Welcome to CS103!

- Lectures are recorded – sorry for being in such a packed room!
- Two Handouts
  - Also available online if you'd like!
- Today:
  - Course Overview
  - Introduction to Set Theory
  - The Limits of Computation

Goals for this Course

Goals for this Course

- How do we prove something with absolute certainty?
  - **Discrete Mathematics**
- What problems can we solve with computers?
  - **Computability Theory**
- Why are some problems harder to solve than others?
  - **Complexity Theory**

Course Staff

Keith Schwarz (htiek@cs.stanford.edu)

Kyle Brogle (broglek@stanford.edu)
Berkeley Churchill (berkc@stanford.edu)
Yifei Huang (yifei@stanford.edu)
Jamie Irvine (jirvine@stanford.edu)
Nicholas Isaacs (nisaacs@stanford.edu)
Jeffrey Jacobs (jjacobs3@stanford.edu)
Michael Kim (mpkim@stanford.edu)
Stephen Macke (smacke@stanford.edu)
Sathish Nagappan (srn@stanford.edu)
Neha Nayak (nayakne@stanford.edu)
Dilli Paudel (drpaudel@stanford.edu)
Narek Tovmasyan (ntarmen1@stanford.edu)

Course Staff Mailing List:
cs103-aut1314-staff@lists.stanford.edu

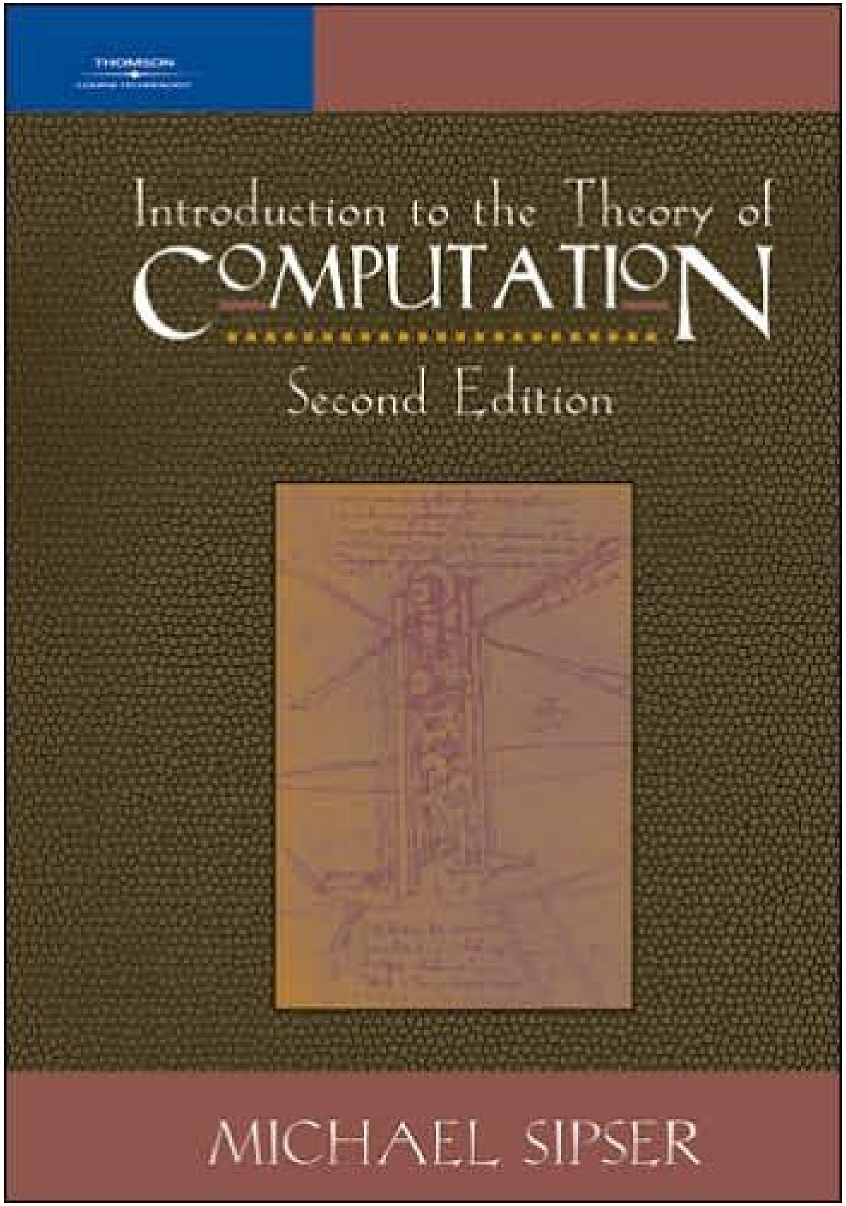
The Course Website

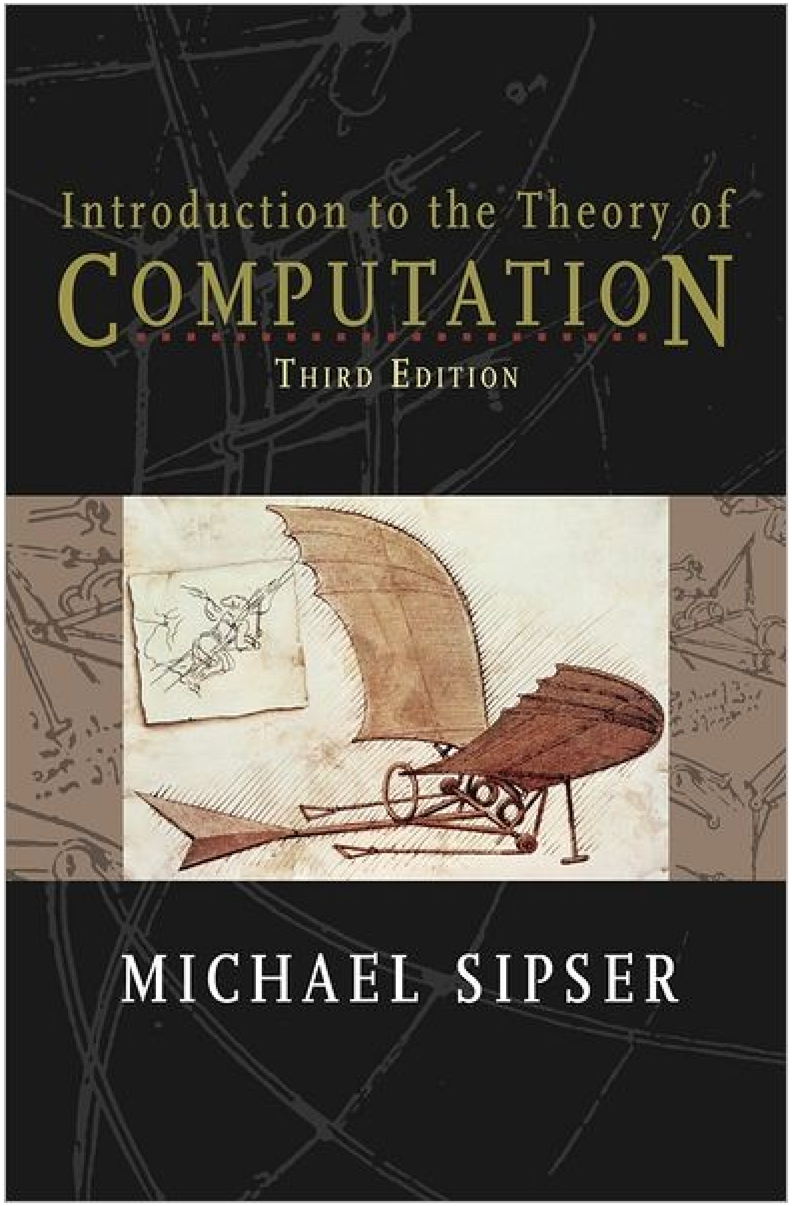
http://cs103.stanford.edu

“Prerequisite”

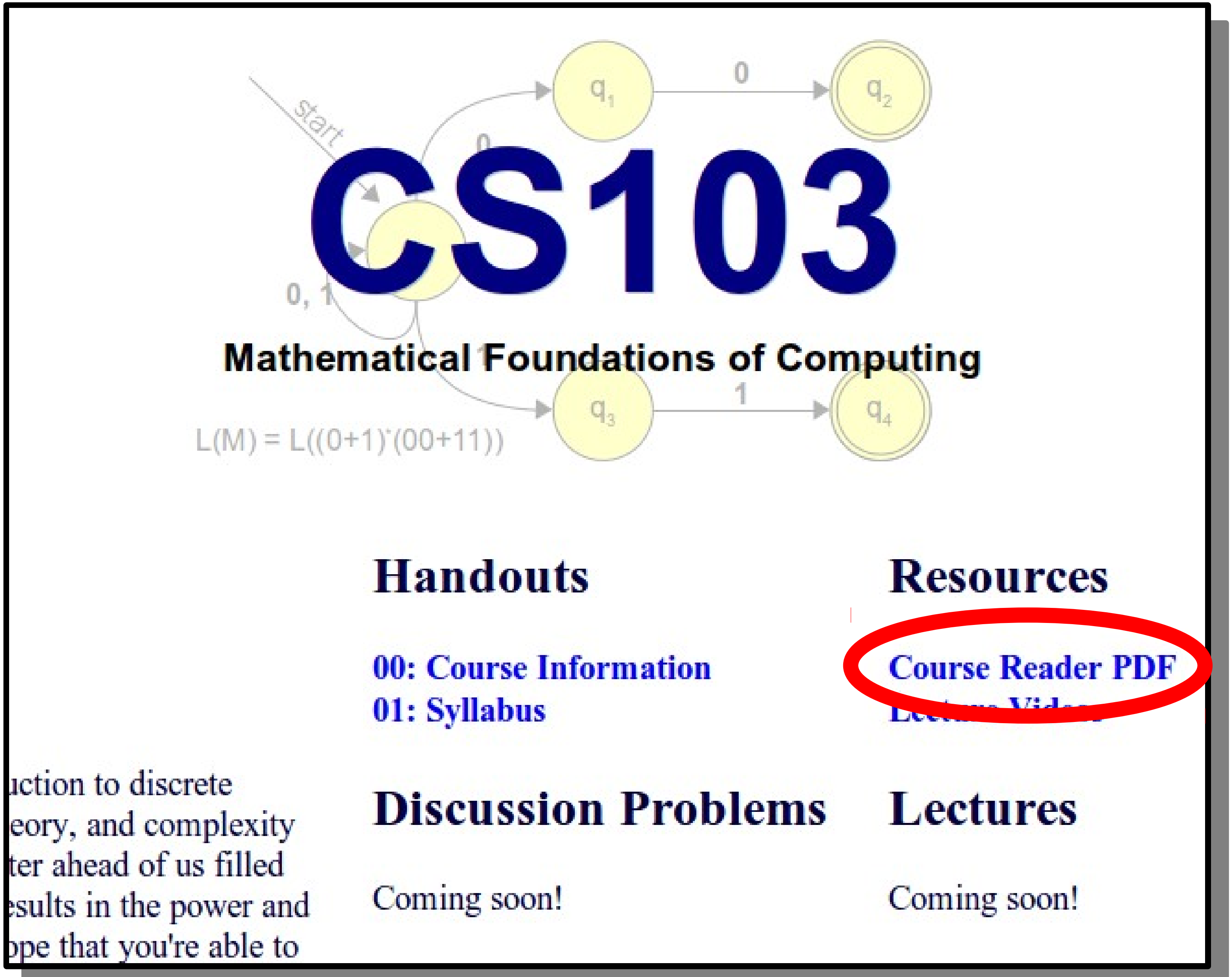
CS106A

Recommended Reading

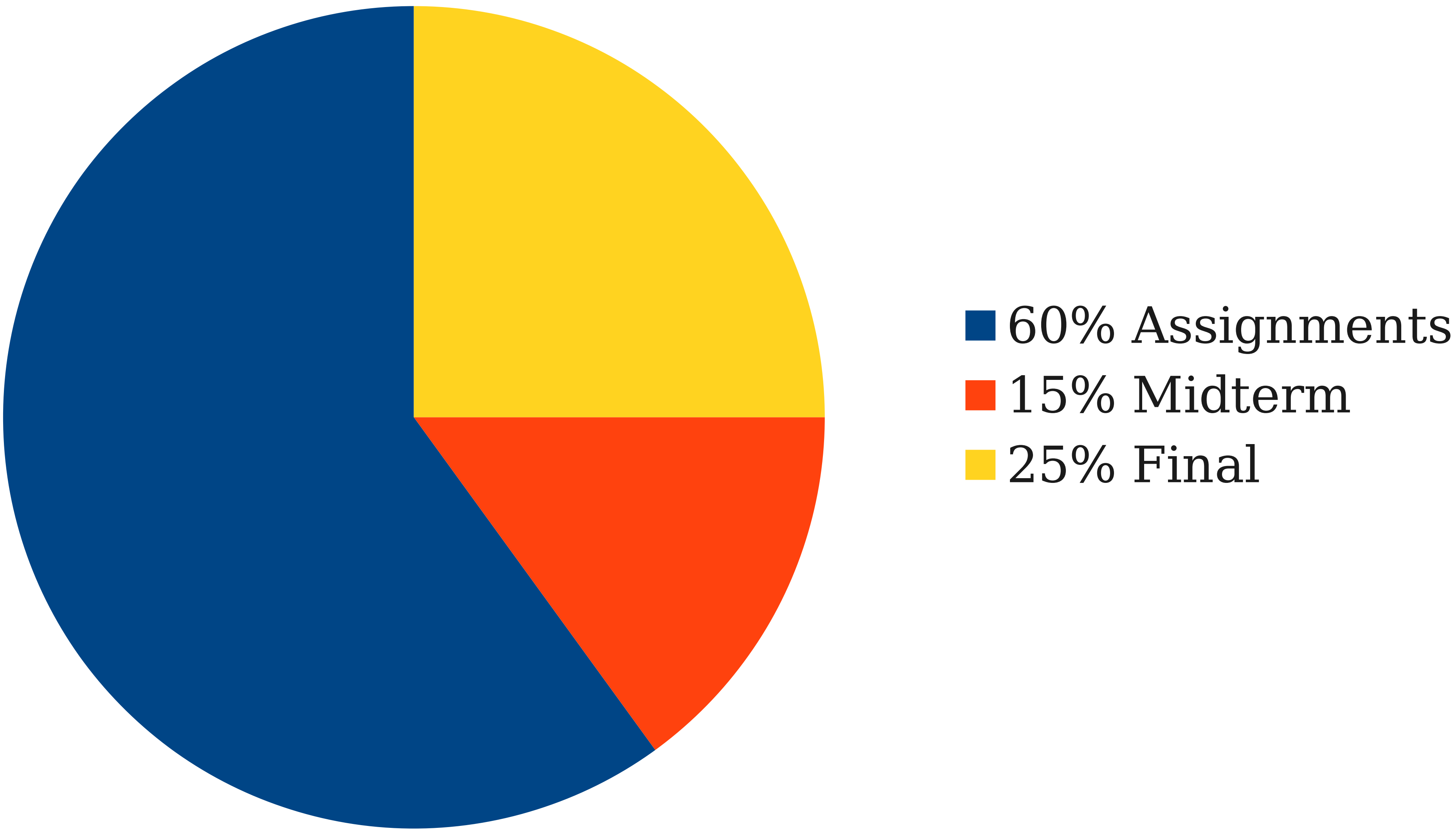




Online Course Notes



Grading Policies



Let's Get Started!

Introduction to Set Theory

“CS103 students”

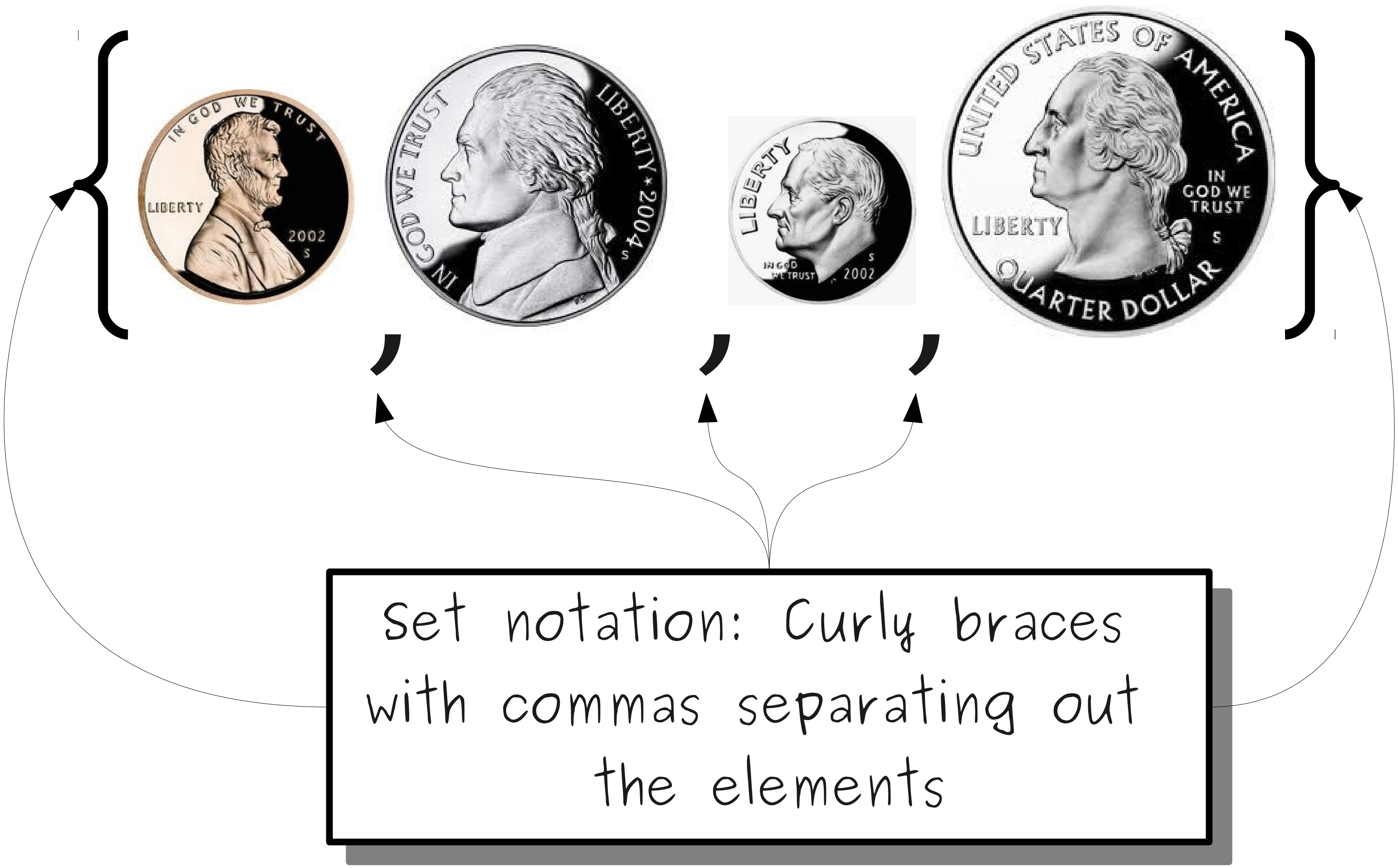
“All the computers on the Stanford network.”

“Cool people”

“The chemical elements”

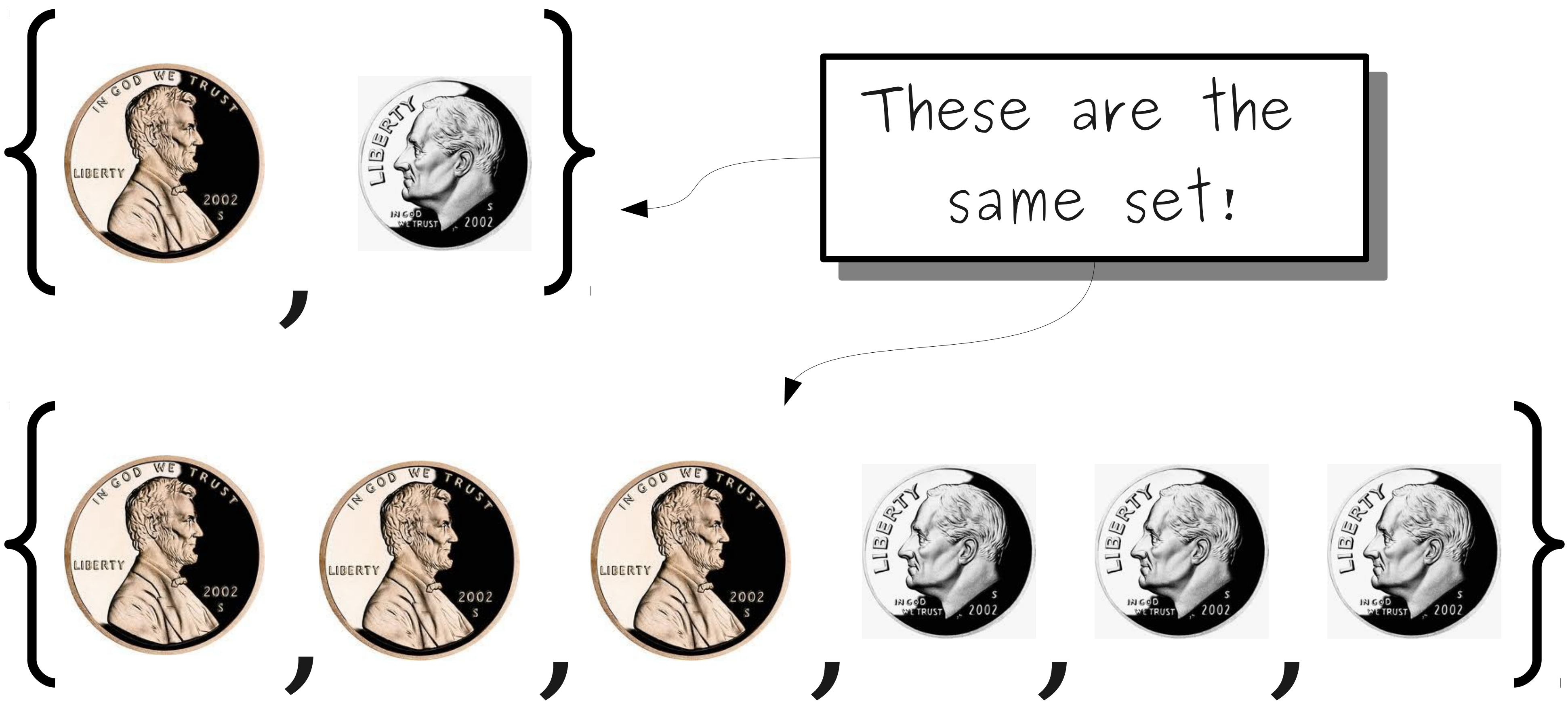
“Cute animals”

“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).

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

The empty set contains no elements.

We use this symbol to denote the empty set.

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

This set contains nothing at all.

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

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

Are these equal to one another?

This is a number.

This is a set. It contains a number.

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

Are these equal to one another?

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 an element of the set or it isn't.

Infinite Sets

- Some sets contain *infinitely many* elements!
- The **natural numbers**, ℕ: { 0, 1, 2, 3, …}
    - Some mathematicians 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.
    - $e \in \mathbb{R}$, $\pi \in \mathbb{R}$, $4 \in \mathbb{R}$, etc.

Describing Complex Sets

- Here are some English descriptions of infinite sets:

  “All even numbers.”

  “All real numbers less than 137.”

  “All negative integers.”

- We can't list the (infinitely many!) elements of these sets!
- How would we rigorously describe them?

Even Natural Numbers

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

The set of all n

where

n is a natural number

and n is even

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

Set Builder Notation

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

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

- For example:

$$\{ \ r \mid r \in \mathbb{R} \text{ and } r < 137 \ \}$$

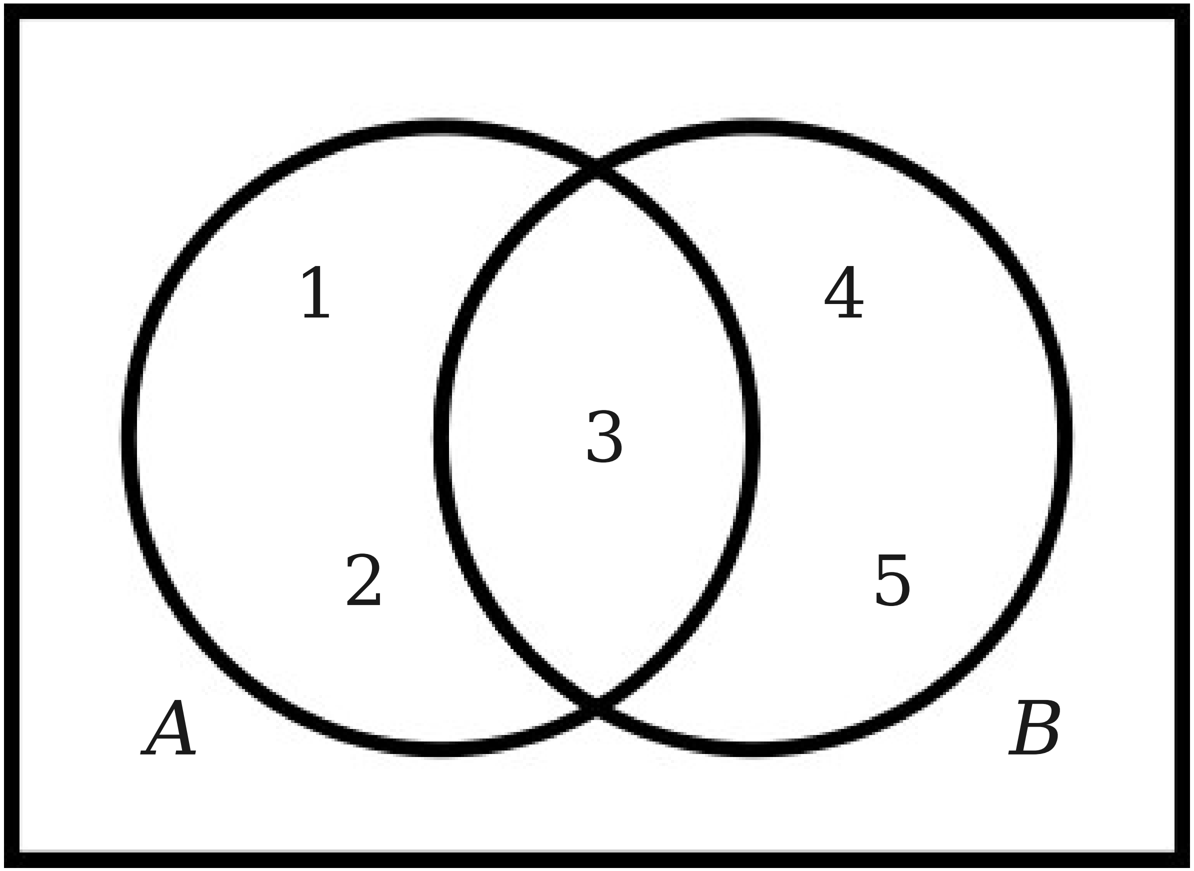
$$\{ \ n \mid n \text{ is a power of two } \}$$

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

$$\{ \ a \mid a \text{ is cute animal } \}$$

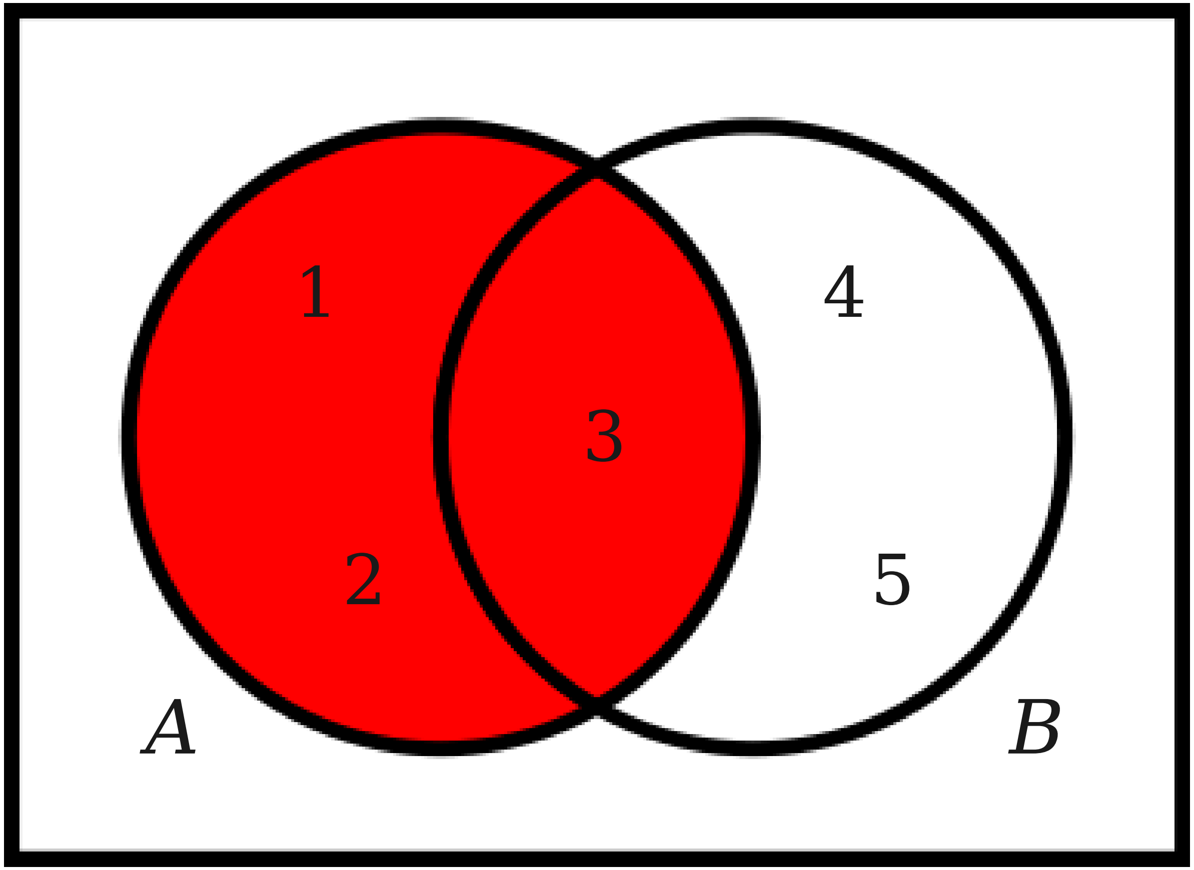
Combining Sets

Venn Diagrams



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

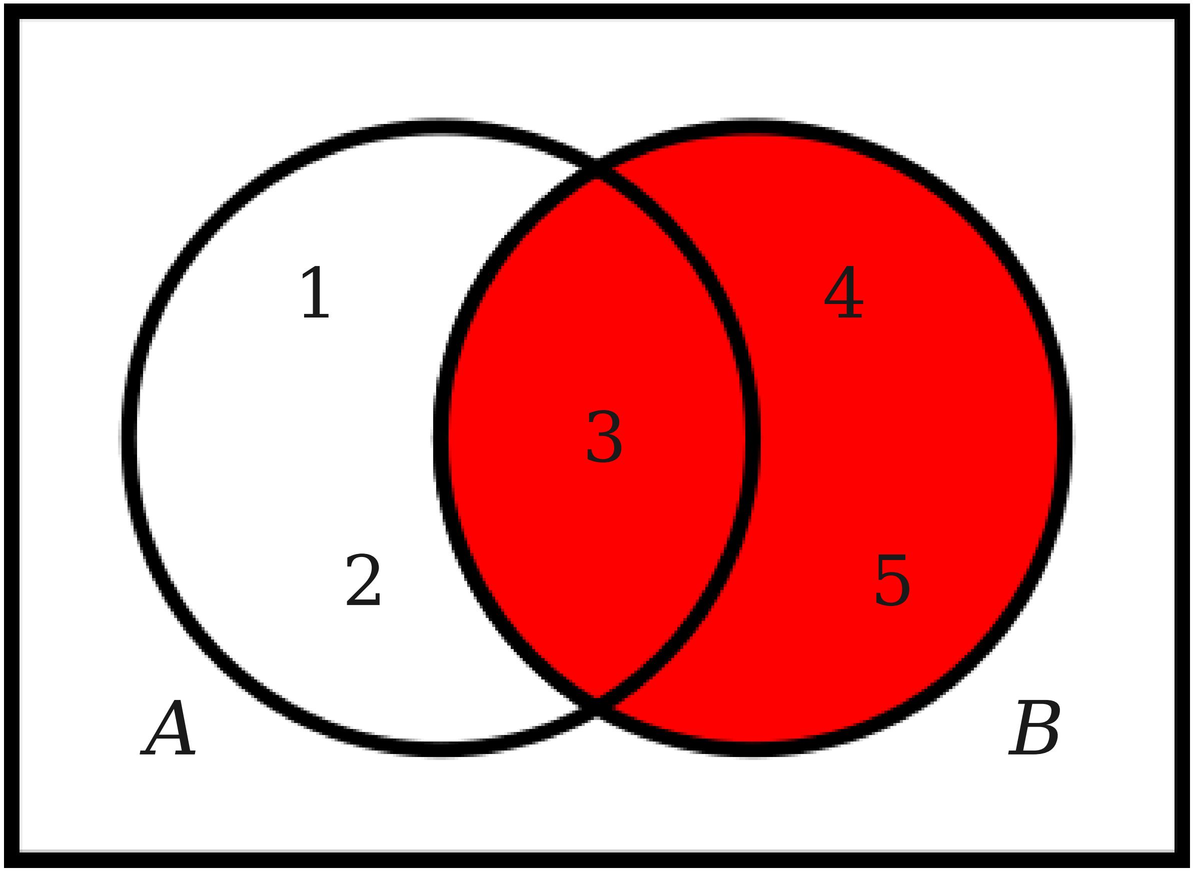
Venn Diagrams



A

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

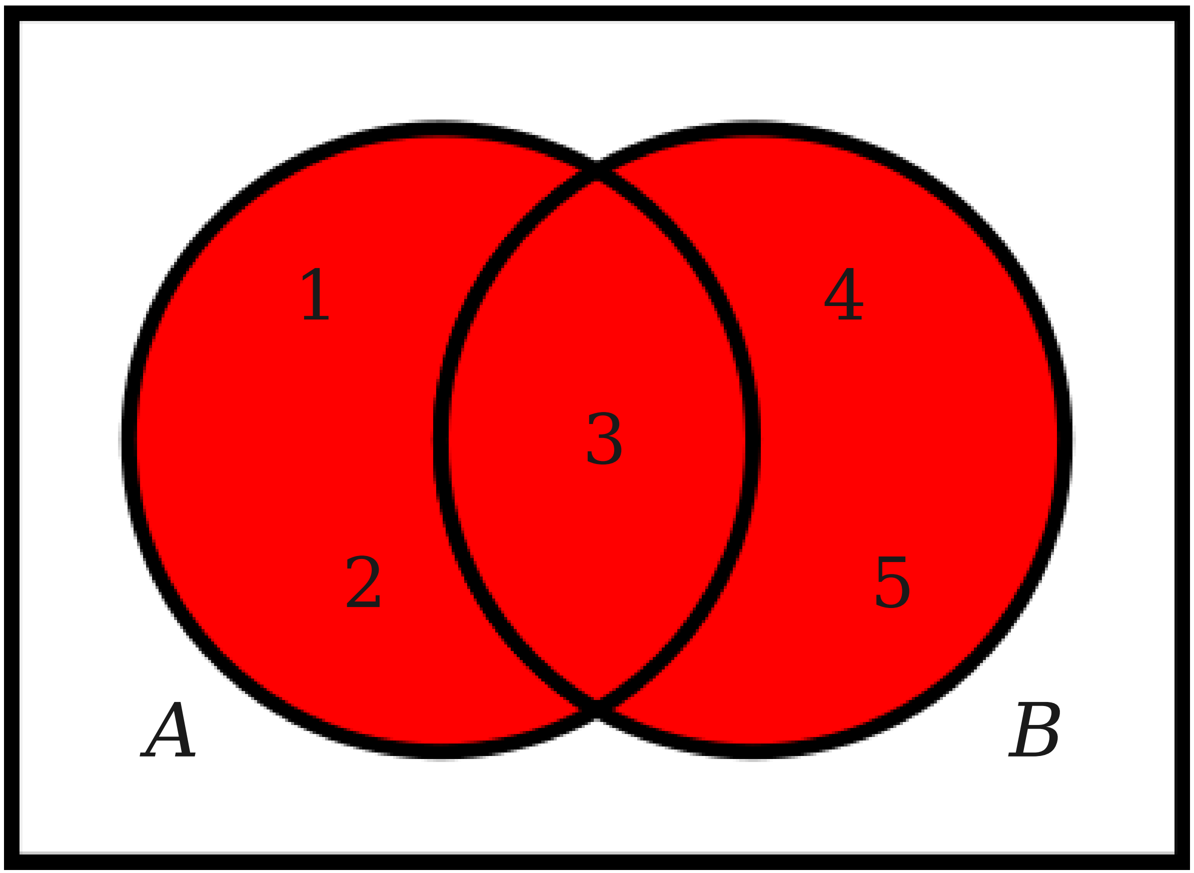
Venn Diagrams



B

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

Venn Diagrams



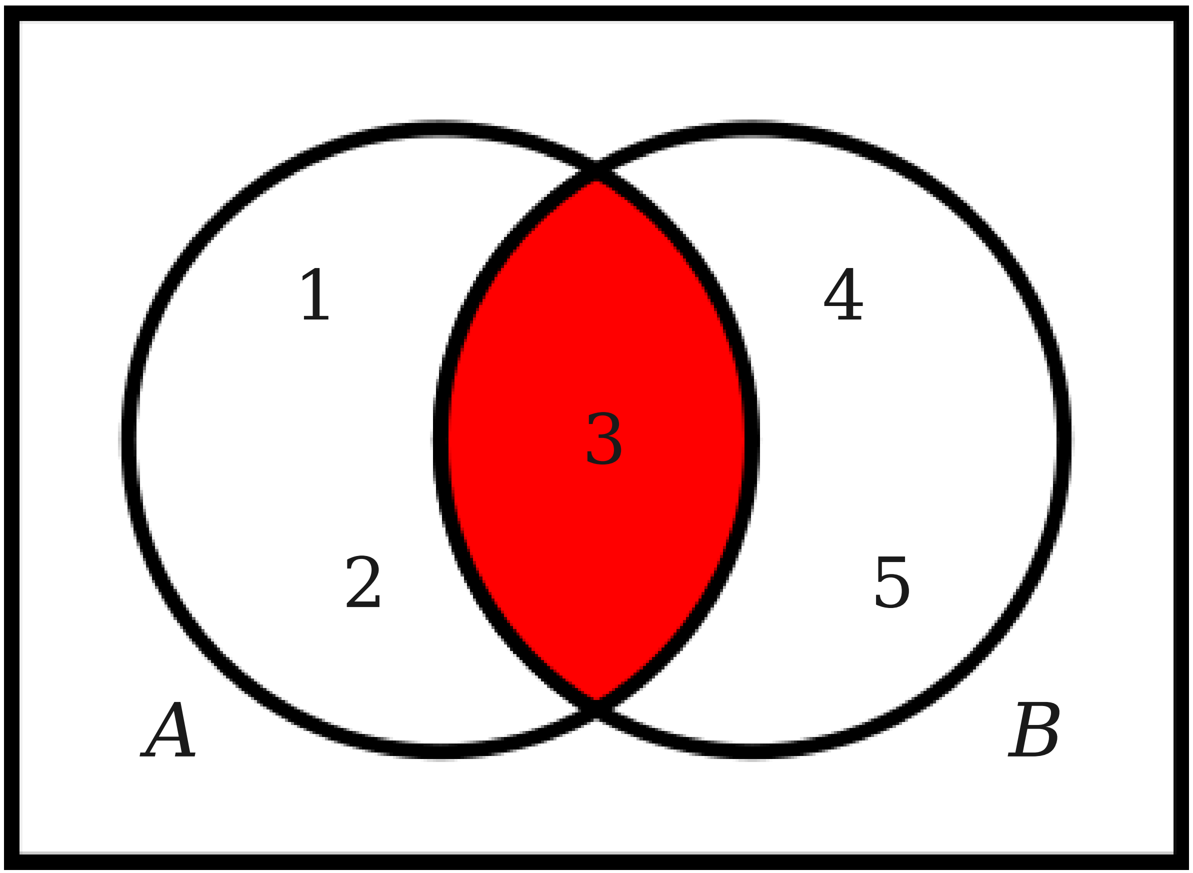
Union

$A \cup B$

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

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

Venn Diagrams



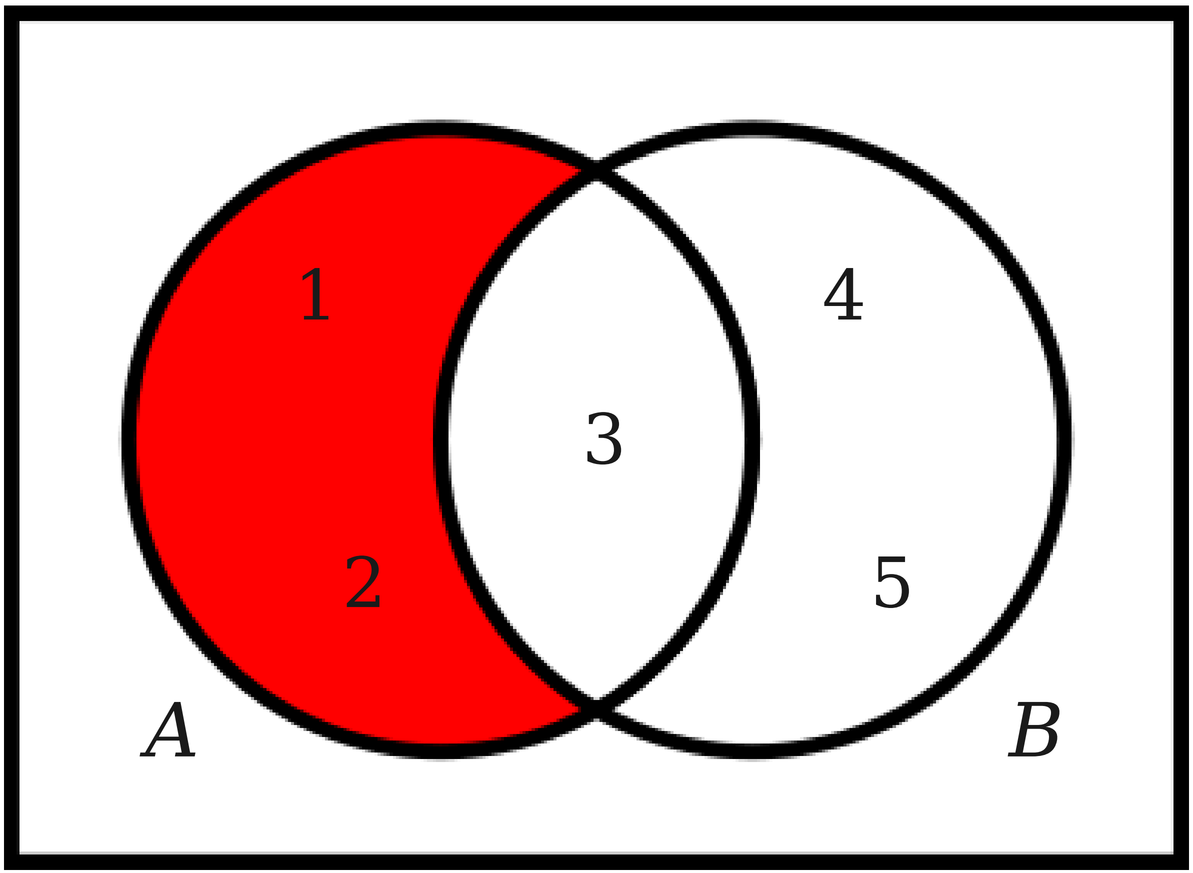
Intersection

$A \cap B$

$\{ 3 \}$

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

Venn Diagrams



Difference

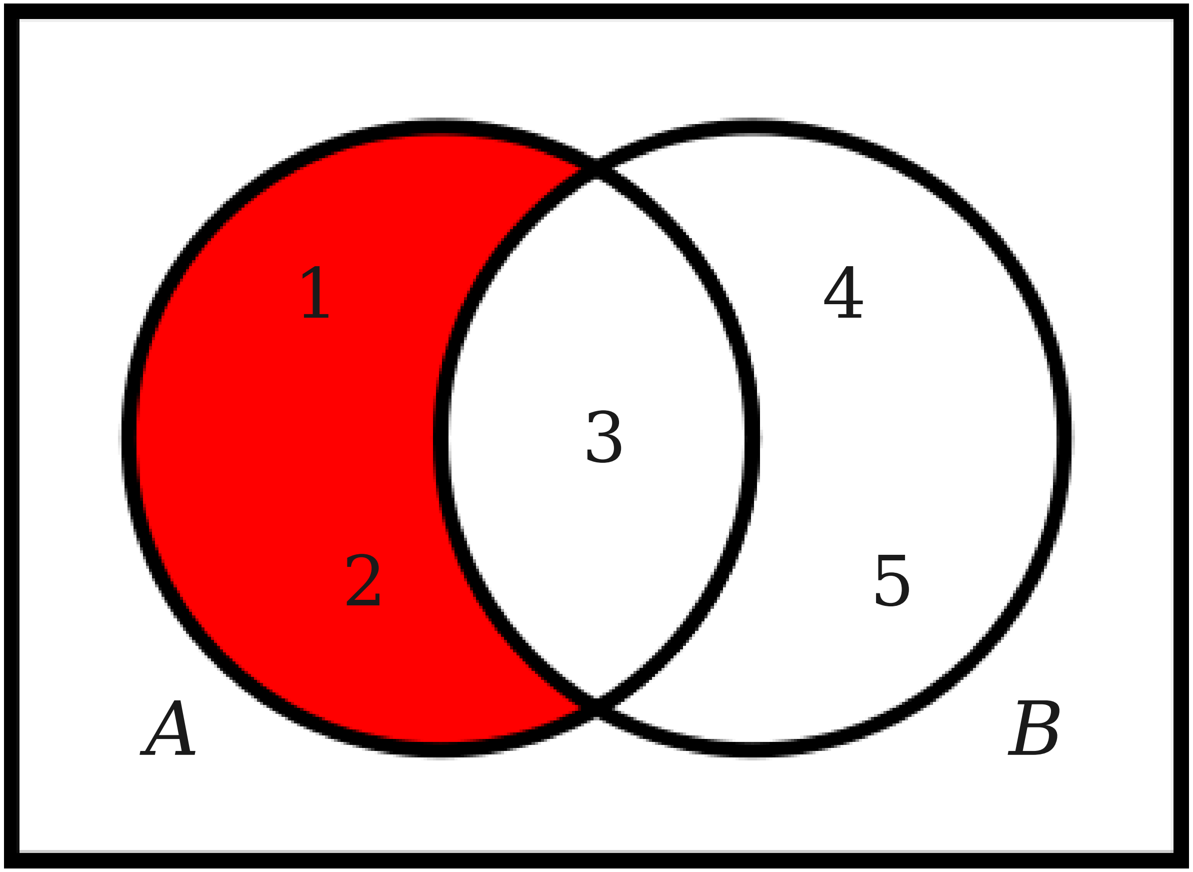
$A - B$

$\{ 1, 2 \}$

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

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

Venn Diagrams



Difference

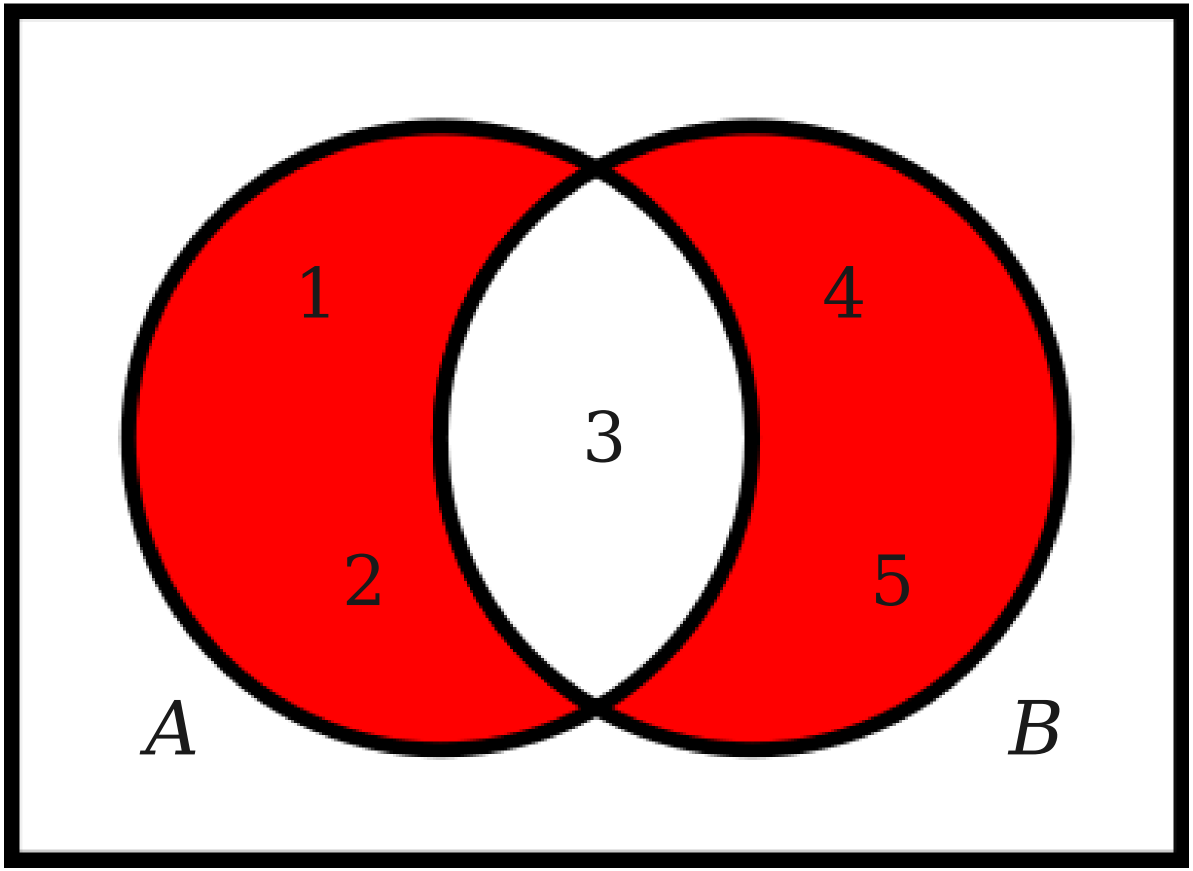
$A \setminus B$

$\{ 1, 2 \}$

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

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

Venn Diagrams



Symmetric Difference

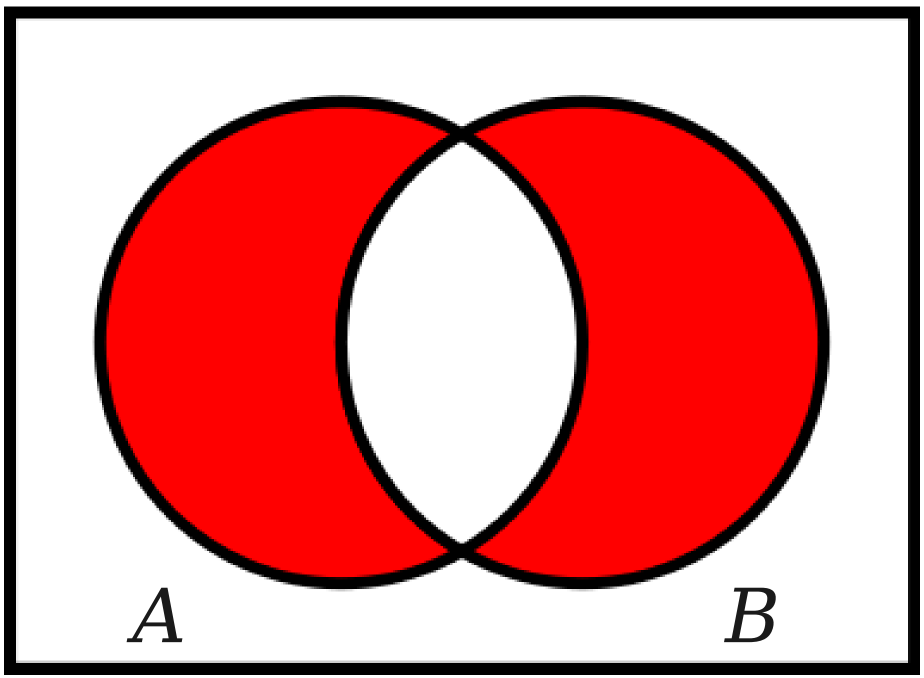
$A \, \Delta \, B$

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

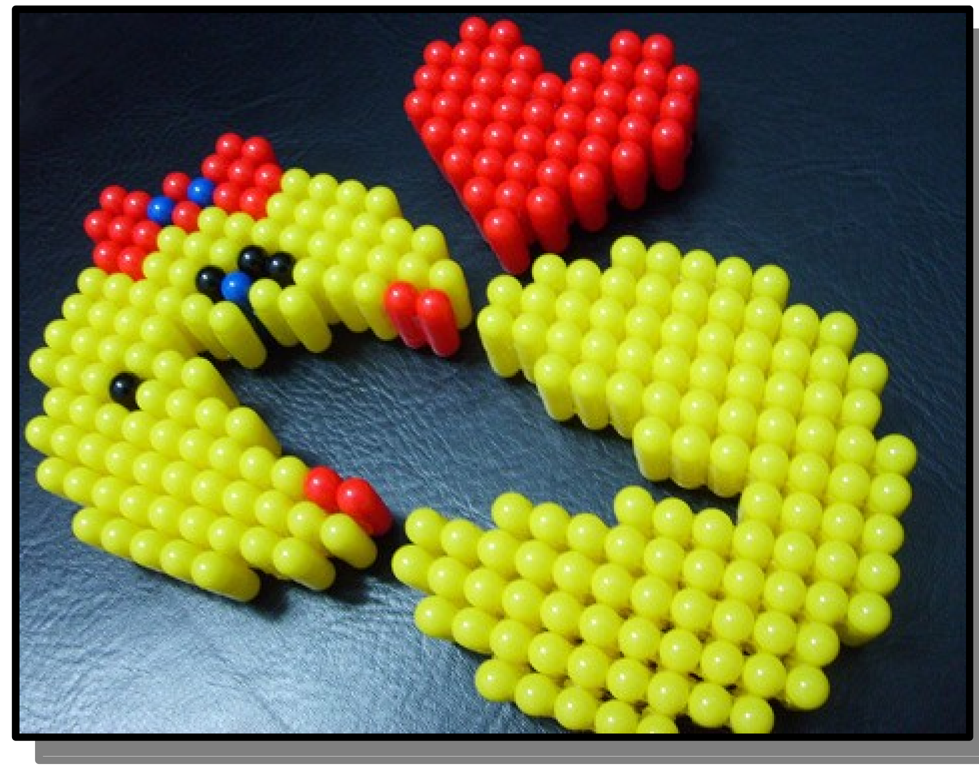
$A = \{ 1, 2, 3 \}$

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

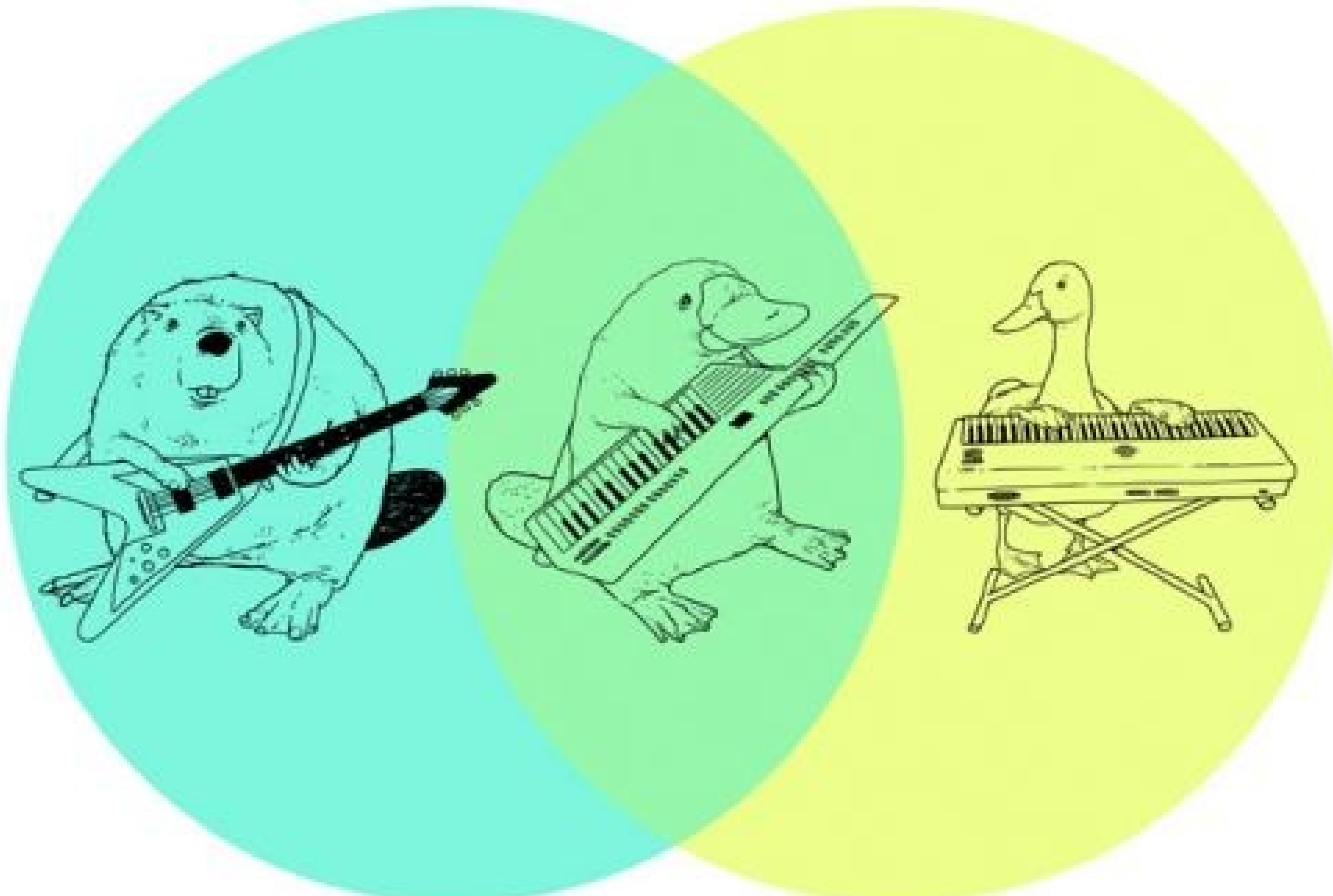
Venn Diagrams



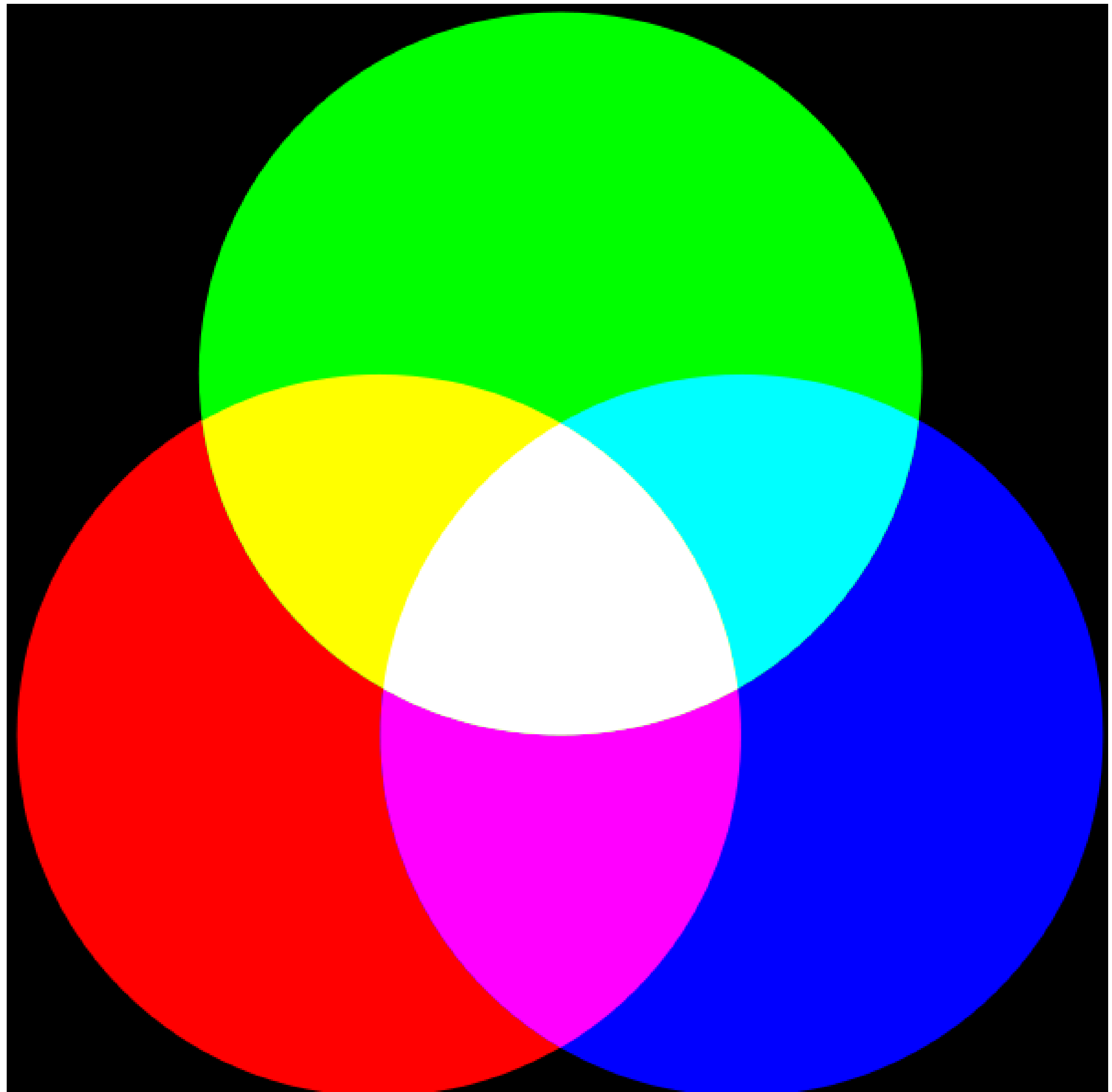
$A \,\Delta\, B$



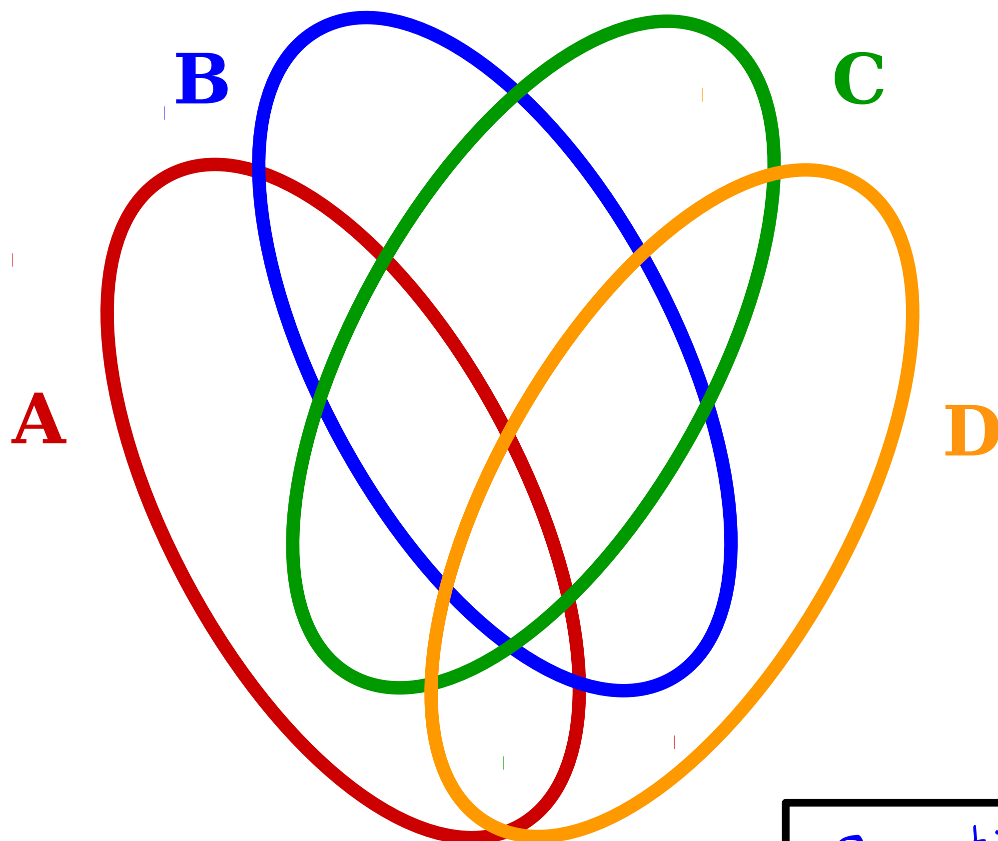
Venn Diagrams



Venn Diagrams for Three Sets

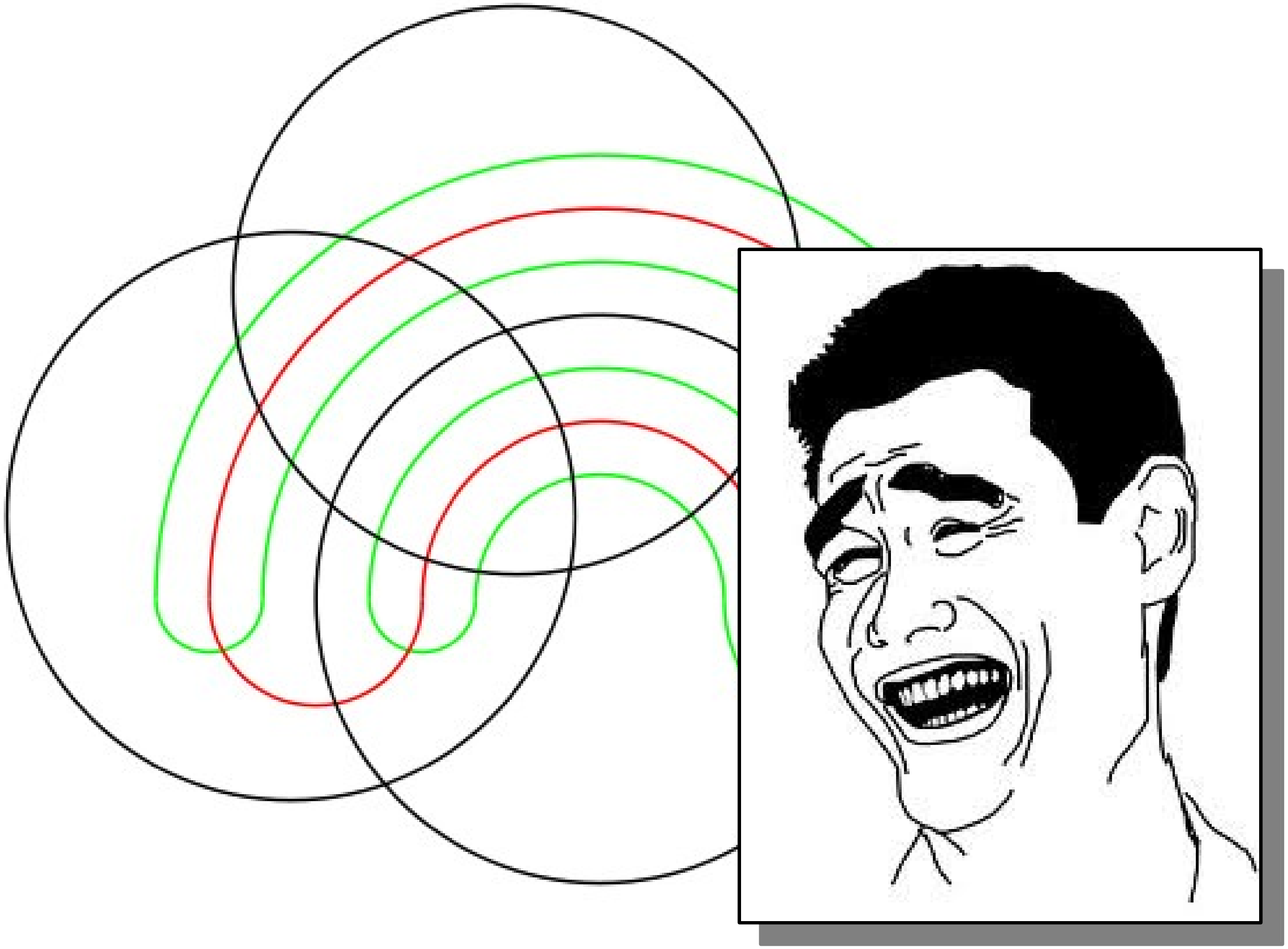


Venn Diagrams for Four Sets



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

Venn Diagrams for Five Sets



Venn Diagrams for Seven Sets

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

Subsets and Power Sets

Subsets

- A set S is a **subset** of a set T (denoted $\boldsymbol{S \subseteq T}$) if all elements of S are also elements of T.
- Examples:
  - $\{ 1, 2, 3 \} \subseteq \{ 1, 2, 3, 4 \}$
  - $\mathbb{N} \subseteq \mathbb{Z}$ (*every natural number is an integer*)
  - $\mathbb{Z} \subseteq \mathbb{R}$ (*every integer is a real number*)

What About the Empty Set?

- A set S is a **subset** of a set T (denoted $\boldsymbol{S \subseteq T}$) if all elements of S are also elements of T.
- Is $\emptyset \subseteq S$ for any set S?
- **Yes**: This statement true for all sets S.
- **Vacuous truth**: A statement that is true because it does not apply to anything.
  - "All unicorns are blue."
  - "All unicorns are pink."

Proper Subsets

- A set S is a **subset** of a set T (denoted $\boldsymbol{S \subseteq T}$) if all elements of S are also elements of T.
- By definition, any set is a subset of itself.
- A **proper subset** of a set S is a set T such that $T \subseteq S$ and $T \neq S$.
- There are multiple notations for this: we either write $T \subsetneq S$ or $T \subset S$.

$S = \{$  ,  $\}$

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

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

What is $\wp(\emptyset)$?

Answer: $\{\emptyset\}$

Cardinalities

Cardinality

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

The Cardinality of $\mathbb{N}$

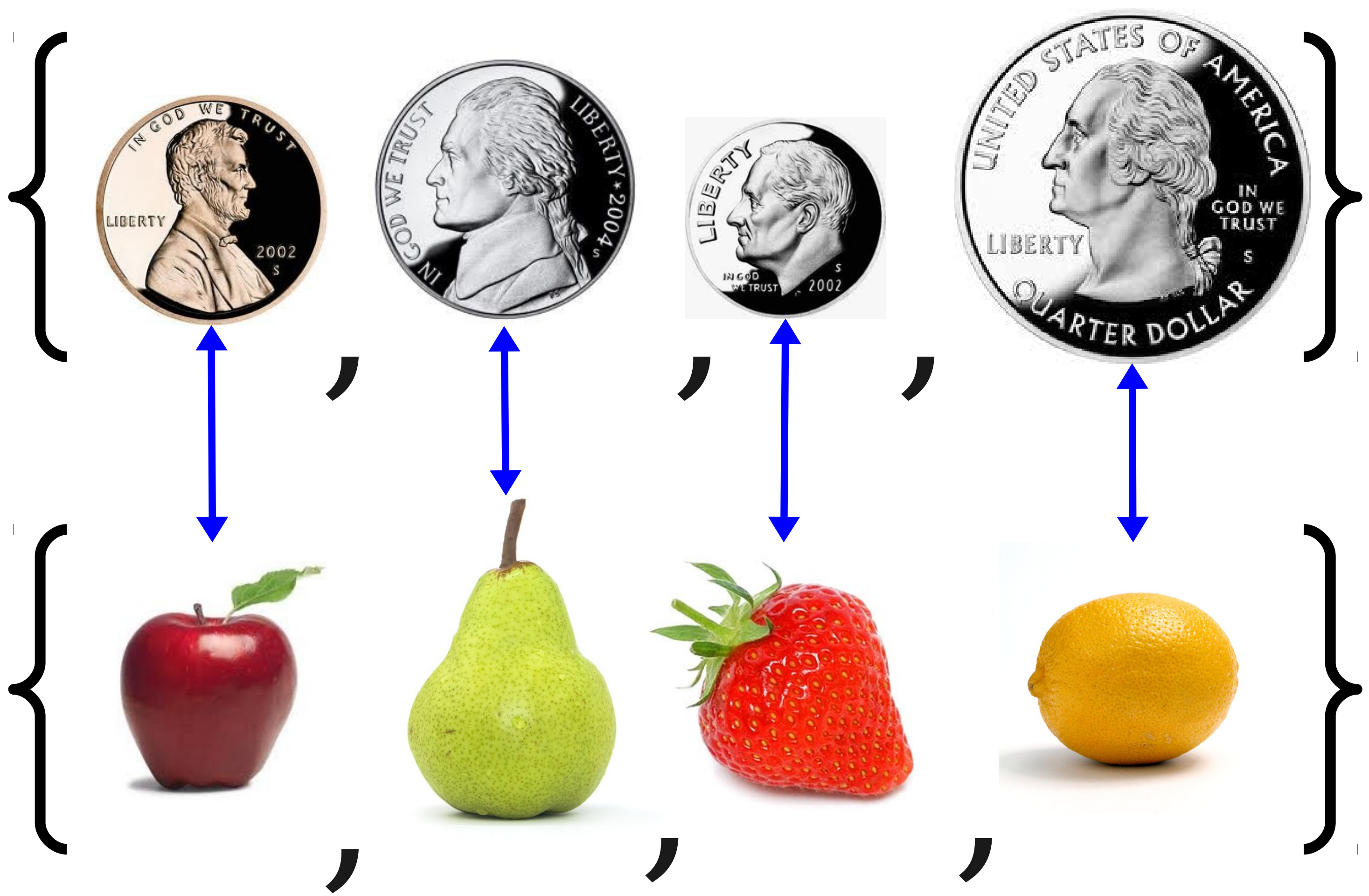
- What is $|\mathbb{N}|$?
  - There are infinitely many natural numbers.
  - $|\mathbb{N}|$ can't be a natural number, since it's infinitely large.
- We need to introduce a new term.
- Definition: $|\mathbb{N}| = \aleph_0$.
  - Pronounced “Aleph-Zero,” “Aleph-Nought,” or “Aleph-Null.”

Consider the set

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

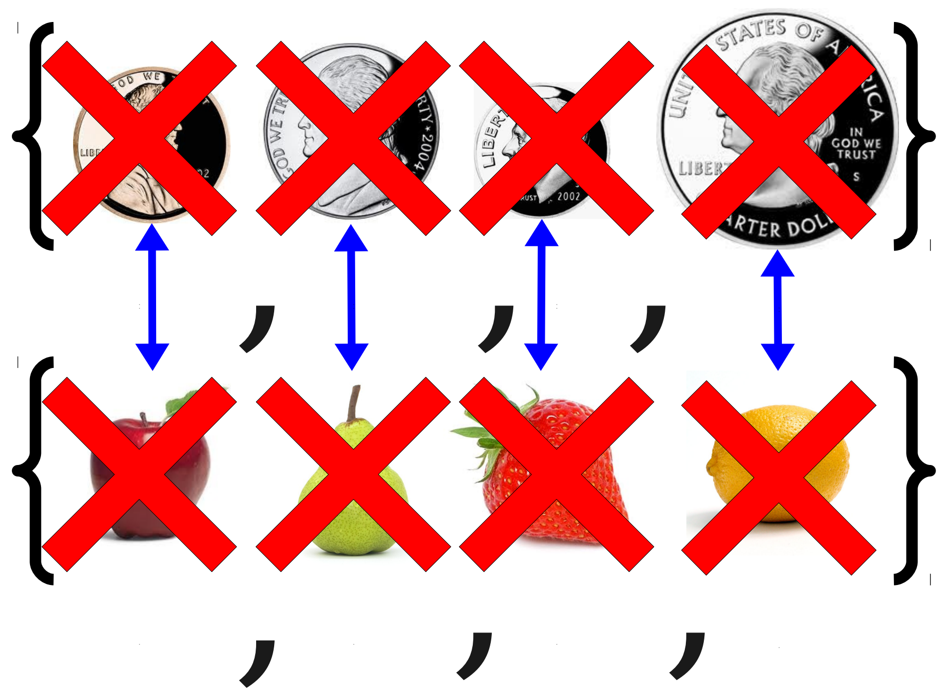
What is $|S|$?

How Big Are These Sets?



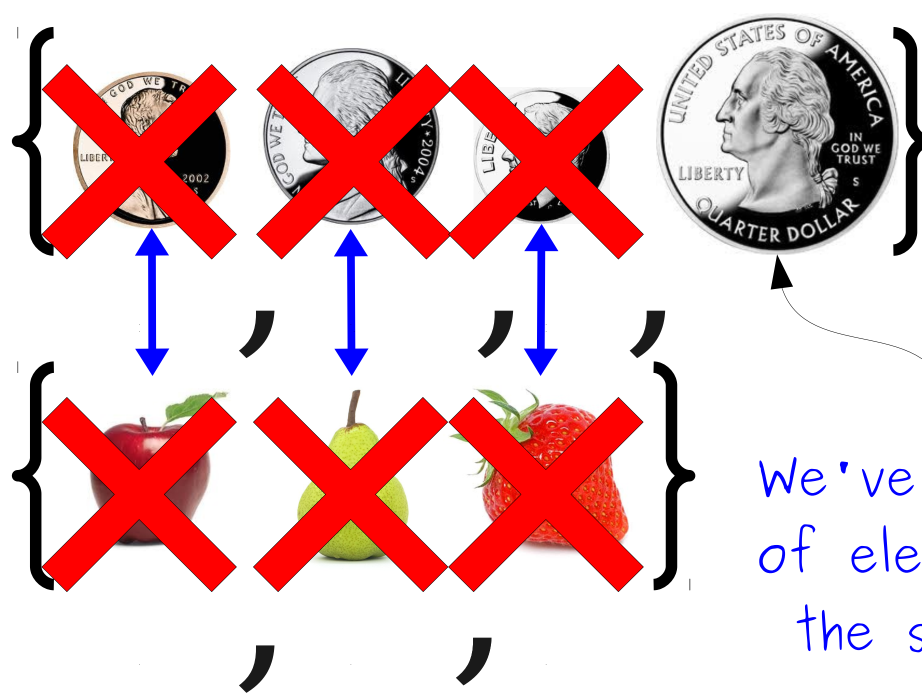
Comparing Cardinalities

- 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

$$\begin{array}{cccccccccccc}
\mathbb{N} & & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \dots \\
 & & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\
S & & 0 & 2 & 4 & 6 & 8 & 10 & 12 & 14 & 16 & \dots
\end{array}$$

$$n \leftrightarrow 2n$$

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

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

Infinite Cardinalities

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

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

$n \leftrightarrow n / 2$ (if n is even)

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

Infinite Cardinalities

$$\begin{array}{ccccccccccc} \mathbb{N} & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & \ldots \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ P & 1 & 2 & 4 & 8 & 16 & 32 & 64 & 128 & \ldots \end{array}$$

$$n \leftrightarrow 2^n$$

$$P = \{ n \mid n \in \mathbb{N} \text{ and } n \text{ is a power of two} \}$$

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

Important Question

Do all infinite sets have
the same cardinality?

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

$S = \{$ 

$,$ 

$\}$

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

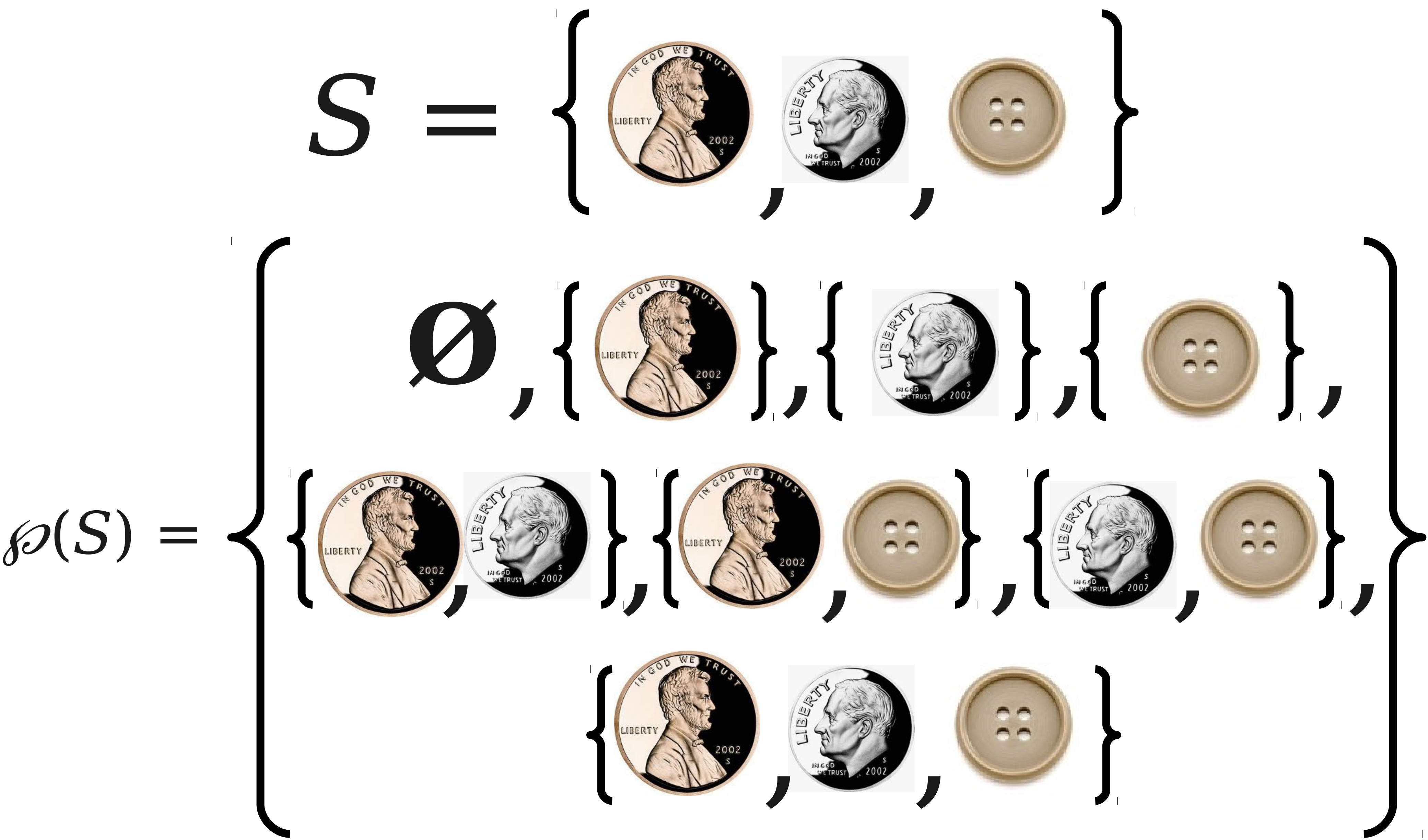
$\}, \{$ 

$\}, \{$ 

$,$ 

$\} \}$

$$\boldsymbol{|S| < |\wp(S)|}$$



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

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

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

$$\mathbf{|S| < |\wp(S)|}$$

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	…

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

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

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

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

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

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

…

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

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

Y	**N**	**N**	**N**	**N**	**Y**	…

Which row in the table is paired with this set?

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

N	**Y**	**Y**	**Y**	**Y**	**N**	…

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

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 strictly smaller than its power set:

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

Infinite Cardinalities

- Recall: $|\mathbb{N}| = \aleph_0$.
- By Cantor's Theorem:

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

- **Not all infinite sets have the same size!**
- **There are infinitely many infinities!**

What does this have to do with computation?

“The set of all computer programs”

“The set of all problems to solve”

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.

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

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.

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

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.
  - The set of all English phrases is no larger than the set of all strings, which is smaller than the set of all problems.
- 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?