Welcome to CS103!

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

Course Staff

Keith Schwarz (htiek@cs.stanford.edu)

Rakesh Achanta (rakesha@stanford.edu)
Kyle Brogle (broglek@stanford.edu)
Maurizio Caligaris (maurizio@cs.stanford.edu)
Justin Heermann (justinlh@stanford.edu)
Nicholas Isaacs (nisaacs@stanford.edu)
Jeffrey Jacobs (jjacobs3@stanford.edu)
Michael Kim (michael.kim@cs.stanford.edu)
Rose Marie Philip (rosep@stanford.edu)
Remington Wong (rwong2@stanford.edu)

Course Staff Mailing List:
cs103-aut1213-staff@lists.stanford.edu

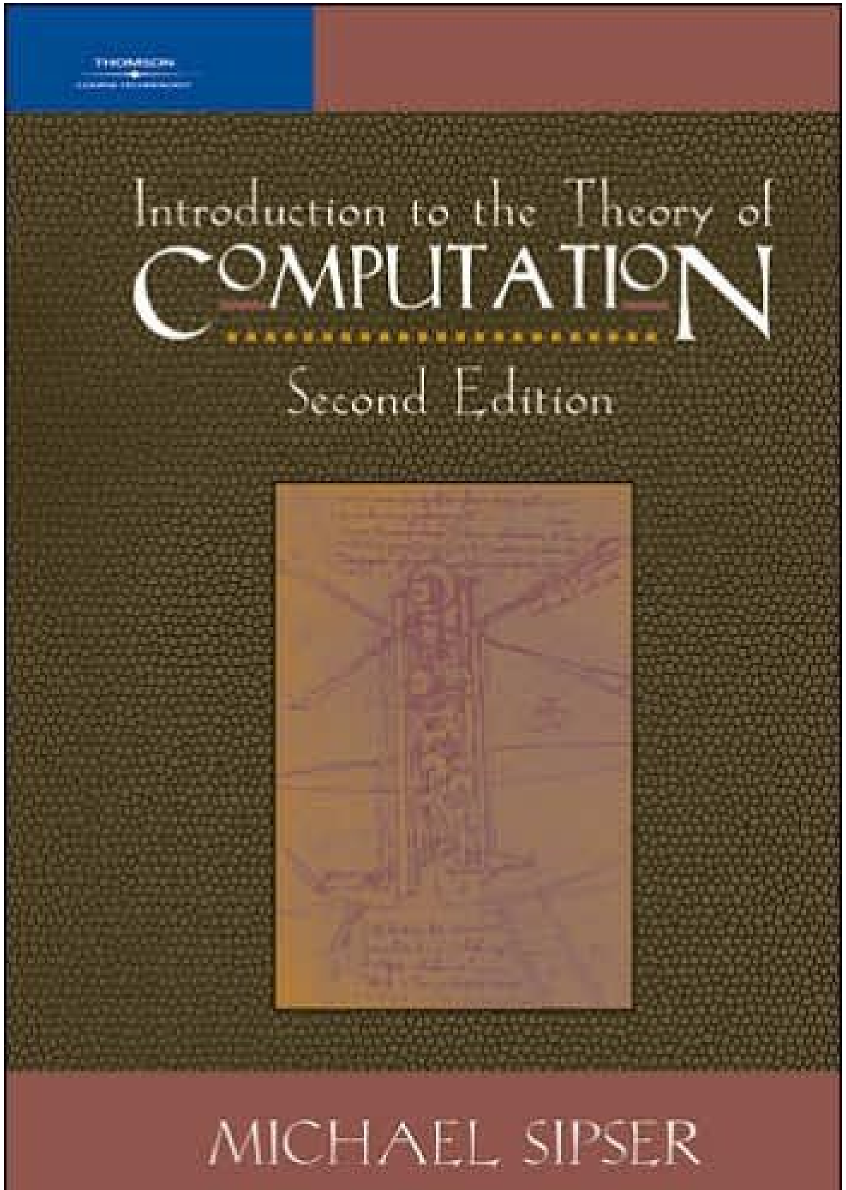
The Course Website

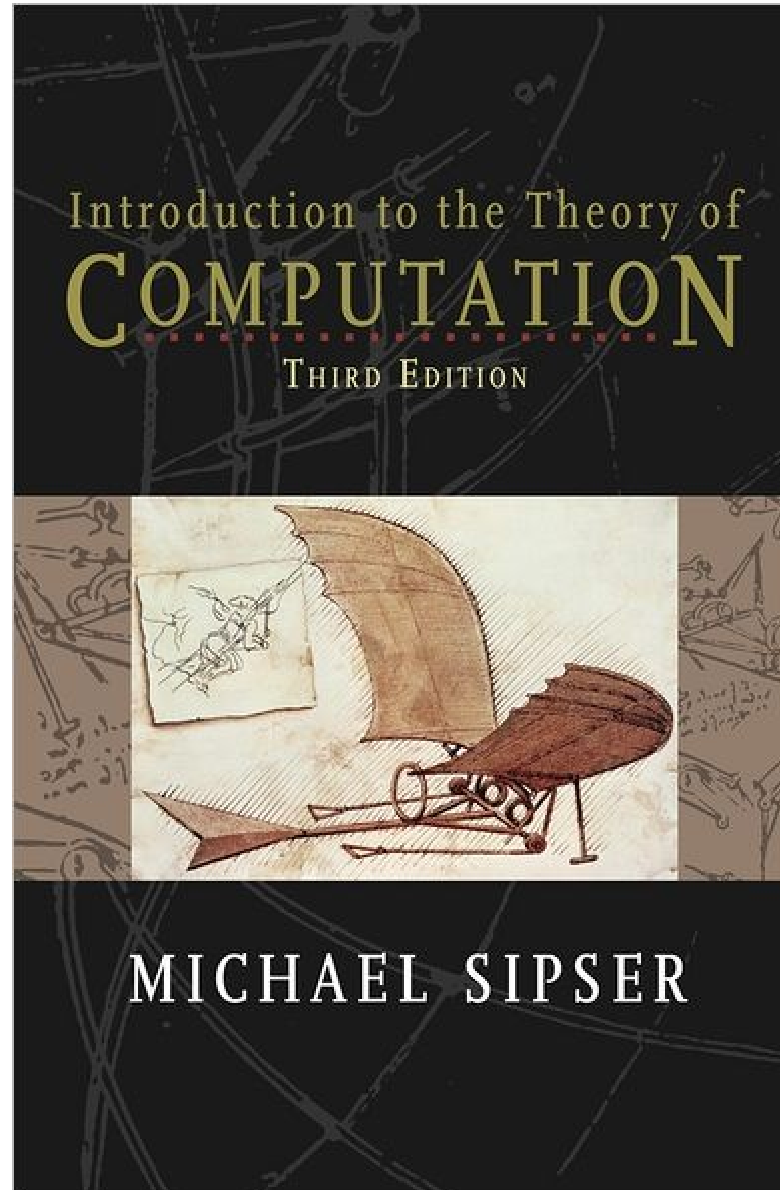
http://cs103.stanford.edu

“Prerequisite”

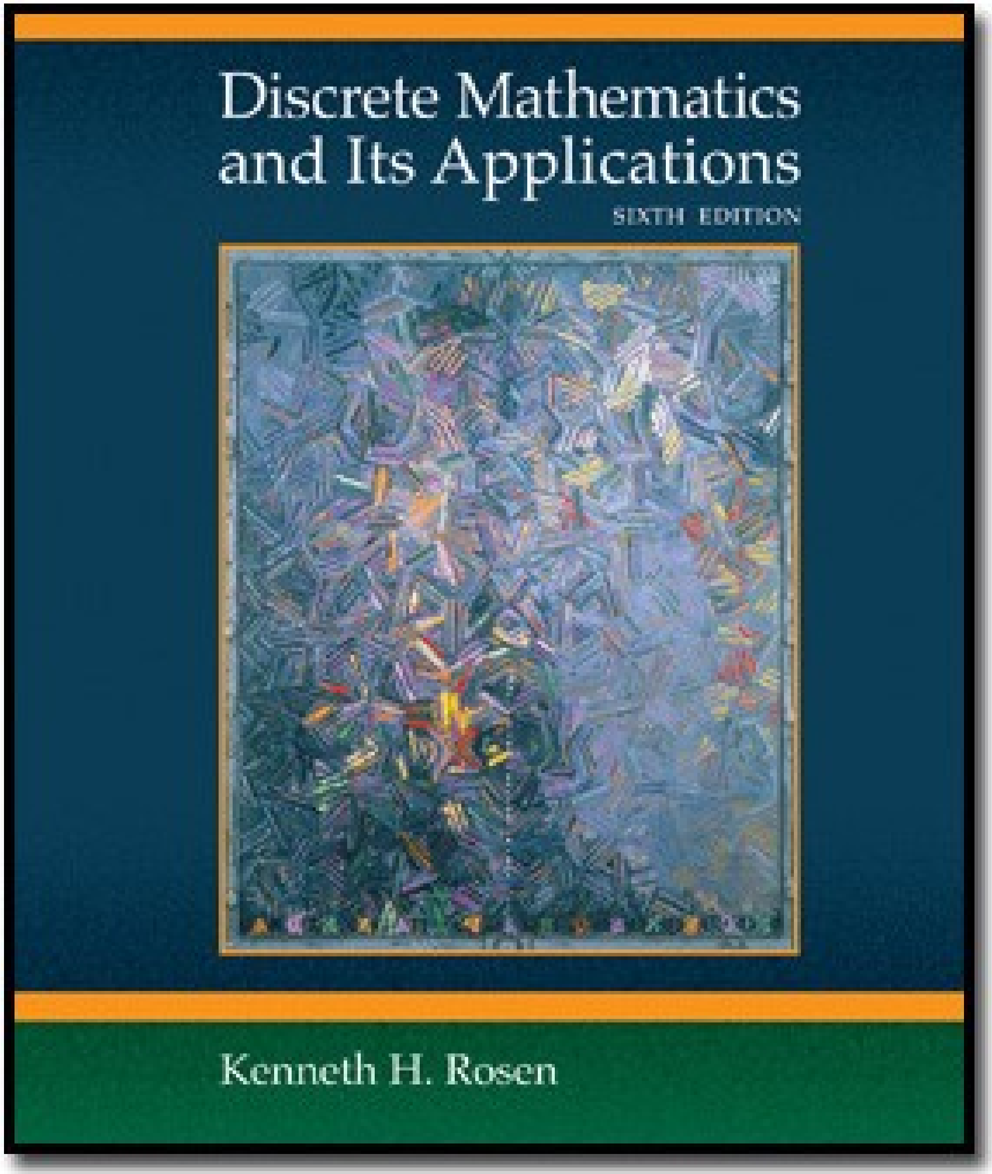
CS106A

Required Reading



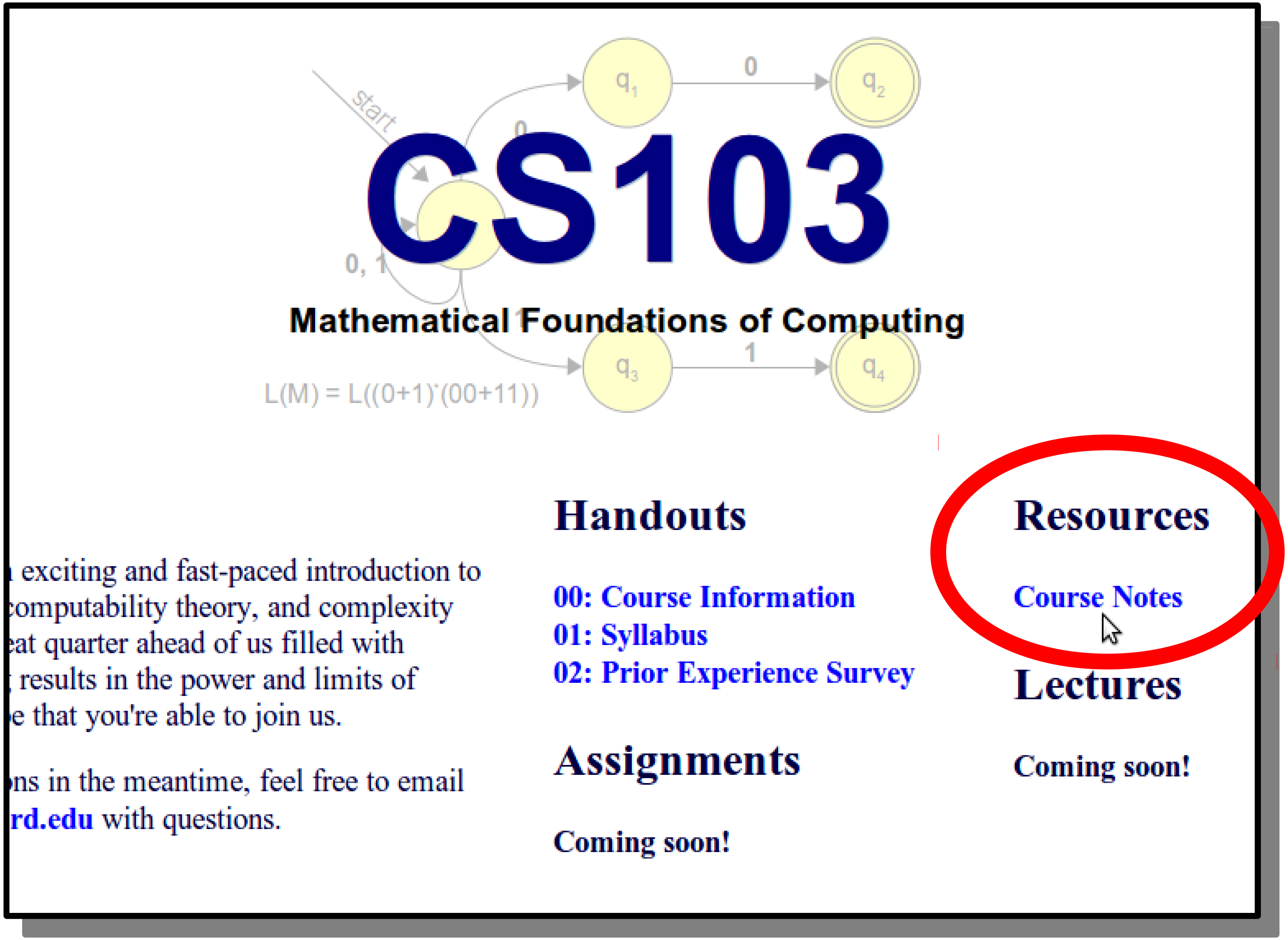


Required Reading

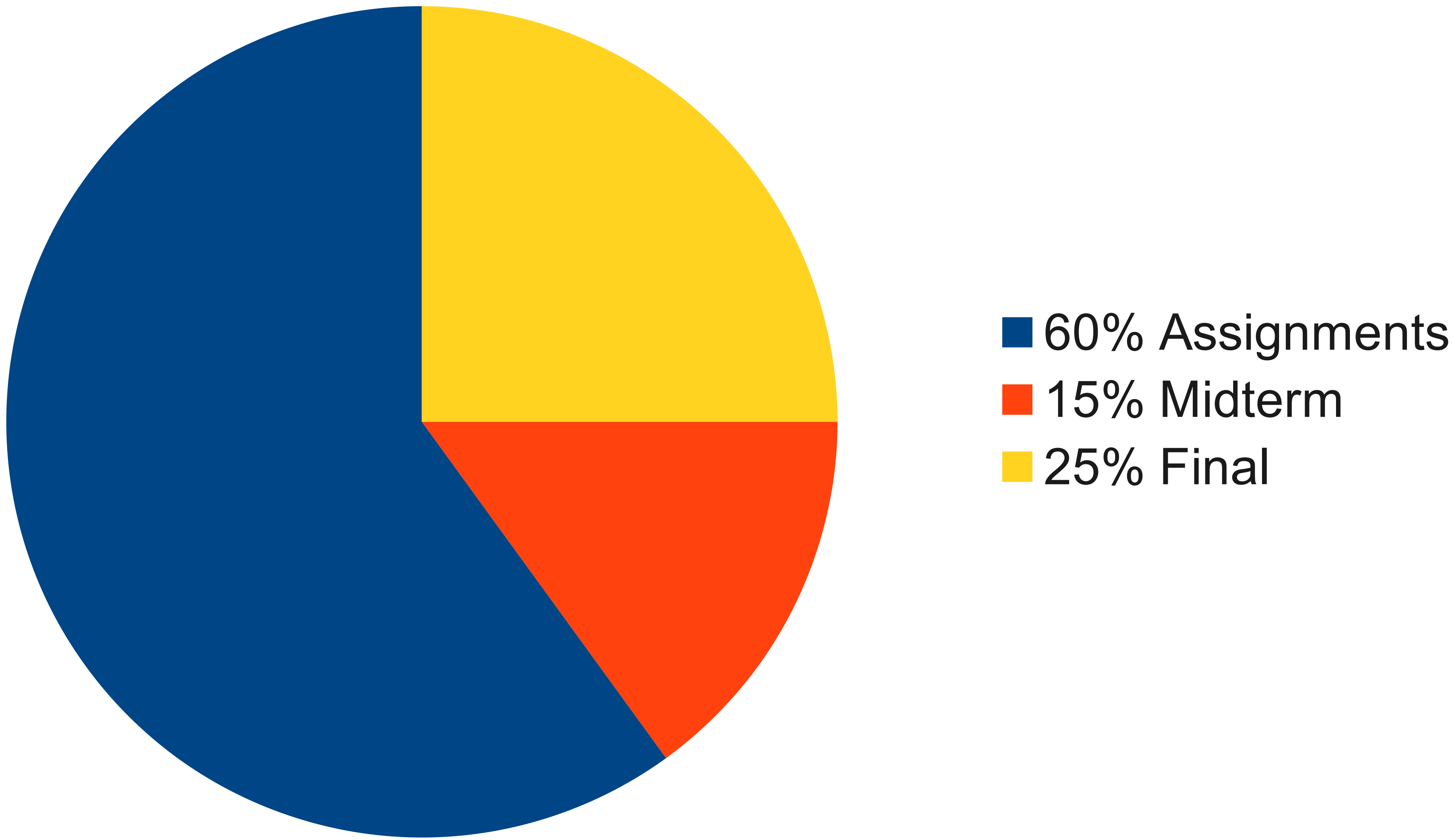


(but just the first chapter)

Online Course Notes



Grading Policies

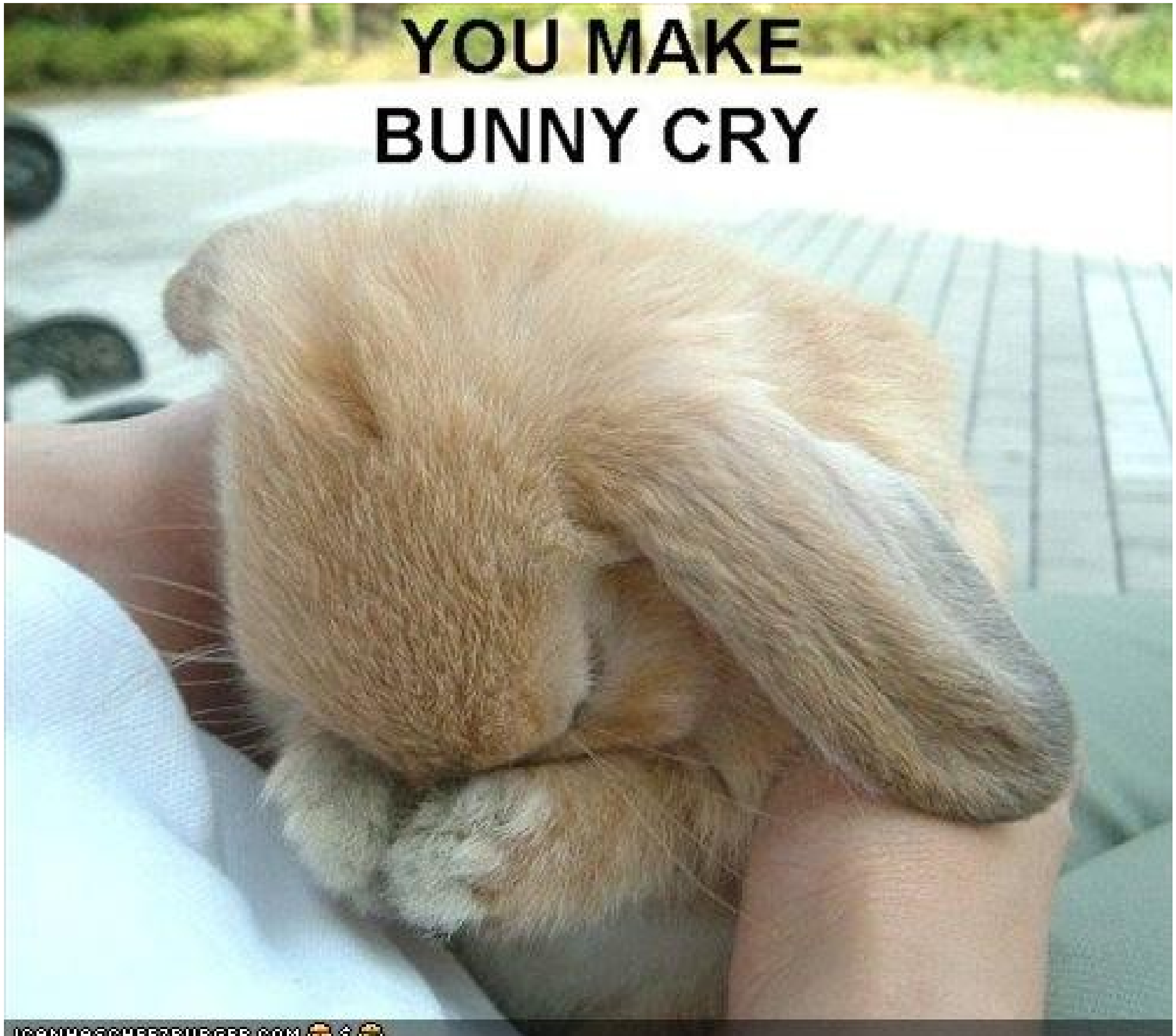


Problem Sessions

7:00 – 7:50PM in 380-380X

Optional, but highly recommended.
Starts next Monday.

A Word on the Honor Code…



A Note to CS106B Students

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

“CS103 students”

“All the computers on the Stanford network.”

“Cool people”

“The chemical elements”

“Cute animals”

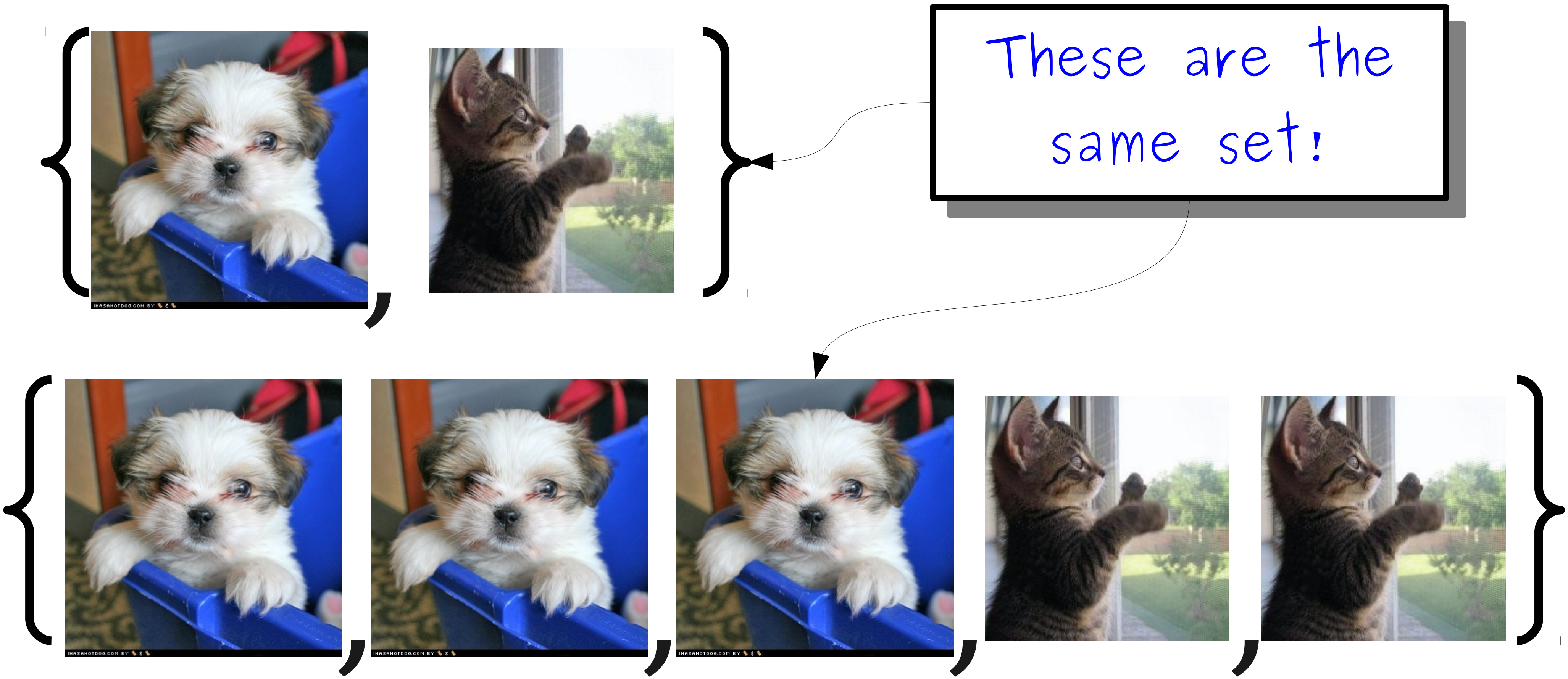
“US coins.”

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

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).

This symbol means "is defined as"

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

We denote it with this symbol

The empty set contains no elements.

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

Membership

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

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

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:

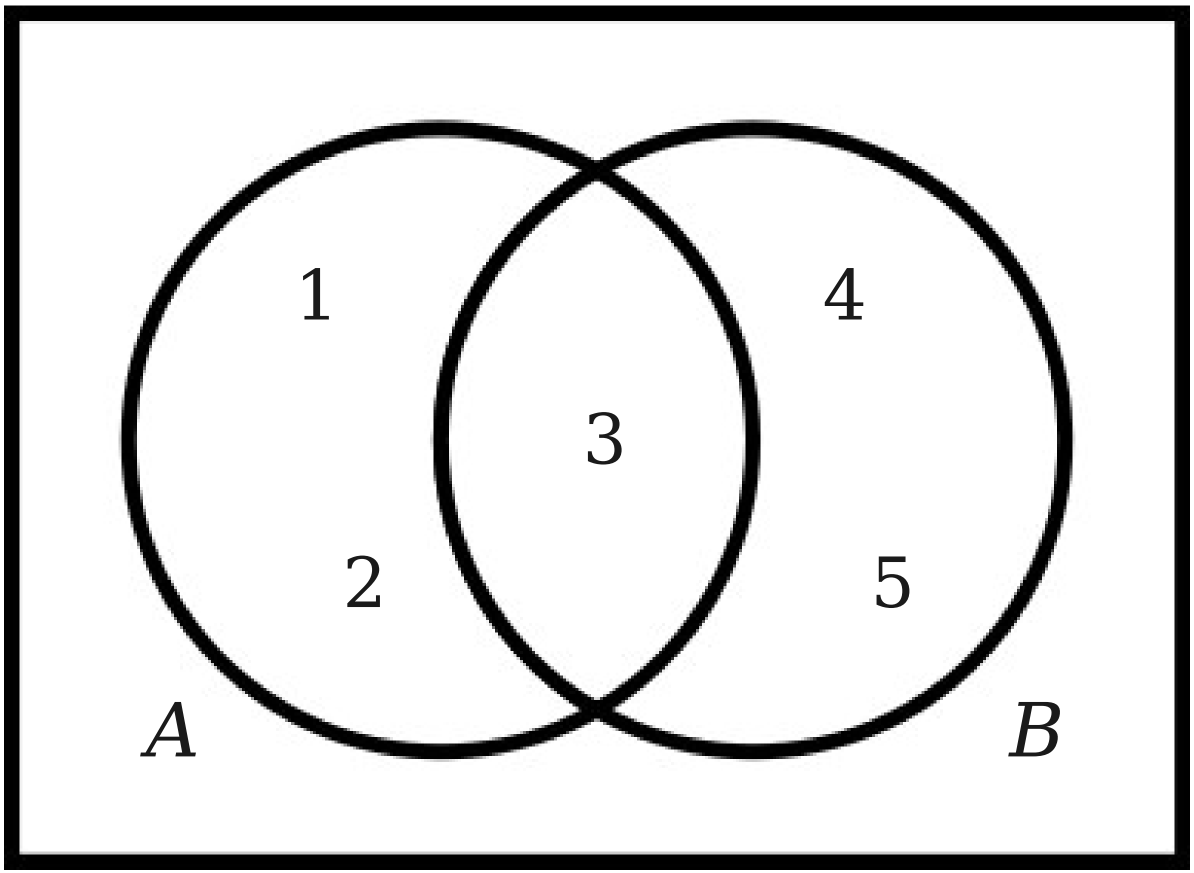
$$\{\ r \mid r \in \mathbb{R}, r < 137\ \}$$

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

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

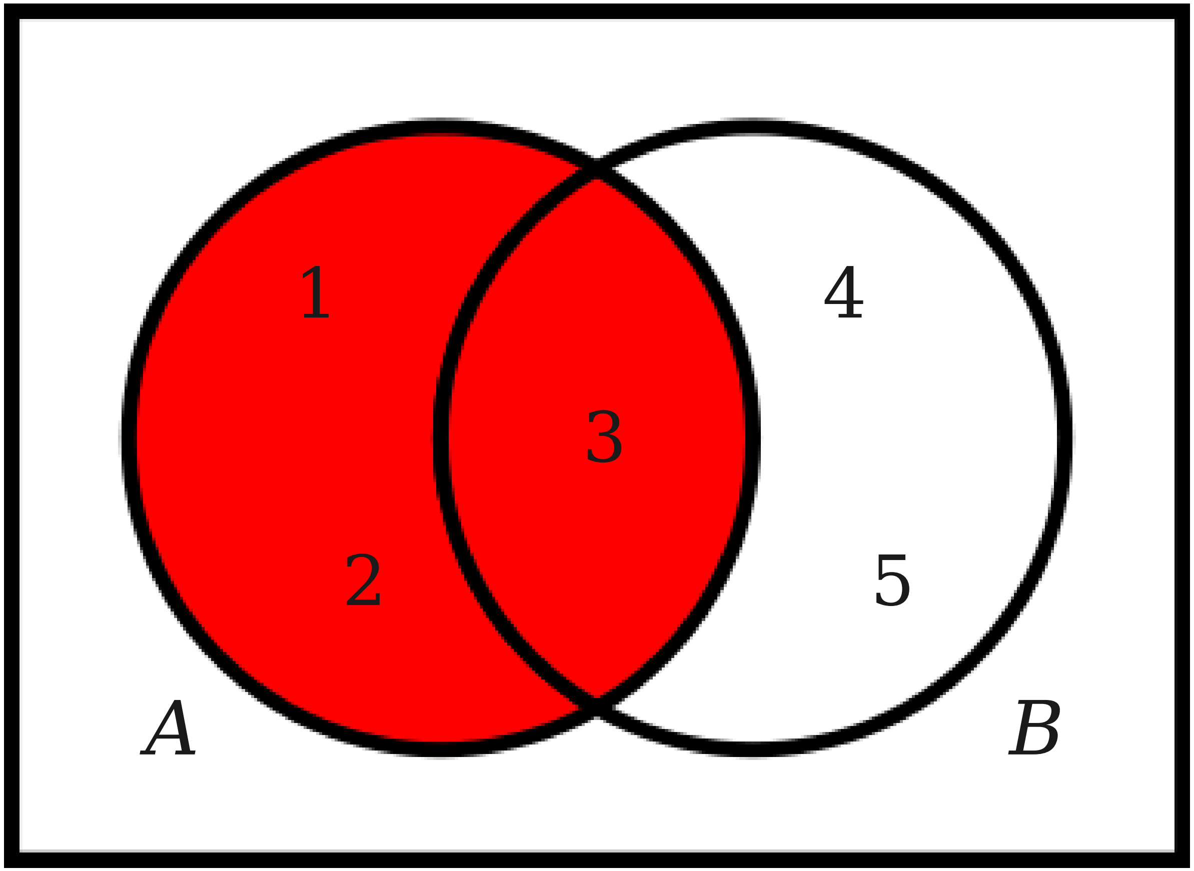
Combining Sets

Venn Diagrams



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

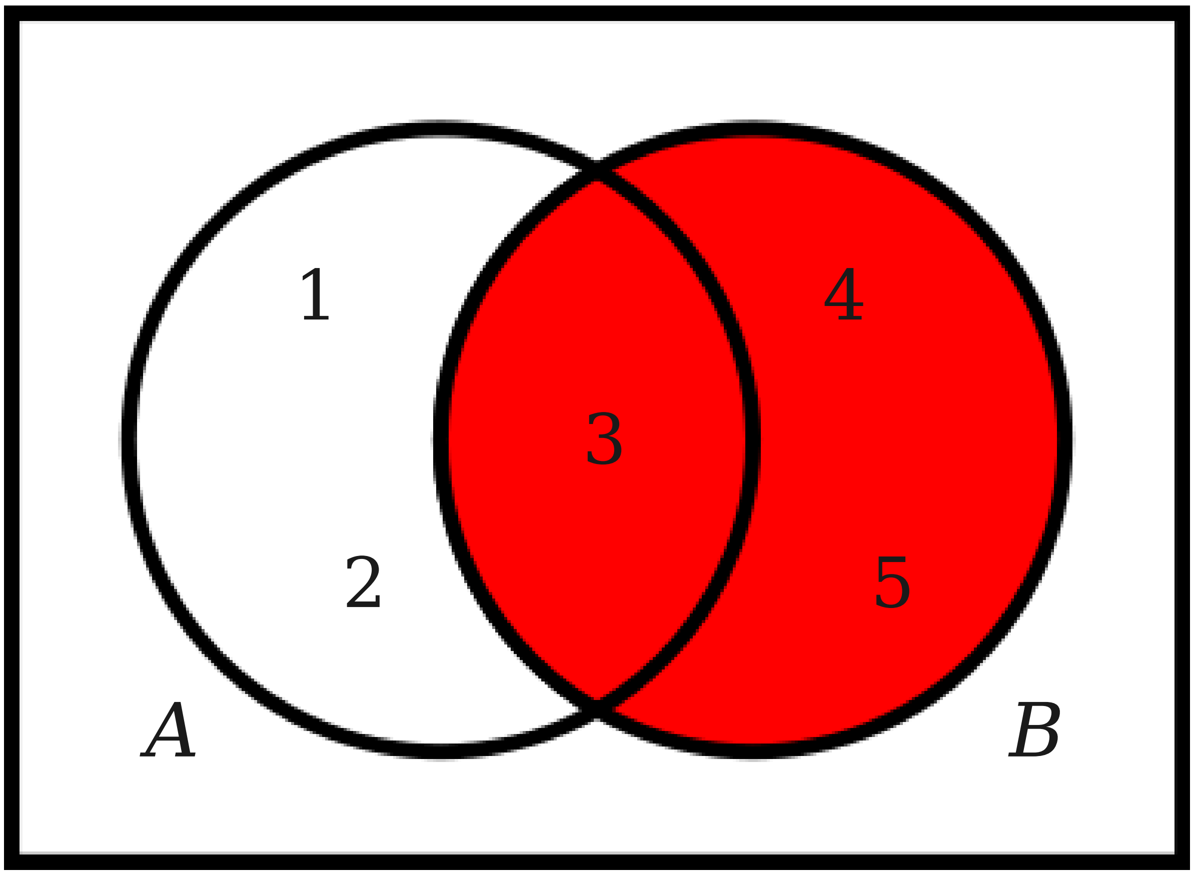
Venn Diagrams



A

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

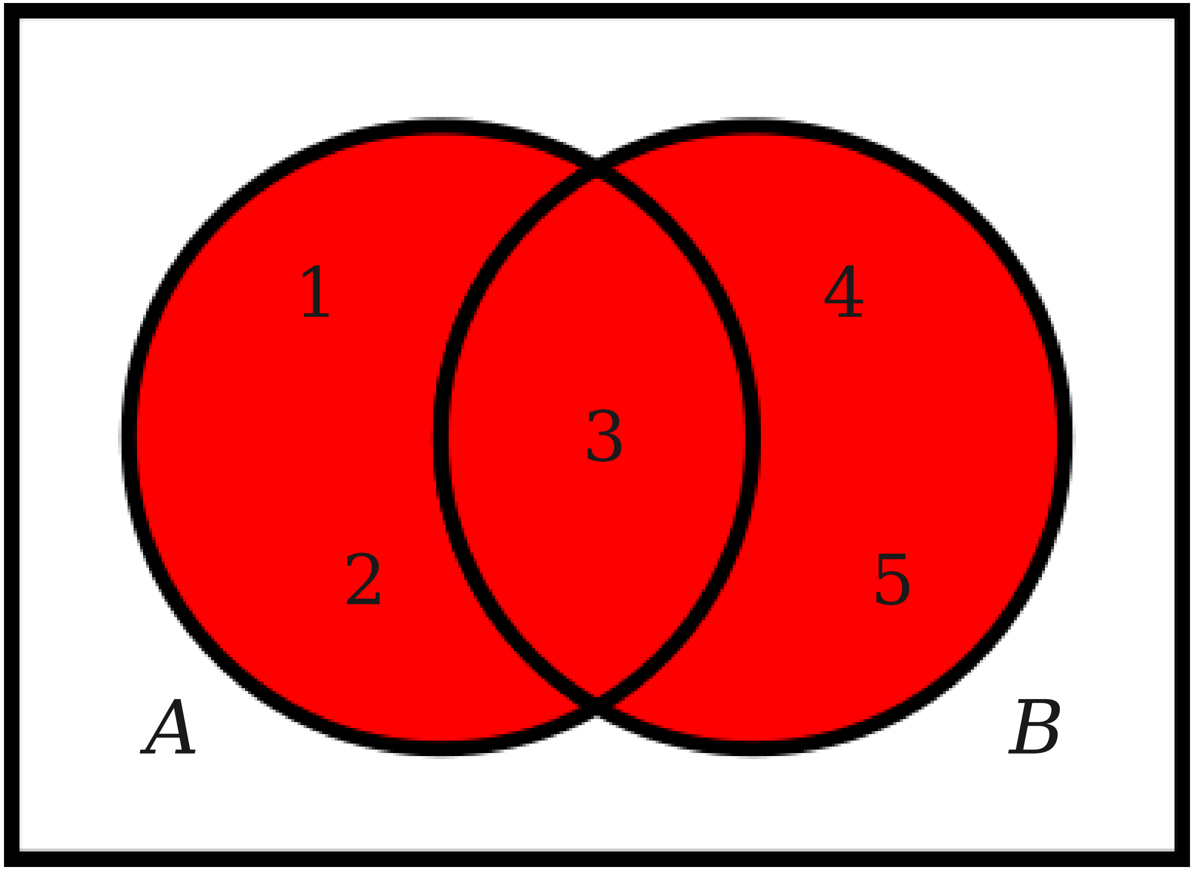
Venn Diagrams



B

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

Venn Diagrams



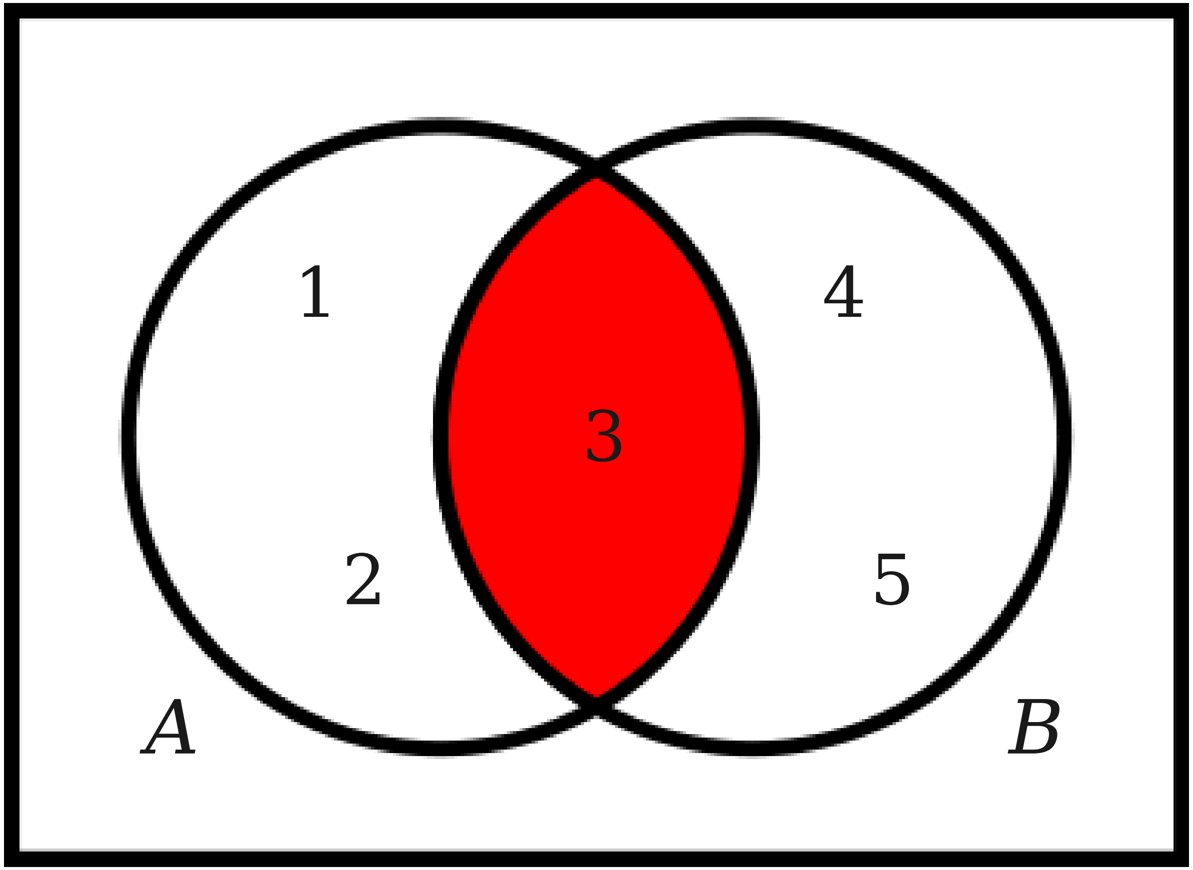
Union

$A \cup B$

{ 1, 2, 3, 4, 5 }

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

Venn Diagrams



Intersection

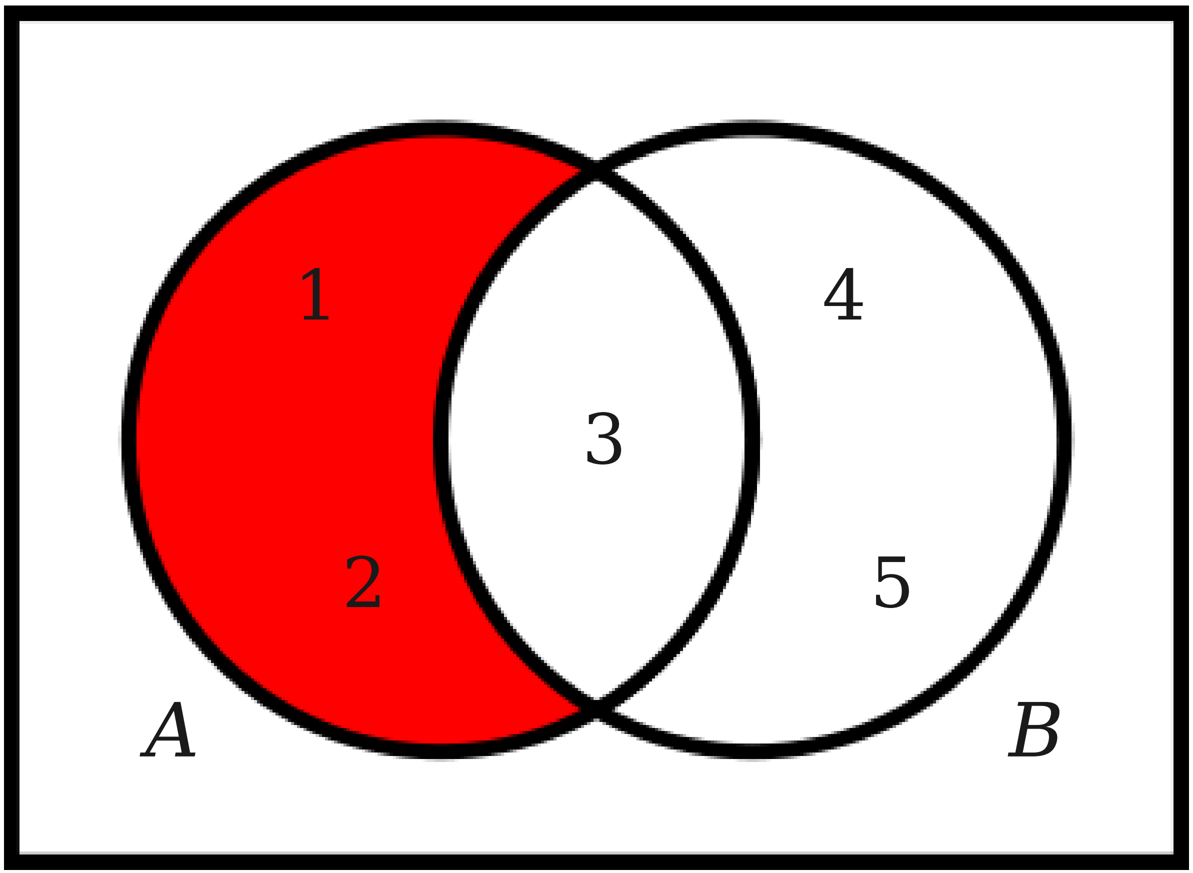
$A \cap B$

$\{ 3 \}$

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

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

Venn Diagrams



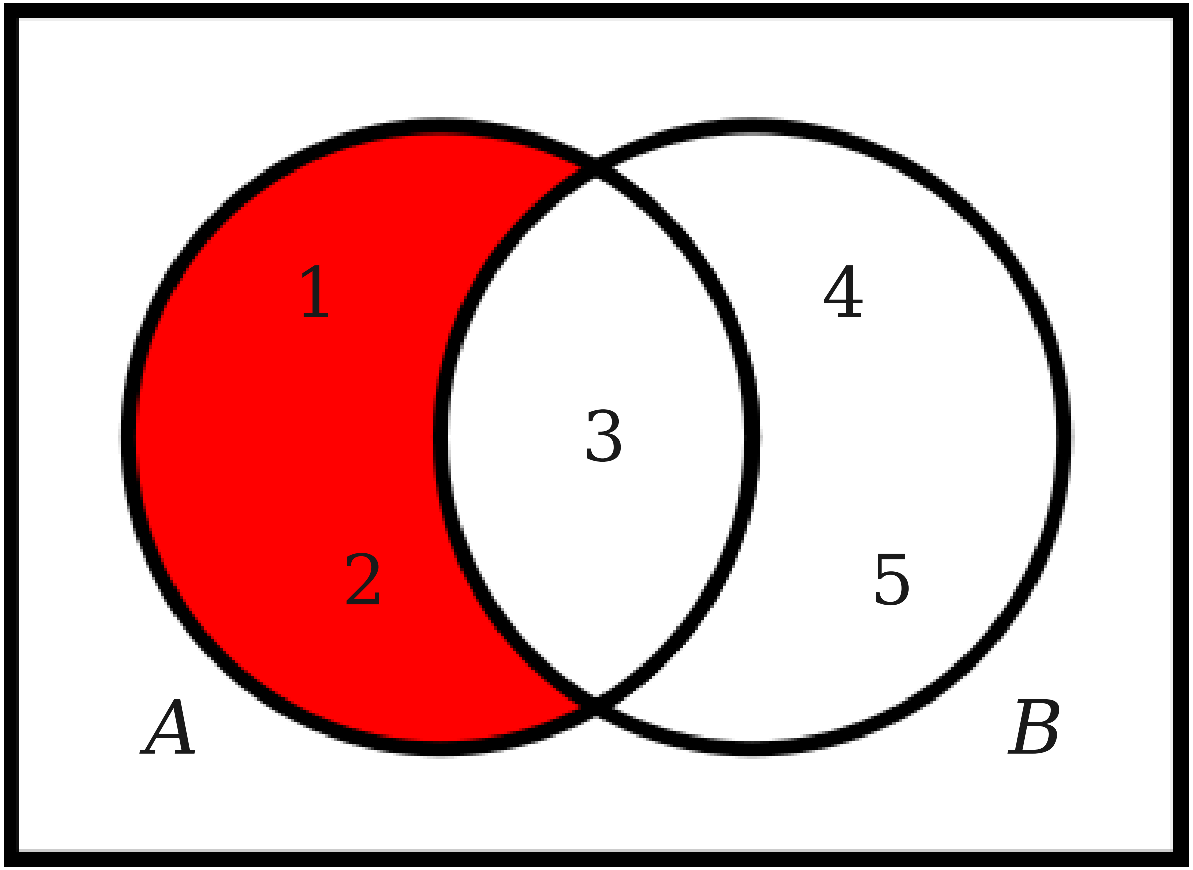
Difference

$A - B$

{ 1, 2 }

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

Venn Diagrams



Difference

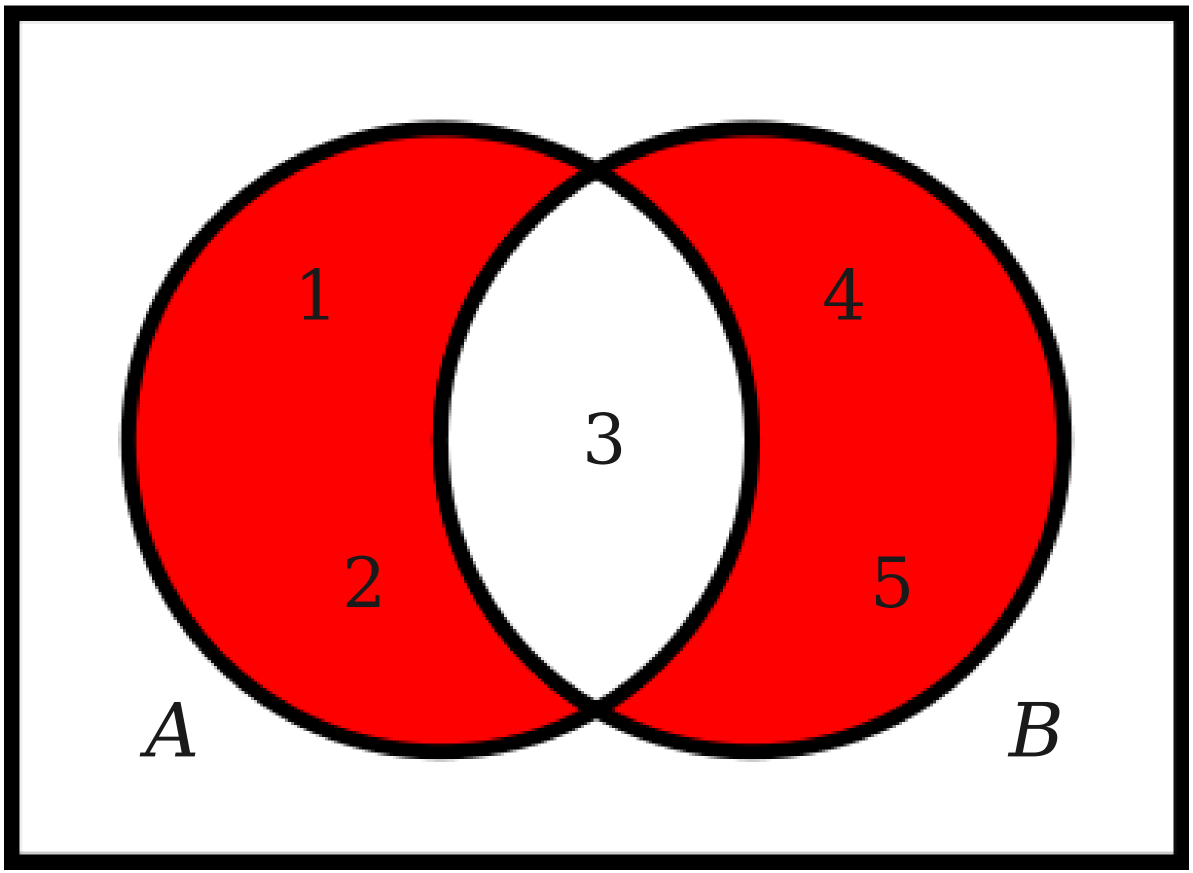
$A \setminus B$

$\{ 1, 2 \}$

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

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

Venn Diagrams



Symmetric Difference

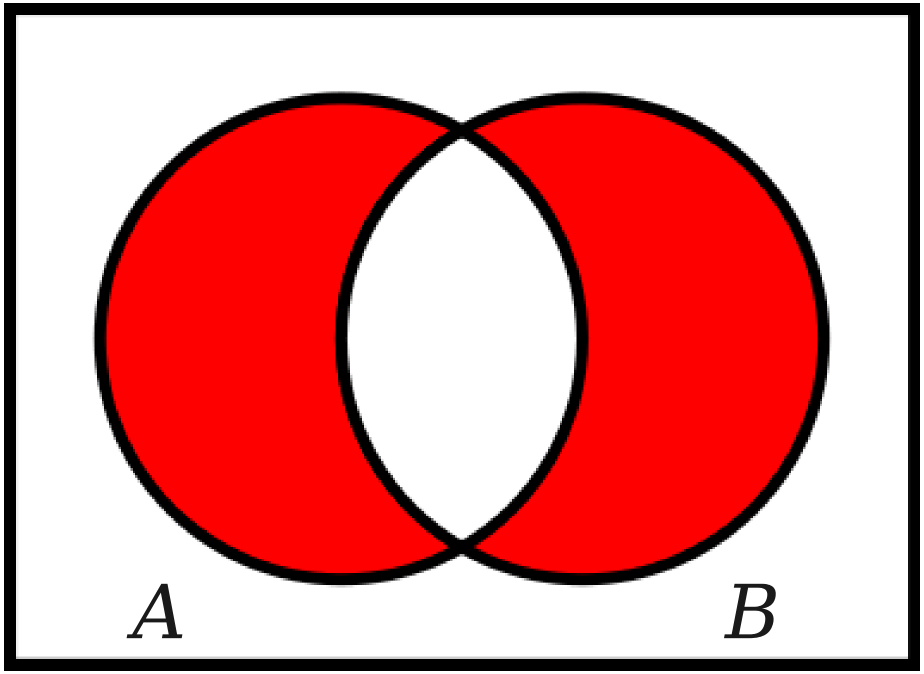
$A \Delta B$

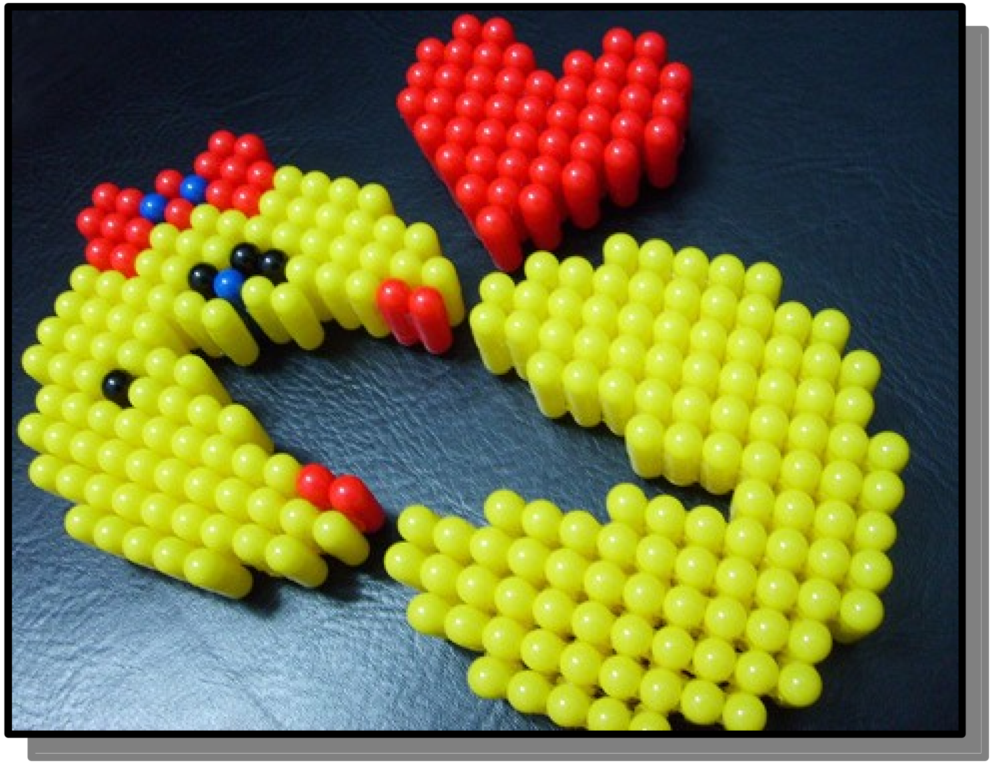
{ 1, 2, 4, 5 }

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

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

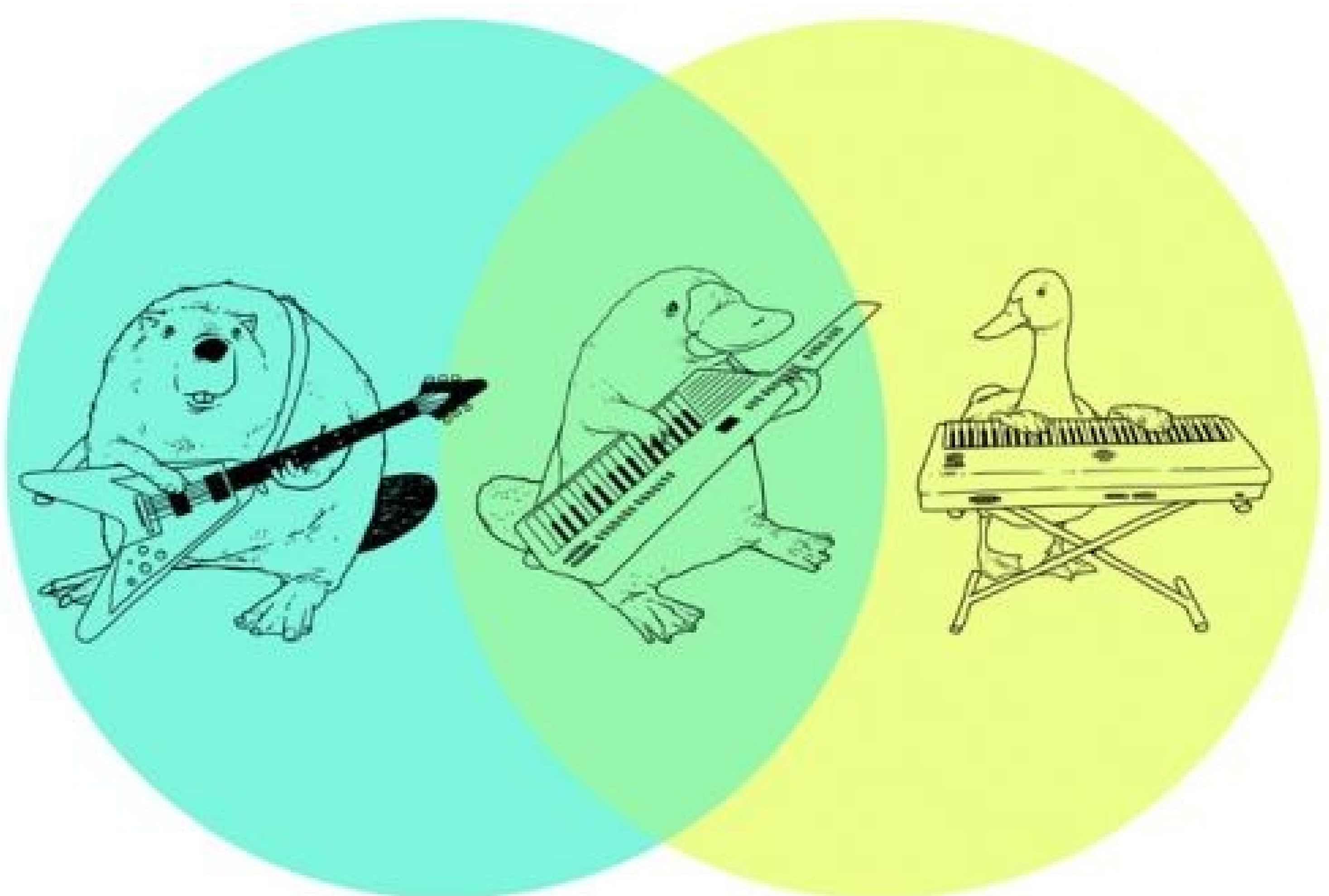
Venn Diagrams



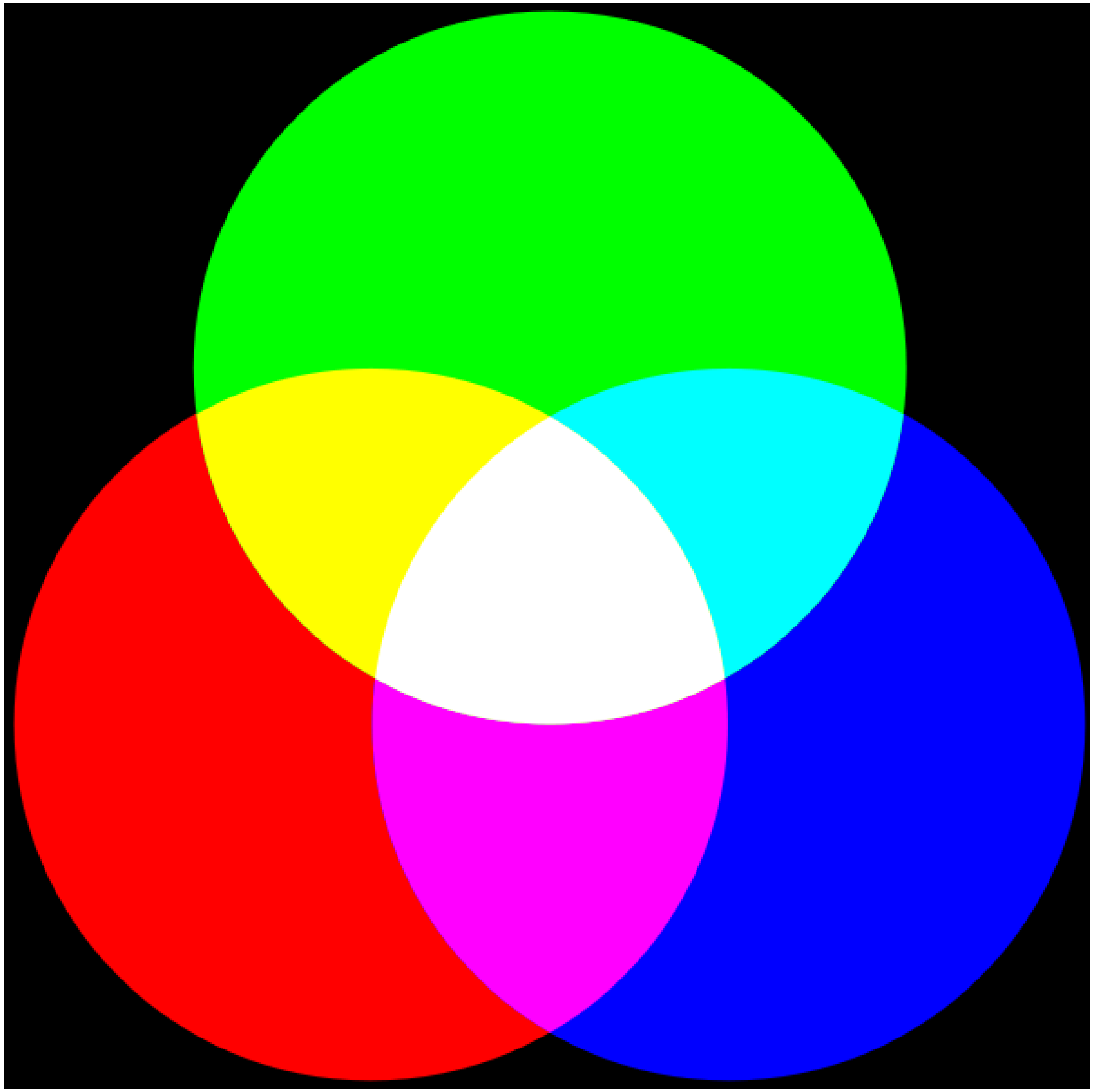


$A \Delta B$

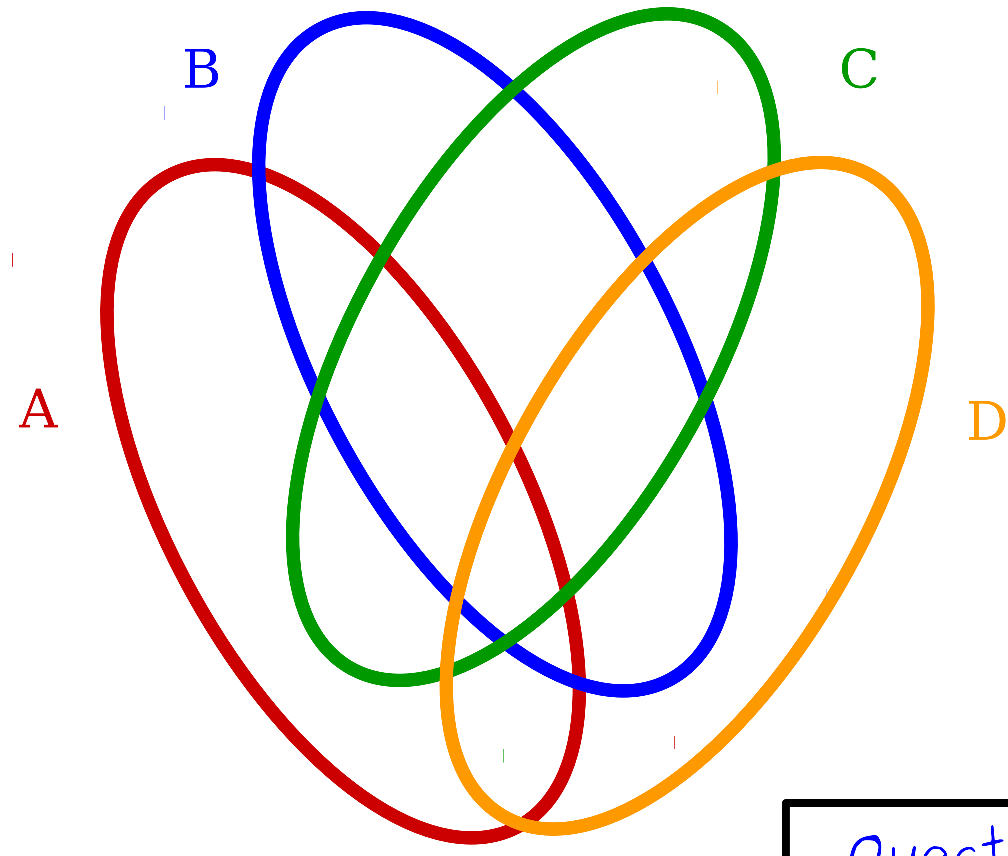
Venn Diagrams



Venn Diagrams for Three Sets



Venn Diagrams for Four Sets



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

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:

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

- We denote this as $S \subseteq T$.
- 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?

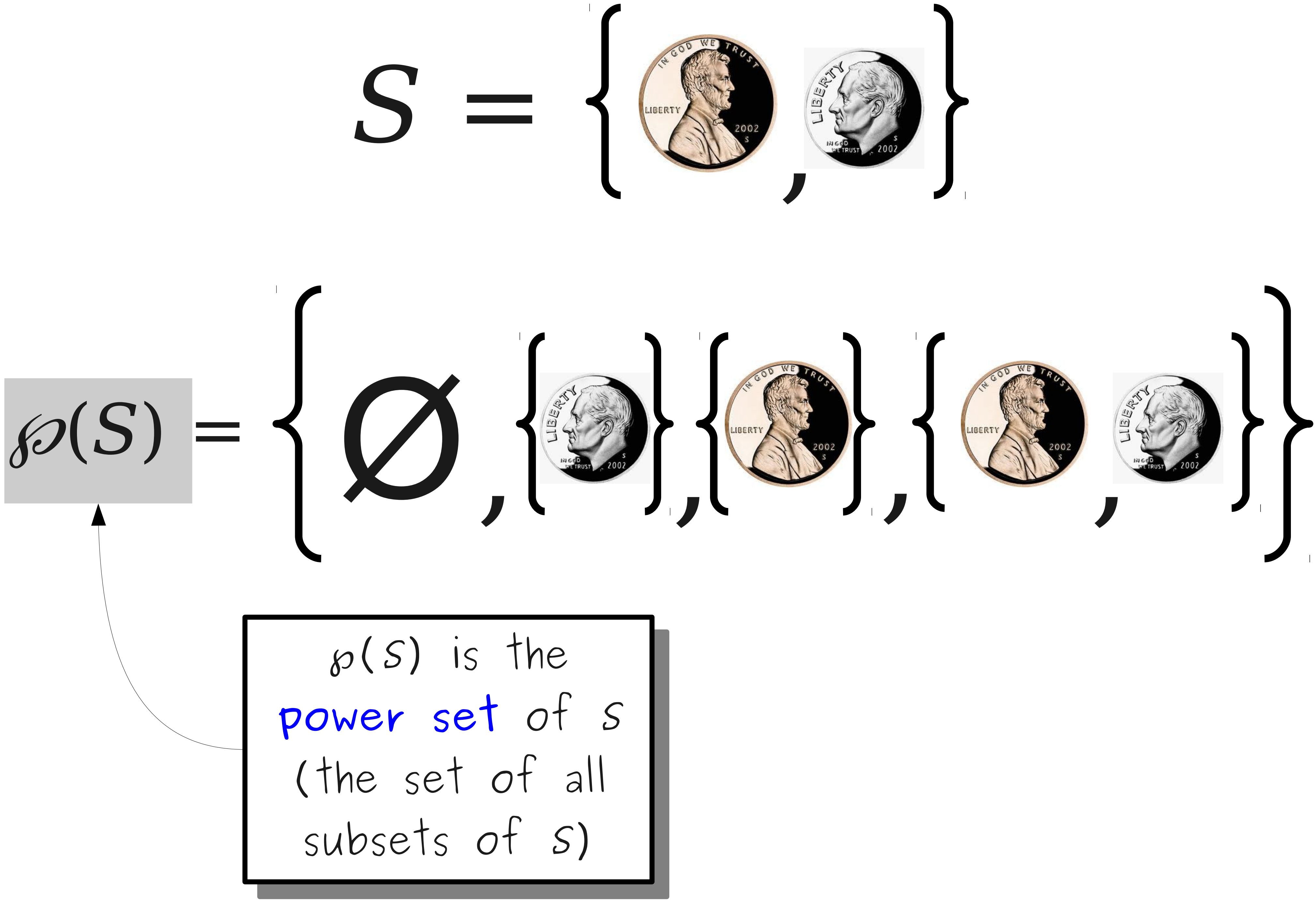
- A set S is a **subset** of some set T if every element of S is also an element in T:

  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) =
∅
℘(S) is the power set of S (the set of all subsets of S)

Cardinalities

Cardinality

- The **cardinality** of a set is the number of elements it contains.
- 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 $\mathbb{N}$

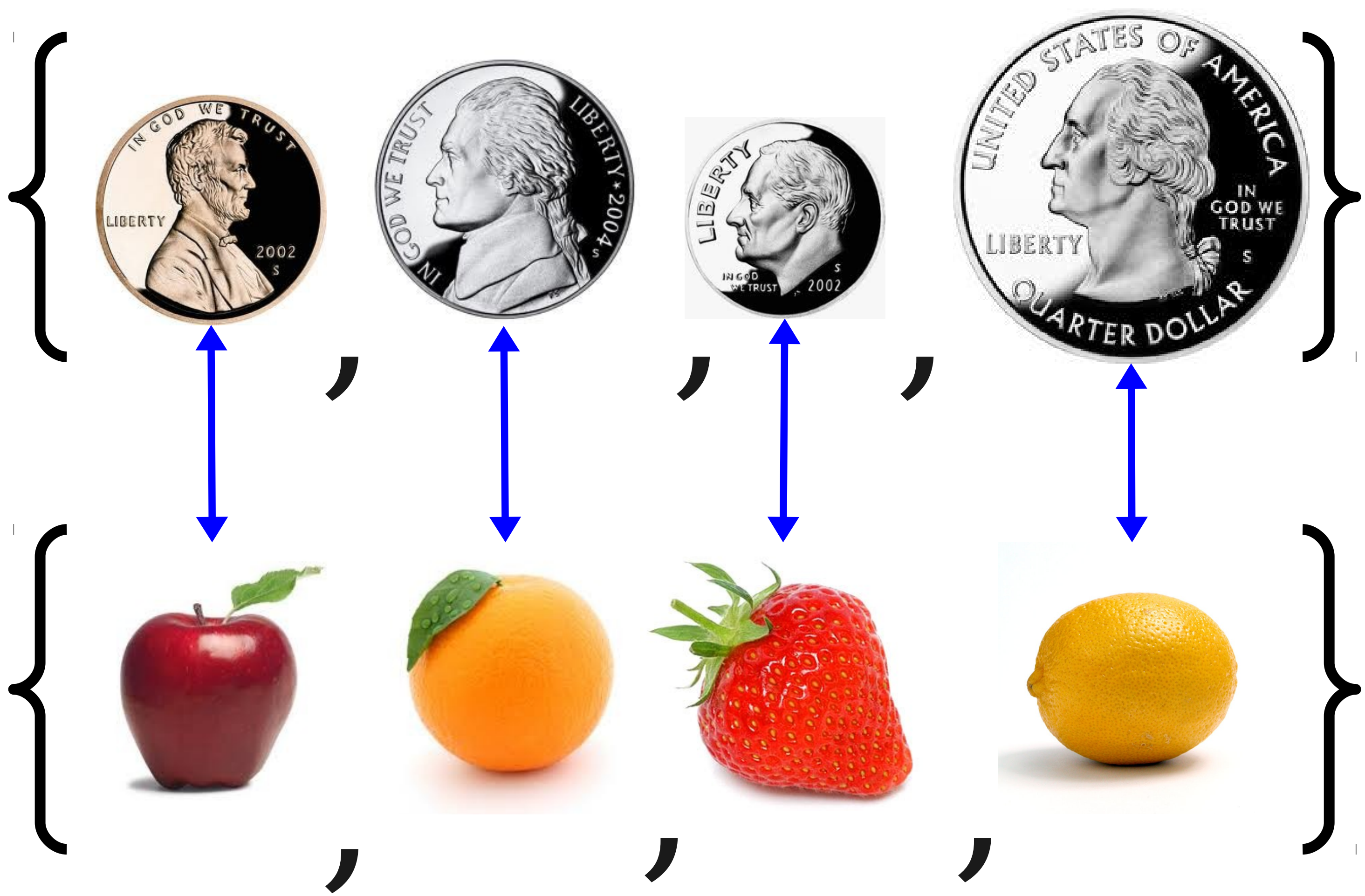
- What is $|\mathbb{N}|$?
  - There are infinitely many natural numbers.
  - $|\mathbb{N}|$ can't be a natural number, since it's infinitely large.
- We need to introduce a new term.
- Definition: $|\mathbb{N}| = \aleph_0$
  - Pronounced “Aleph-Zero,” “Aleph-Nought,” or “Aleph-Null”

Consider the set

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

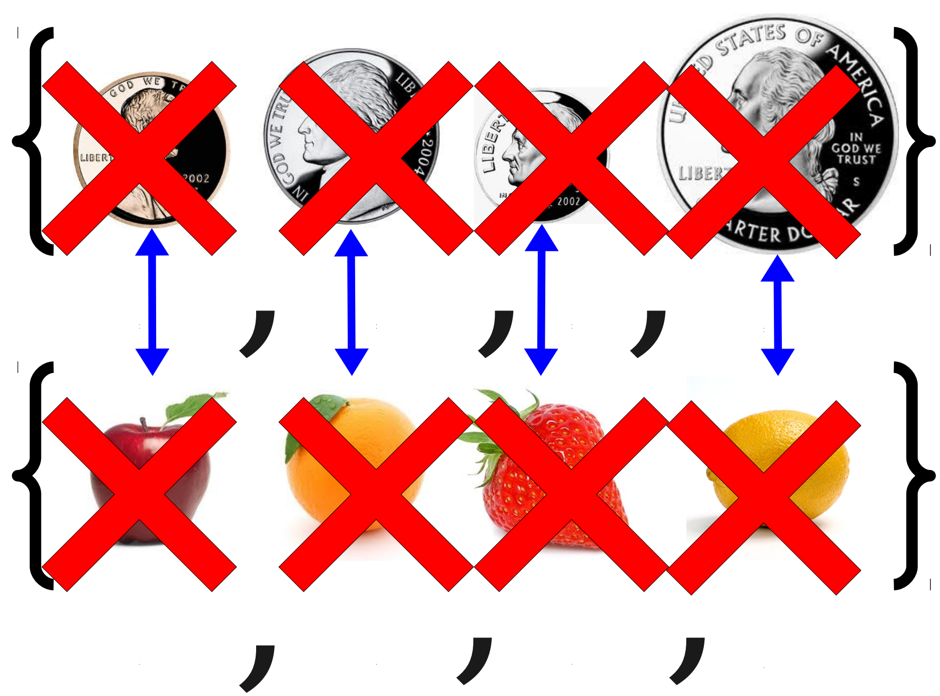
What is $|S|$?

How Big Are These Sets?



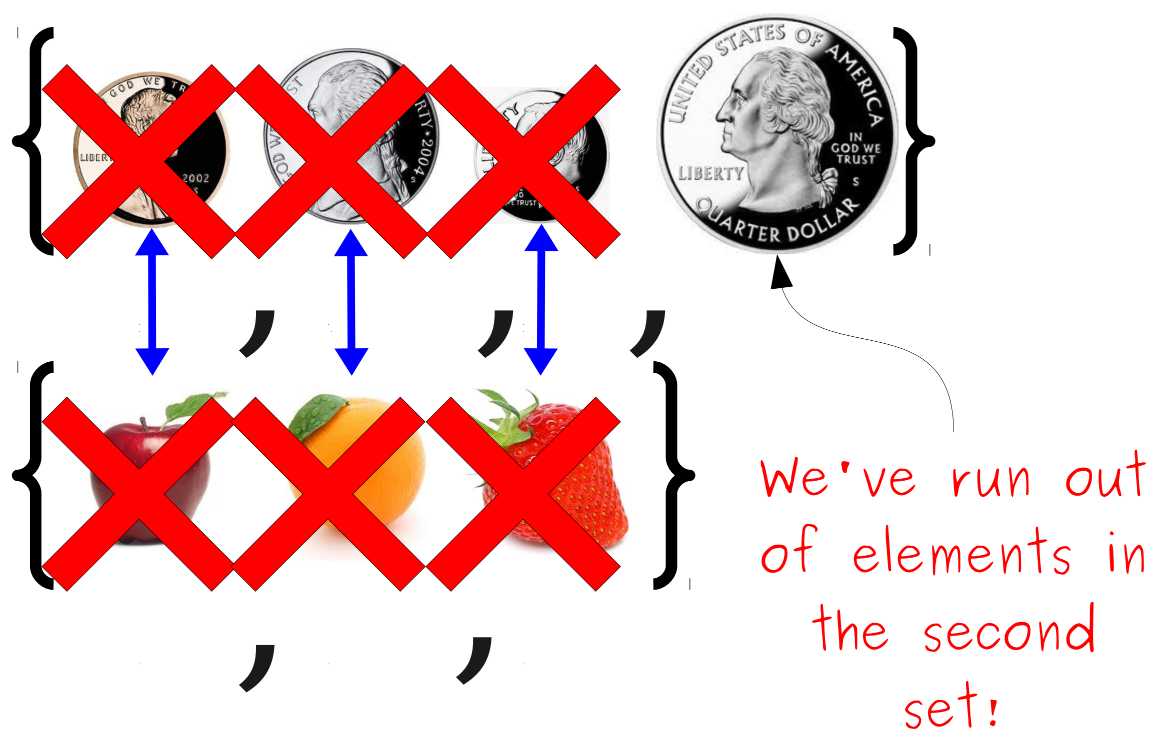
Comparing Cardinalities

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

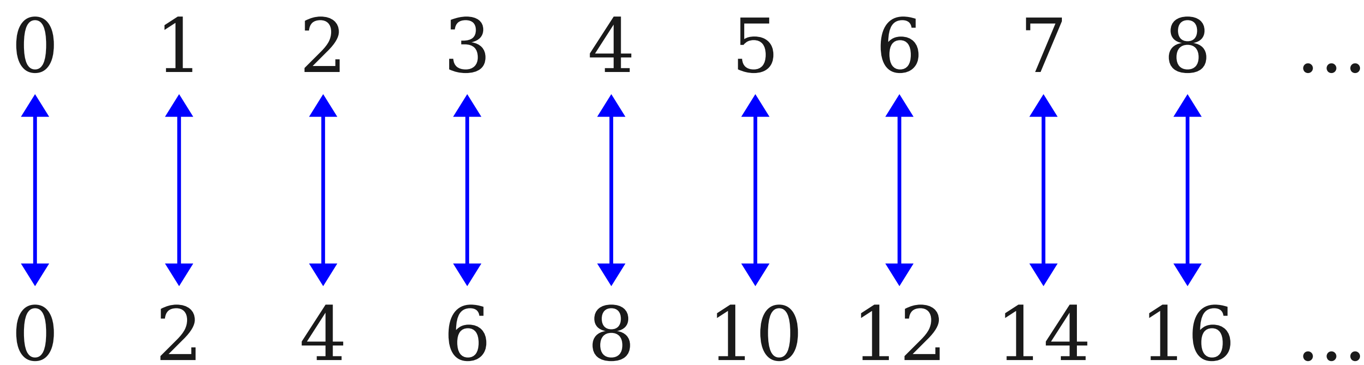


Comparing Cardinalities

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



Infinite Cardinalities



$$n \leftrightarrow 2n$$

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

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

Infinite Cardinalities

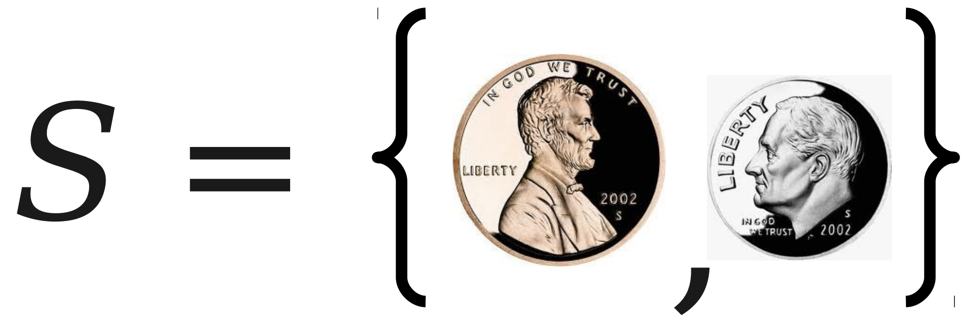
$\mathbb{N}$	0	1	2	3	4	5	6	7	8	...
	↕	↕	↕	↕	↕	↕	↕	↕	↕	
$\mathbb{Z}$	0	1	-1	2	-2	3	-3	4	-4	...

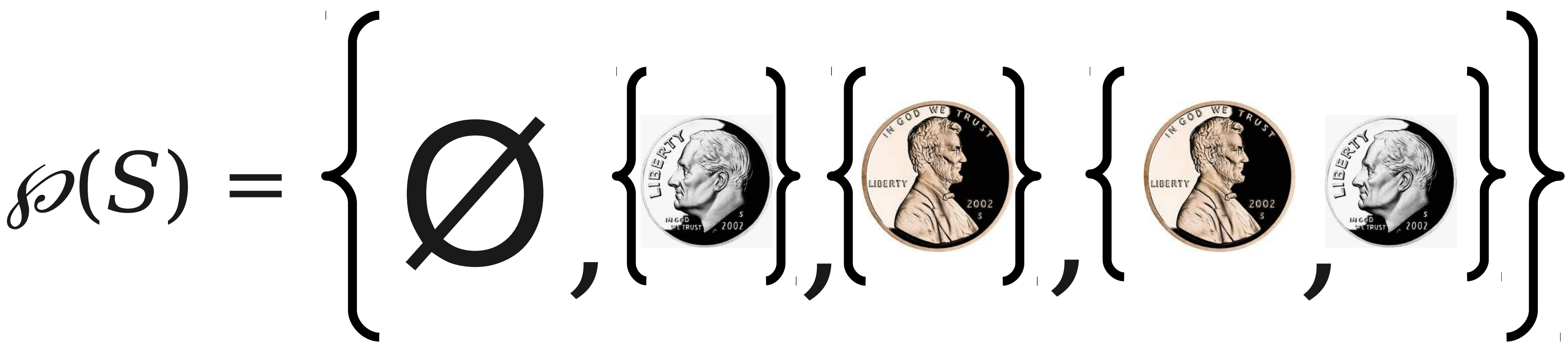
$n \leftrightarrow$ if n is even, then $-n / 2$
if n is odd, then $(n + 1) / 2$

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

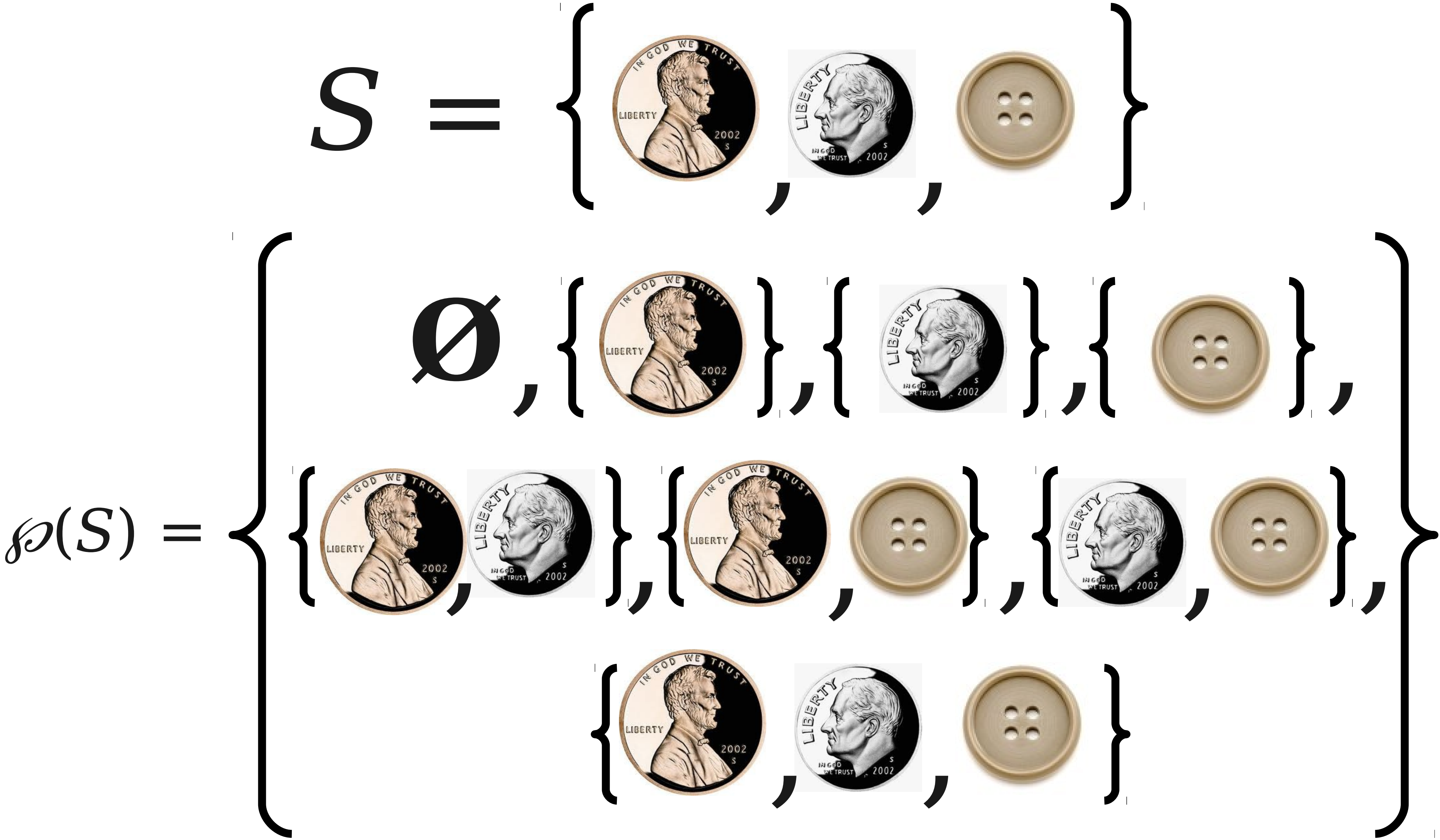
Important Question

Do all infinite sets have the same cardinality?


S =
LIBERTY
IN GOD WE TRUST
2002
S


℘(S) =
∅
LIBERTY
IN GOD WE TRUST
2002
S

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



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

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

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

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

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?

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

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

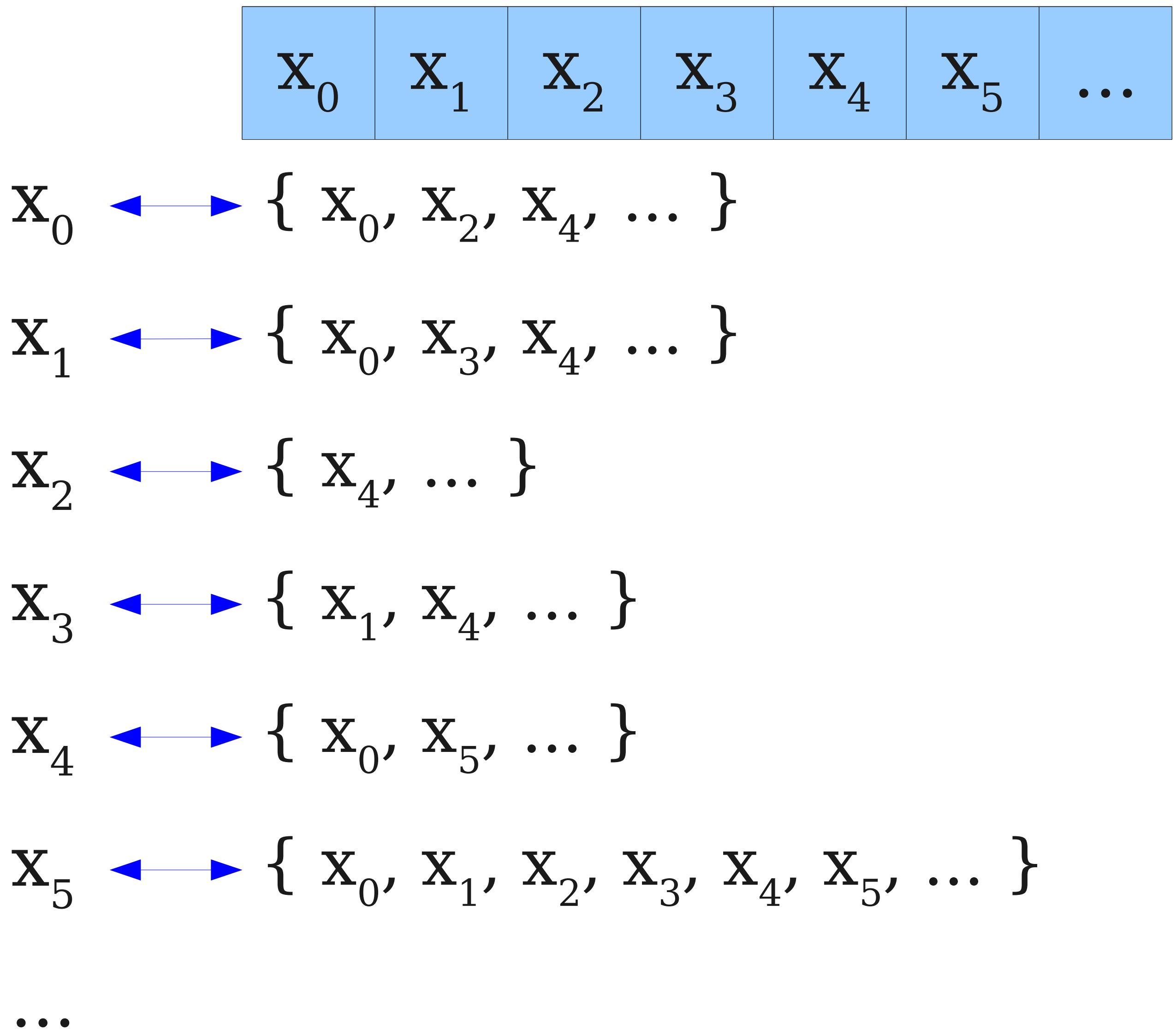
$x_2 \longleftrightarrow \{ x_4, \ldots \}$

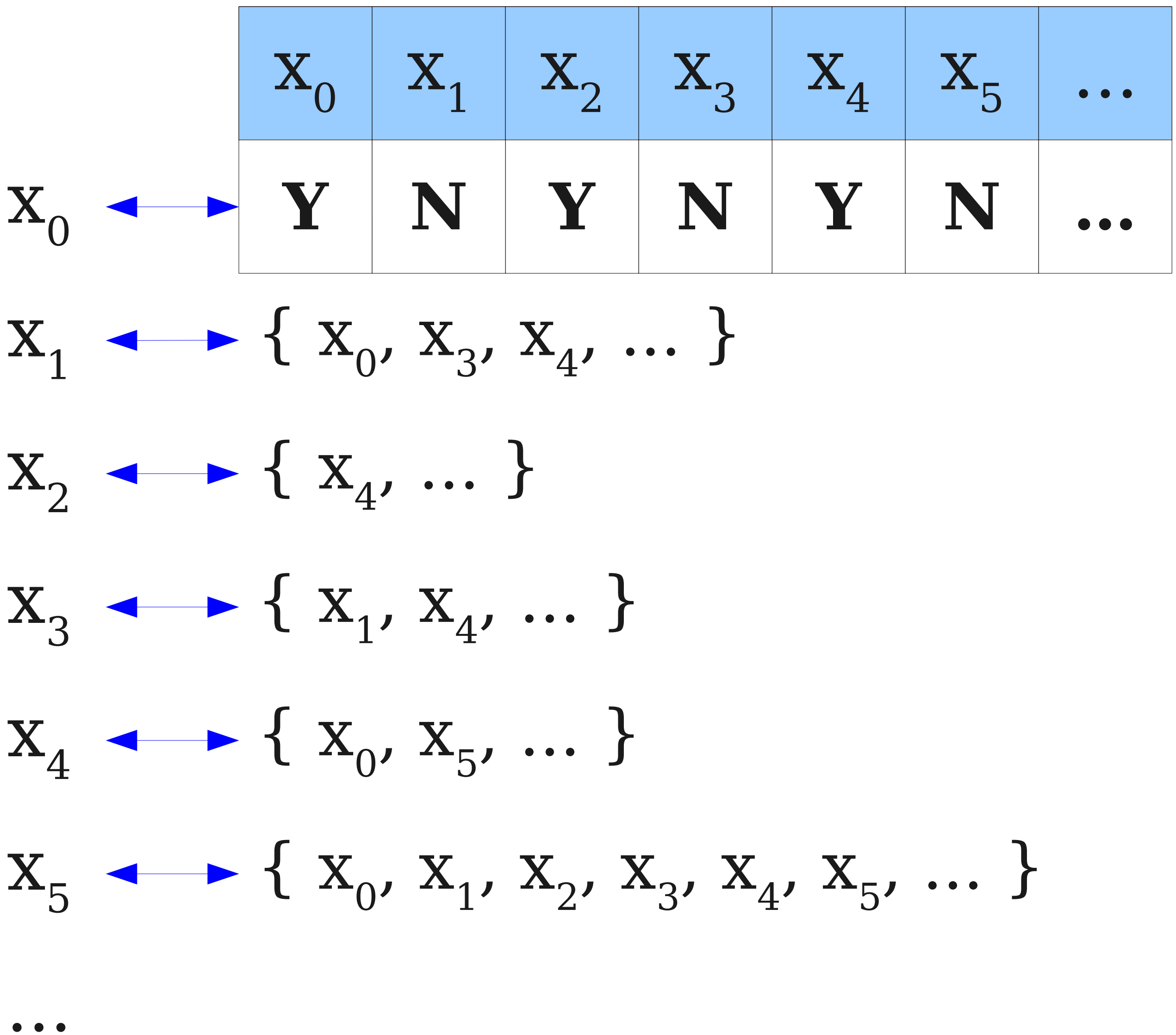
$x_3 \longleftrightarrow \{ x_1, x_4, \ldots \}$

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

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

$\ldots$


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


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	**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**	…
…	…	…	…	…	…	…	…

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**	…

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:

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

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?