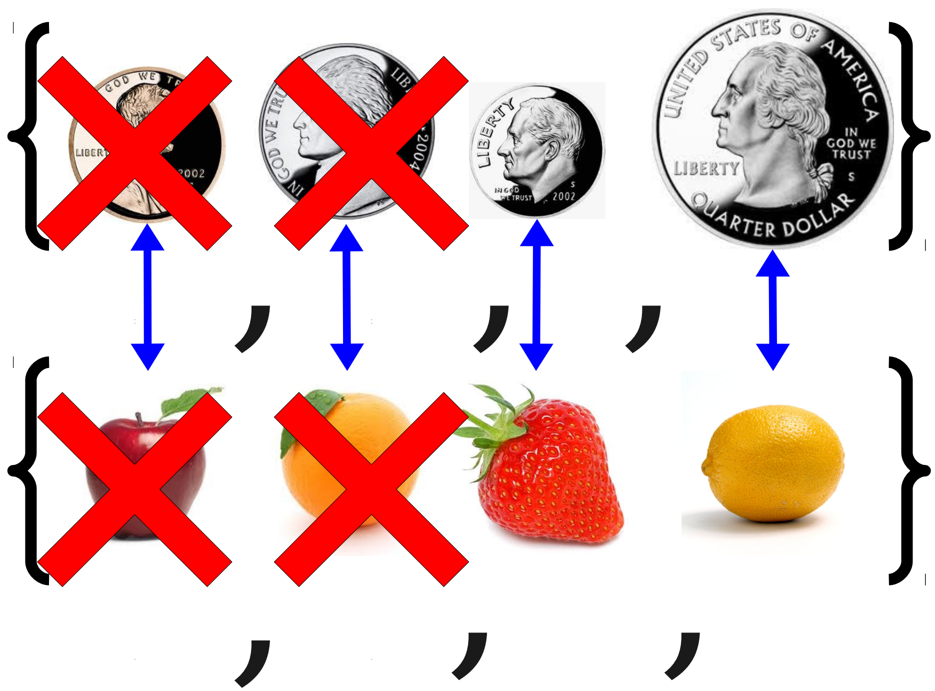
Comparing Cardinalities

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



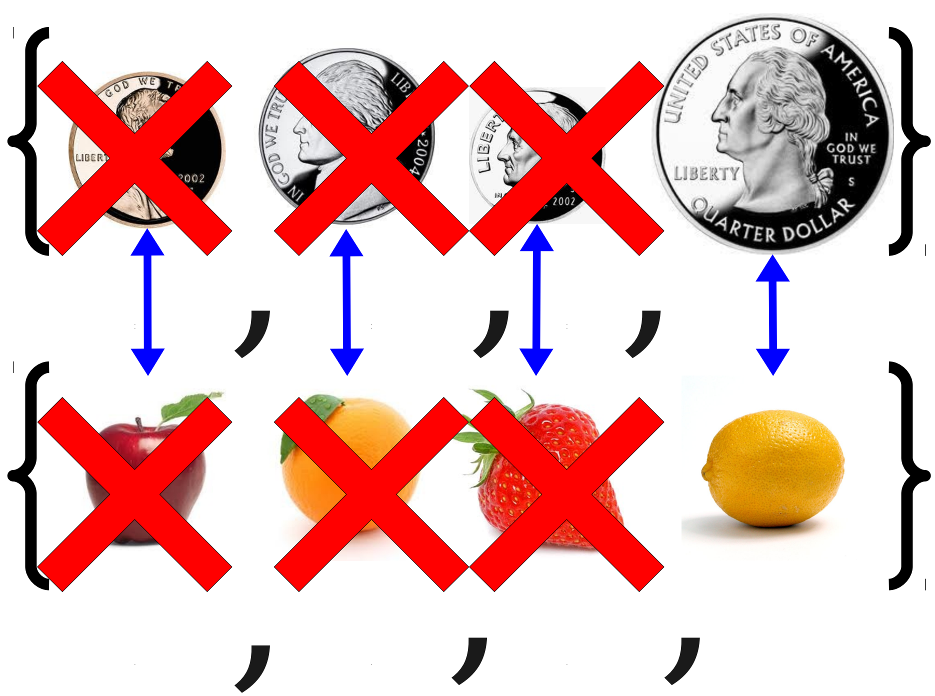
Comparing Cardinalities

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



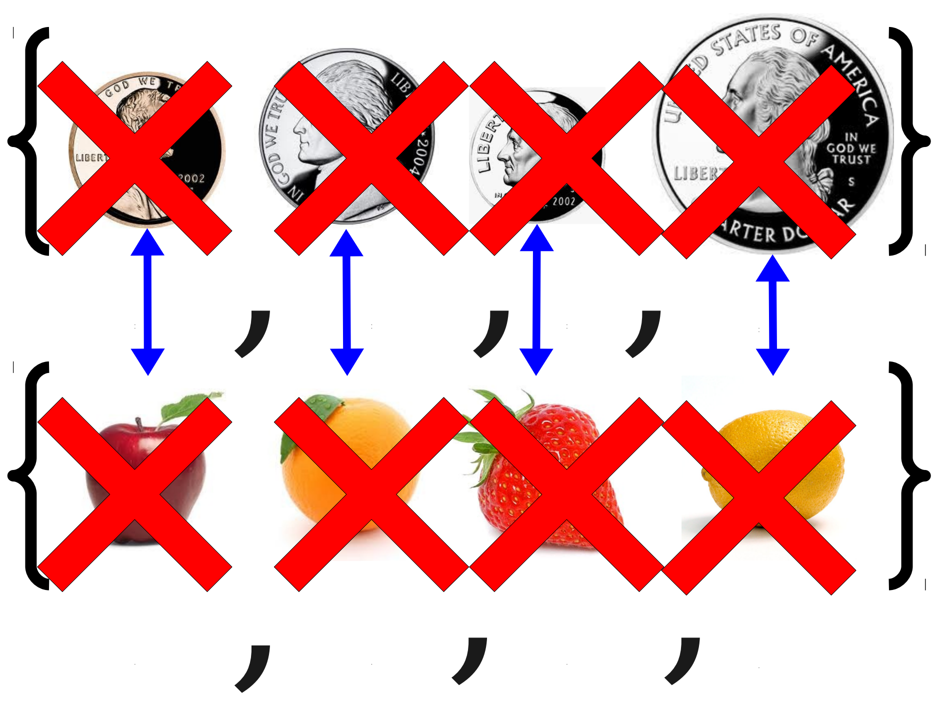
Comparing Cardinalities

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



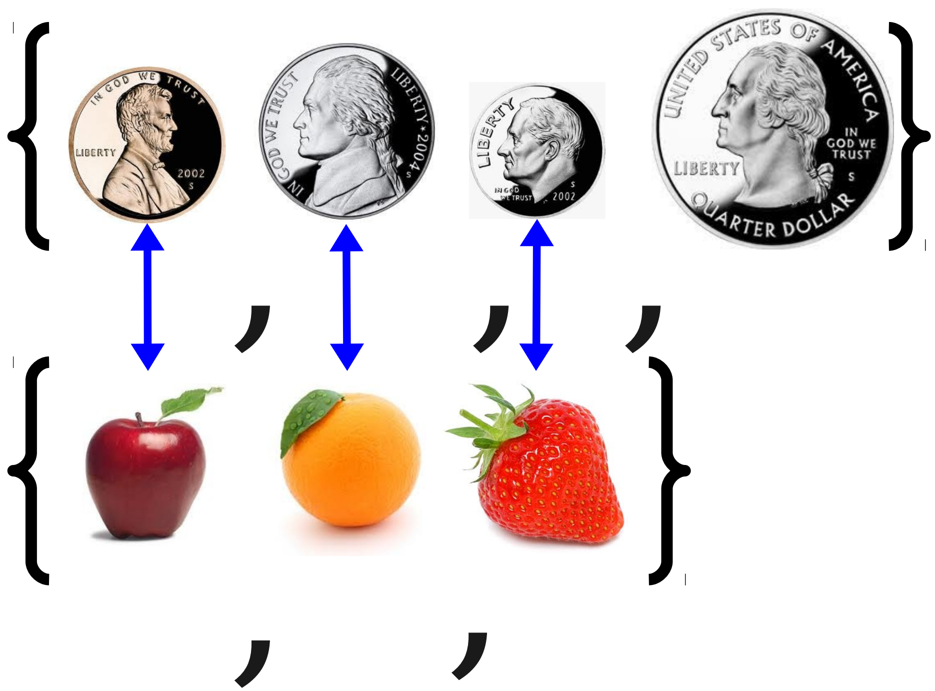
Comparing Cardinalities

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



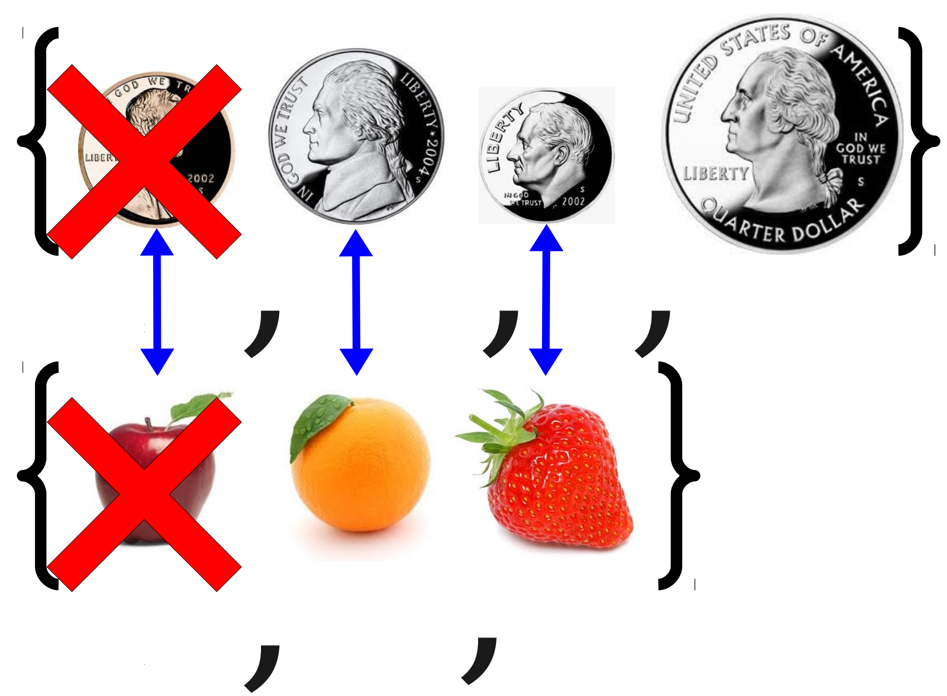
Comparing Cardinalities

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



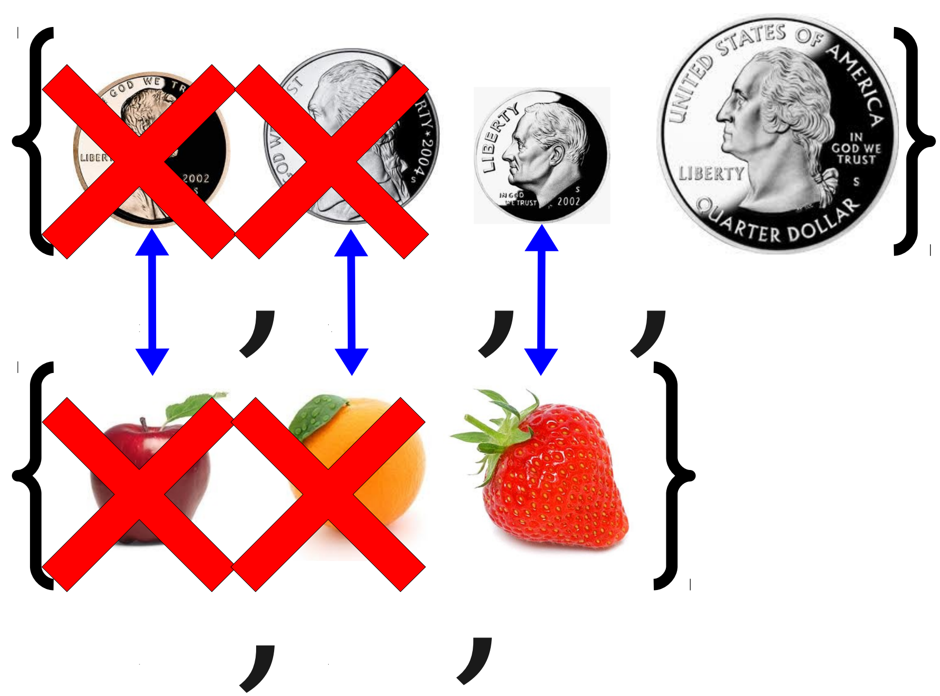
Comparing Cardinalities

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



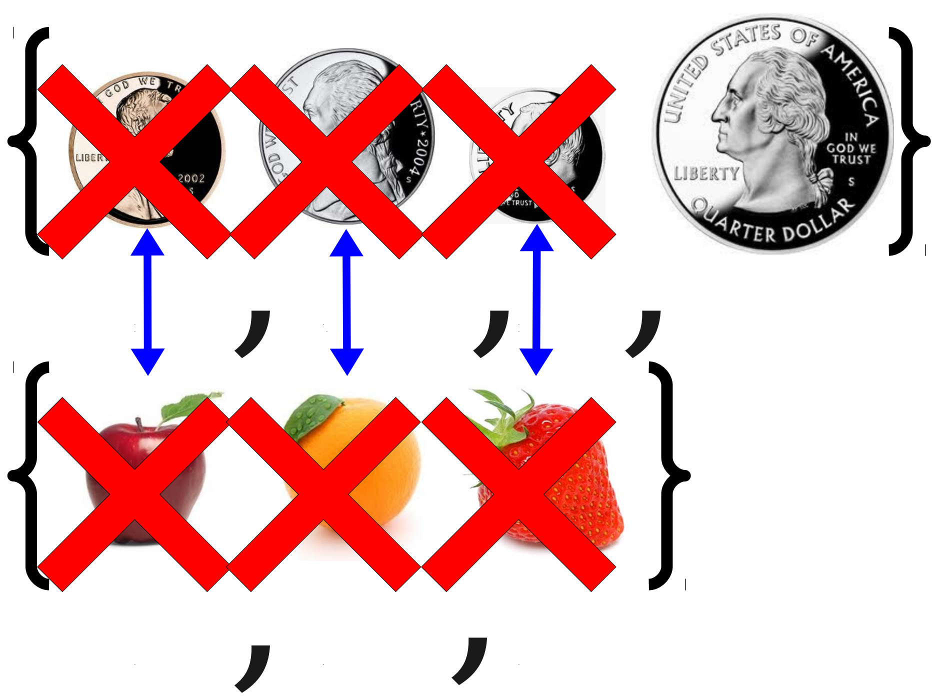
Comparing Cardinalities

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



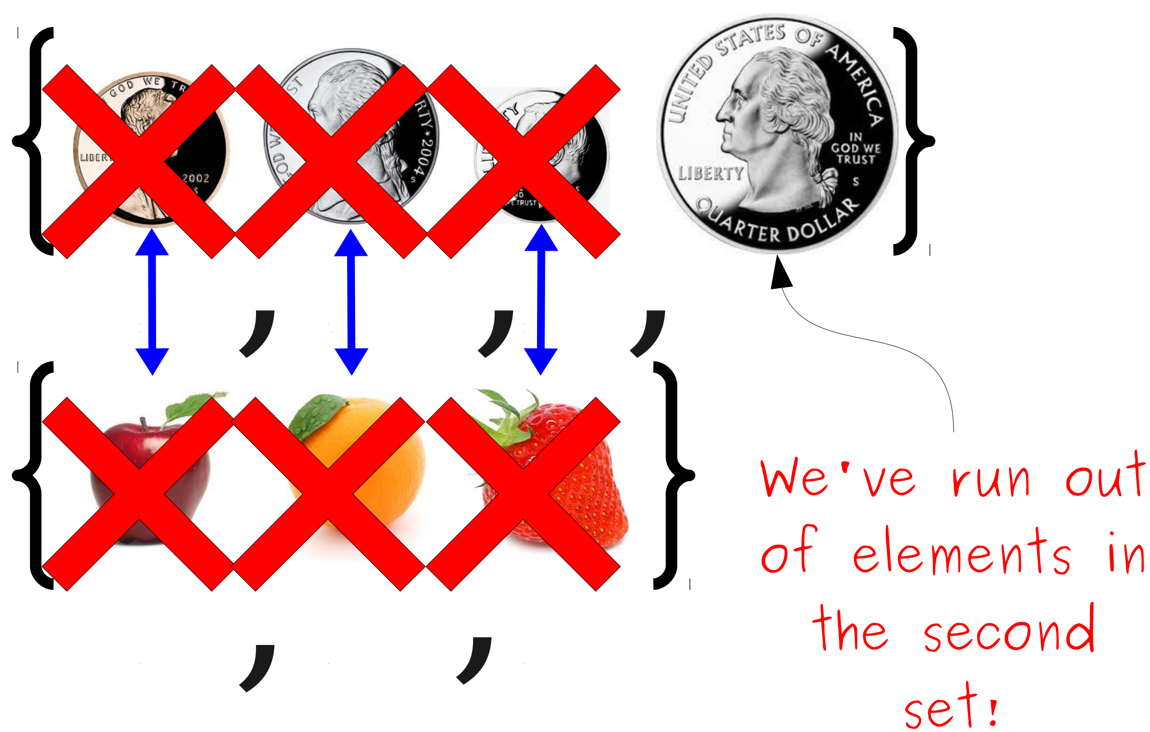
Comparing Cardinalities

- 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:



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

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

$$n \leftrightarrow 2n$$

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	...
$\mathbb{Z}$	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	...

$$n \leftrightarrow \begin{array}{l} \text{if } n \text{ is even, then } -n / 2 \\ \text{if } n \text{ is odd, then } (n + 1) / 2 \end{array}$$

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

Important Question

Do all infinite sets have the same cardinality?

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

$S = \{$ 

, 

$\}$

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

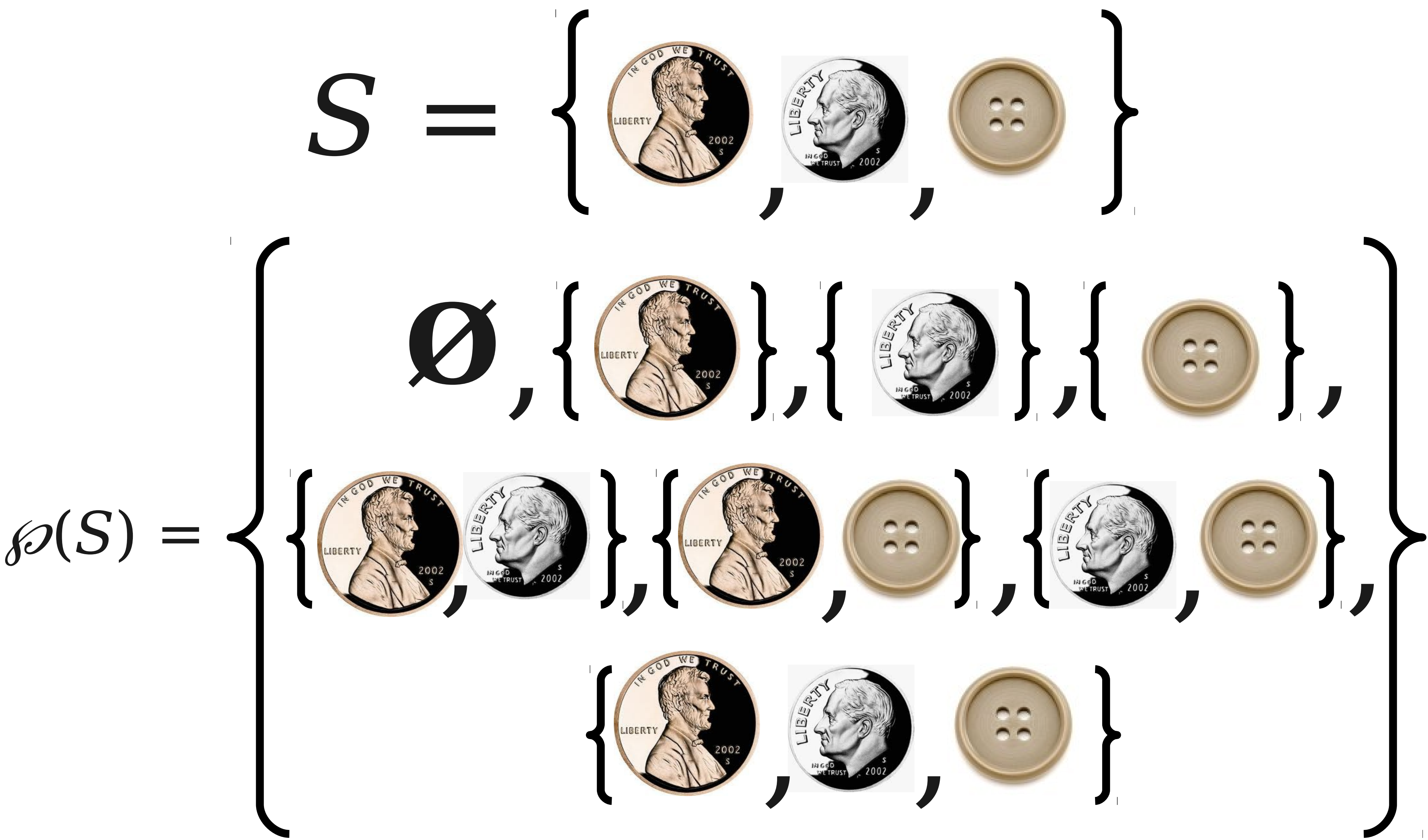
$\}, \{$ 

$\}, \{$ 

, 

$\} \}$

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



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

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

$$\wp(S) = \{$$
$$\varnothing,$$
$$\{a\}, \{b\}, \{c\}, \{d\},$$
$$\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{b, e\}$$
$$\{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\},$$
$$\{a, b, c, d\}$$
$$\}$$

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

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

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

If $|S| = |\wp(S)|$, there has to be a one-to-one correspondence between elements of S and subsets of S.

What might this correspondence look like?

x_0

x_1

x_2

x_3

x_4

x_5

$\cdots$

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

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

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

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

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

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

$\dots$

x_0	x_1	x_2	x_3	x_4	x_5	$\dots$

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

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

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

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

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

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

$$\dots$$

x_0	x_1	x_2	x_3	x_4	x_5	…

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

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

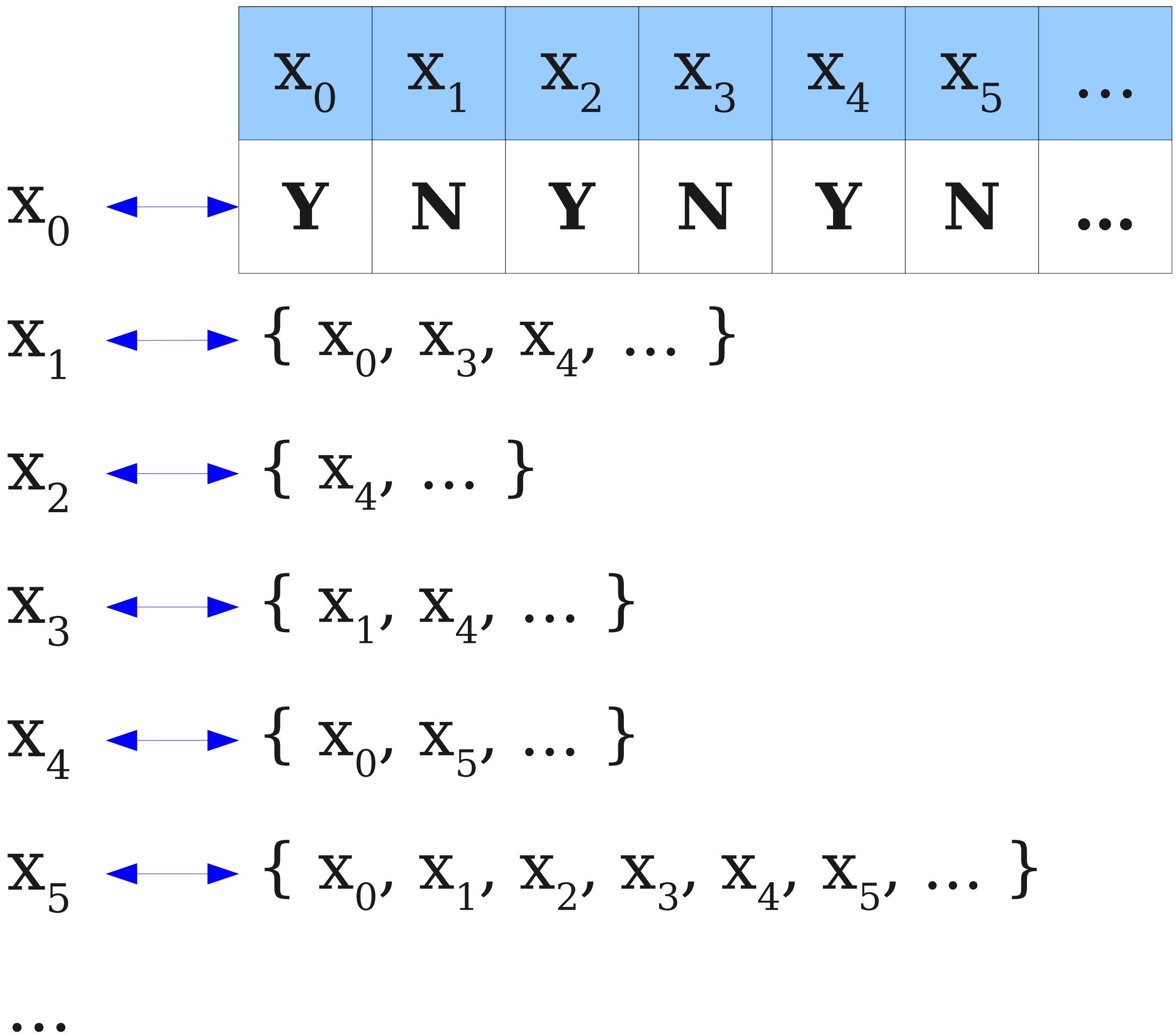
$$x_2 \longleftrightarrow \{\, x_4, \ldots \,\}$$

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

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

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

$\ldots$



x_0 x_1 x_2 x_3 x_4 x_5 ...
x_0 Y N Y N Y N ...
x_1 { x_0, x_3, x_4, ... }
x_2 { x_4, ... }
x_3 { x_1, x_4, ... }
x_4 { x_0, x_5, ... }
x_5 { x_0, x_1, x_2, x_3, x_4, x_5, ... }
...

x_0	x_1	x_2	x_3	x_4	x_5	…

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

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

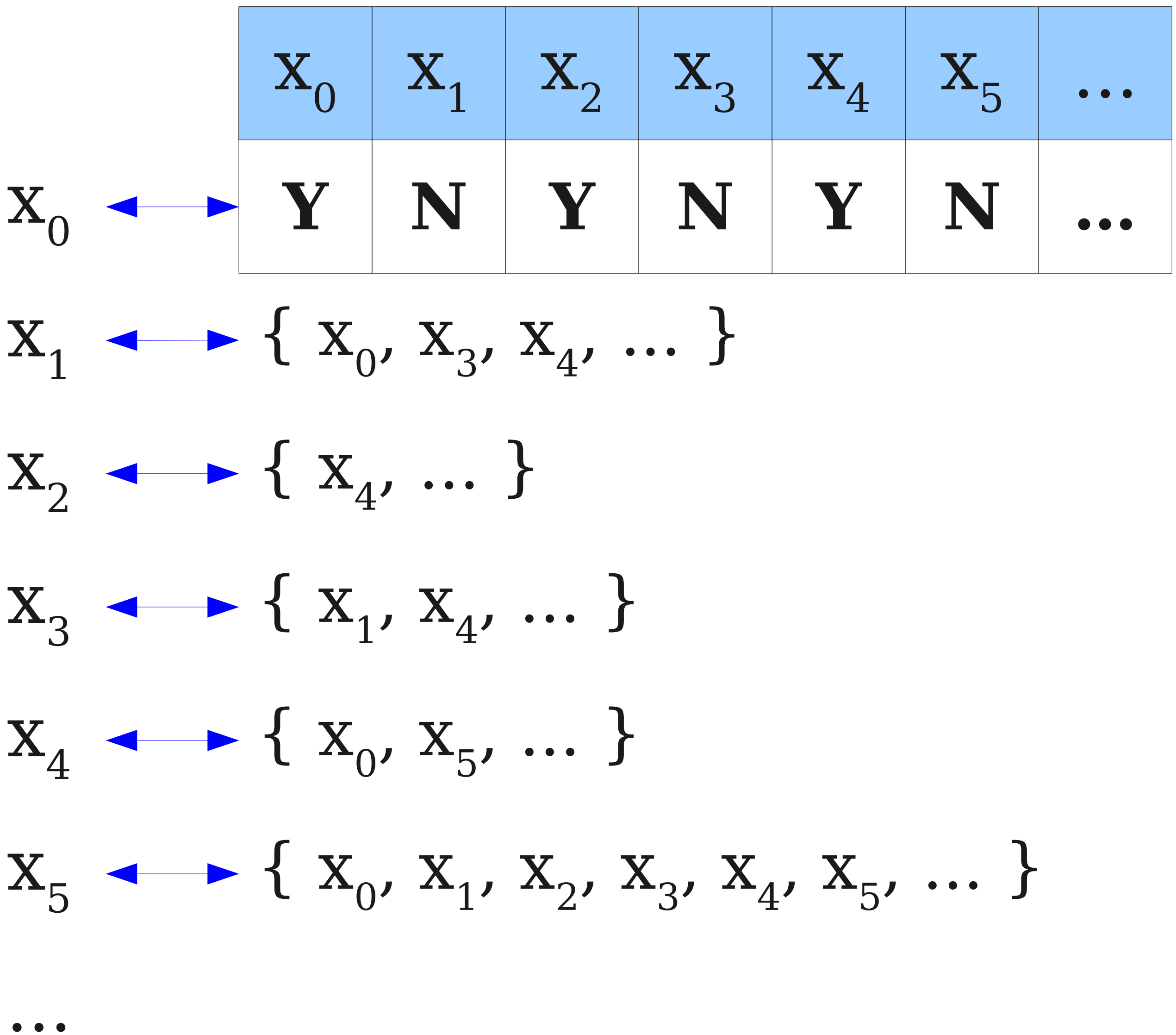
$$x_2 \longleftrightarrow \{\, x_4, \ldots \,\}$$

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

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

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

$$\ldots$$



x0 x1 x2 x3 x4 x5 ...
x0 Y N Y N Y N ...
x1 { x0, x3, x4, ... }
x2 { x4, ... }
x3 { x1, x4, ... }
x4 { x0, x5, ... }
x5 { x0, x1, x2, x3, x4, x5, ... }
...

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

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

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

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

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

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

…

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

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

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

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

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

...

	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**	**…**

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

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

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

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

…

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

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

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

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

...

	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**	**…**

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

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

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

…

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

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

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

...

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

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

…

	x_0	x_1	x_2	x_3	x_4	x_5	...
x_0	**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_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_4	**Y**	**N**	**N**	**N**	**N**	**Y**	…
x_5	**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_4	**Y**	**N**	**N**	**N**	**N**	**Y**	…
x_5	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	…
…	…	…	…	…	…	…	…

$$\left\{ \mathbf{x_0}, \quad \mathbf{x_5}, \quad \ldots \right\}$$

	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**	...

	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**	…
…	…	…	…	…	…	…	…

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**	...
...	...	...	...	...	...	...	...

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_4	**Y**	**N**	**N**	**N**	**N**	**Y**	…
X_5	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	…
…	…	…	…	…	…	…	…

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

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_4	**Y**	**N**	**N**	**N**	**N**	**Y**	…
x_5	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	…
…	…	…	…	…	…	…	…

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

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_4	**Y**	**N**	**N**	**N**	**N**	**Y**	…
x_5	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	…
…	…	…	…	…	…	…	…

$$\{\ \mathbf{x_1},\ \mathbf{x_2},\ \mathbf{x_3},\ \mathbf{x_4},\ \dots\ \}$$

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**	…
…	…	…	…	…	…	…	…

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

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_4	**Y**	**N**	**N**	**N**	**N**	**Y**	...
x_5	**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_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**	…
…	…	…	…	…	…	…	…

Which row in the table is paired with this set?

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_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?

	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

- The **complemented diagonal** cannot appear anywhere in the table.
  - In row n, the nth 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**: Every set is smaller than its power set:

For any set S, $|S| < |\wp(S)|$

Infinite Cardinalities

- Recall: $|\mathbb{N}| = \aleph_0$.
- 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 are multiple different infinities.**

What does this have to do with computation?

“The set of all computer programs”

“The set of all problems to solve”

Strings and Problems

- Consider the set of all strings:

  { “”, “a”, “b”, “c”, …, “aa”, “ab”, “ac,” … }

- For any set of strings *S*, we can solve the following problem about *S*:

  Write a program that accepts as input a string, then prints out whether or not that string belongs to set *S*.

- Therefore, there are at least as many problems to solve as there are sets of strings.

Every computer program is a string.

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

|Programs| ≤ |Strings| < |Sets of Strings| ≤ |Problems|

Every computer program is a string.

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

|Programs| < |Problems|

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

It Gets Worse

- Because there are more problems 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* problems than solutions.
- In fact, if you pick a totally random problem, the probability that you can solve it is *zero*.

But then it gets better...

Where We're Going

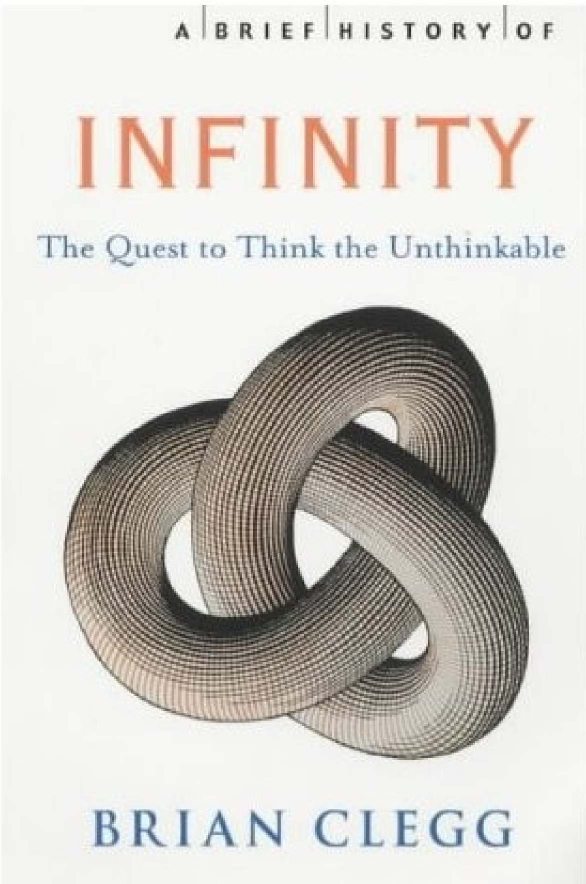
- **Given this hard theoretical limit, what *can* we compute?**
  - What are the hardest problems we *can* solve?
  - How powerful of a computer do we need to solve these problems?
  - Of what we can compute, what can we compute *efficiently*?
- **What tools do we need to reason about this?**
  - How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

Next Time

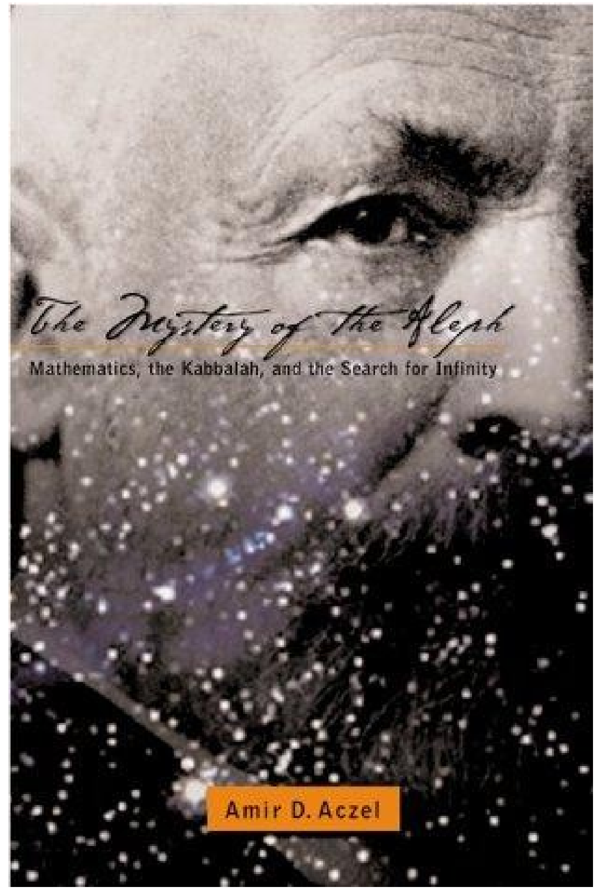
- **Mathematical Proof**
  - What is a mathematical proof?
  - How can we prove things with certainty?

Direct Proofs

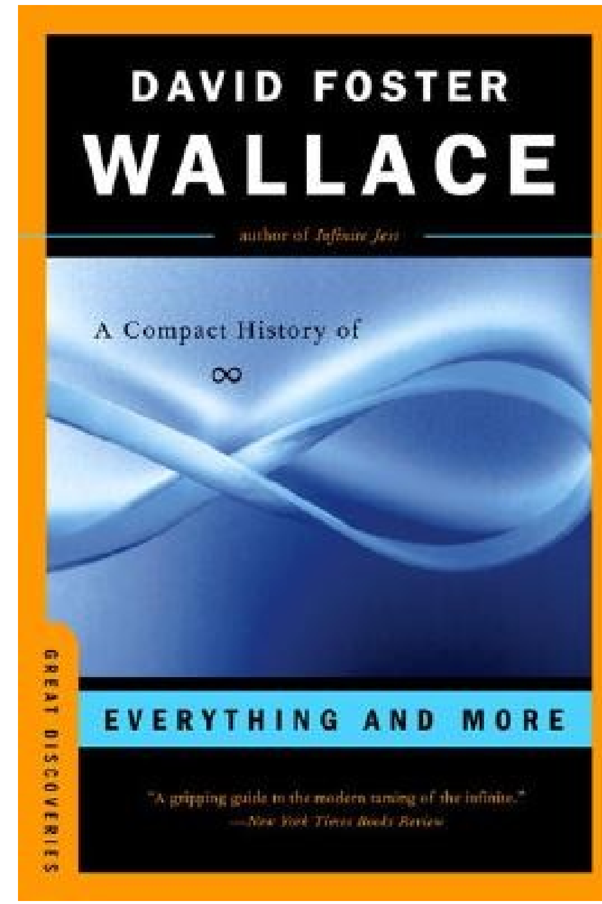
Recommended Reading



A Brief History of Infinity



The Mystery of the Aleph



Everything and More

What is a Proof?

Induction and Deduction

- In the sciences, much reasoning is done **inductively**.
  - Conduct a series of experiments and find a rule that explains all the results.
  - Conclude that there is a general principle explaining the results.
  - Even if all data are correct, the conclusion might be incorrect.
- In mathematics, reasoning is done **deductively**.
  - Begin with a series of statements assumed to be true.
  - Apply logical reasoning to show that some conclusion necessarily follows.
  - If all the starting assumptions are correct, the conclusion necessarily must be correct.

Structure of a Mathematical Proof

- Begin with a set of initial assumptions called **hypotheses**.
- Apply logical reasoning to derive the final result (the **conclusion**) from the hypotheses.
- Assuming that all intermediary steps are sound logical reasoning, the conclusion follows from the hypotheses.

Direct Proofs

Direct Proofs

- A **direct proof** is the simplest type of proof.
- Starting with an initial set of hypotheses, apply simple logical steps to prove the conclusion.
  - *Directly* proving that the result is true.
- Contrasts with **indirect proofs**, which we'll see on Friday.

Two Quick Definitions

- An integer n is **even** if there is some integer k such that $n = 2k$.
  - This means that 0 is even.
- An integer n is **odd** if there is some integer k such that $n = 2k + 1$.
- We'll assume the following for now:
  - Every integer is either even or odd.
  - No integer is both even and odd.

A Simple Direct Proof

Theorem: If n is even, then n^2 is even.

A Simple Direct Proof

Theorem: If n is even, then n^2 is even.
Proof: Let n be an even integer.

A Simple Direct Proof

Theorem: If n is even, then n^2 is even.
Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

A Simple Direct Proof

Theorem: If n is even, then n^2 is even.
Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

A Simple Direct Proof

Theorem: If n is even, then n^2 is even.
Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Since $2k^2$ is an integer, this means that there is some integer m (namely, $2k^2$) such that $n^2 = 2m$.

A Simple Direct Proof

Theorem: If n is even, then n^2 is even.

Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Since $2k^2$ is an integer, this means that there is some integer m (namely, $2k^2$) such that $n^2 = 2m$.

Thus n^2 is even. ■

A Simple Direct Proof

Theorem: If n is even, then n^2 is even.
Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Since $2k^2$ is an integer, this means that there is some integer m (namely, $2k^2$) such that $n^2 = 2m$.

Thus n^2 is even. ■

This symbol means "end of proof"

A Simple Direct Proof

Theorem: If n is even, then n^2 is even.
Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Since $2k^2$ is an integer, this means that there is some integer m (namely, $2k^2$) such that $n^2 = 2m$.

Thus n^2 is even. ■

A Simple Direct Proof

Theorem: If n is even, then n^2 is even.

Proof: Let n be an even integer.

Sin … er k

suc …

To prove a statement of the form

"If *P*, then *Q*"

Assume that ***P*** is true, then show that ***Q*** must be true as well.

Thi … $2(2k^2)$.

Sin … hat

the … ^{2}) such

that $n^2 = 2m$.

Thus n^2 is even. ■

A Simple Direct Proof

Theorem: If n is even, then n^2 is even.
Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Since $2k^2$ is an integer, this means that there is some integer m (namely, $2k^2$) such that $n^2 = 2m$.

Thus n^2 is even. ■

A Simple Direct Proof

Theorem: If n is even, then n^2 is even.
Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This mea).

Since $2k$
there is ch
that $n^2 =$

Thus n^2 is even. ■

This is the definition of an even integer. When writing a mathematical proof, it's common to call back to the definitions.

A Simple Direct Proof

Theorem: If n is even, then n^2 is even.
Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Since $2k^2$ is an integer, this means that there is some integer m (namely, $2k^2$) such that $n^2 = 2m$.

Thus n^2 is even. ■

A Simple Direct Proof

Theorem: If n is even, then n^2 is even.
Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Since 2

there is … uch

that n^2

Thus n^2

Notice how we use the value of ***k*** that we obtained above. Giving names to quantities, even if we aren't fully sure what they are, allows us to manipulate them. This is similar to variables in programs.

A Simple Direct Proof

Theorem: If n is even, then n^2 is even.
Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Since $2k^2$ is an integer, this means that there is some integer m (namely, $2k^2$) such that $n^2 = 2m$.

Thus n^2 is even. ■

A Simple Direct Proof

Theorem: If n is even, then n^2 is even.

Proof: Let n b

Since n

such th

This me

^{2}).

Our ultimate goal is to prove that n^2 is even. This means that we need to find some m such that $n^2 = 2m$. Here, we're explicitly showing how we can do that.

Since $2k^2$ is an integer, this means that there is some integer m (namely, $2k^2$) such that $n^2 = 2m$.

Thus n^2 is even. ■

A Simple Direct Proof

Theorem: If n is even, then n^2 is even.
Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Since $2k^2$ is an integer, this means that there is some integer m (namely, $2k^2$) such that $n^2 = 2m$.

Thus n^2 is even. ■

A Simple Direct Proof

Theorem: If n is even, then n^2 is even.

Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Since 2

there is ... uch

that n^2

Hey, that's what we were trying to show! We're done now.

Thus n^2 is even. ■

Another Direct Proof

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Another Direct Proof

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Another Direct Proof

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

How do we prove that this is true for *any* choice of sets?

Proving Something Always Holds

- Many statements have the form

For any *X*, P(*X*) is true.

- Examples:

For all integers n, if n is even, n^2 is even.

For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

For all sets S, $|S| < |\wp(S)|$.

- How do we prove these statements when there are infinitely many cases to check?

Arbitrary Choices

- To prove that P(x) is true for all possible x, show that no matter what choice of x you make, P(x) must be true.
- Start the proof by making an arbitrary choice of x:
  - "Let x be chosen arbitrarily."
  - "Let x be an arbitrary even integer."
  - "Let x be an arbitrary set containing 137."
  - "Consider any x."
- Demonstrate that P(x) holds true for this choice of x.
- Conclude that since the choice of x was arbitrary, P(x) must hold true for all choices of x.

Another Direct Proof

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Another Direct Proof

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets with $A \subseteq B$ and $B \subseteq C$.

Another Direct Proof

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets with $A \subseteq B$ and $B \subseteq C$.

Another Direct Proof

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets with $A \subseteq B$ and $B \subseteq C$.

We're showing here that regardless of what A, B, and C you pick, the result will still be true.

Another Direct Proof

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets with $A \subseteq B$ and $B \subseteq C$.

Another Direct Proof

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets with $A \subseteq B$ and $B \subseteq C$.

To prove a statement of the form

"If *P*, then *Q*"

Assume that ***P*** is true, then show that ***Q*** must be true as well.

Another Direct Proof

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets with $A \subseteq B$ and $B \subseteq C$.

By definition, since $A \subseteq B$, every $x \in A$ also satisfies $x \in B$.

Another Direct Proof

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets with $A \subseteq B$ and $B \subseteq C$.

By definition, since $A \subseteq B$, every $x \in A$ also satisfies $x \in B$.

By definition, since $B \subseteq C$, every $x \in B$ also satisfies $x \in C$.

Another Direct Proof

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets with $A \subseteq B$ and $B \subseteq C$.

By definition, since $A \subseteq B$, every $x \in A$ also satisfies $x \in B$.

By definition, since $B \subseteq C$, every $x \in B$ also satisfies $x \in C$.

Consequently, any $x \in A$ satisfies $x \in C$.

Another Direct Proof

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets with $A \subseteq B$ and $B \subseteq C$.

By definition, since $A \subseteq B$, every $x \in A$ also satisfies $x \in B$.

By definition, since $B \subseteq C$, every $x \in B$ also satisfies $x \in C$.

Consequently, any $x \in A$ satisfies $x \in C$.

Thus $A \subseteq C$.

Another Direct Proof

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets with $A \subseteq B$ and $B \subseteq C$.

By definition, since $A \subseteq B$, every $x \in A$ also satisfies $x \in B$.

By definition, since $B \subseteq C$, every $x \in B$ also satisfies $x \in C$.

Consequently, any $x \in A$ satisfies $x \in C$.

Thus $A \subseteq C$. ■

An Incorrect Proof

An Incorrect Proof

Theorem: For any integer n, if n is even, n has no odd divisors.

An Incorrect Proof

Theorem: For any integer n, if n is even, n has no odd divisors.

Proof: Consider an arbitrary even natural number, say, 16. 16 is even, and it has no odd divisors. Since our choice was arbitrary, for any arbitrary n, if n is even, n has no odd divisors. ■

An Incorrect Proof

Theorem: For any integer n, if n is even, n has no odd divisors.

Proof: Consider an arbitrary even natural number, say, 16. 16 is even, and it has no odd divisors. Since our choice was arbitrary, for any arbitrary n, if n is even, n has no odd divisors. ■

An Incorrect Proof

Theorem: E … n has no
odd divisor …

Proof: Cons … al number,
say, 16. 16 … visors.
Since our c … rbitrary
n, if n is ev …

ar·bi·trar·y

adjective /ˈärbiˌtrerē/

1. Based on random choice or personal whim, rather than any reason or system - *“his mealtimes were entirely arbitrary”*

2. *(of power or a ruling body)* Unrestrained and autocratic in the use of authority - *“arbitrary rule by King and bishops has been made impossible”*

3. *(of a constant or other quantity)* Of unspecified value

Source: Google

ar·bi·trar·y
adjective /ˈärbiˌtrerē/

1. Based on random choice or personal whim, rather than any reason or system - *“his mealtimes were entirely arbitrary”*

2. *(of power or a ruling body)* Unrestrained and autocratic in the use of authority - *“arbitrary rule by King and bishops has been made impossible”*

3. *(of a constant or other quantity)* Of unspecified value

Use this definition

Source: Google

ar·bi·trar·y
adjective /ˈärbiˌtrerē/

Not this one!

1. Based on random choice or personal whim, rather than any reason or system - *“his mealtimes were entirely arbitrary”*

2. *(of power or a ruling body)* Unrestrained and autocratic in the use of authority - *“arbitrary rule by King and bishops has been made impossible”*

3. *(of a constant or other quantity)* Of unspecified value

Use this definition

Source: Google

To prove something is true for all x, **do not** choose an x and base the proof off of your choice!

Instead, leave x unspecified and show that no matter what x is, the specified property must hold.

Another Incorrect Proof

Theorem: For any sets A and B, $A \subseteq A \cap B$.

Another Incorrect Proof

Theorem: For any sets A and B, $A \subseteq A \cap B$.

Proof: We need to show that if $x \in A$, then $x \in A \cap B$ as well.

Another Incorrect Proof

Theorem: For any sets A and B, $A \subseteq A \cap B$.

Proof: We need to show that if $x \in A$, then $x \in A \cap B$ as well.

Consider any arbitrary $x \in A \cap B$.

Another Incorrect Proof

Theorem: For any sets A and B, $A \subseteq A \cap B$.

Proof: We need to show that if $x \in A$, then $x \in A \cap B$ as well.

Consider any arbitrary $x \in A \cap B$. This means that $x \in A$ and $x \in B$, so $x \in A$ as required. ■

Another Incorrect Proof

Theorem: For any sets A and B, $A \subseteq A \cap B$.

Proof: We need to show that if $x \in A$, then $x \in A \cap B$ as well.

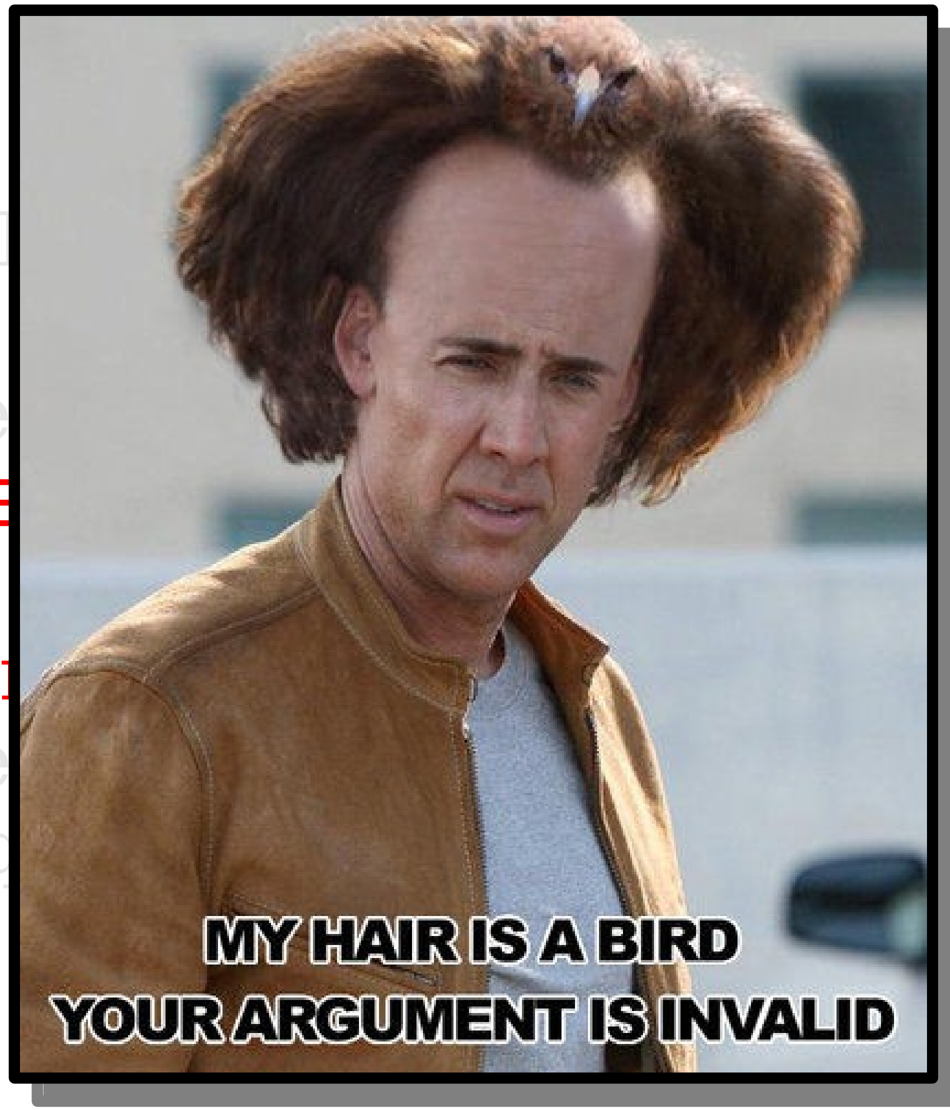
Consider any arbitrary $x \in A \cap B$. This means that $x \in A$ and $x \in B$, so $x \in A$ as required. ■

Another Incorrect Proof

Theorem: I $A \cap B$.

Proof: We A, then $x \in$

Co $A \cap B$. This me so $x \in A$ as rec



If you want to prove that P implies Q,
assume P and prove Q.

Don't assume Q and then prove P!

An Entirely Different Proof

Theorem: There exists a natural number $n > 0$ such that the sum of all natural numbers less than n is equal to n.

An Entirely Different Proof

Theorem: There exists a natural number $n > 0$ such that the sum of all natural numbers less than n is equal to n.

An Entirely Different Proof

Theorem: There exists a natural number $n > 0$ such that the sum of all natural numbers less than n is equal to n.

This is a fundamentally different type of proof that what we've done before. Instead of showing that every object has some property, we want to show that some object has a given property.

Universal vs. Existential Statements

- A **universal statement** is a statement of the form

For all *x*, P(*x*) is true.

- We've seen how to prove these statements.

Universal vs. Existential Statements

- A **universal statement** is a statement of the form

  For all *x*, P(*x*) is true.

- We've seen how to prove these statements.
- An **existential statement** is a statement of the form

  There exists an *x* for which P(*x*) is true.

- How do you prove an existential statement?

Proving an Existential Statement

- We will see several different ways to prove “there is some x for which P(x) is true.”
- Simple approach: Just go and find some x for which P(x) is true!
  - In our case, we need to find a positive natural number n such that that sum of all smaller natural numbers is equal to n.
  - Can we find one?

An Entirely Different Proof

Theorem: There exists a natural number $n > 0$ such that the sum of all natural numbers less than n is equal to n.

An Entirely Different Proof

Theorem: There exists a natural number $n > 0$ such that the sum of all natural numbers less than n is equal to n.

Proof: Take $n = 3$.

There are three natural numbers smaller than 3: 0, 1, and 2.

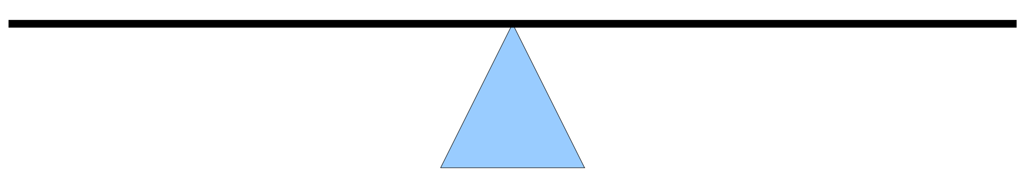
We have $0 + 1 + 2 = 3$.

Thus 3 is a natural number greater than zero equal to the sum of all smaller natural numbers. ■

The Counterfeit Coin Problem

Problem Statement

- You are given a set of three seemingly identical coins, two of which are real and one of which is counterfeit.
- The counterfeit coin weighs more than the rest of the coins.
- You are given a balance. Using only one weighing on the balance, find the counterfeit coin.



Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

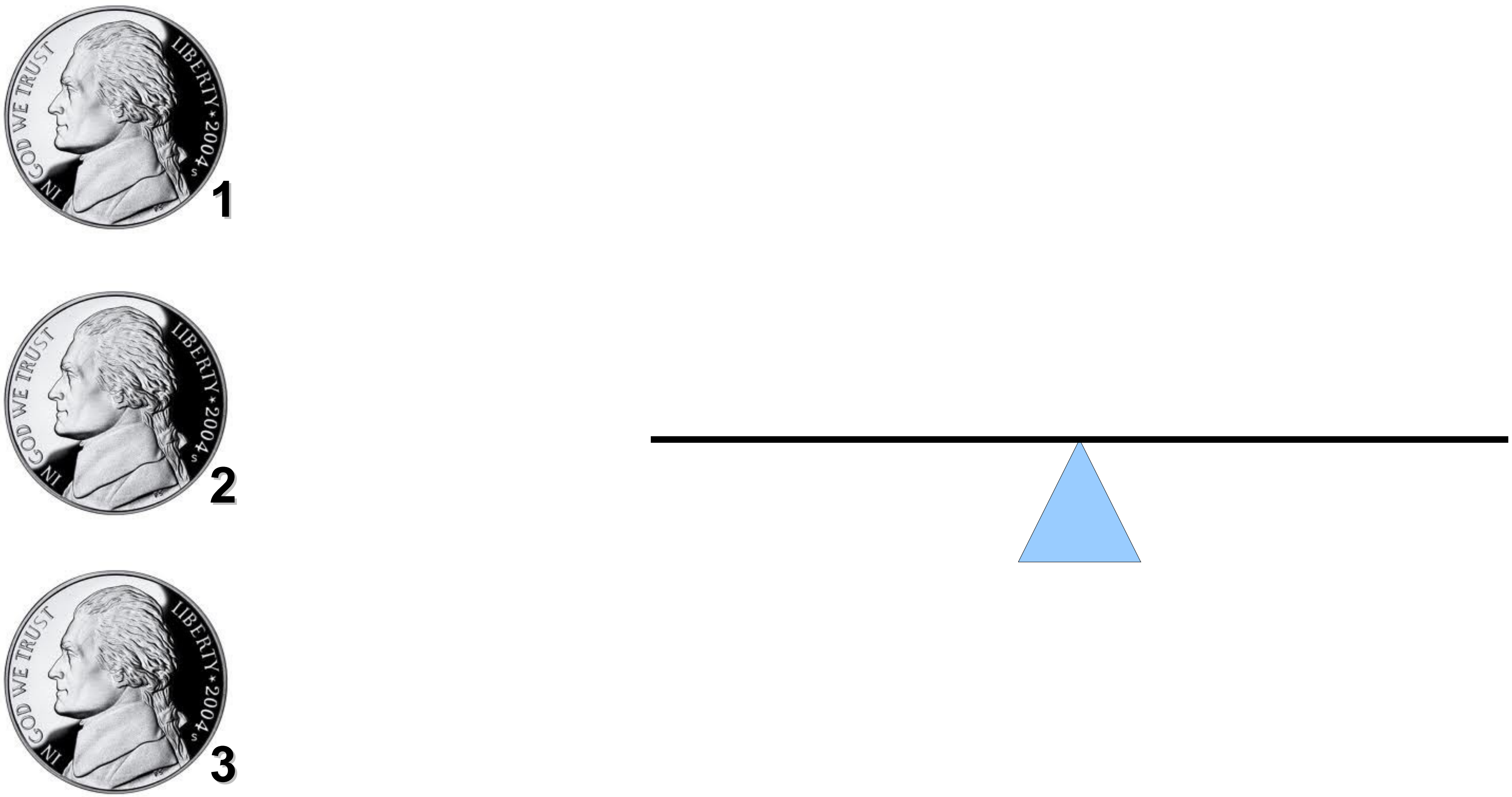
Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

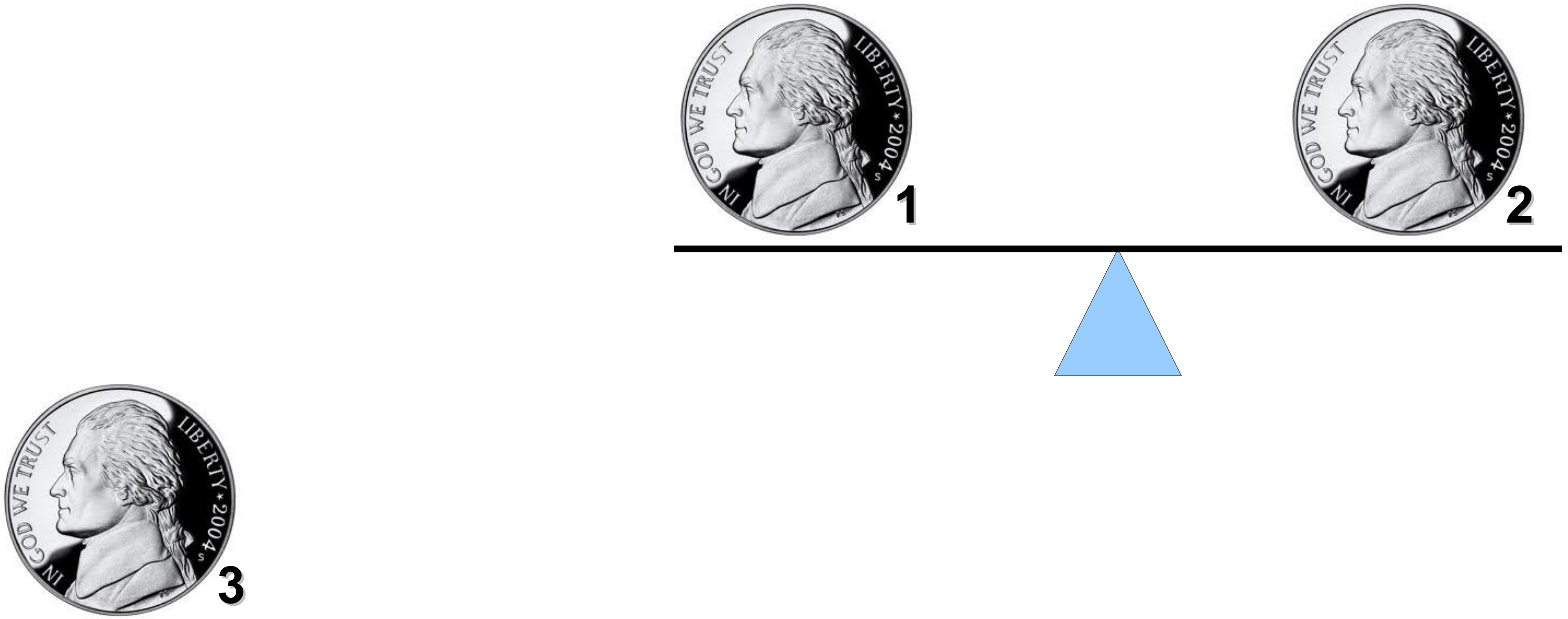
This is an existential statement.

We should try to look for an actual way to do this.

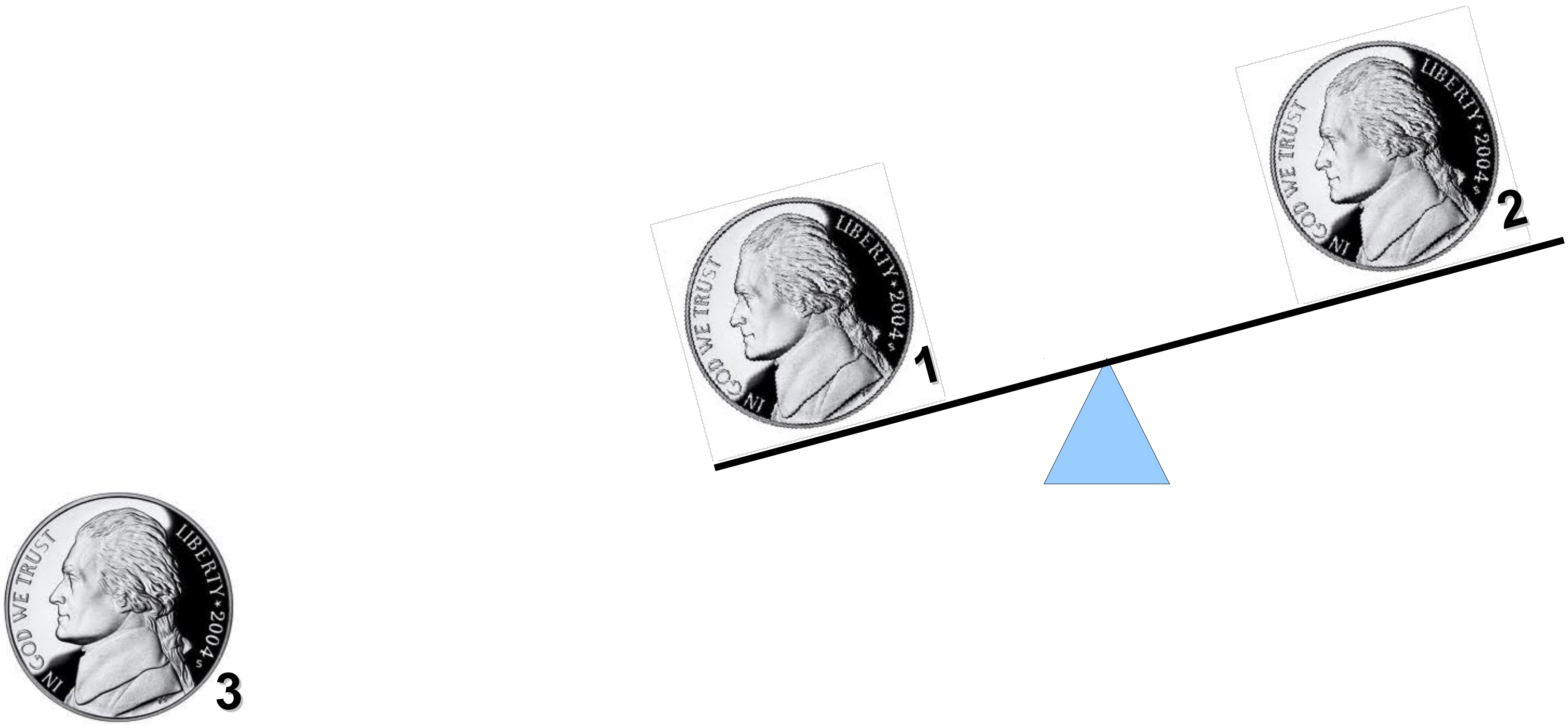
Finding the Counterfeit Coin



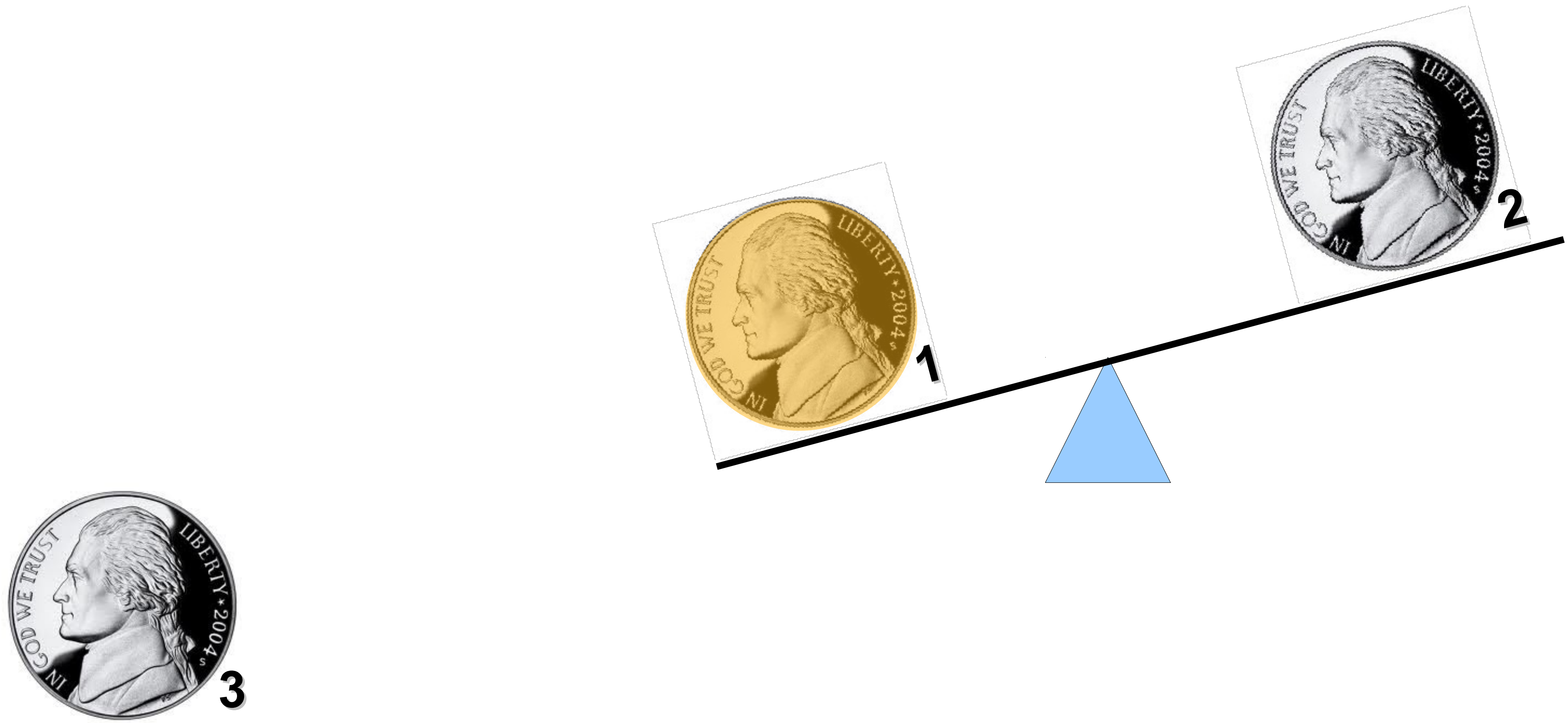
Finding the Counterfeit Coin



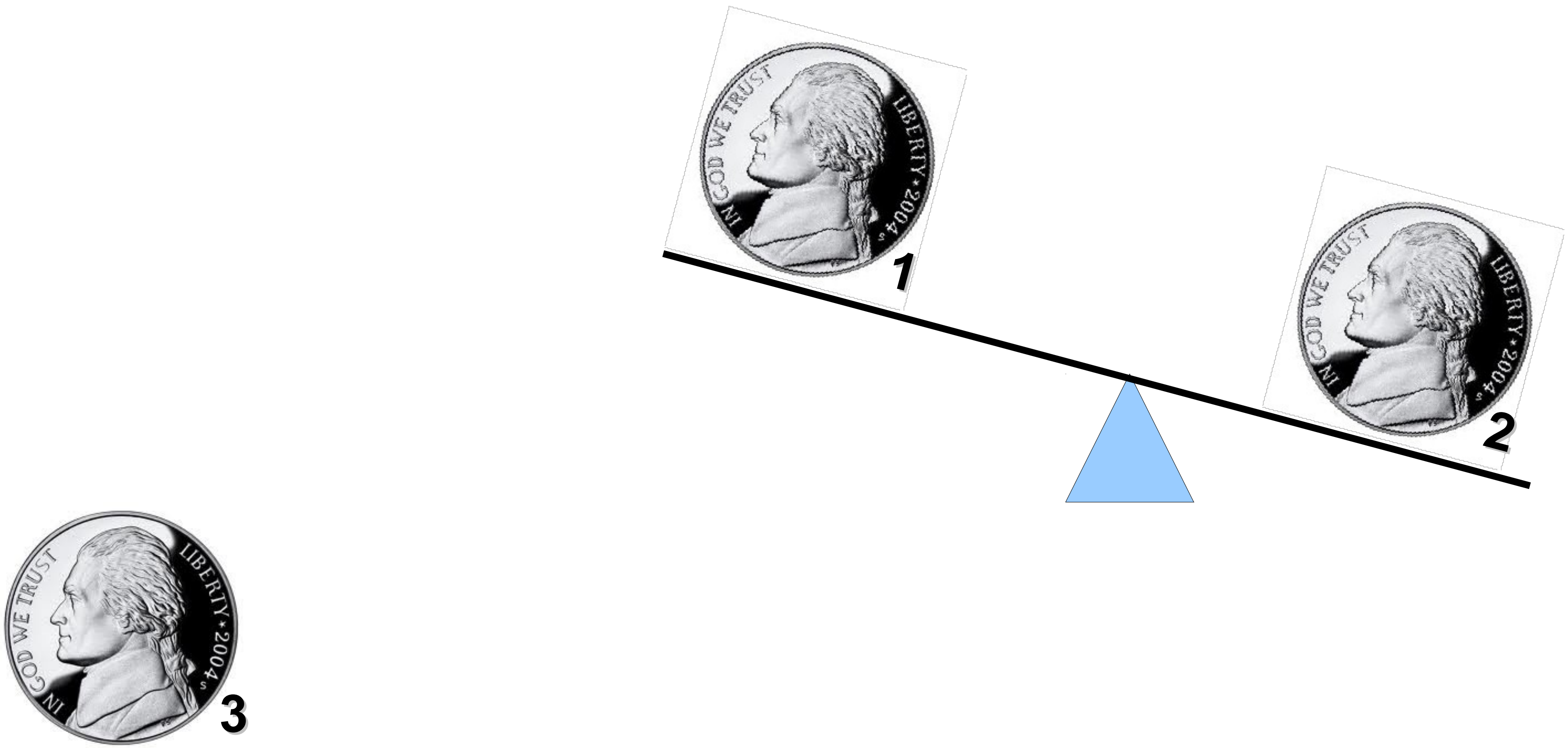
Finding the Counterfeit Coin



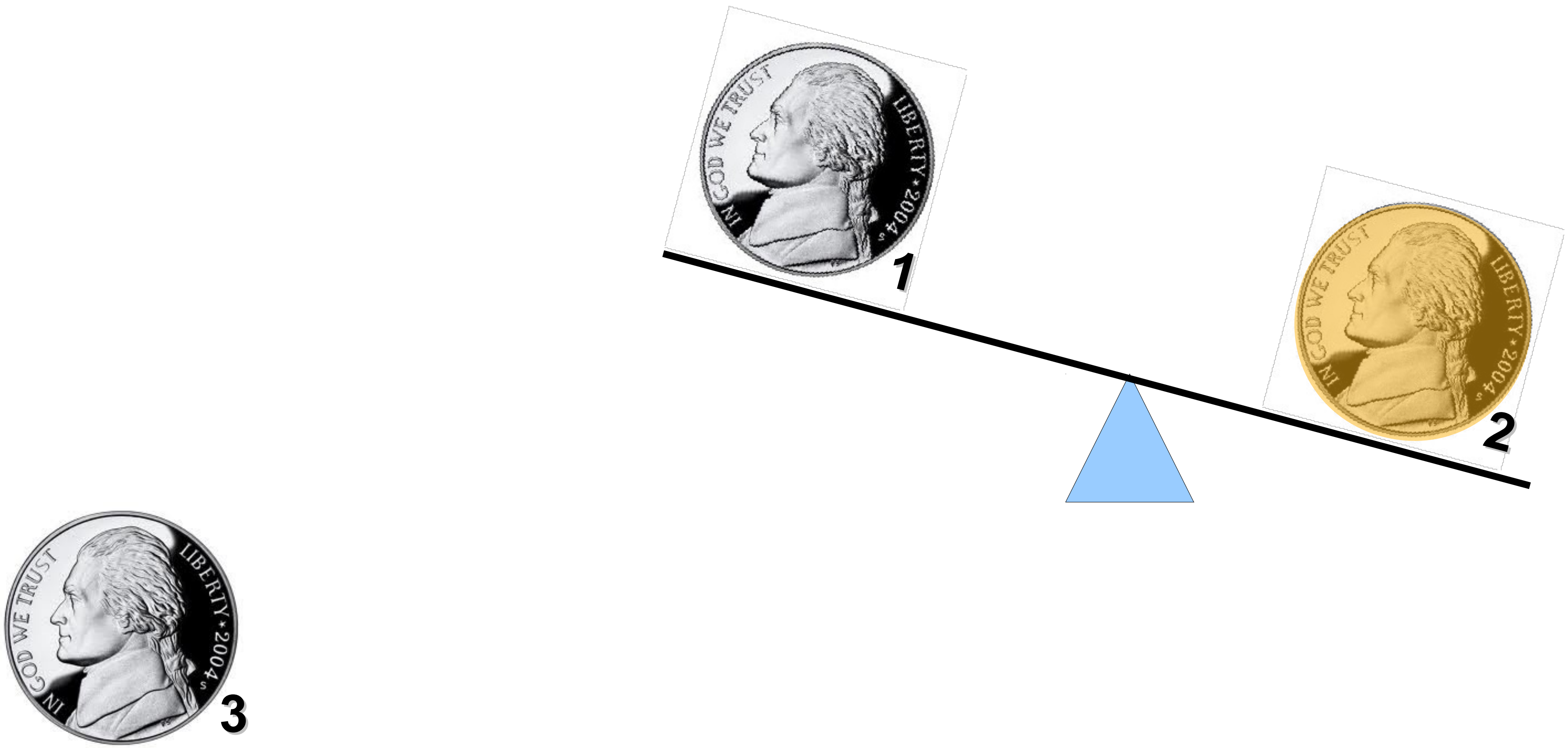
Finding the Counterfeit Coin



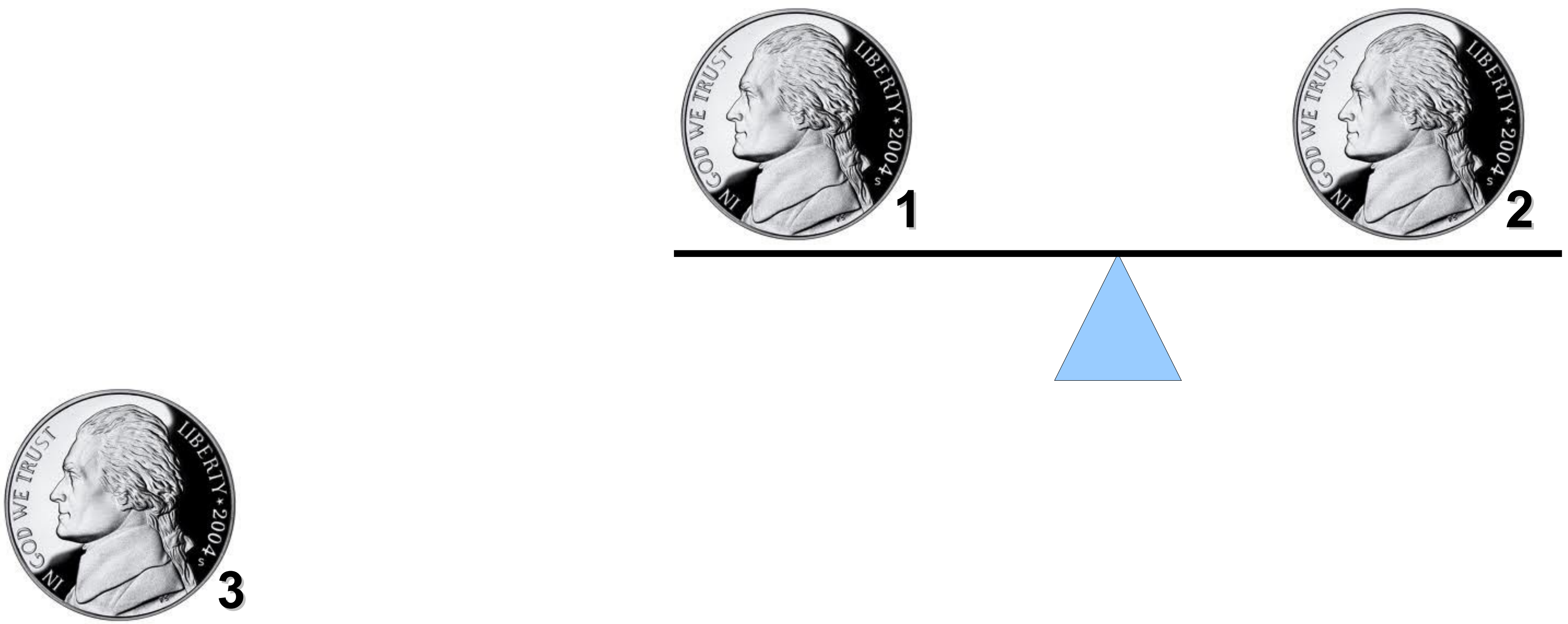
Finding the Counterfeit Coin



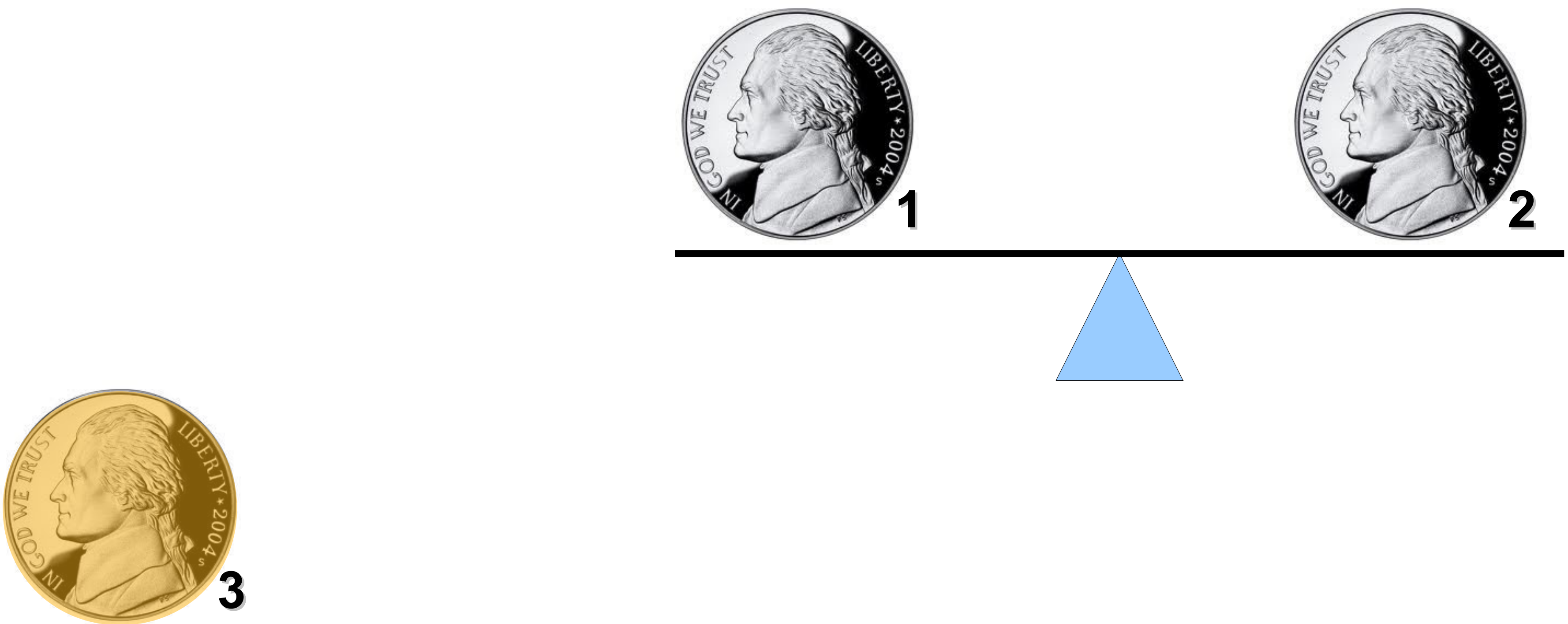
Finding the Counterfeit Coin



Finding the Counterfeit Coin



Finding the Counterfeit Coin



Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Coin A is heavier than coin B.

Case 2: Coin B is heaver than coin A.

Case 3: Coins A and B have the same weight.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Coin A is heavier than coin B.

Case 2: Coin B is heaver than coin A.

Case 3: Co

This is called a proof by cases (alternatively, a proof by exhaustion) and works by showing that the theorem is true regardless of what specific outcome arises.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Coin A is heavier than coin B. Then coin A is counterfeit.

Case 2: Coin B is heaver than coin A.

Case 3: Coins A and B have the same weight.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Coin A is heavier than coin B. Then coin A is counterfeit.

Case 2: Coin B is heaver than coin A. Then coin B is counterfeit.

Case 3: Coins A and B have the same weight.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Coin A is heavier than coin B. Then coin A is counterfeit.

Case 2: Coin B is heaver than coin A. Then coin B is counterfeit.

Case 3: Coins A and B have the same weight. Then coin C is counterfeit, because coins A and B are both honest.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Coin A is heavier than coin B. Then coin A is counterfeit.

Case 2: Coin B is heaver than coin A. Then coin B is counterfeit.

Case 3: Coins A and B have the same weight. Then coin C is counterfeit, because coins A and B are both honest.

In each case we can locate the counterfeit coin, so with just one weighing it is possible to find the counterfeit coin.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Coin A is heavier than coin B. Then coin A is counterfeit.

Case 2: Coin B is heaver than coin A. Then coin B is counterfeit.

Case 3: Coins A and B have the same weight. Then coin C is counterfeit, because coins A and B are both honest.

In each case we can locate the counterfeit coin, so with just one weighing it is possible to find the counterfeit coin.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

In a proof by cases, after demonstrating each case, you should summarize the cases afterwards to make your point clearer.

is counterfeit, because coins A and B are both honest.

In each case we can locate the counterfeit coin, so with just one weighing it is possible to find the counterfeit coin.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Coin A is heavier than coin B. Then coin A is counterfeit.

Case 2: Coin B is heaver than coin A. Then coin B is counterfeit.

Case 3: Coins A and B have the same weight. Then coin C is counterfeit, because coins A and B are both honest.

In each case we can locate the counterfeit coin, so with just one weighing it is possible to find the counterfeit coin.

Theorem: Given three coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in one weighing.

Proof: Label the three coins A, B, and C. Put coins A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Coin A is heavier than coin B. Then coin A is counterfeit.

Case 2: Coin B is heaver than coin A. Then coin B is counterfeit.

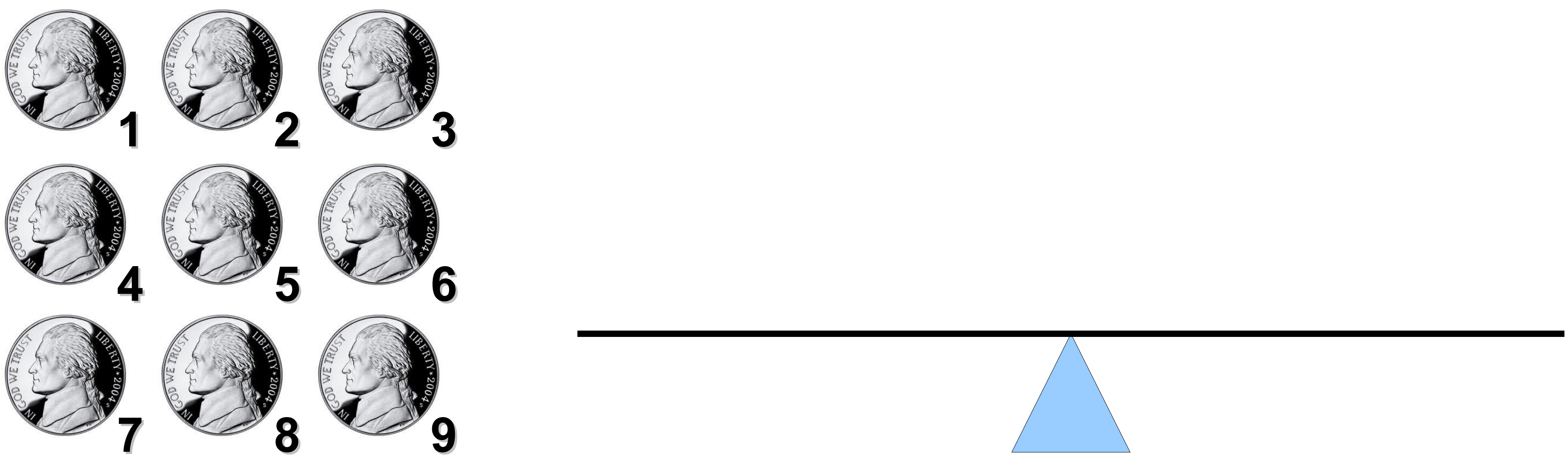
Case 3: Coins A and B have the same weight. Then coin C is counterfeit, because coins A and B are both honest.

In each case we can locate the counterfeit coin, so with just one weighing it is possible to find the counterfeit coin. ■

A Harder Problem

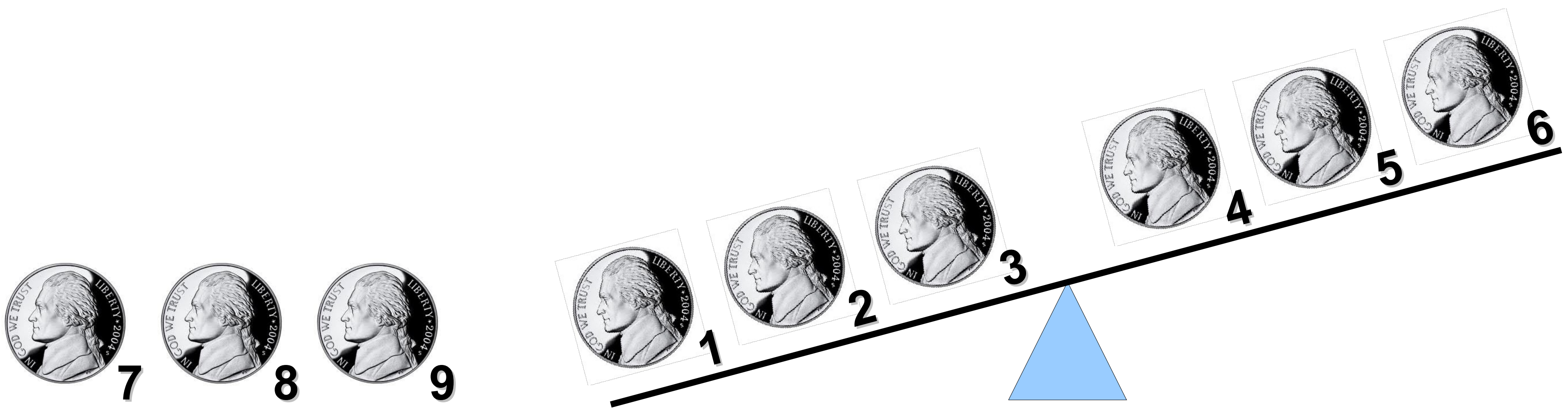
- You are given a set of **nine** seemingly identical coins, eight of which are real and one of which is counterfeit.
- The counterfeit coin weighs more than the rest of the coins.
- You are given a balance. Using only **two** weighings on the balance, find the counterfeit coin.

Finding the Counterfeit Coin

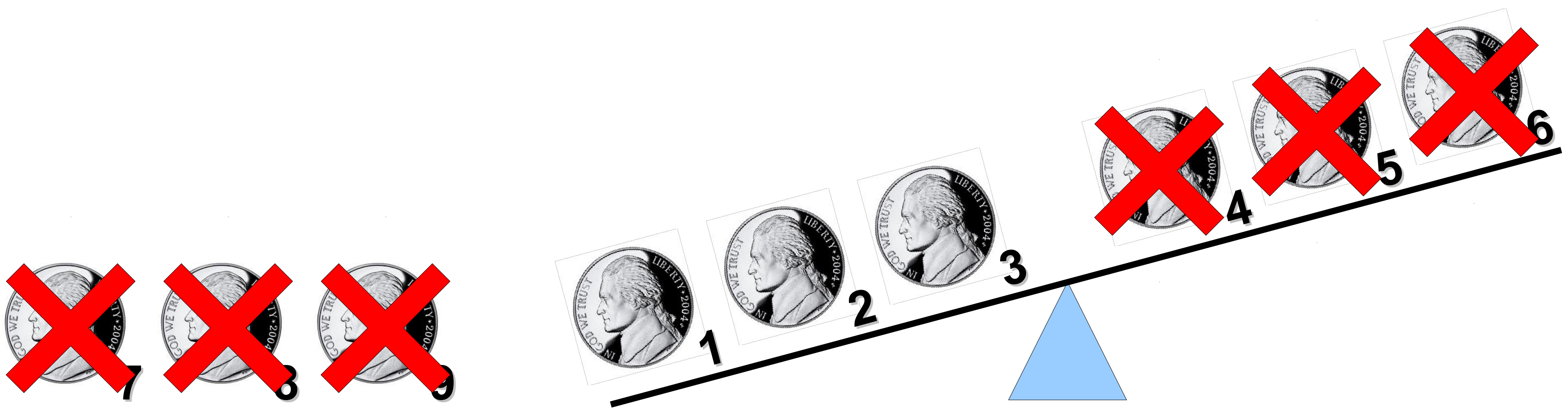


Finding the Counterfeit Coin

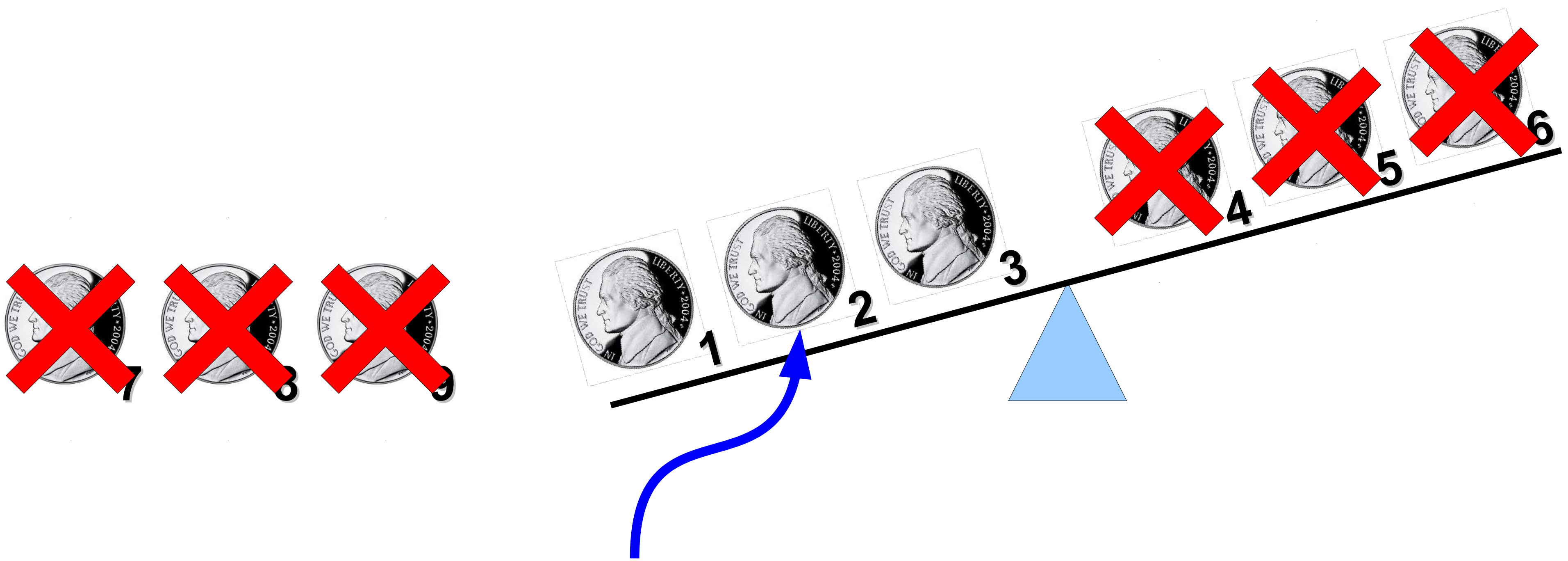
Finding the Counterfeit Coin



Finding the Counterfeit Coin

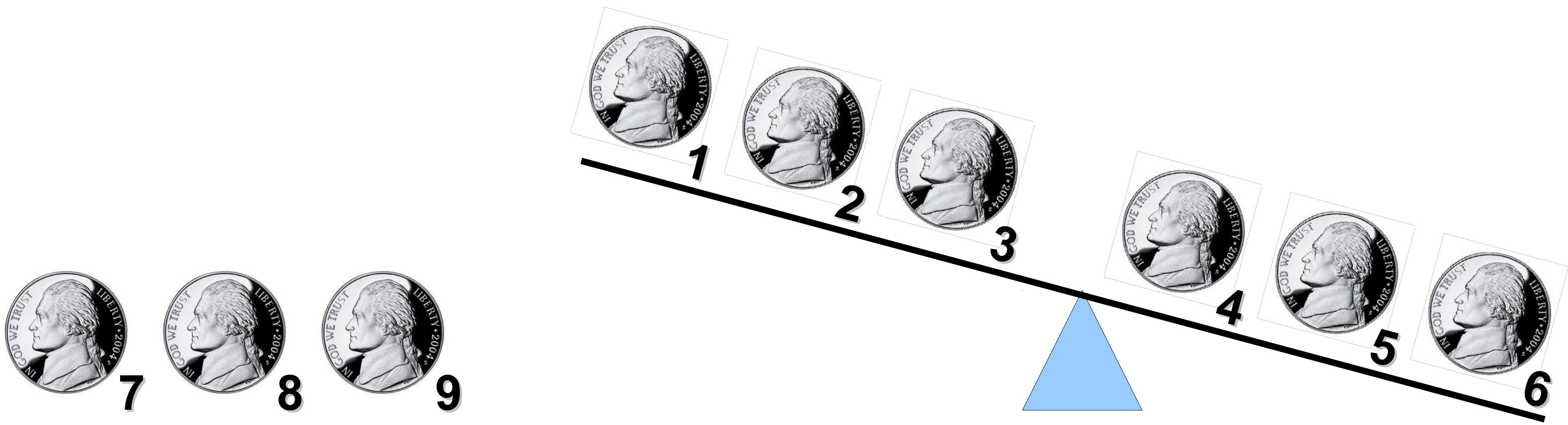


Finding the Counterfeit Coin

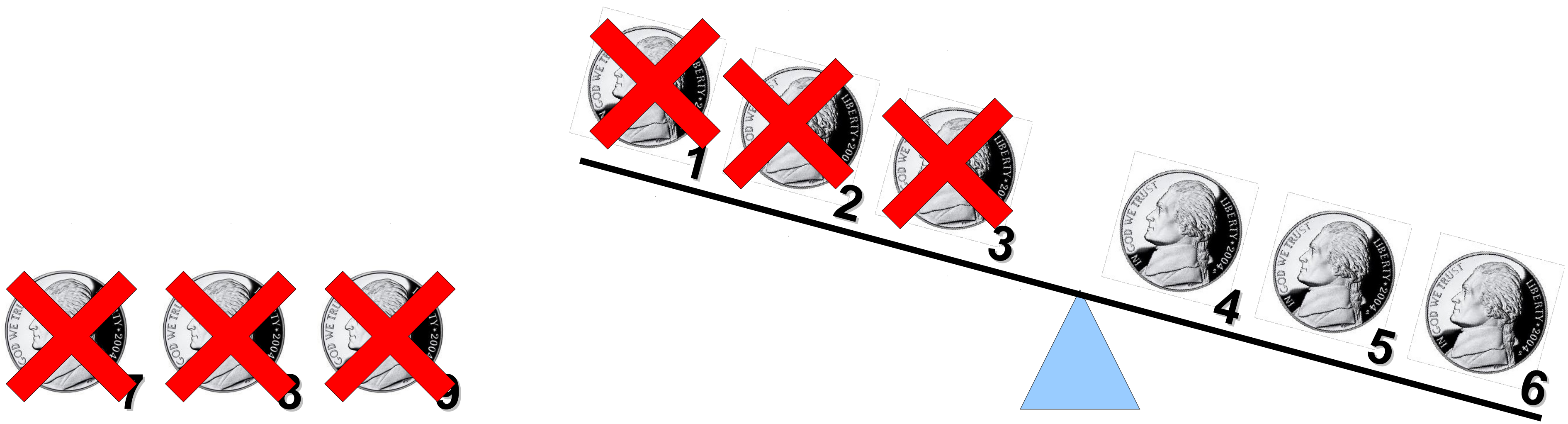


Now we have one weighing to find the counterfeit out of these three.

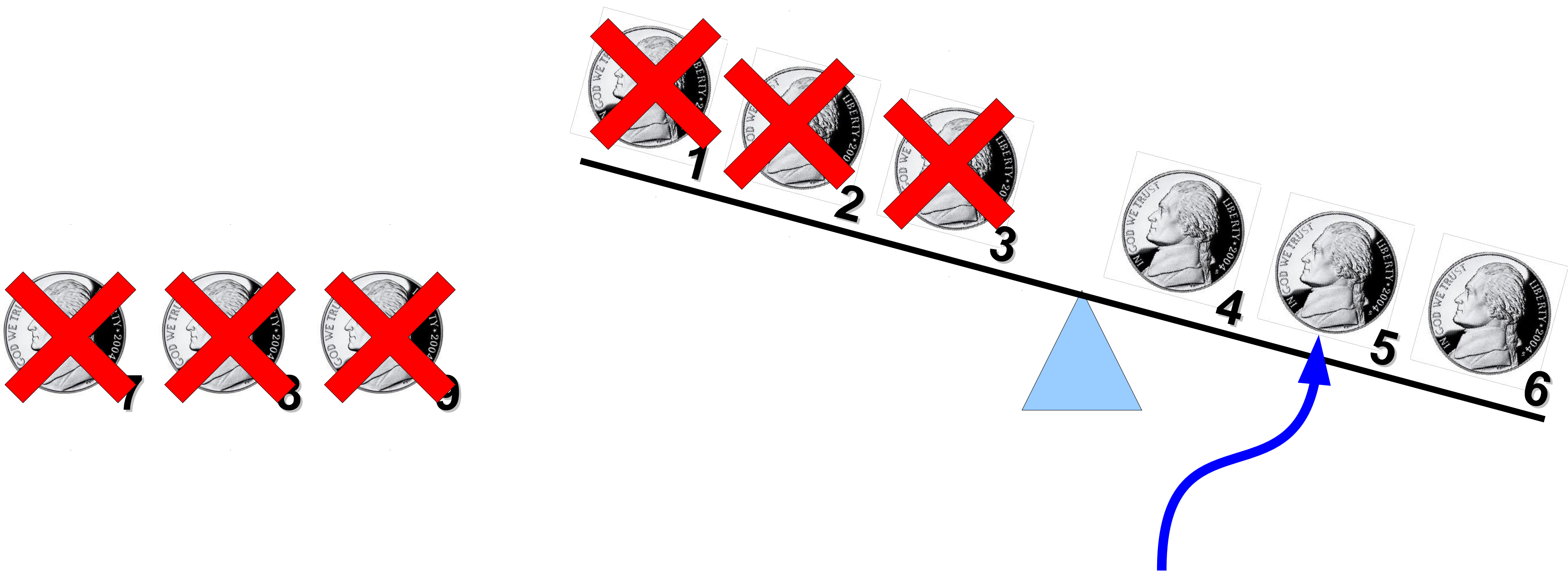
Finding the Counterfeit Coin



Finding the Counterfeit Coin



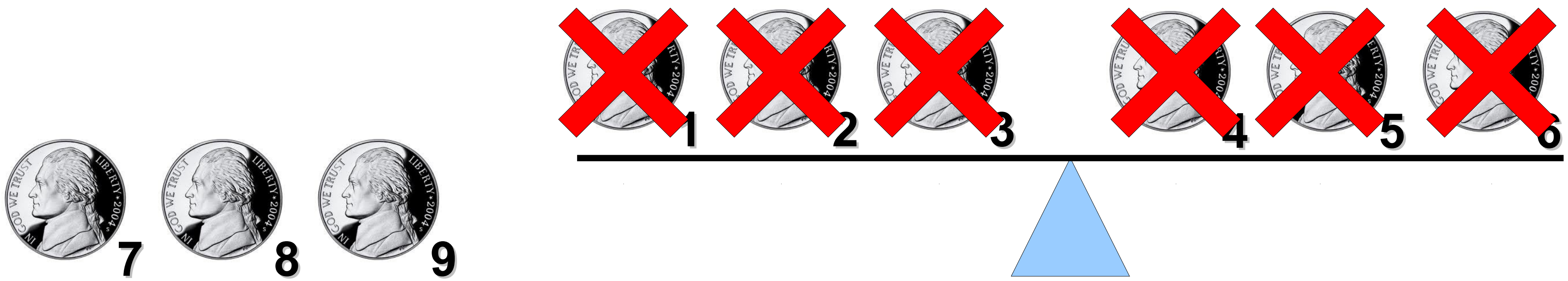
Finding the Counterfeit Coin



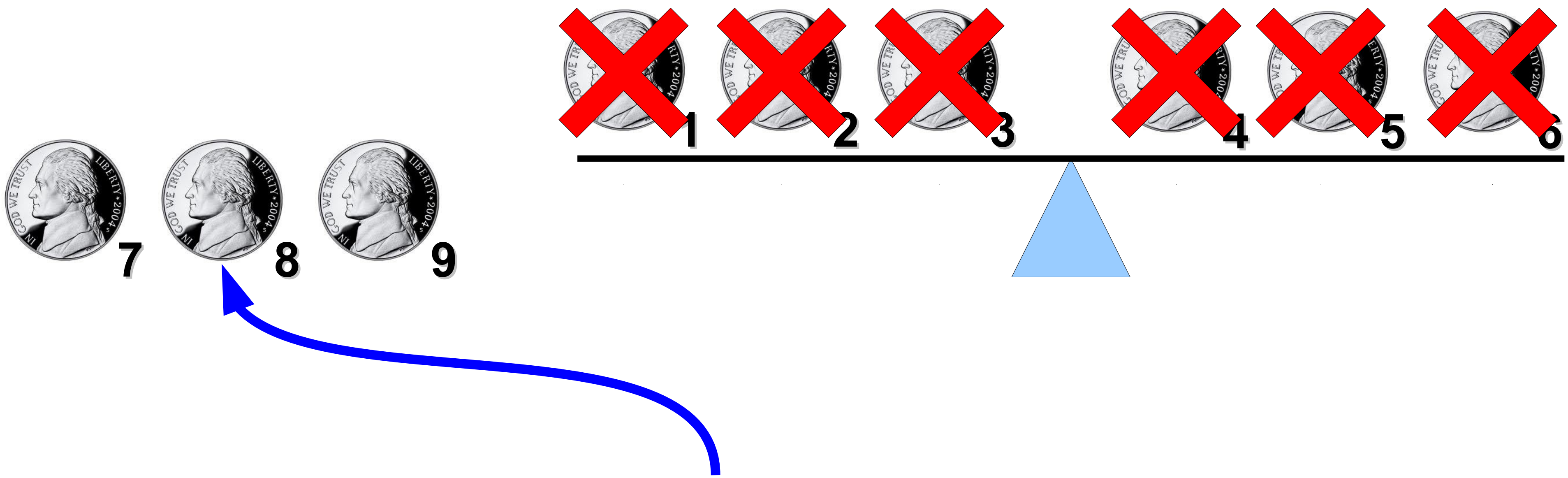
Now we have one weighing to find the counterfeit out of these three.

Finding the Counterfeit Coin

Finding the Counterfeit Coin



Finding the Counterfeit Coin



Now we have one weighing to find the counterfeit out of these three.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B.

Case 2: Group B is heavier than group A.

Case 3: Groups A and B have the same weight.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B. Then some coin in group A must be counterfeit.

Case 2: Group B is heavier than group A.

Case 3: Groups A and B have the same weight.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B. Then some coin in group A must be counterfeit.

Case 2: Group B is heavier than group A. Then some coin in group B must be counterfeit.

Case 3: Groups A and B have the same weight.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B. Then some coin in group A must be counterfeit.

Case 2: Group B is heavier than group A. Then some coin in group B must be counterfeit.

Case 3: Groups A and B have the same weight. Then some coin in group C must be counterfeit, because the counterfeit coin is not in group A or group B.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B. Then some coin in group A must be counterfeit.

Case 2: Group B is heavier than group A. Then some coin in group B must be counterfeit.

Case 3: Groups A and B have the same weight. Then some coin in group C must be counterfeit, because the counterfeit coin is not in group A or group B.

In each case, we can narrow down which of the nine coins is counterfeit to one of three.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B. Then some coin in group A must be counterfeit.

Case 2: Group B is heavier than group A. Then some coin in group B must be counterfeit.

Case 3: Groups A and B have the same weight. Then some coin in group C must be counterfeit, because the counterfeit coin is not in group A or group B.

In each case, we can narrow down which of the nine coins is counterfeit to one of three. Using our earlier result, we can find which of these three is counterfeit in just one weighing.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B. Then some coin in group A must be counterfeit.

Case 2: Group B is heavier than group A. Then some coin in group B must be counterfeit.

Case 3: Groups A and B have the same weight. Then some coin in group C must be counterfeit, because the counterfeit coin is not in group A or group B.

In each case, we can narrow down which of the nine coins is counterfeit to one of three. Using our earlier result, we can find which of these three is counterfeit in just one weighing.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

When proving a result, it's perfectly fine to refer to theorems you've proven earlier! Here, we cite our theorem from before and say it's possible to find which of three coins is the counterfeit.

In this course, feel free to refer to any theorem that we've proven in lecture, in the course notes, in the book, in section, or in previous problem sets when writing your proofs.

In each case, we can narrow down which of the nine coins is counterfeit to one of three. Using our earlier result, we can find which of these three is counterfeit in just one weighing.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B. Then some coin in group A must be counterfeit.

Case 2: Group B is heavier than group A. Then some coin in group B must be counterfeit.

Case 3: Groups A and B have the same weight. Then some coin in group C must be counterfeit, because the counterfeit coin is not in group A or group B.

In each case, we can narrow down which of the nine coins is counterfeit to one of three. Using our earlier result, we can find which of these three is counterfeit in just one weighing.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B. Then some coin in group A must be counterfeit.

Case 2: Group B is heavier than group A. Then some coin in group B must be counterfeit.

Case 3: Groups A and B have the same weight. Then some coin in group C must be counterfeit, because the counterfeit coin is not in group A or group B.

In each case, we can narrow down which of the nine coins is counterfeit to one of three. Using our earlier result, we can find which of these three is counterfeit in just one weighing. Consequently, it's possible to find which of the nine coins is counterfeit in just two weighings.

Theorem: Given nine coins, one of which weighs more than the rest, and a balance, there is a way to find which coin is counterfeit in two weighings.

Proof: Split the coins into three groups of three coins each (call them A, B, and C). Put groups A and B on opposite sides of the balance. There are three possible outcomes:

Case 1: Group A is heavier than group B. Then some coin in group A must be counterfeit.

Case 2: Group B is heavier than group A. Then some coin in group B must be counterfeit.

Case 3: Groups A and B have the same weight. Then some coin in group C must be counterfeit, because the counterfeit coin is not in group A or group B.

In each case, we can narrow down which of the nine coins is counterfeit to one of three. Using our earlier result, we can find which of these three is counterfeit in just one weighing. Consequently, it's possible to find which of the nine coins is counterfeit in just two weighings. ■

Relations Between Proofs

- Proofs often build off of one another: large results are almost often accomplished by building off of previous work.
  - Like writing a large program – split the work into smaller methods, across different classes, etc. instead of putting the whole thing into `main`.
- A result that is proven specifically as a stepping stone toward a larger result is called a **lemma**.
- We can treat the proof of the three-coin case as a lemma in the larger proof about nine coins.
  - The result in itself isn't particularly impressive, but it helps us prove a more advanced result.

Our Very Second Lemma

- Set equality is defined as follows

$A = B$ precisely when
for every $x \in A$, $x \in B$ and vice-versa.

- This definition makes it a bit tricky to prove that two sets are equal.
- Instead, we will prove the following result:

For any sets A and B,
if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Lemma: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Lemma: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof:

Lemma: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets such that $A \subseteq B$ and $B \subseteq A$.

Lemma: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets such that $A \subseteq B$ and $B \subseteq A$.

Lemma: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets such that $A \subseteq B$ and $B \subseteq A$.

Lemma: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets such that $A \subseteq B$ and $B \subseteq A$.

By definition, $A \subseteq B$ means that for all $x \in A$, $x \in B$.

Lemma: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets such that $A \subseteq B$ and $B \subseteq A$.

By definition, $A \subseteq B$ means that for all $x \in A$, $x \in B$.

By definition, $B \subseteq A$ means that for all $x \in B$, $x \in A$.

Lemma: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets such that $A \subseteq B$ and $B \subseteq A$.

By definition, $A \subseteq B$ means that for all $x \in A$, $x \in B$.

By definition, $B \subseteq A$ means that for all $x \in B$, $x \in A$.

Thus whenever $x \in A$, $x \in B$ and whenever $x \in B$, $x \in A$ as well.

Lemma: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets such that $A \subseteq B$ and $B \subseteq A$.

By definition, $A \subseteq B$ means that for all $x \in A$, $x \in B$.

By definition, $B \subseteq A$ means that for all $x \in B$, $x \in A$.

Thus whenever $x \in A$, $x \in B$ and whenever $x \in B$, $x \in A$ as well.

Consequently, A = B.

Lemma: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets such that $A \subseteq B$ and $B \subseteq A$.

By definition, $A \subseteq B$ means that for all $x \in A$, $x \in B$.

By definition, $B \subseteq A$ means that for all $x \in B$, $x \in A$.

Thus whenever $x \in A$, $x \in B$ and whenever $x \in B$, $x \in A$ as well.

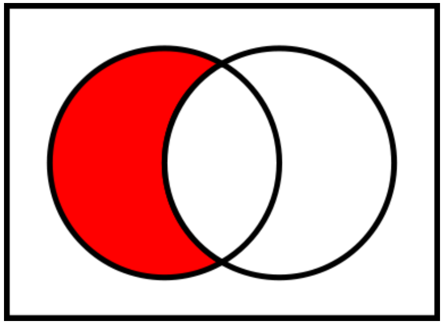
Consequently, A = B. ■

Using Our Lemma

- We can use this lemma to prove properties of how sets relate to one another.
- For example, let's prove that $(A - B) \cup B = A \cup B$.

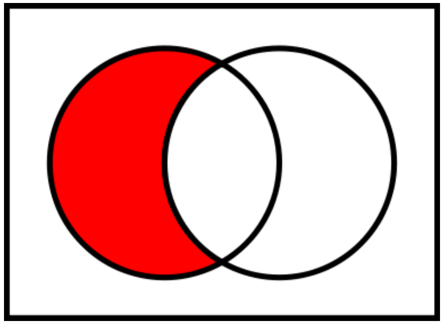
Using Our Lemma

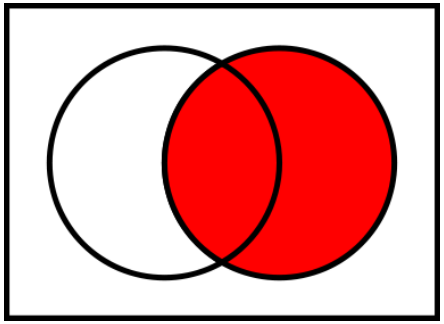
- We can use this lemma to prove properties of how sets relate to one another.
- For example, let's prove that $(A - B) \cup B = A \cup B$.



Using Our Lemma

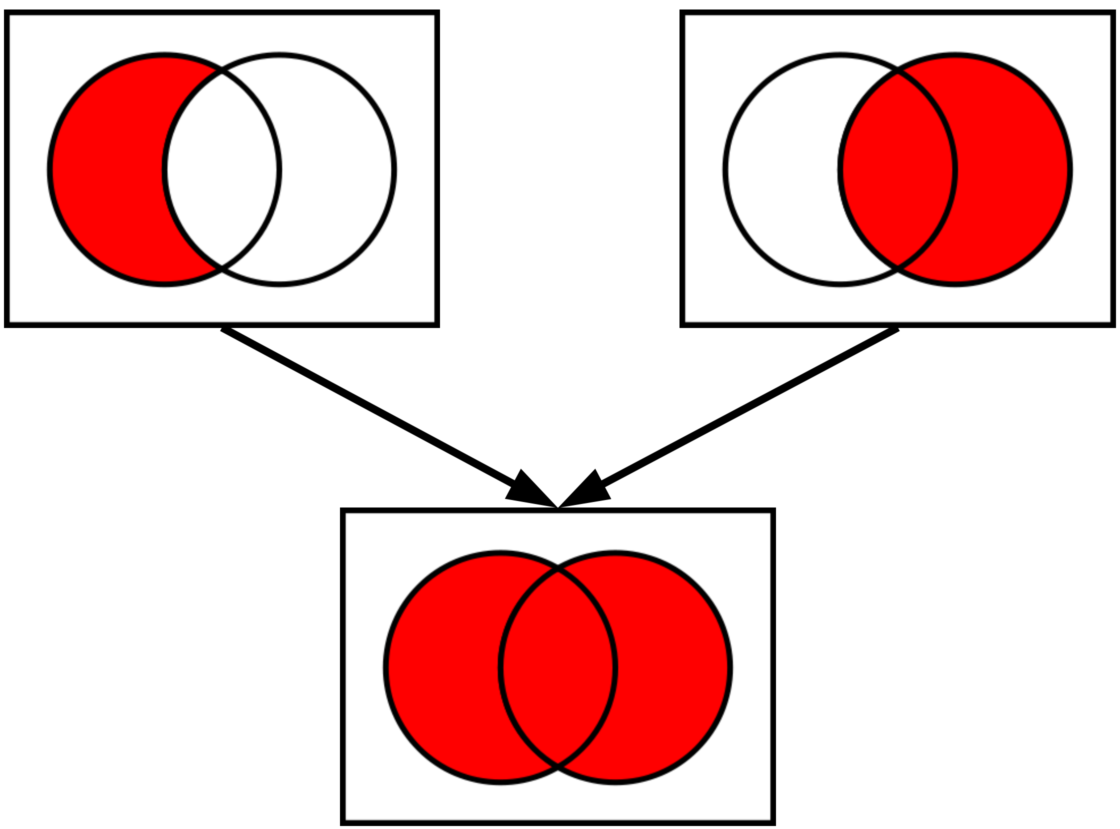
- We can use this lemma to prove properties of how sets relate to one another.
- For example, let's prove that $(A - B) \cup B = A \cup B$.





Using Our Lemma

- We can use this lemma to prove properties of how sets relate to one another.
- For example, let's prove that $(A - B) \cup B = A \cup B$.



Using Our Lemma

- We can use this lemma to prove properties of how sets relate to one another.
- For example, let's prove that $(A - B) \cup B = A \cup B$.
- Proof idea: Show that each set is a subset of the other.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.
Proof: Let A and B be arbitrary sets.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Proof: Let A and B be arbitrary sets.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Proof: Let A and B be arbitrary sets.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.
Proof: Let A and B be arbitrary sets. Consider any $x \in (A - B) \cup B$.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in (A - B) \cup B$.

By definition, $(A - B) \cup B$ is the set of all x where $x \in A - B$ or $x \in B$, so we have that $x \in A - B$ or $x \in B$.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in (A - B) \cup B$.

By definition, $(A - B) \cup B$ is the set of all x where $x \in A - B$ or $x \in B$, so we have that $x \in A - B$ or $x \in B$. We consider these two cases separately:

Case 1: $x \in A - B$.

Case 2: $x \in B$.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in (A - B) \cup B$.

By definition, $(A - B) \cup B$ is the set of all x where $x \in A - B$ or $x \in B$, so we have that $x \in A - B$ or $x \in B$. We consider these two cases separately:

Case 1: $x \in A - B$. By definition, $A - B$ is the set of all x where $x \in A$ and $x \notin B$.

Case 2: $x \in B$.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in (A - B) \cup B$.

By definition, $(A - B) \cup B$ is the set of all x where $x \in A - B$ or $x \in B$, so we have that $x \in A - B$ or $x \in B$. We consider these two cases separately:

Case 1: $x \in A - B$. By definition, $A - B$ is the set of all x where $x \in A$ and $x \notin B$. This means that $x \in A$, and so $x \in A \cup B$ as well.

Case 2: $x \in B$.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in (A - B) \cup B$.

By definition, $(A - B) \cup B$ is the set of all x where $x \in A - B$ or $x \in B$, so we have that $x \in A - B$ or $x \in B$. We consider these two cases separately:

Case 1: $x \in A - B$. By definition, $A - B$ is the set of all x where $x \in A$ and $x \notin B$. This means that $x \in A$, and so $x \in A \cup B$ as well.

Case 2: $x \in B$. Then $x \in A \cup B$ as well.

Lemma 1: For any sets A and B, $(A - B) \cup B \subseteq A \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in (A - B) \cup B$.

By definition, $(A - B) \cup B$ is the set of all x where $x \in A - B$ or $x \in B$, so we have that $x \in A - B$ or $x \in B$. We consider these two cases separately:

Case 1: $x \in A - B$. By definition, $A - B$ is the set of all x where $x \in A$ and $x \notin B$. This means that $x \in A$, and so $x \in A \cup B$ as well.

Case 2: $x \in B$. Then $x \in A \cup B$ as well.

In either case, any $x \in (A - B) \cup B$ also satisfies $x \in A \cup B$, so $(A - B) \cup B \subseteq A \cup B$ as required. ■

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$.

Case 2: $x \in A$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$. Given that $x \in A$, we know that either $x \in B$ or $x \notin B$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$. Given that $x \in A$, we know that either $x \in B$ or $x \notin B$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$. Given that $x \in A$, we know that either $x \in B$ or $x \notin B$.

We're already doing a proof by cases, but inside this particular case there's two more cases to consider. There's nothing wrong with that; just like nested loops in a program, we can have nested cases.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$. Given that $x \in A$, we know that either $x \in B$ or $x \notin B$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$. Given that $x \in A$, we know that either $x \in B$ or $x \notin B$. If $x \in B$, then $x \in (A - B) \cup B$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$. Given that $x \in A$, we know that either $x \in B$ or $x \notin B$. If $x \in B$, then $x \in (A - B) \cup B$. Otherwise, $x \notin B$, but $x \in A$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$. Given that $x \in A$, we know that either $x \in B$ or $x \notin B$. If $x \in B$, then $x \in (A - B) \cup B$. Otherwise, $x \notin B$, but $x \in A$. Thus $x \in A - B$, and therefore $x \in (A - B) \cup B$.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$. Given that $x \in A$, we know that either $x \in B$ or $x \notin B$. If $x \in B$, then $x \in (A - B) \cup B$. Otherwise, $x \notin B$, but $x \in A$. Thus $x \in A - B$, and therefore $x \in (A - B) \cup B$.

In either case, any $x \in (A - B) \cup B$ also satisfies $x \in A \cup B$, so $(A - B) \cup B \subseteq A \cup B$ as required.

Lemma 2: For any sets A and B, $A \cup B \subseteq (A - B) \cup B$.

Proof: Let A and B be arbitrary sets. Consider any $x \in A \cup B$. By definition, $A \cup B$ is the set of all x where $x \in A$ or $x \in B$. We consider two cases:

Case 1: $x \in B$. Then $x \in (A - B) \cup B$ as well.

Case 2: $x \in A$. Given that $x \in A$, we know that either $x \in B$ or $x \notin B$. If $x \in B$, then $x \in (A - B) \cup B$. Otherwise, $x \notin B$, but $x \in A$. Thus $x \in A - B$, and therefore $x \in (A - B) \cup B$.

In either case, any $x \in (A - B) \cup B$ also satisfies $x \in A \cup B$, so $(A - B) \cup B \subseteq A \cup B$ as required. ■

Theorem: For any sets A and B, $(A - B) \cup B = A \cup B$.

Proof: Let A and B be arbitrary sets.

By Lemma 1, $(A - B) \cup B \subseteq A \cup B$.

By Lemma 2, $A \cup B \subseteq (A - B) \cup B$.

Consequently, by our earlier lemma,
$(A - B) \cup B = A \cup B$. ■

Next Time

- Indirect Proofs
  - Proof by contradiction.
  - Proof by contrapositive.