Welcome to CS103!

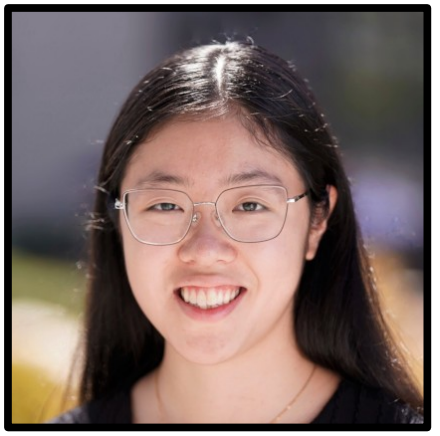
Are there “laws of physics”
in computer science?

Key Questions in CS103

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

The Teaching Team

Robyn Reiss
(Instructor)



Joyce Lu
(TA)

Robyn's Email: robyn.reiss@stanford.edu

Staff Email List: cs103-sum2526-staff@lists.stanford.edu

Course Website

https://cs103.stanford.edu

All course content will be hosted here, except for lecture videos.

Prerequisite / Corequisite

CS106B

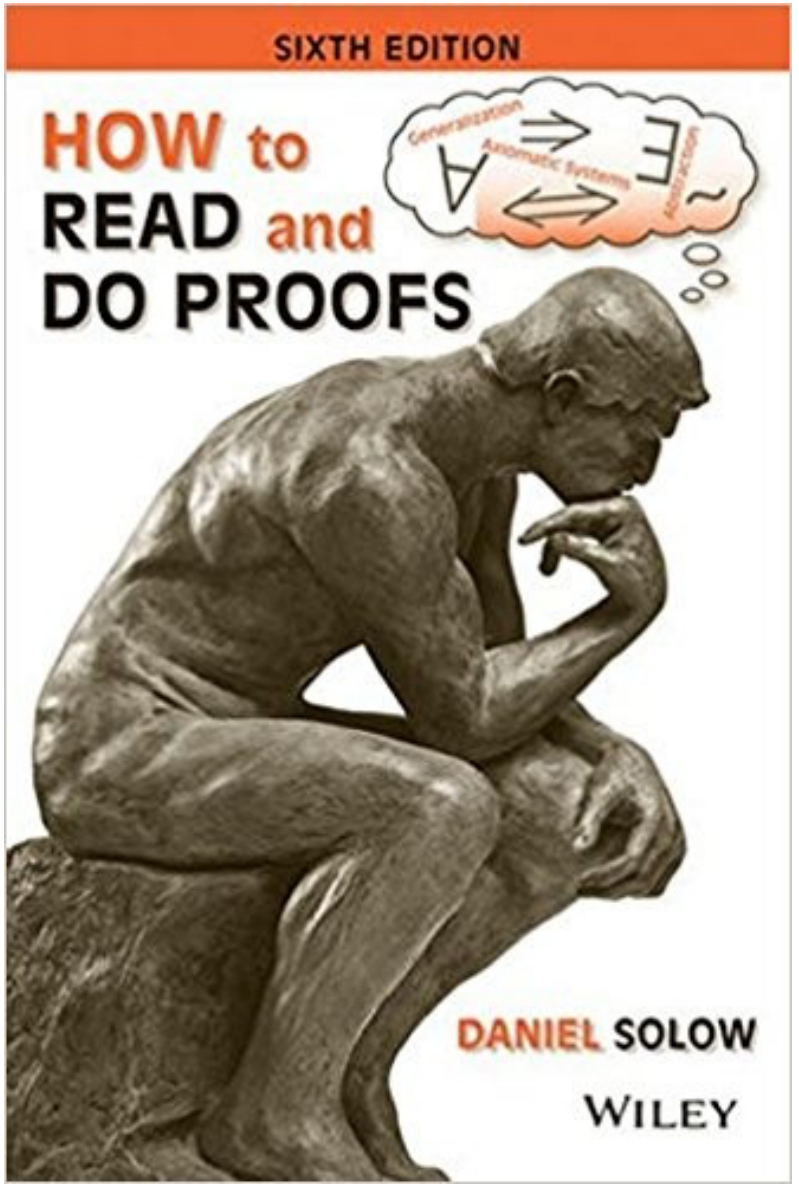
Some problem sets will have small coding components. We'll also reference some concepts from CS106B, particularly recursion, throughout the quarter.

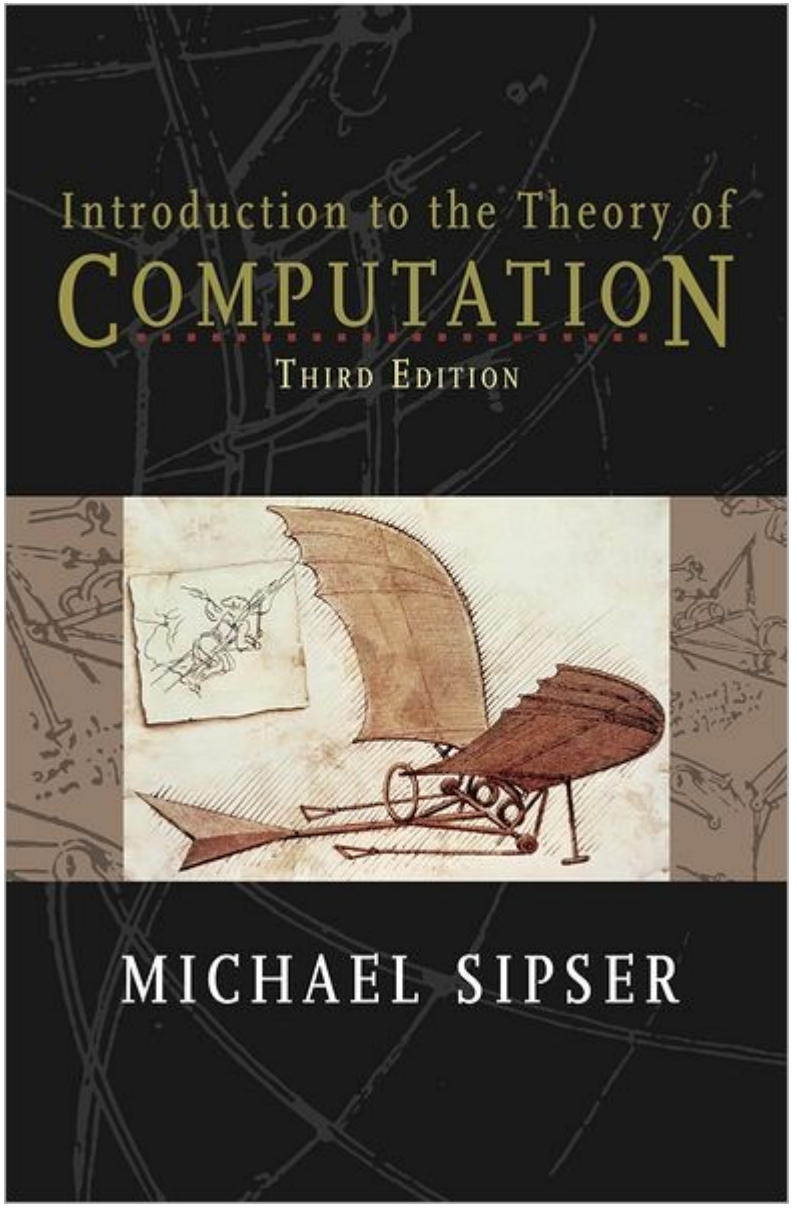
There aren't any math prerequisites for this course – high-school algebra should be enough!

Problem Set 0

- Problem Set 0 went out on Tuesday. It's due this ***Friday* at 1pm**. (Other problem sets will be due **Thursdays at 1pm**.)
  - Even though this just involves setting up your compiler and submitting things, please start this one early. If you start things on Friday morning, we can't help you troubleshoot Qt Creator issues!

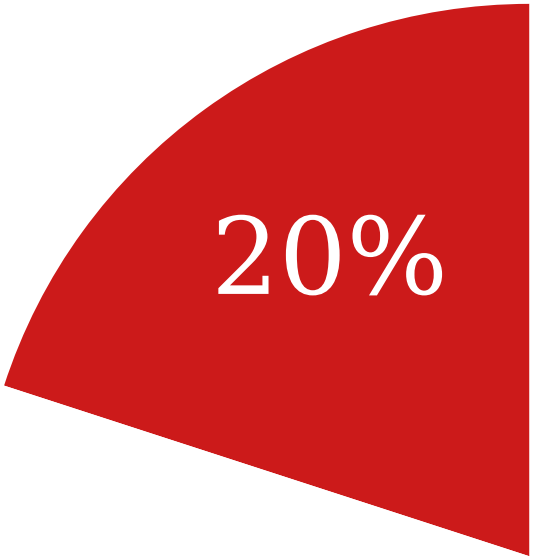
Recommended Reading





Grading

Grading

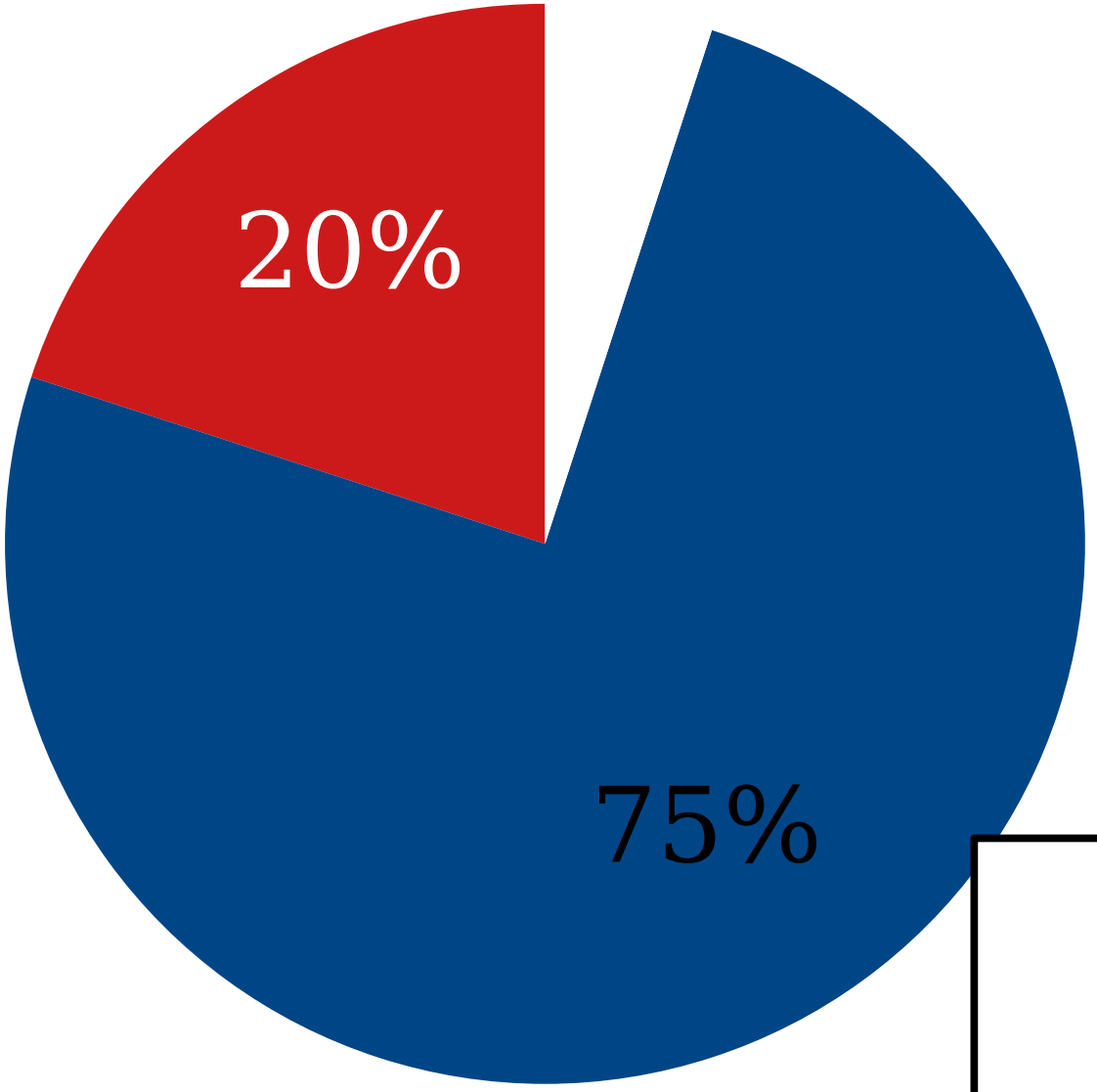


Problem Sets

Eight Problem Sets

Problem sets may be completed individually or in pairs (except PS0).

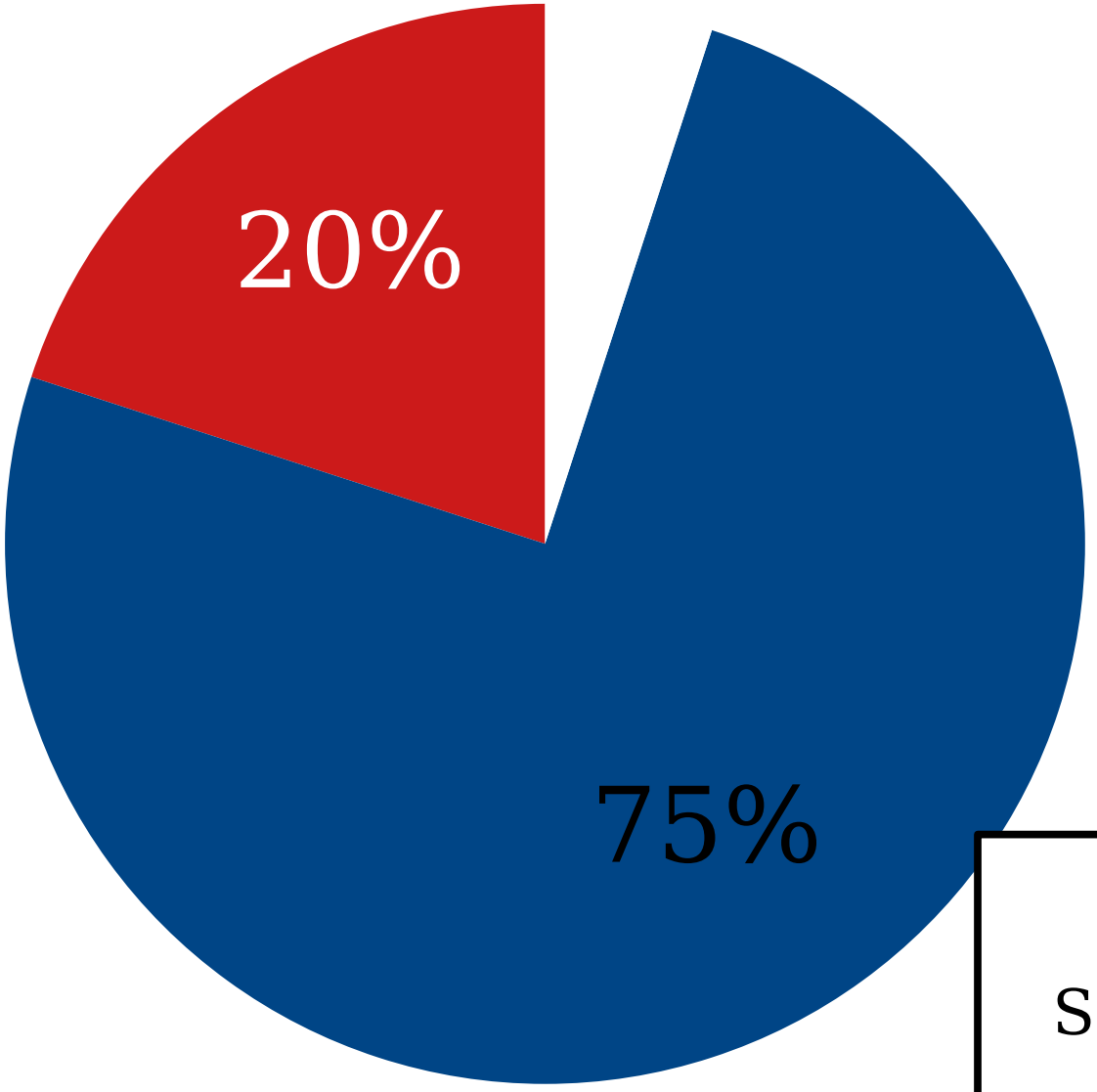
Grading



Midterm Exam

Tuesday, July 21st,
3:00PM - 6:00PM

Grading

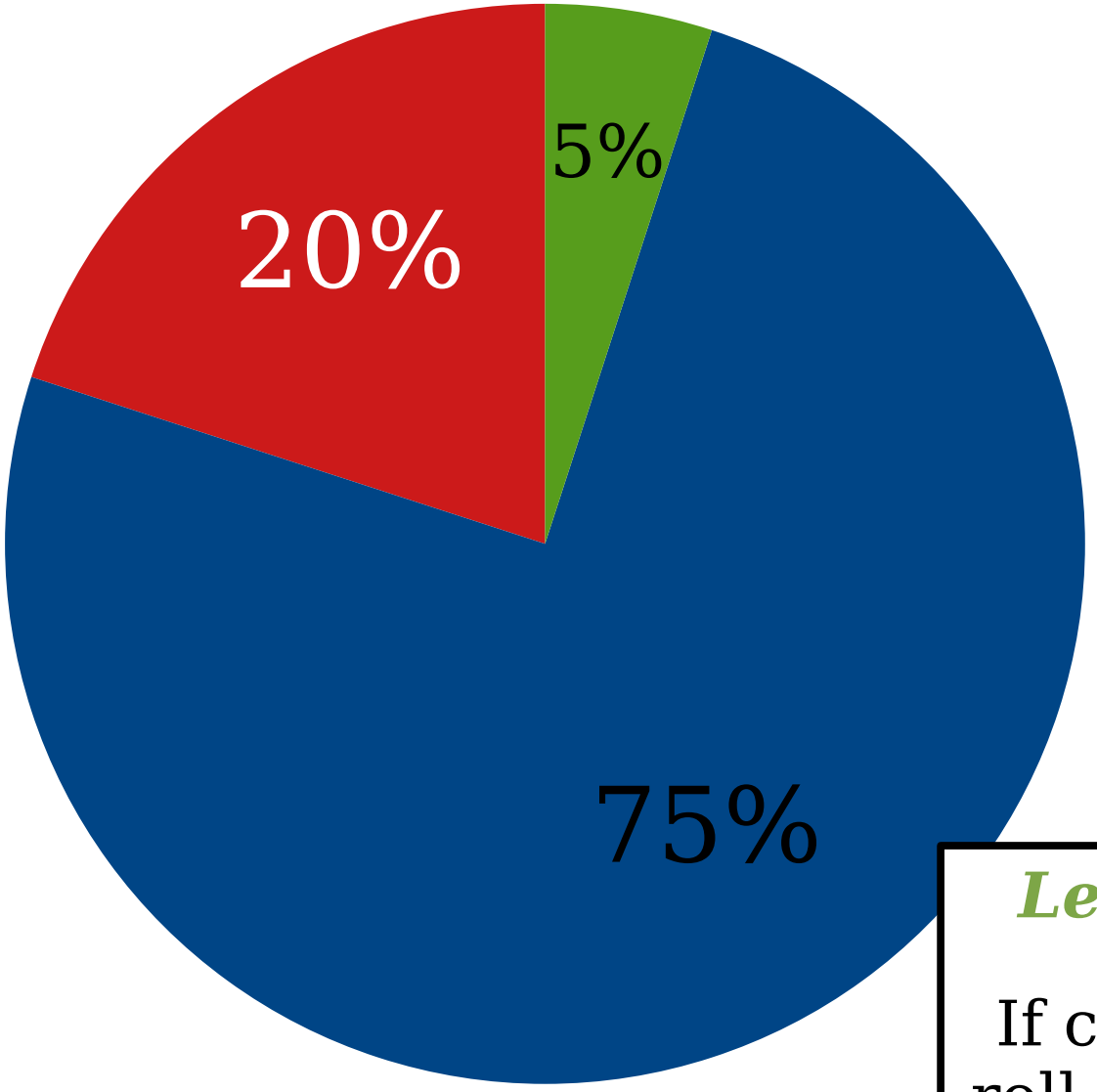


- Problem Sets
- Exams
- Lecture Participation

Final Exam

Saturday, August 15th,
3:30PM - 6:30PM

Grading



- Problem Sets
- Exams
- Lecture Participation

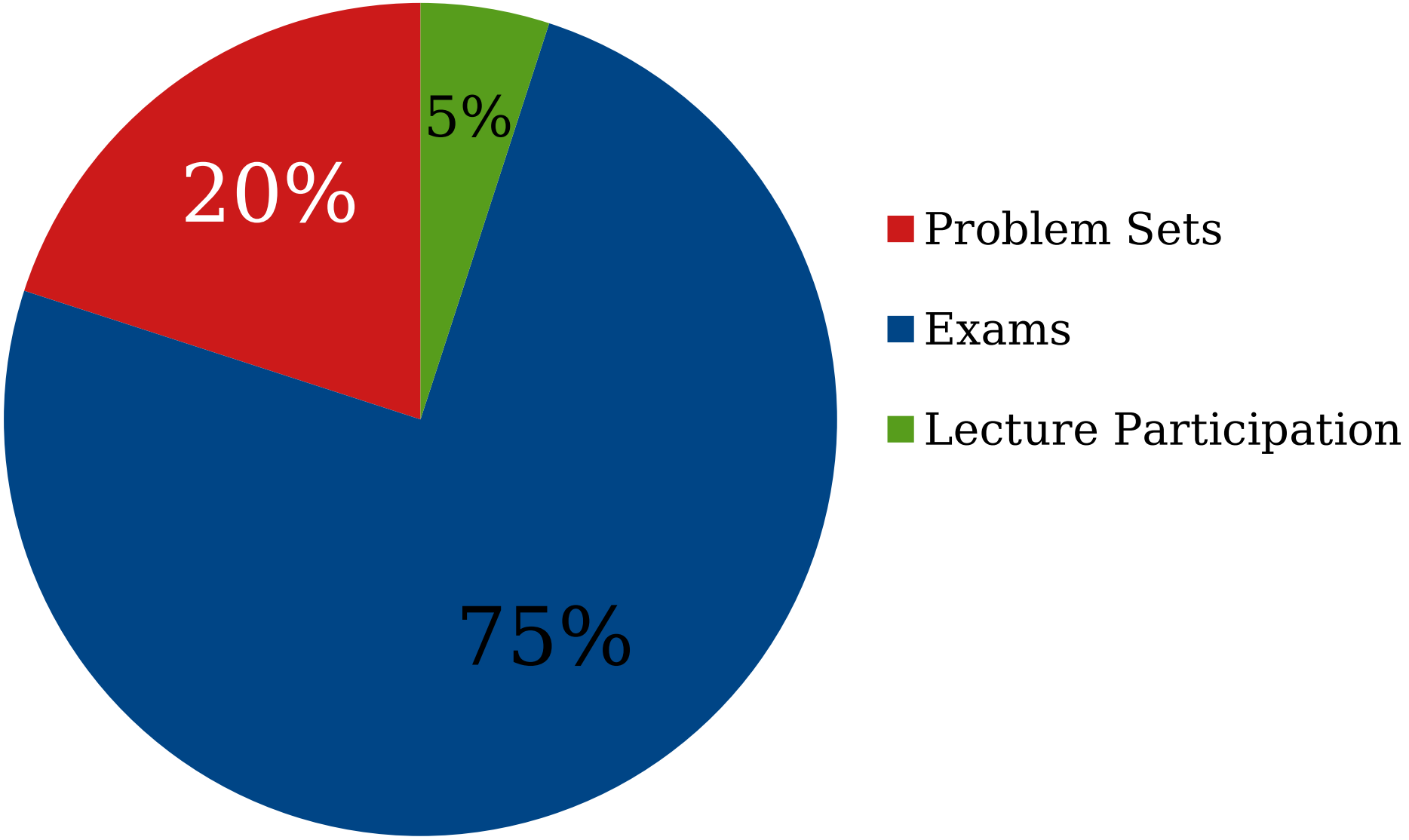
Lecture Participation

If cannot attend, can roll 5% into Final

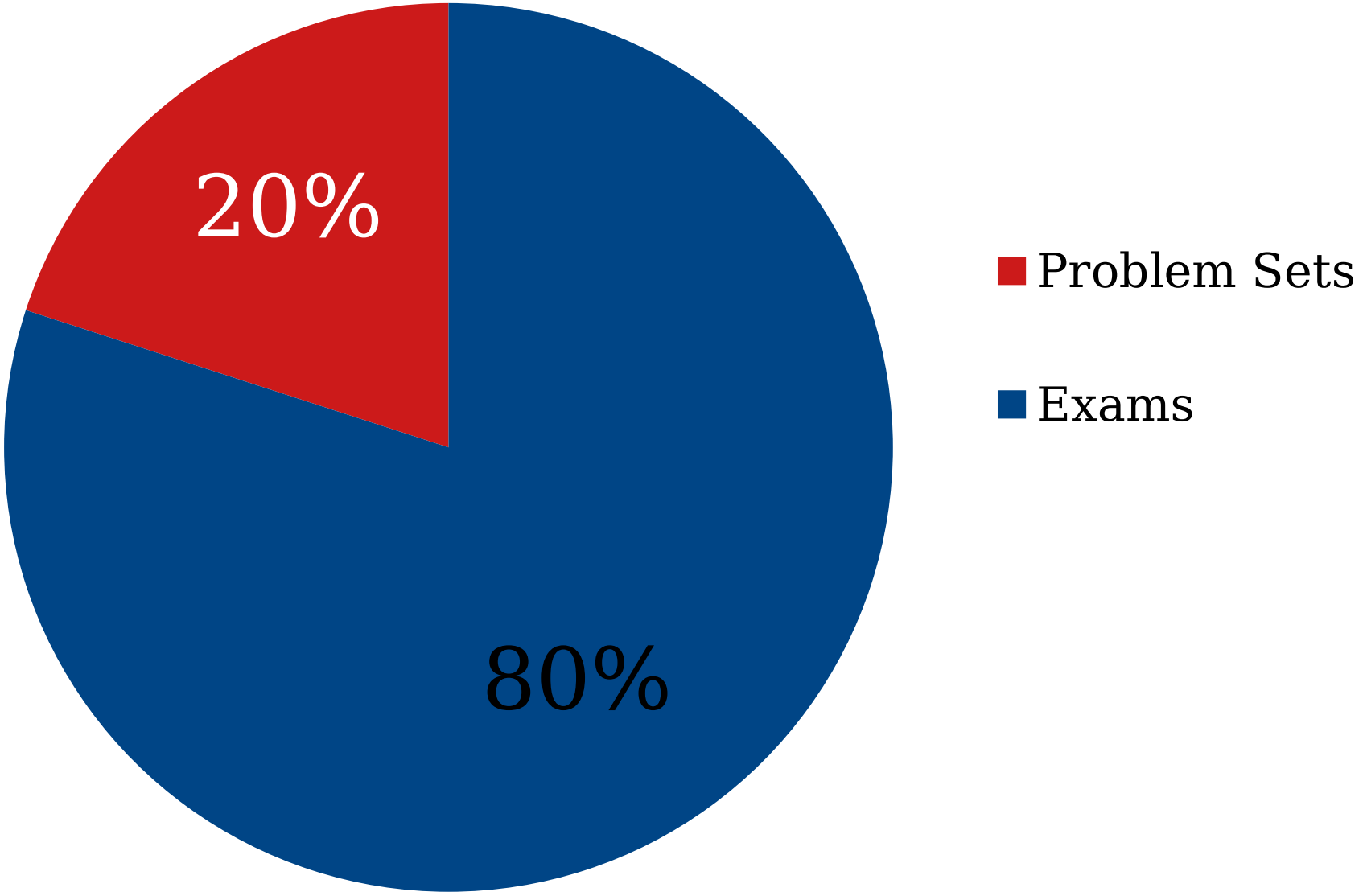
Lecture Participation

- Lecture attendance/participation is recorded via Poll Everywhere.
- Submit answers to all questions during a lecture (regardless of response correctness) to receive credit.
- 3 excused absences across the quarter.
- Lecture attendance is expected, please contact Robyn otherwise
  - There will be an option to substitute your final exam instead of that 5%
  - If you are part of CGOE, we will renormalize the remaining 95% of your grade back up to 100%.

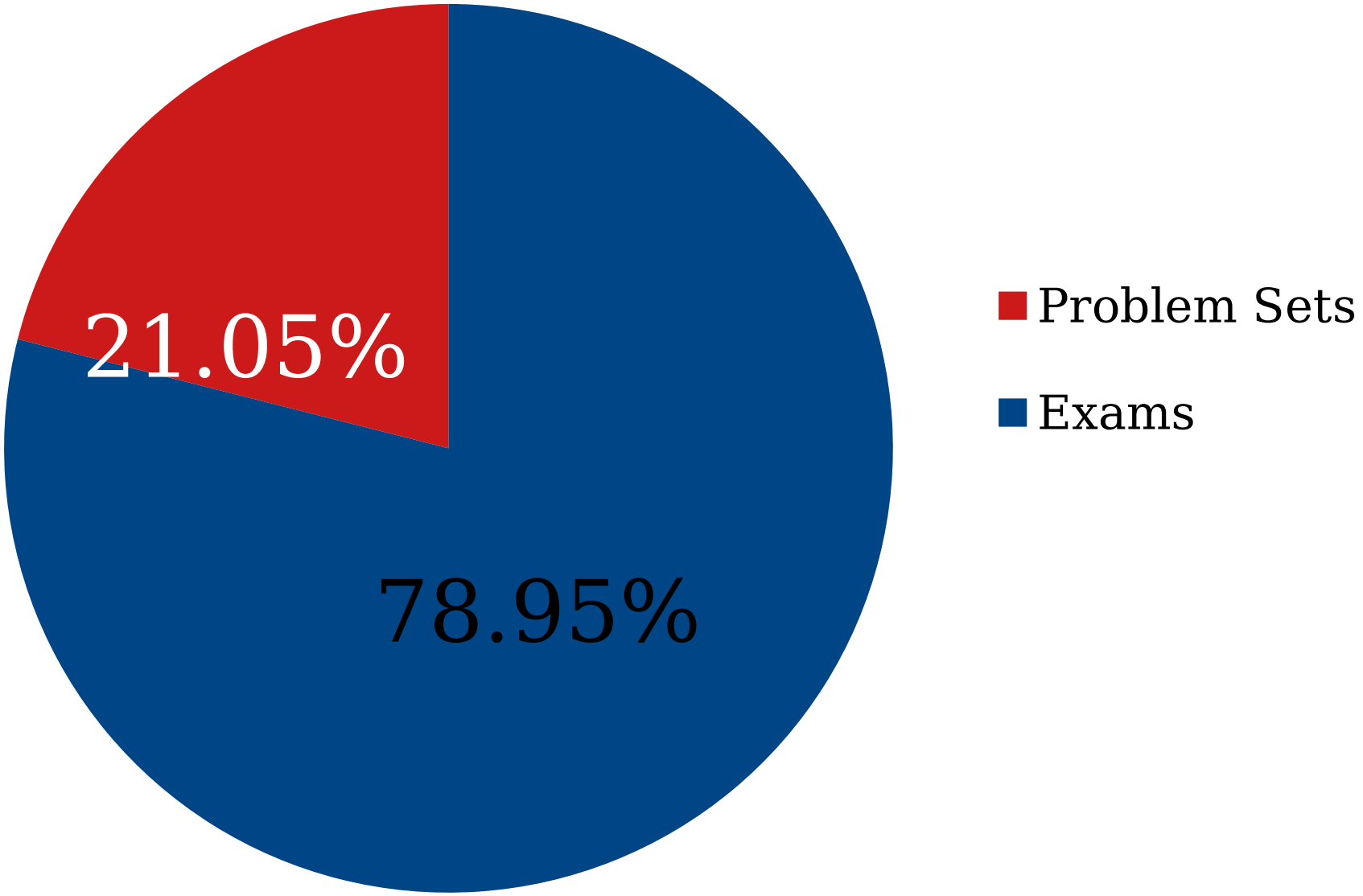
Grading



Alternate Grading Breakdown



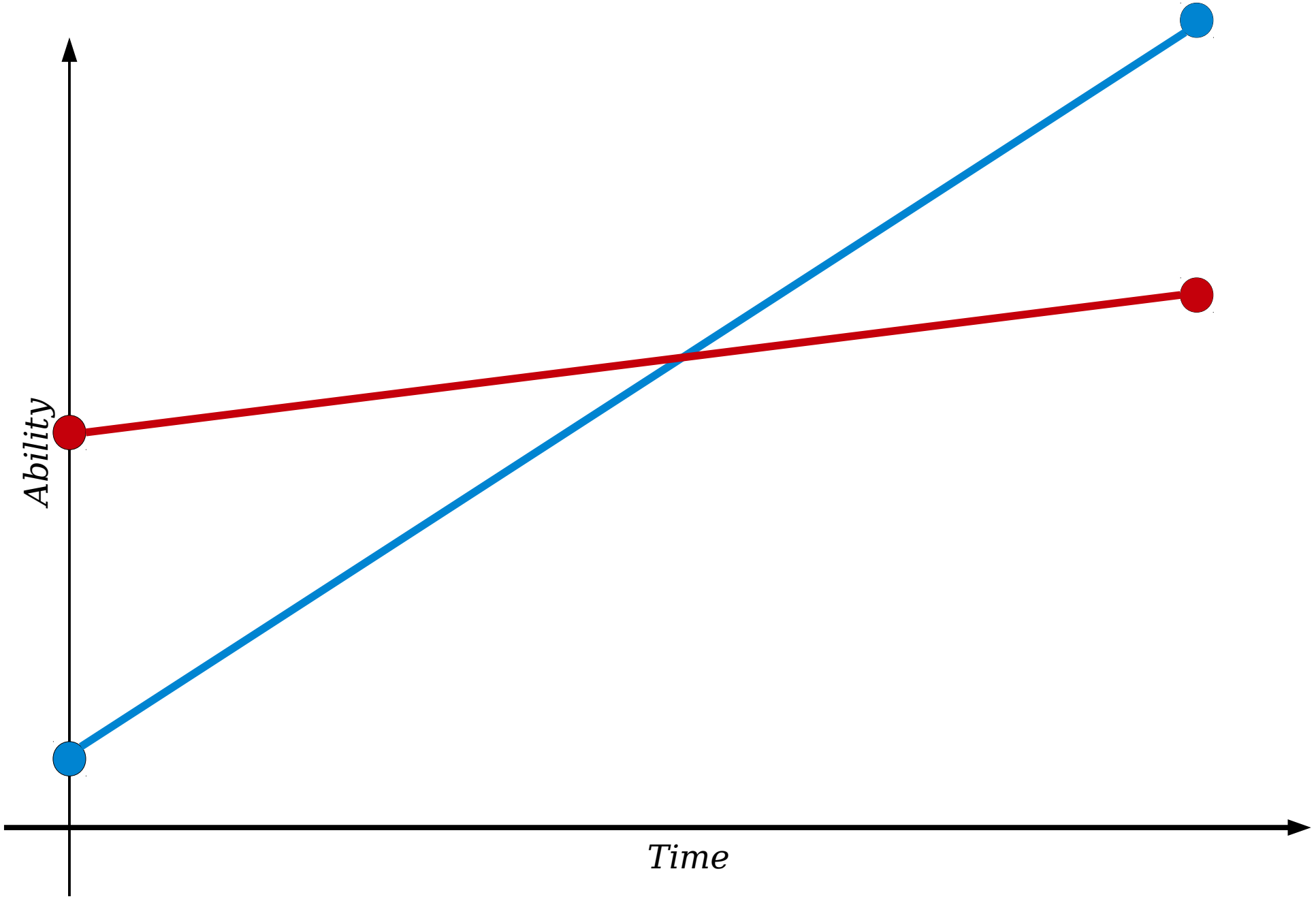
Alternate Grading Breakdown (CGOE)



How to Succeed in CS103

Proof-Based Mathematics

- Most high-school math classes – with the exception of geometry – focus on *calculation*.
- CS103 focuses on *argumentation*.
- Your goal is to *see why things are true,* not *check that they work in a few cases*.
- Be curious! Ask questions. Try things out on your own. You'll learn this material best if you engage with it and refuse to settle for a “good enough” understanding.



"A little slope makes up for a lot of *y*-intercept."

- John Ousterhout

Don't Psych Yourself Out

- It is ***perfectly normal*** to get stuck or be confused when learning math.
- We've all been on the Struggle Bus. Don't be afraid to ask for help!

Getting Good at Math

- ***Engage with the concepts.*** Work through lots of practice problems. Play around with new terms and definitions on your own time to see how they work.
- ***Ask for help when you need it.*** We're here to help you. We want you to succeed, so let us know what we can do to help!
- ***Work in groups.*** Get help from the TAs, your problem set partner, and other students.

We've got a big journey ahead of us.

Let's get started!

Introduction to Set Theory

“CS103 students”

“Cool people”

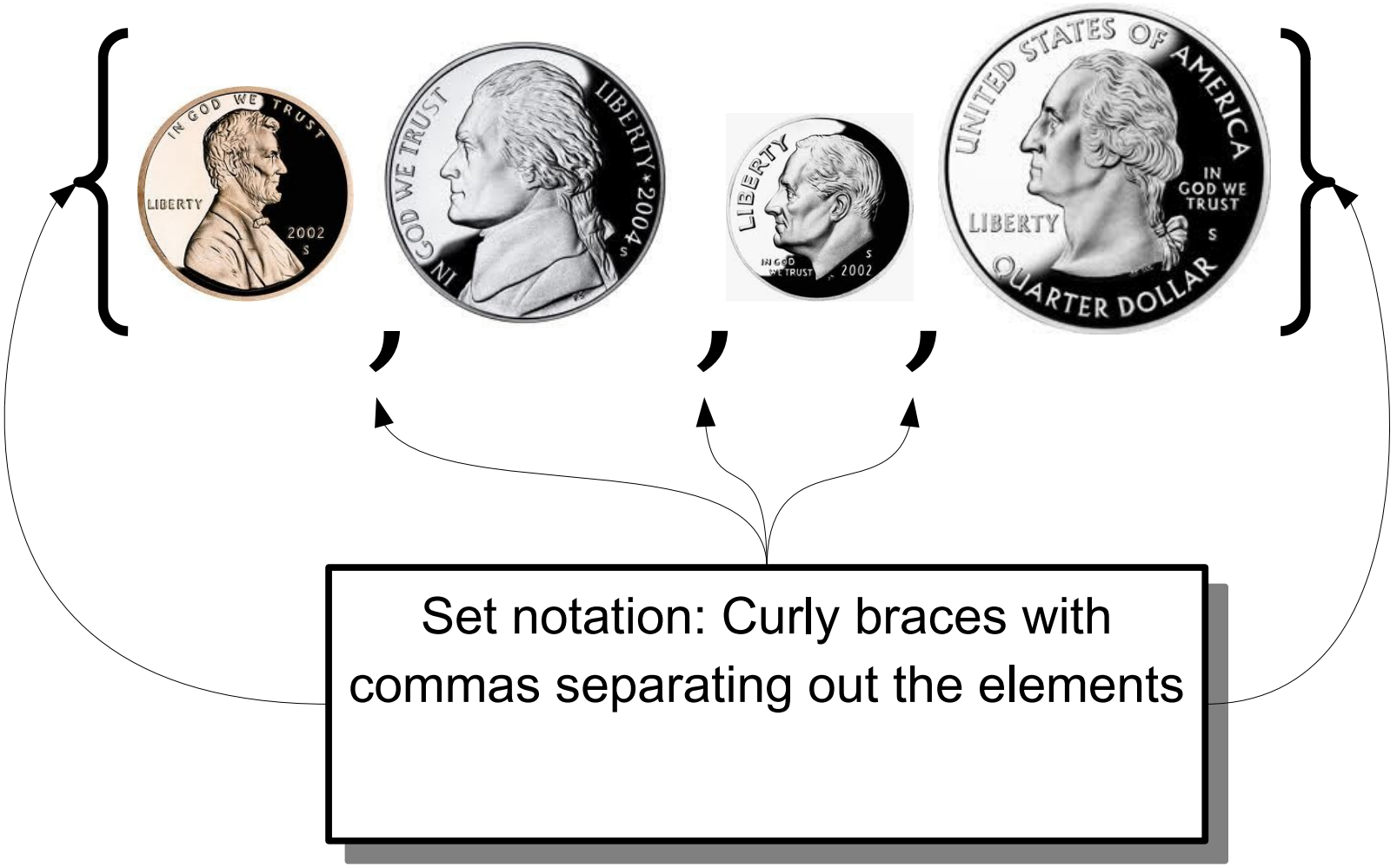
“The chemical elements”

“Cute animals”

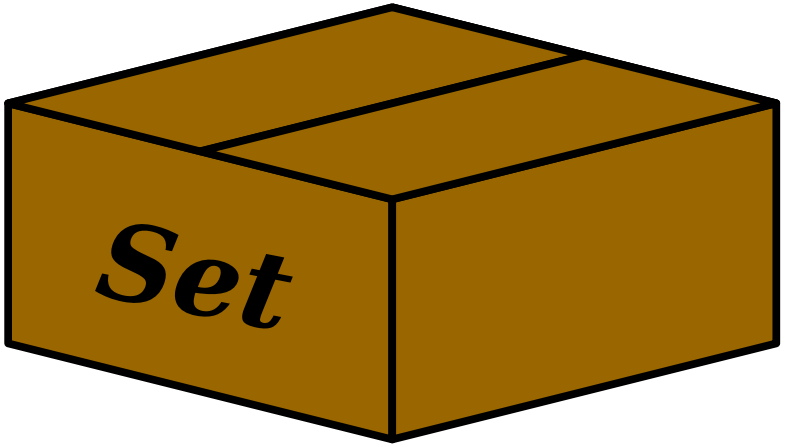
“US coins”

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

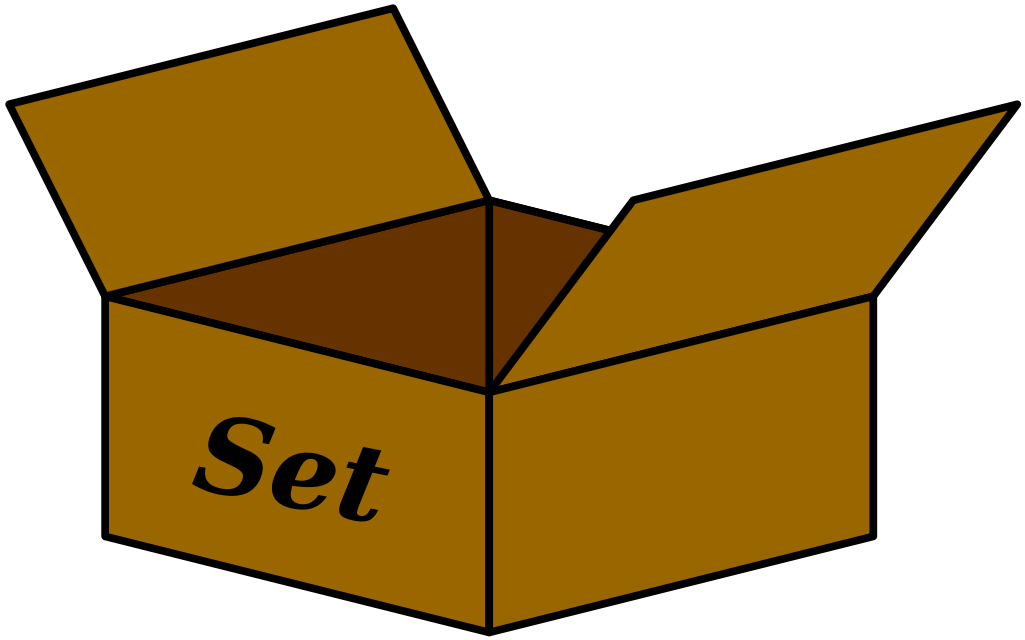
A ***set*** is an unordered collection of distinct objects, which may be anything, including other sets.



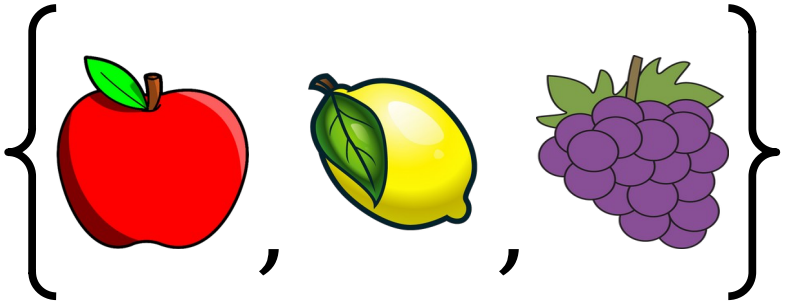
A ***set*** is an unordered collection of distinct objects, which may be anything, including other sets.

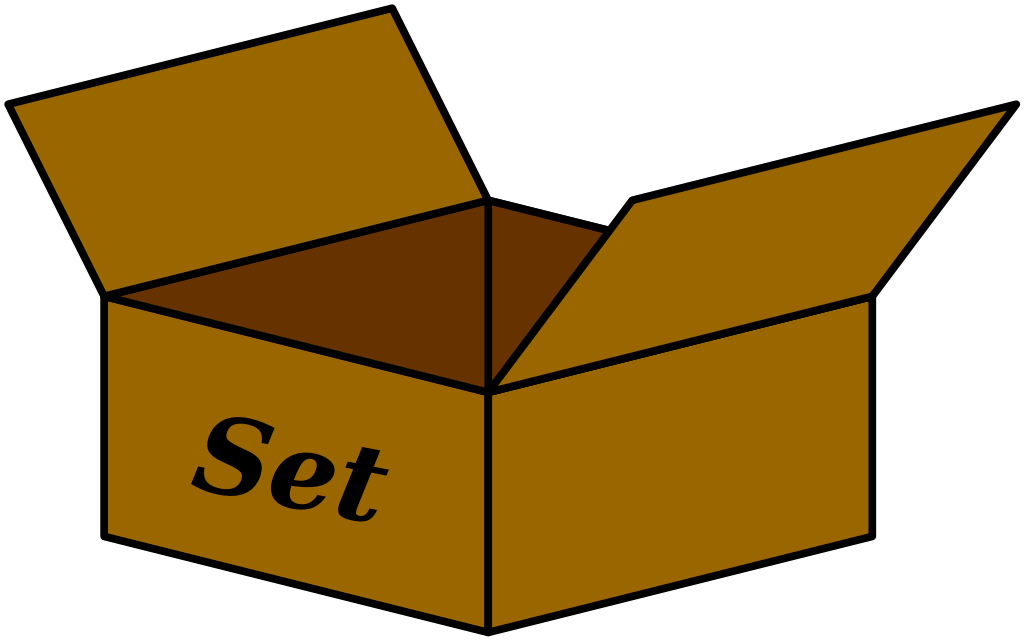


Two sets are equal when they have the same contents, ignoring order.

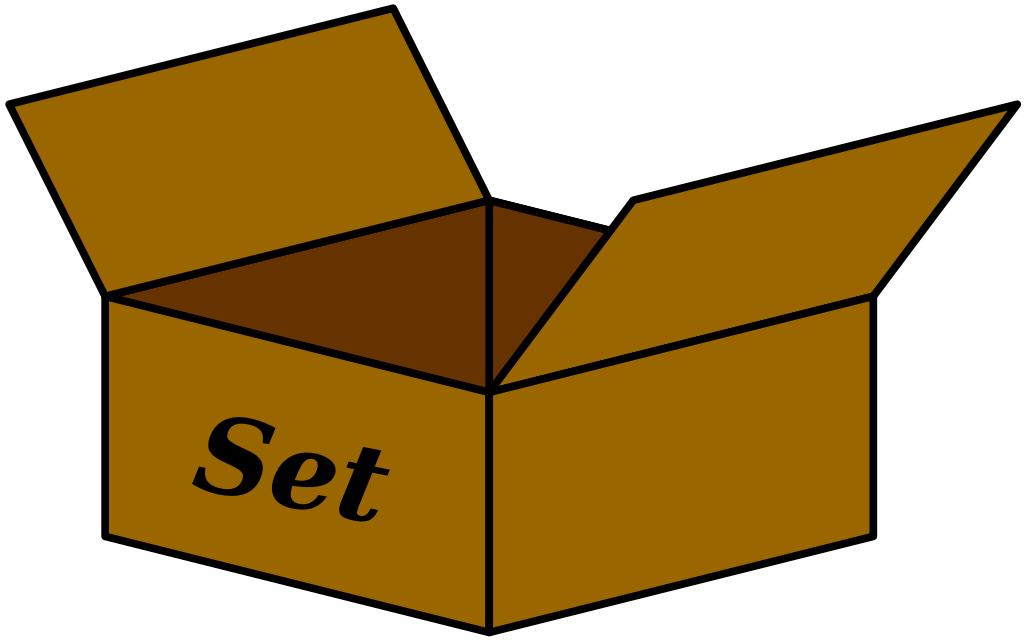


Two sets are equal when they have the same contents, ignoring order.

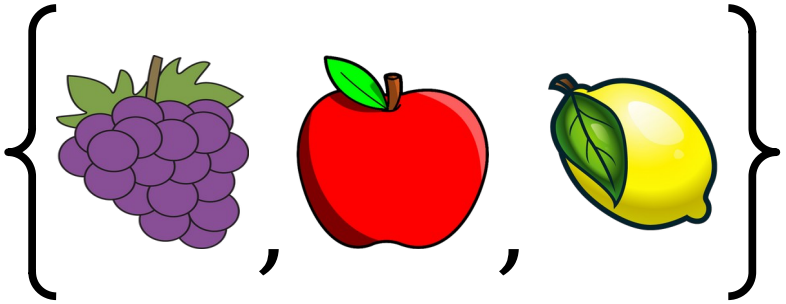


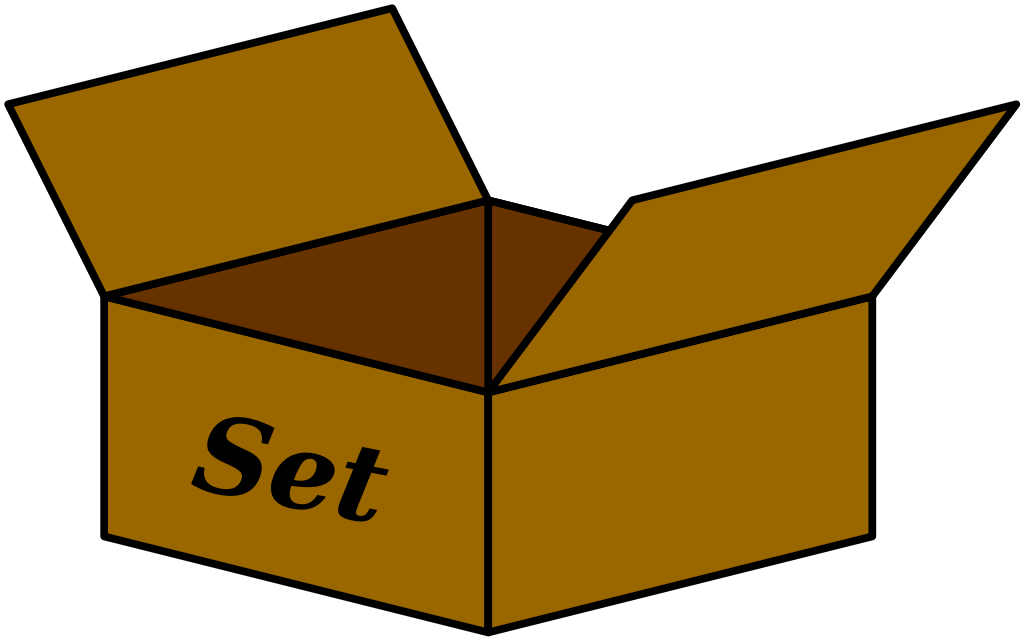


Two sets are equal when they have the same contents, ignoring order.

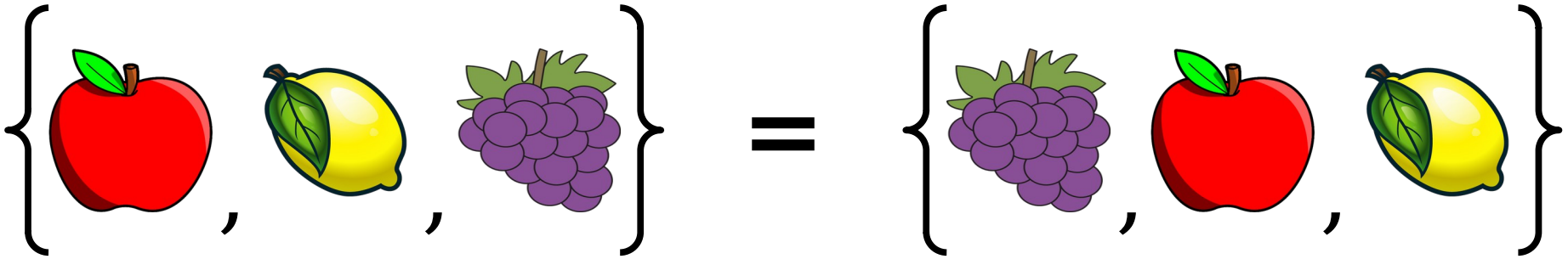


Two sets are equal when they have the same contents, ignoring order.



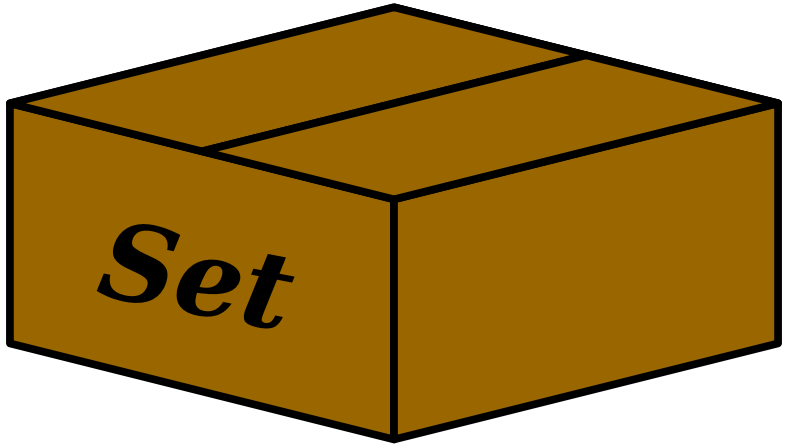


Two sets are equal when they have the same contents, ignoring order.

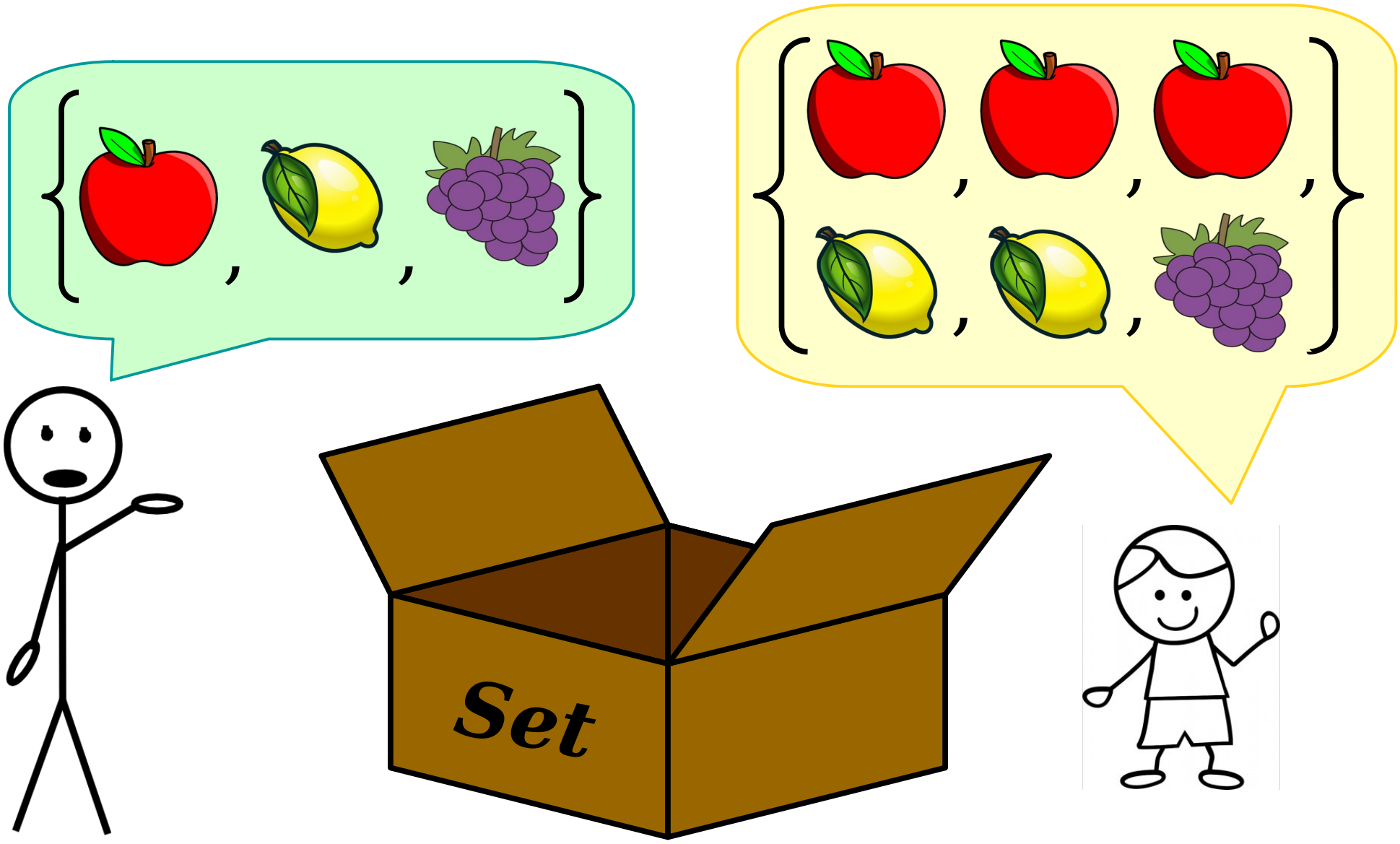


These are two different descriptions of exactly the same set.

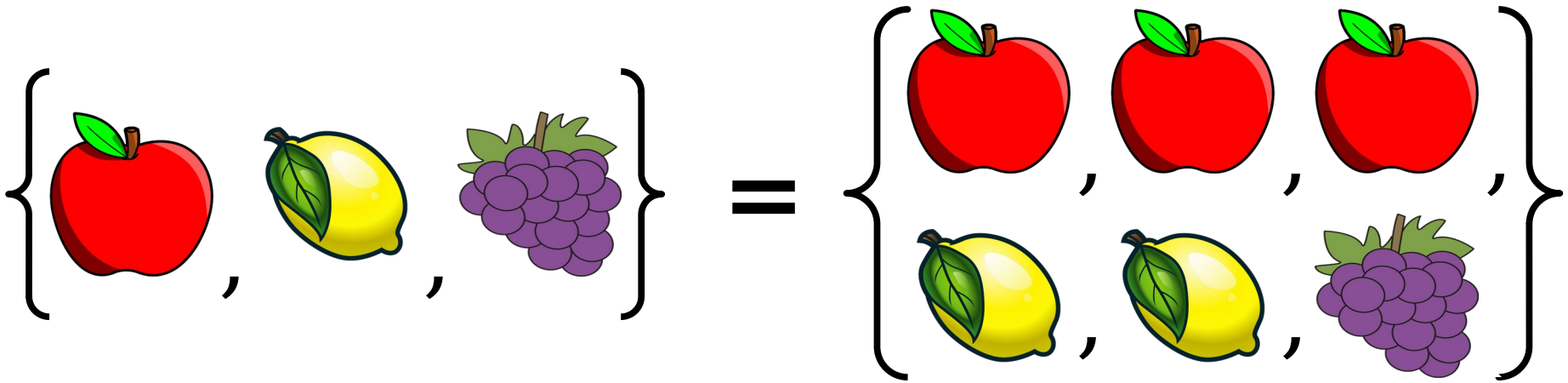
Two sets are equal when they have the same contents, ignoring order.



Sets cannot contain duplicate elements.
Any repeated elements are ignored.



Sets cannot contain duplicate elements.
Any repeated elements are ignored.



These are two different descriptions of exactly the same set.

Sets cannot contain duplicate elements.
Any repeated elements are ignored.

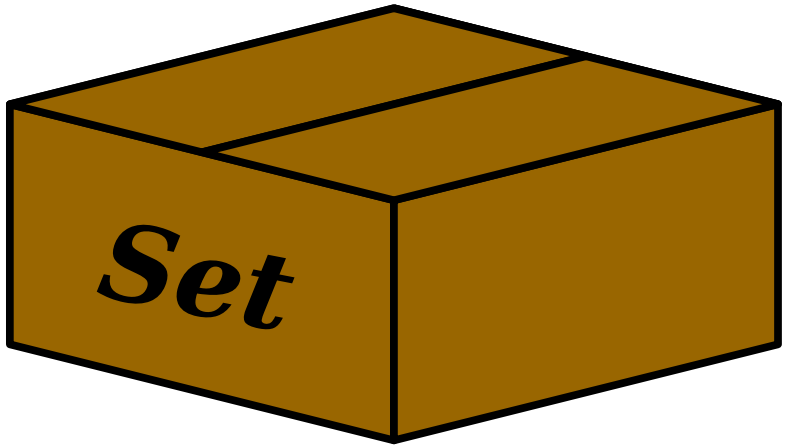
The objects that make up a set are called the ***elements*** of that set.

The objects that make up a set are called the ***elements*** of that set.

The objects that make up a set are called the ***elements*** of that set.

This symbol means “is not an element of.”

The objects that make up a set are called the ***elements*** of that set.

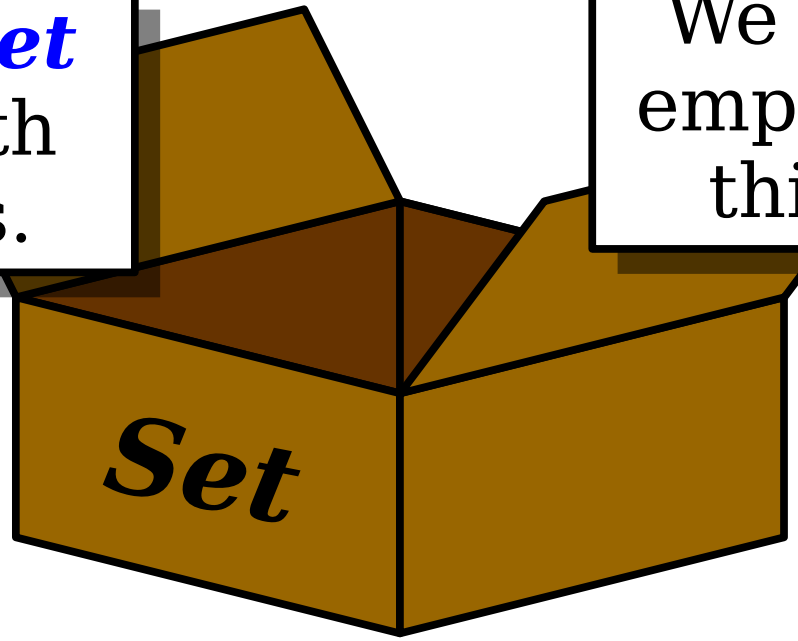


Sets can contain any number of elements.

$\{\ \} = \emptyset$

The ***empty set*** is the set with no elements.

We denote the empty set using this symbol.



Sets can contain any number of elements.

$$1 \stackrel{?}{=} \{1\}$$

Question: Are these two objects equal?

Discuss with your neighbors!

$$1 \stackrel{?}{=} \{1\}$$

Question: Are these objects equal?

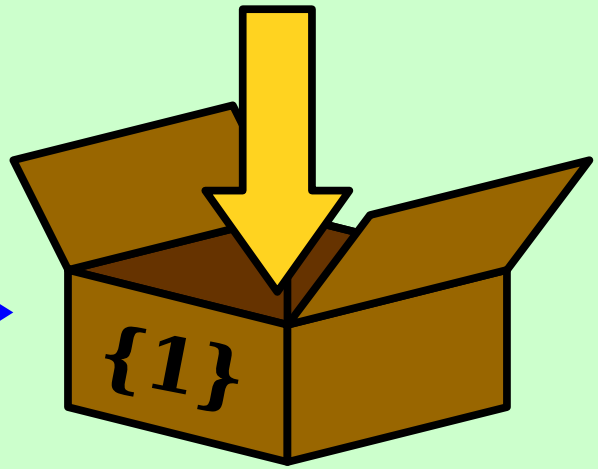
$$1 \stackrel{?}{=} \{1\}$$

This is a number.

1

1

This is a set.
It contains a number.



Question: Are these objects equal?

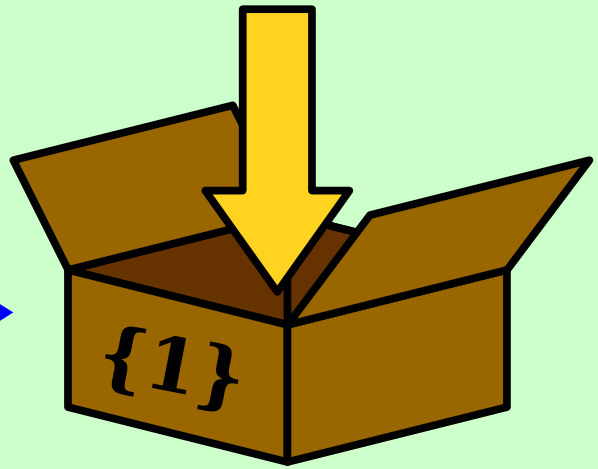
$$1 \neq \{1\}$$

This is a number.

1

1

This is a set.
It contains a number.



Question: Are these objects equal?

$$\emptyset \stackrel{?}{=} \{\emptyset\}$$

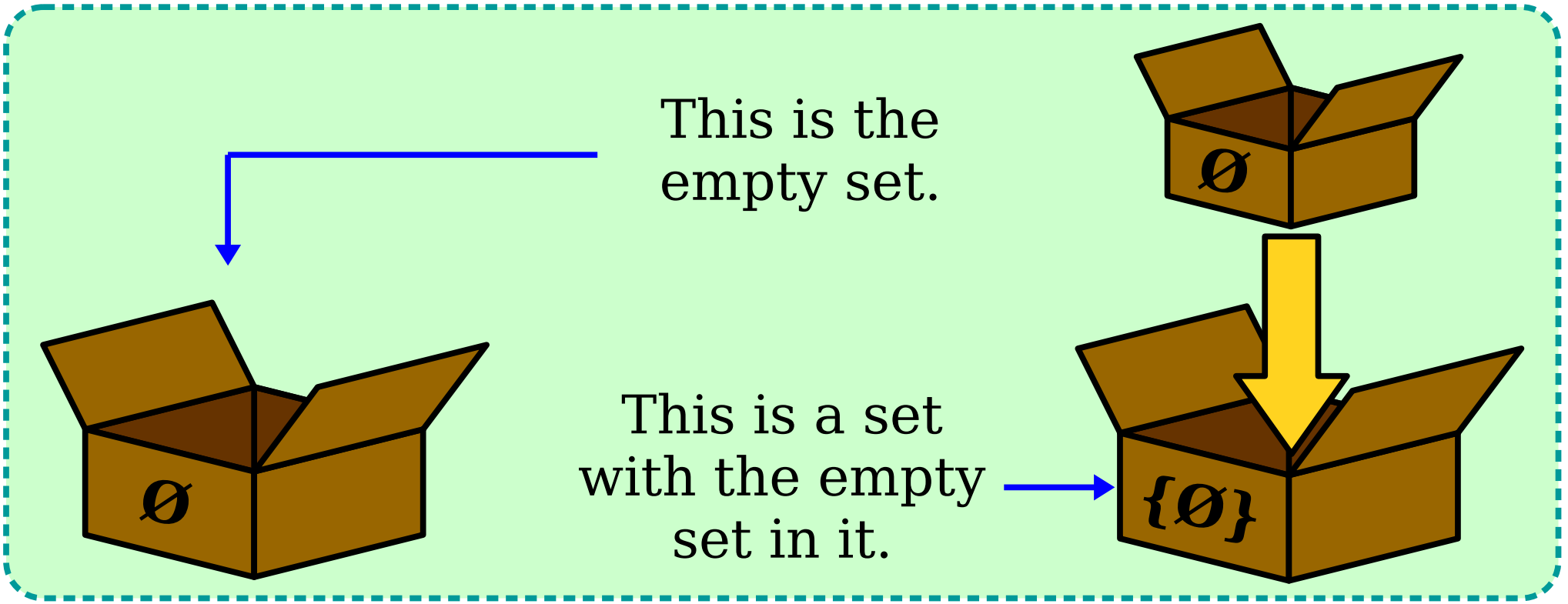
Question: Are these two objects equal?

Discuss with your neighbors!

$$\emptyset \stackrel{?}{=} \{\emptyset\}$$

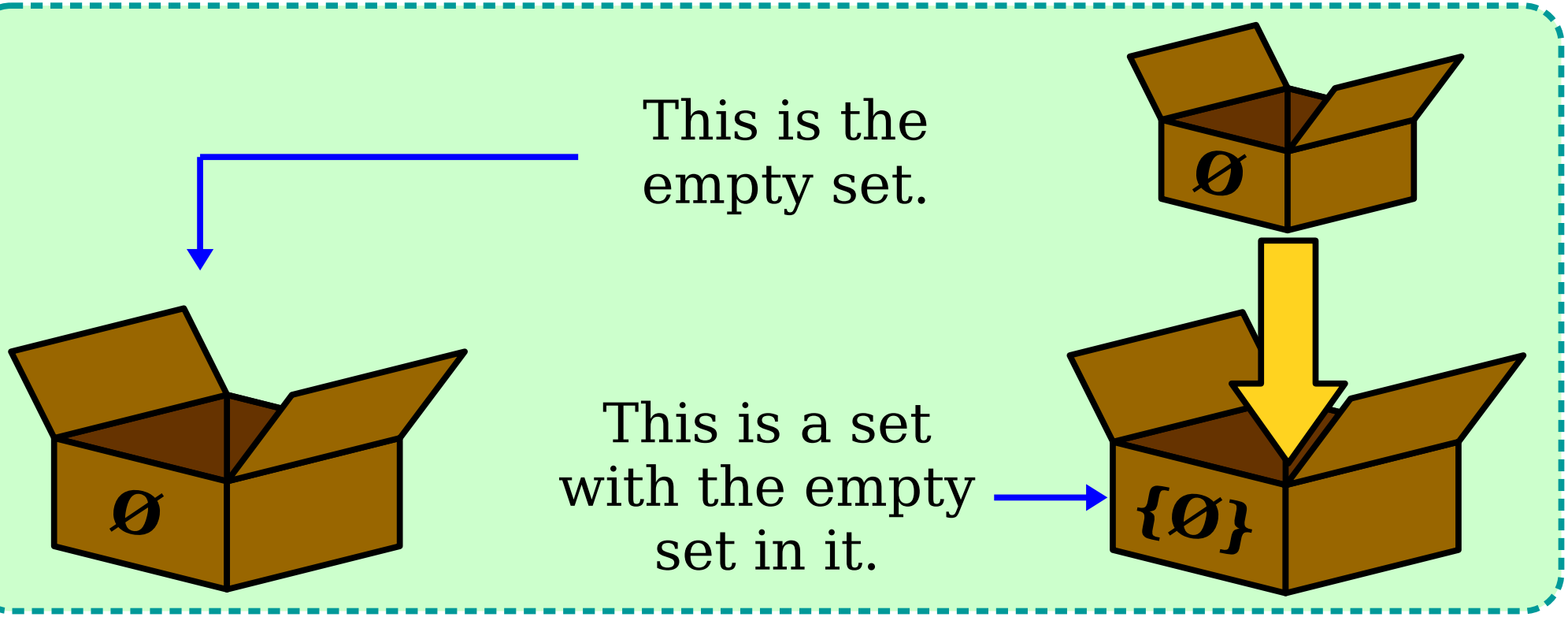
Question: Are these objects equal?

$$\emptyset \stackrel{?}{=} \{\emptyset\}$$



Question: Are these objects equal?

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



Question: Are these objects equal?

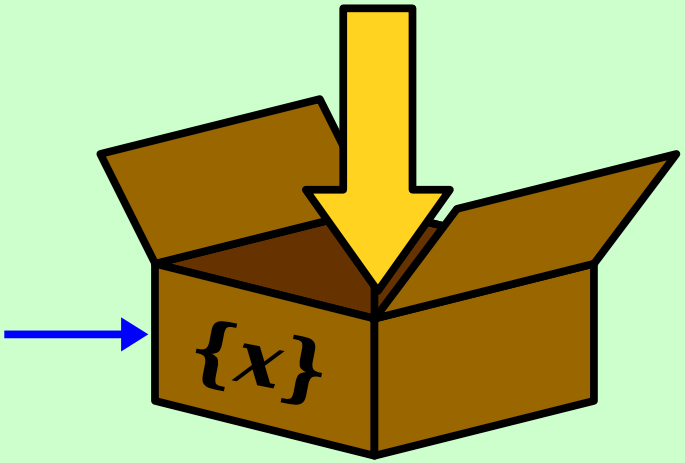
$$x \neq \{x\}$$

This is x itself.

x

x

This is a box that has x inside it.



No object x is equal to the set containing x.

Infinite Sets

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

  “The set of all even natural numbers.”

  “The set of all real numbers less than 137.”

  “The set of all negative integers.”

- To describe complex sets like these mathematically, we'll use ***set-builder notation***.

Even Natural Numbers

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

Even Natural Numbers

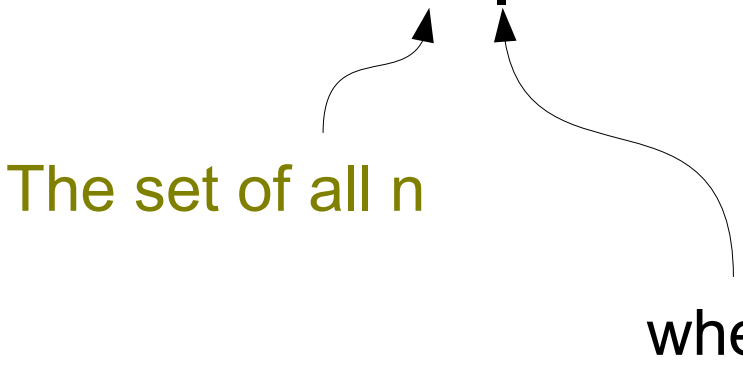
$$\{\ n \mid n \in \mathbb{N} \text{ and } n \text{ is even}\ \}$$

Even Natural Numbers

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

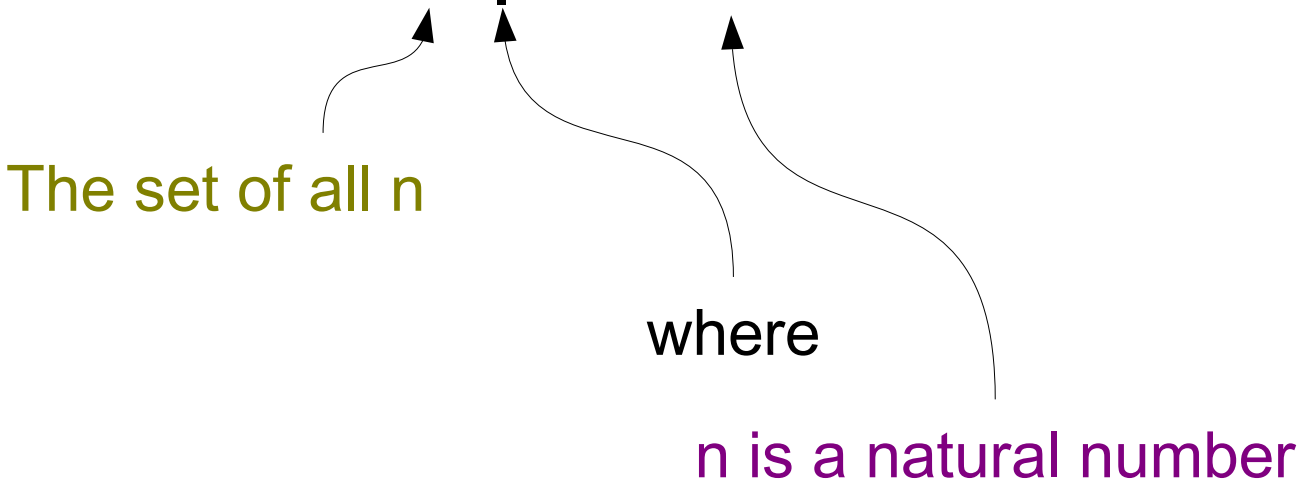
Even Natural Numbers

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

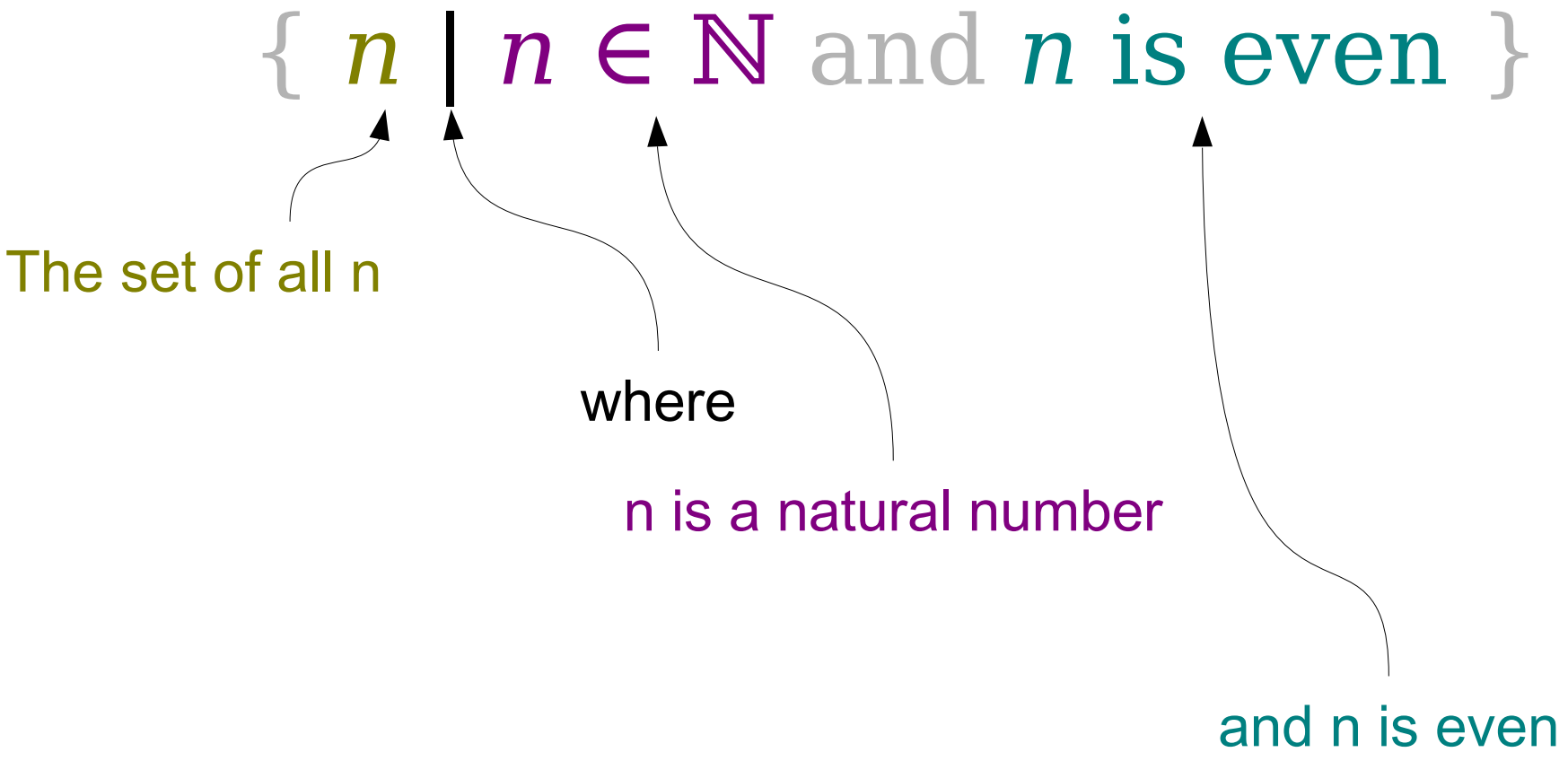


Even Natural Numbers

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

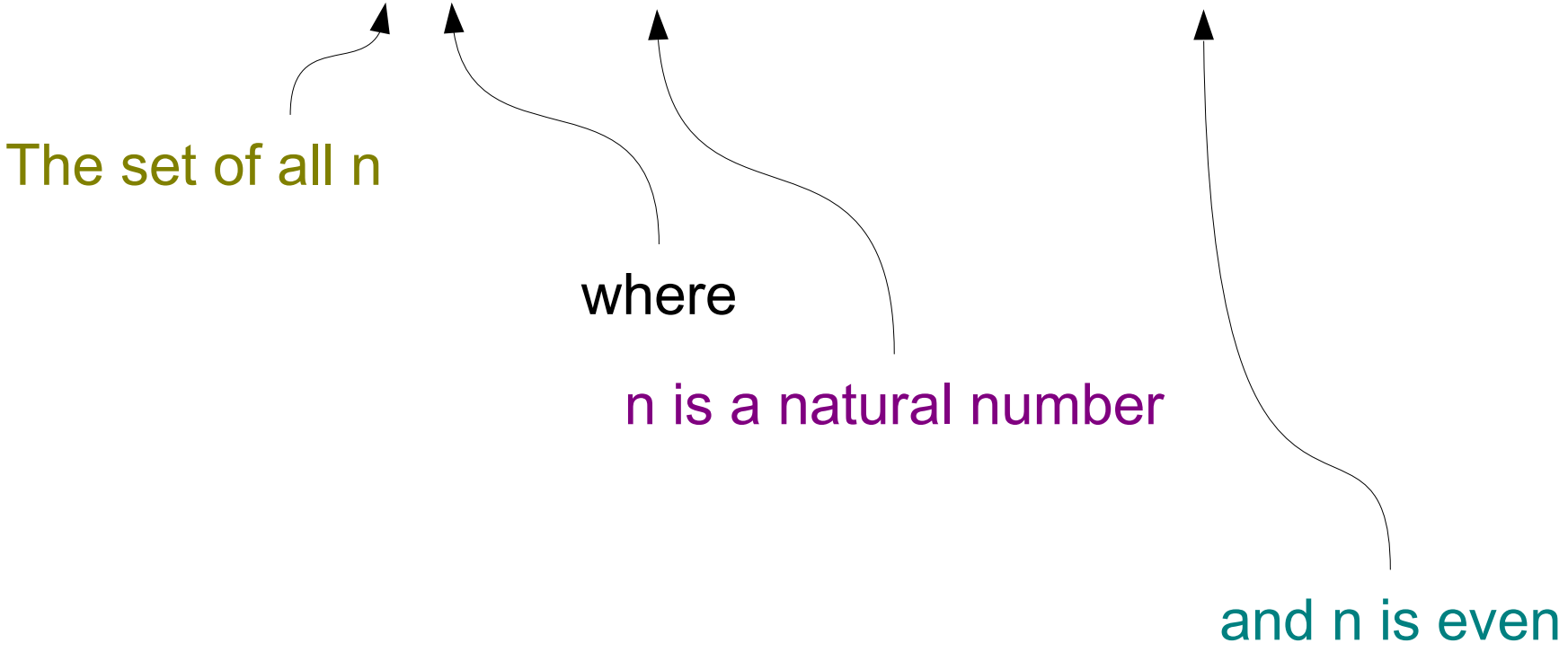


Even Natural Numbers



Even Natural Numbers

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



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

Set Builder Notation

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

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

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

- For example:

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

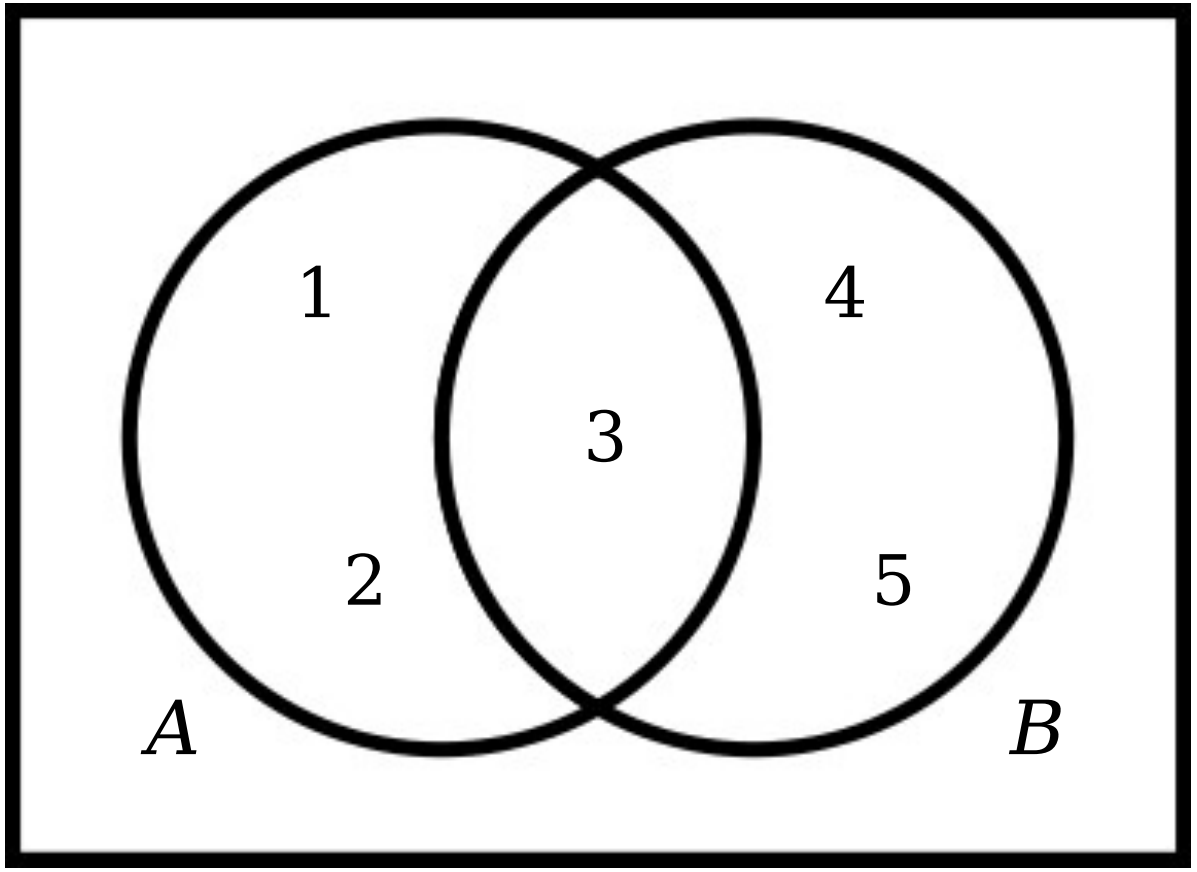
$\{\ C \mid C \text{ is a set of US currency}\ \}$

$\{\ r \in \mathbb{R} \mid r < 3\ \}$

$\{\ n \in \mathbb{N} \mid n < 3\ \}$ **(the set {0, 1, 2})**

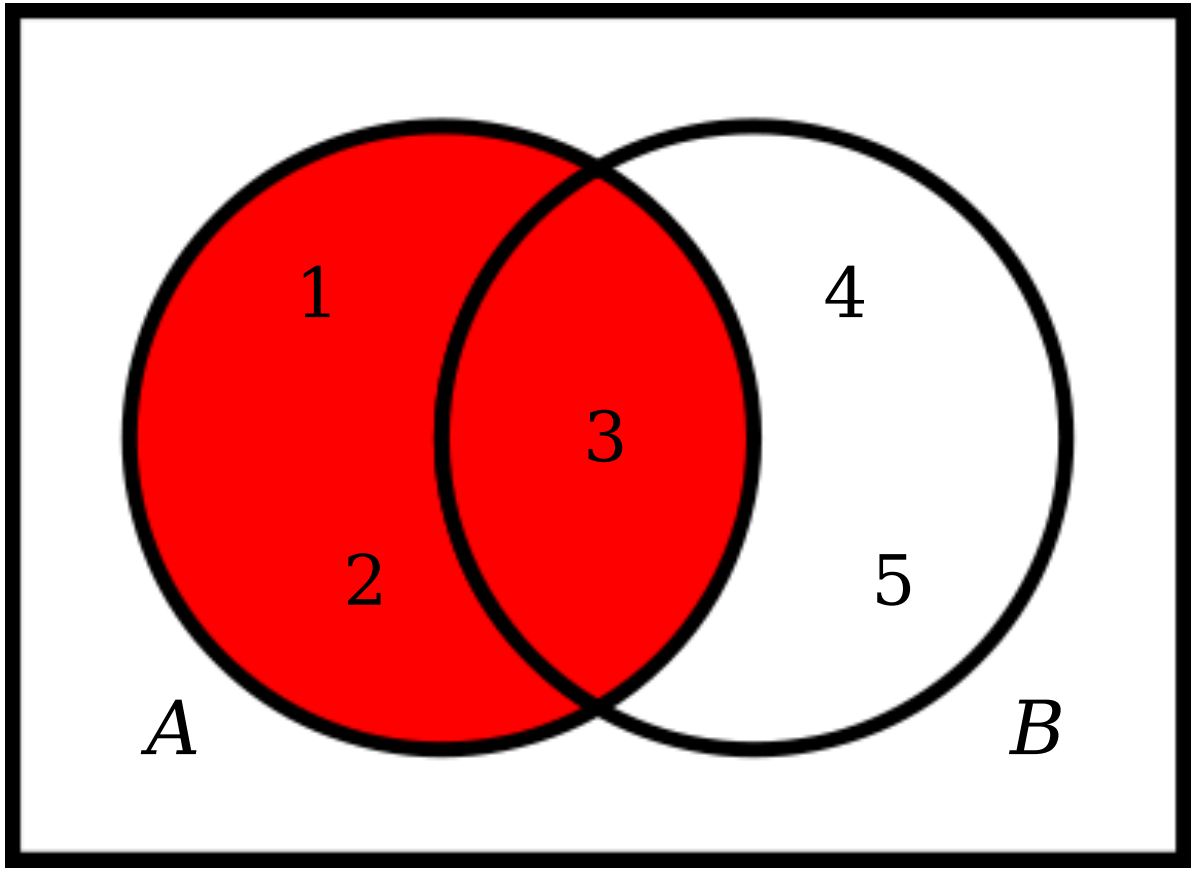
Combining Sets

Venn Diagrams



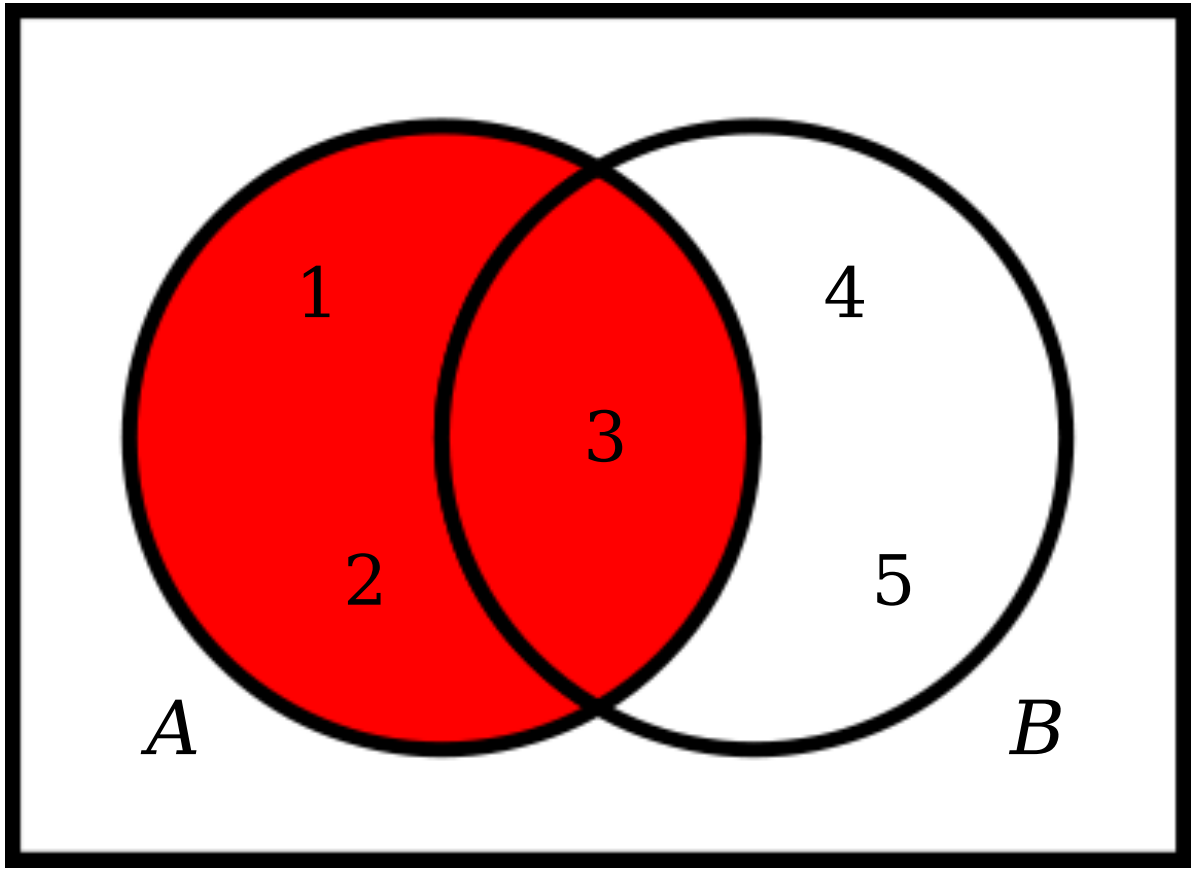
$A = \{ 1, 2, 3 \}$
$B = \{ 3, 4, 5 \}$

Venn Diagrams



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

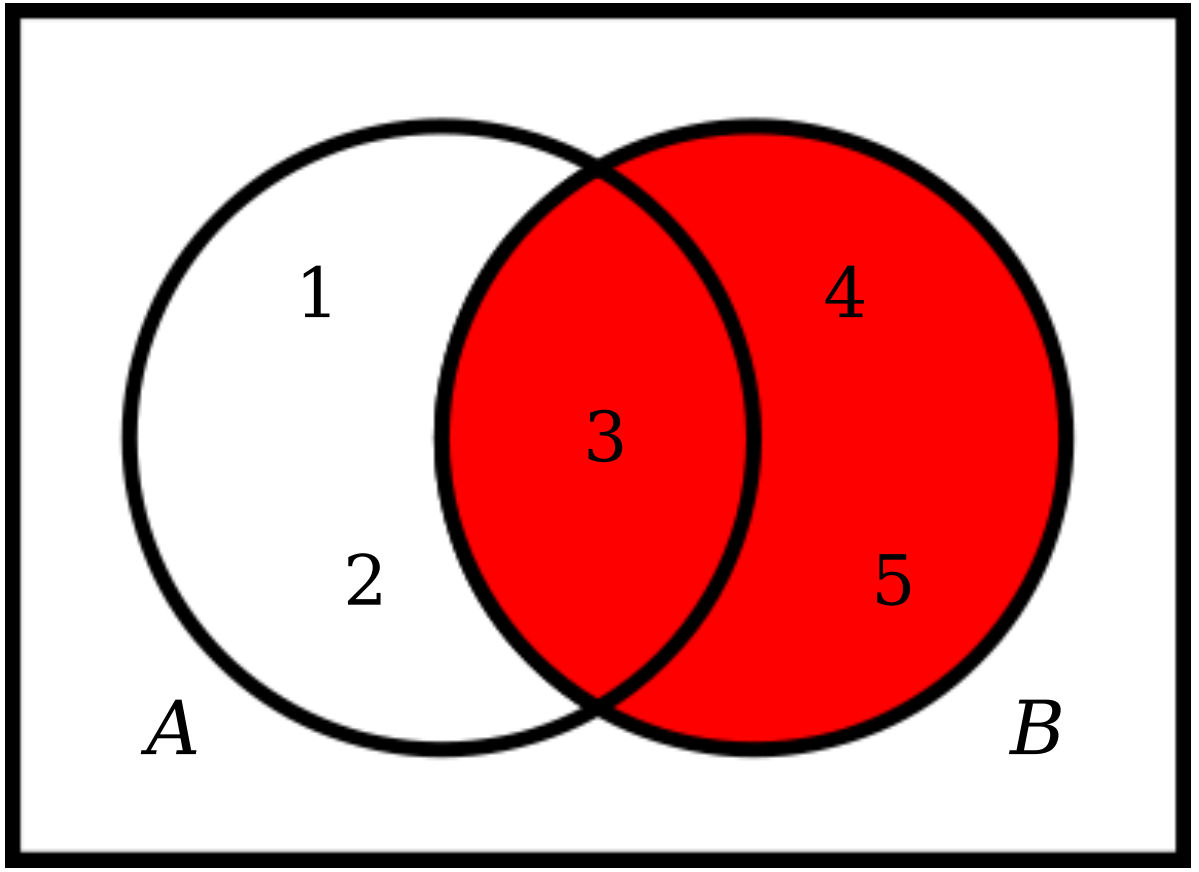
Venn Diagrams



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

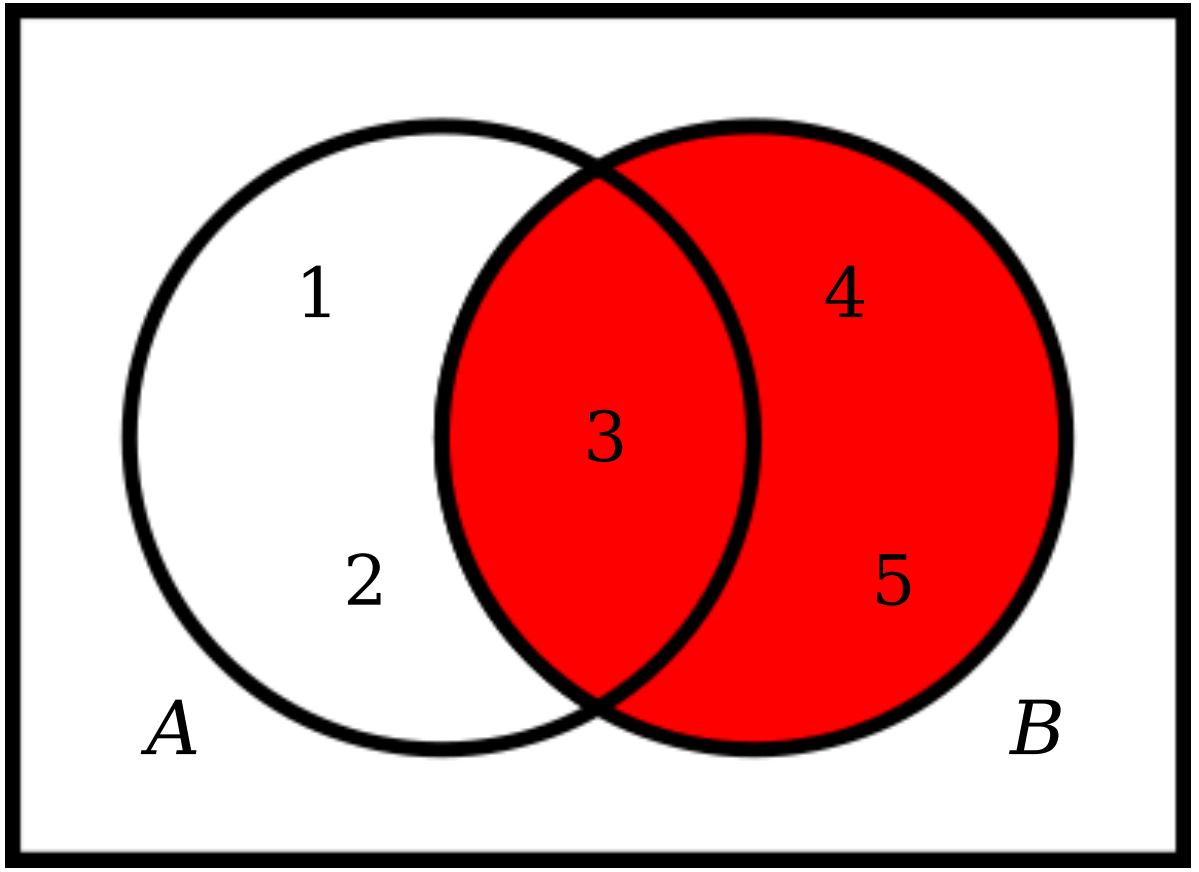
A

Venn Diagrams



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

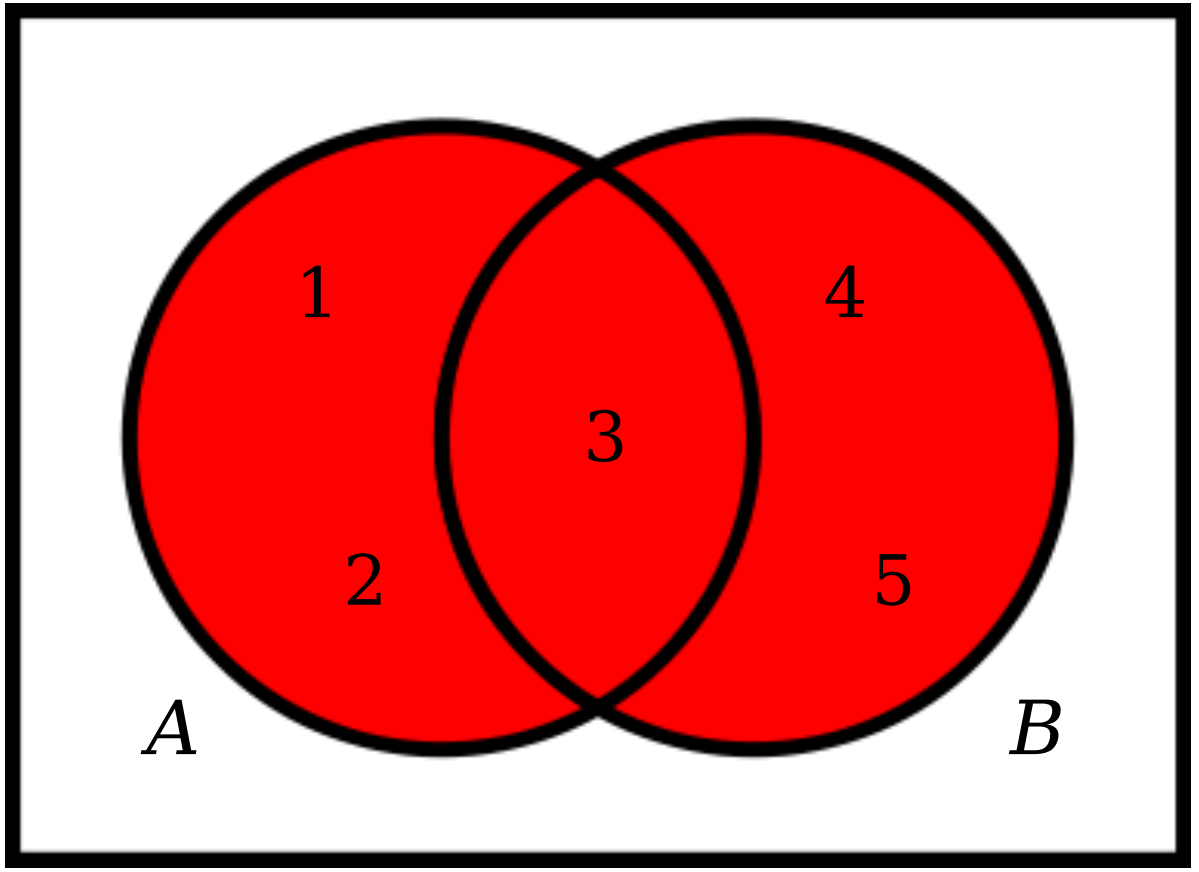
Venn Diagrams



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

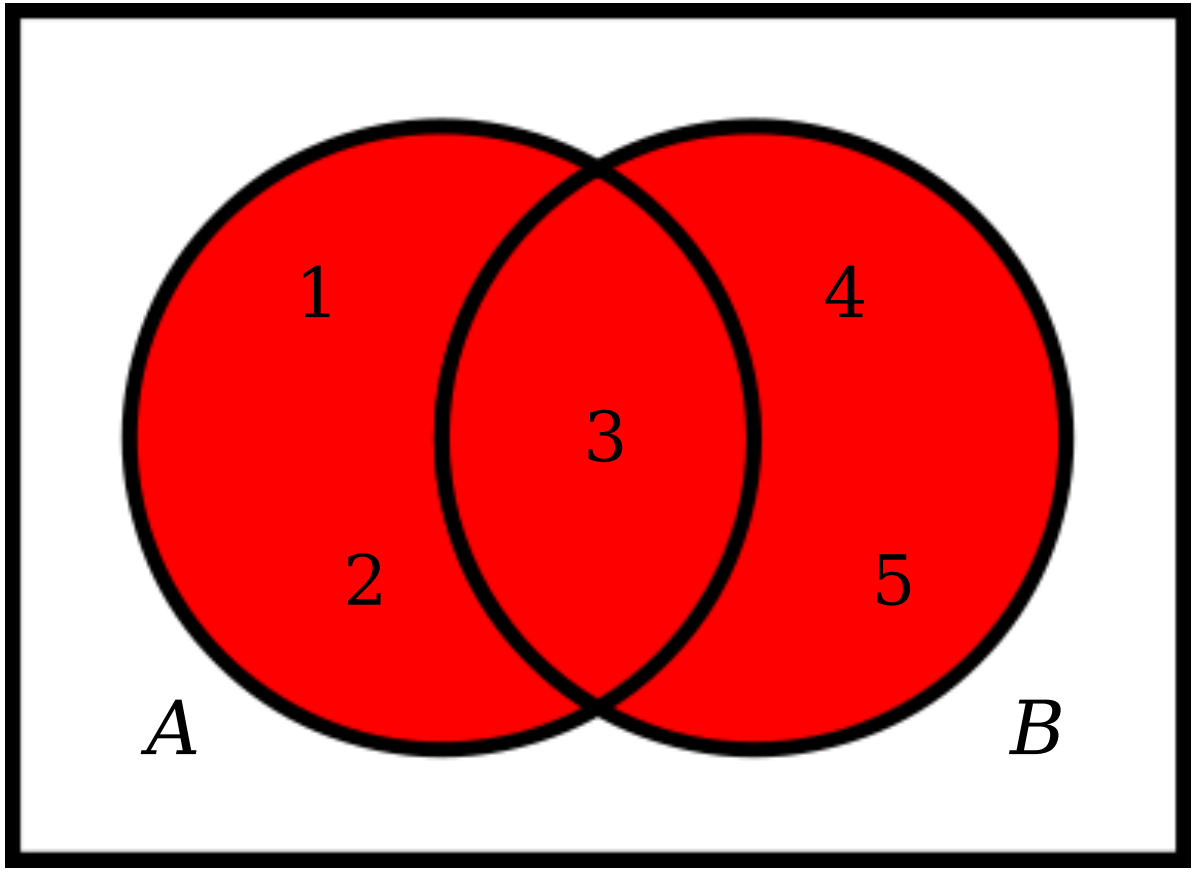
B

Venn Diagrams



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

Venn Diagrams



Union

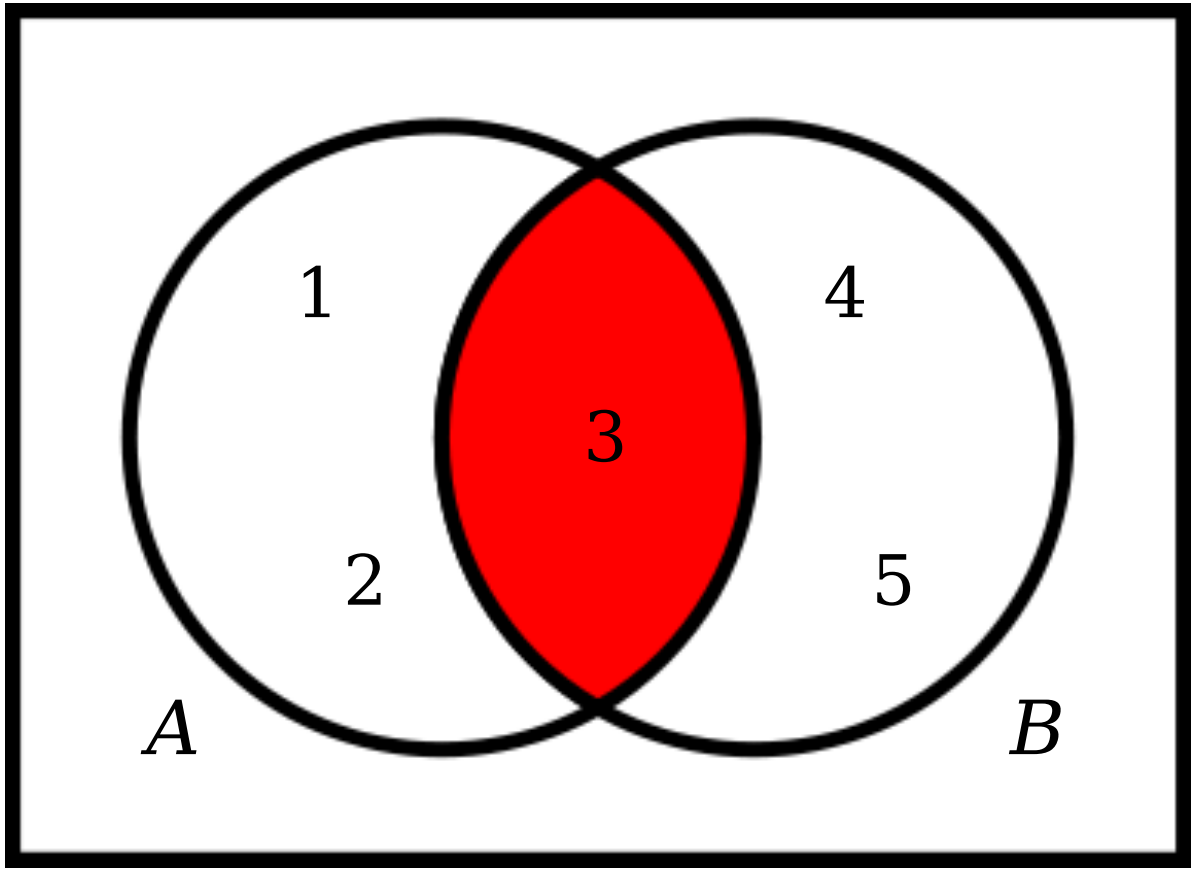
$A \cup B$

{ 1, 2, 3, 4, 5 }

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

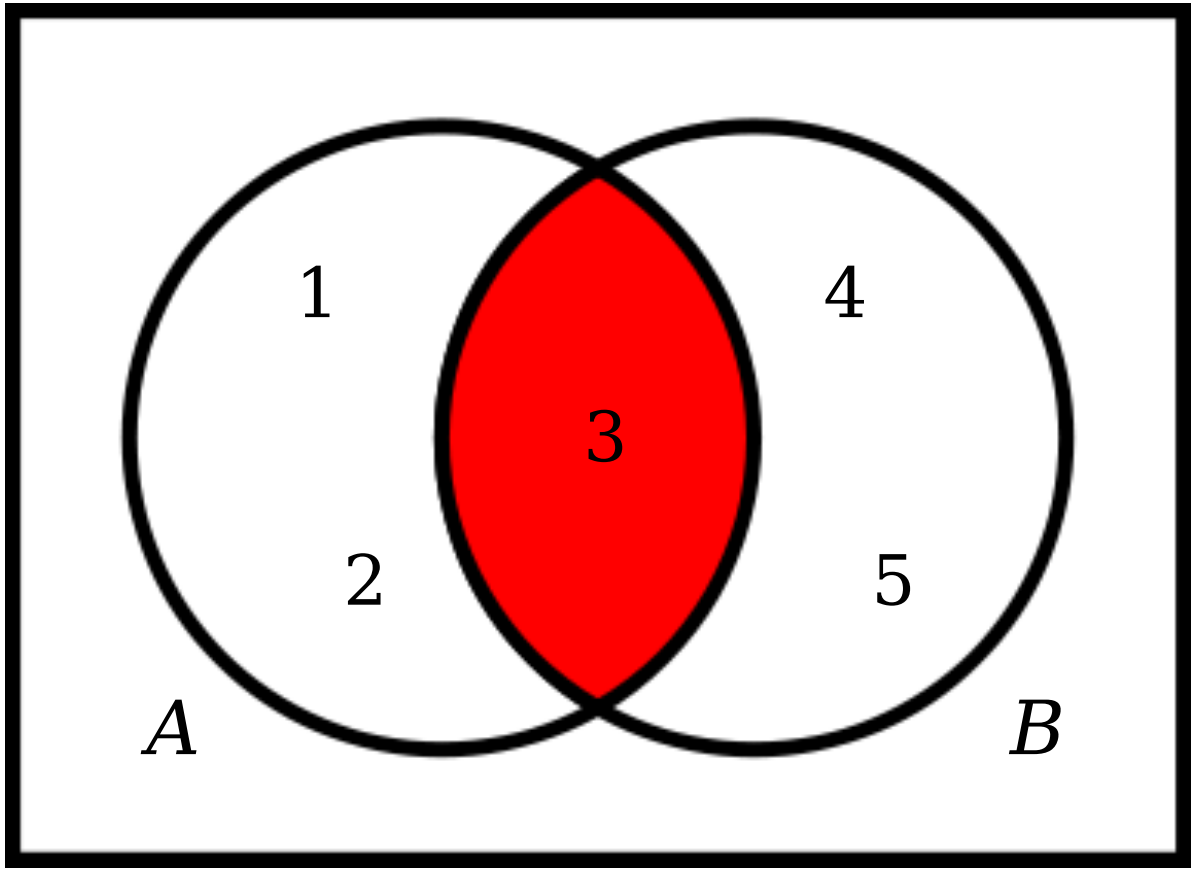
$B = \{ 3, 4, 5 \}$

Venn Diagrams



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

Venn Diagrams



Intersection

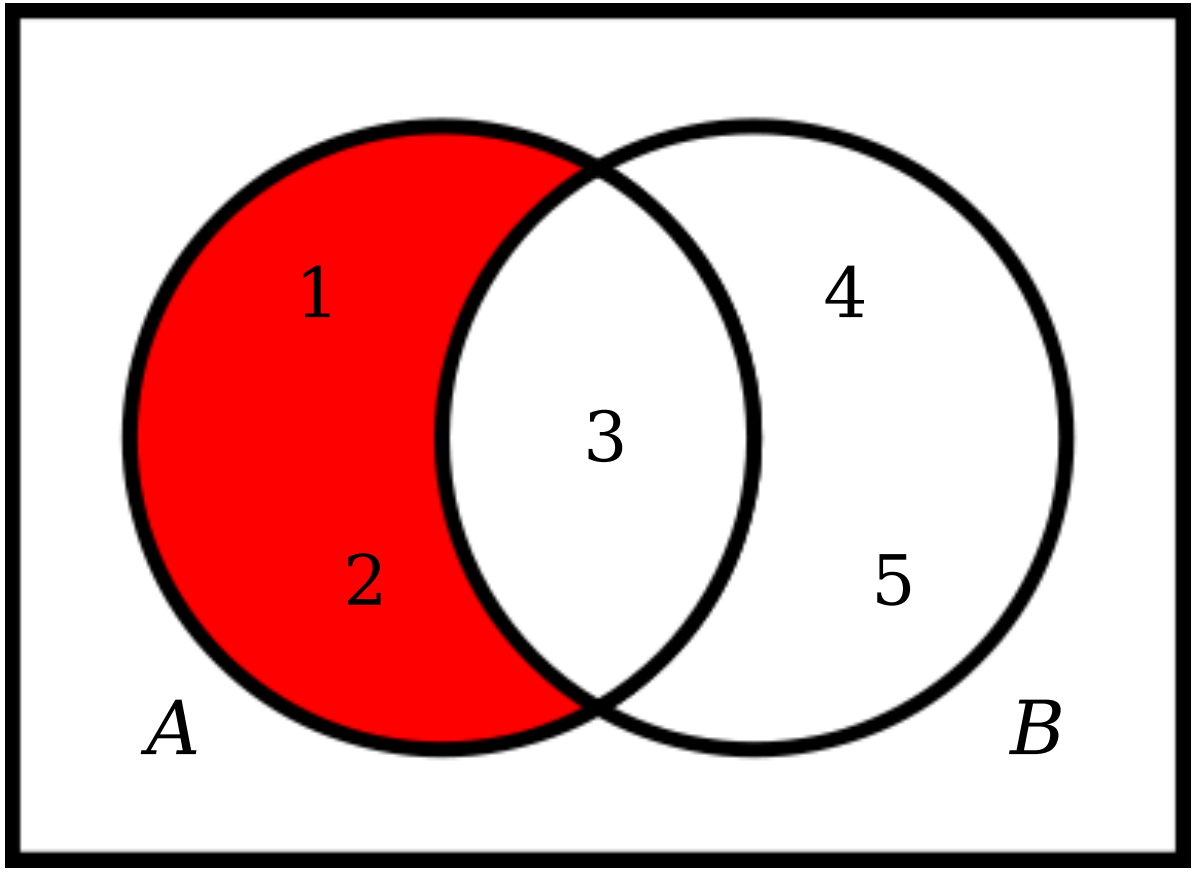
$A \cap B$

{ 3 }

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

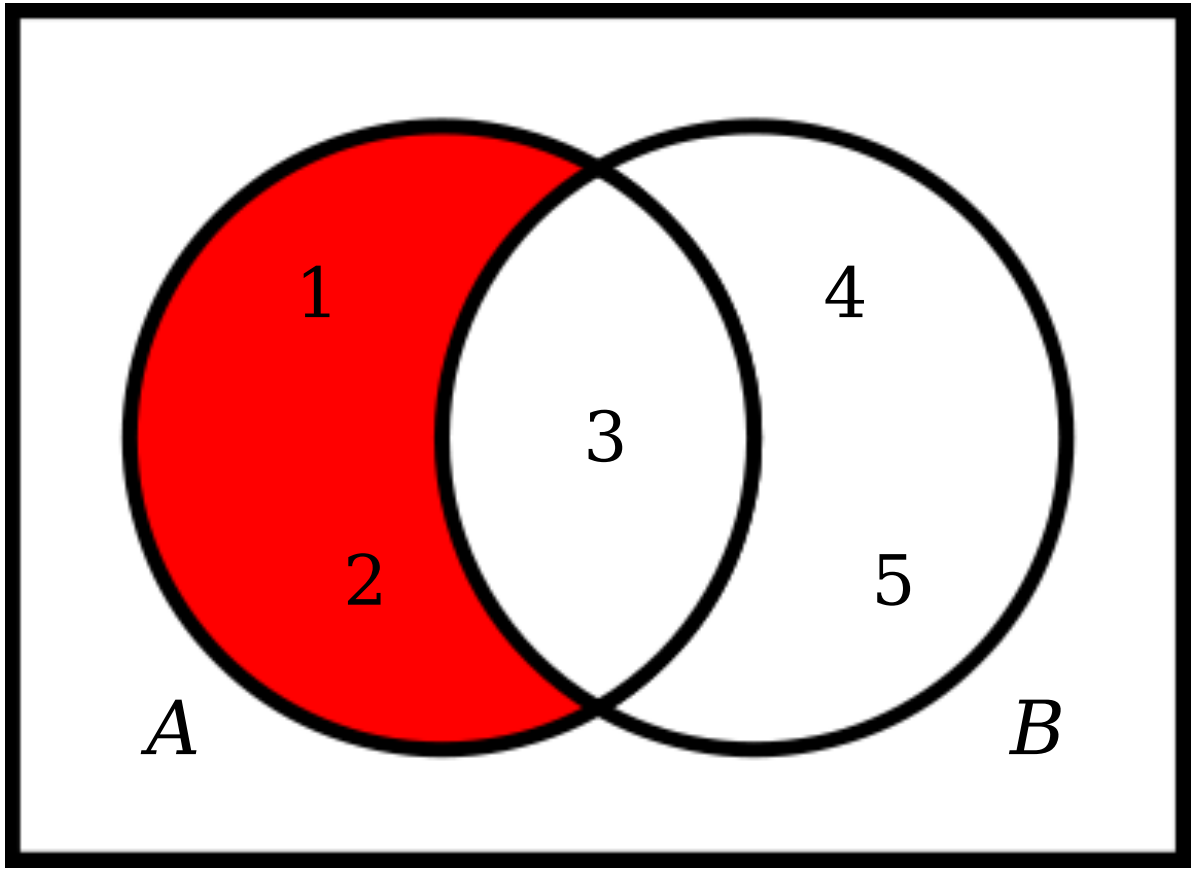
$B = \{ 3, 4, 5 \}$

Venn Diagrams



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

Venn Diagrams



Difference

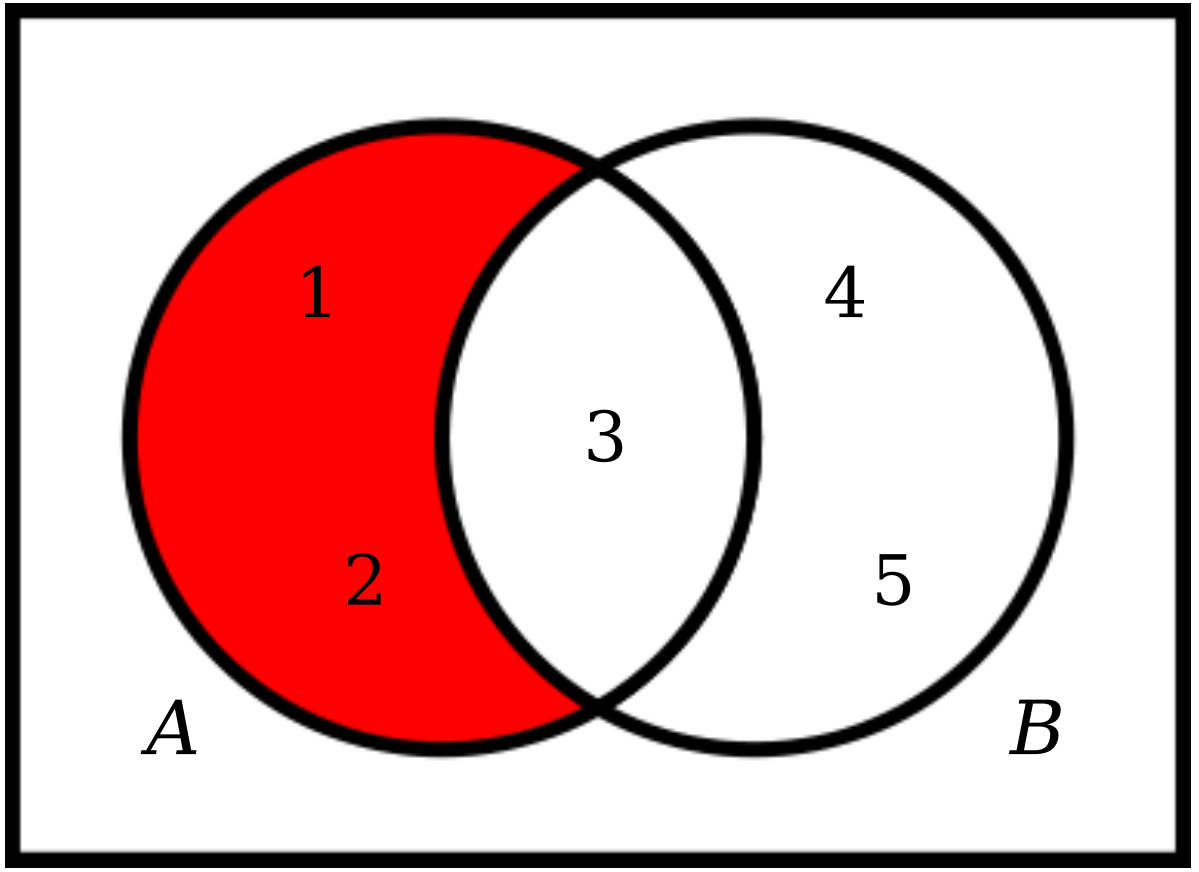
$A - B$

{ 1, 2 }

A = { 1, 2, 3 }

B = { 3, 4, 5 }

Venn Diagrams



Difference

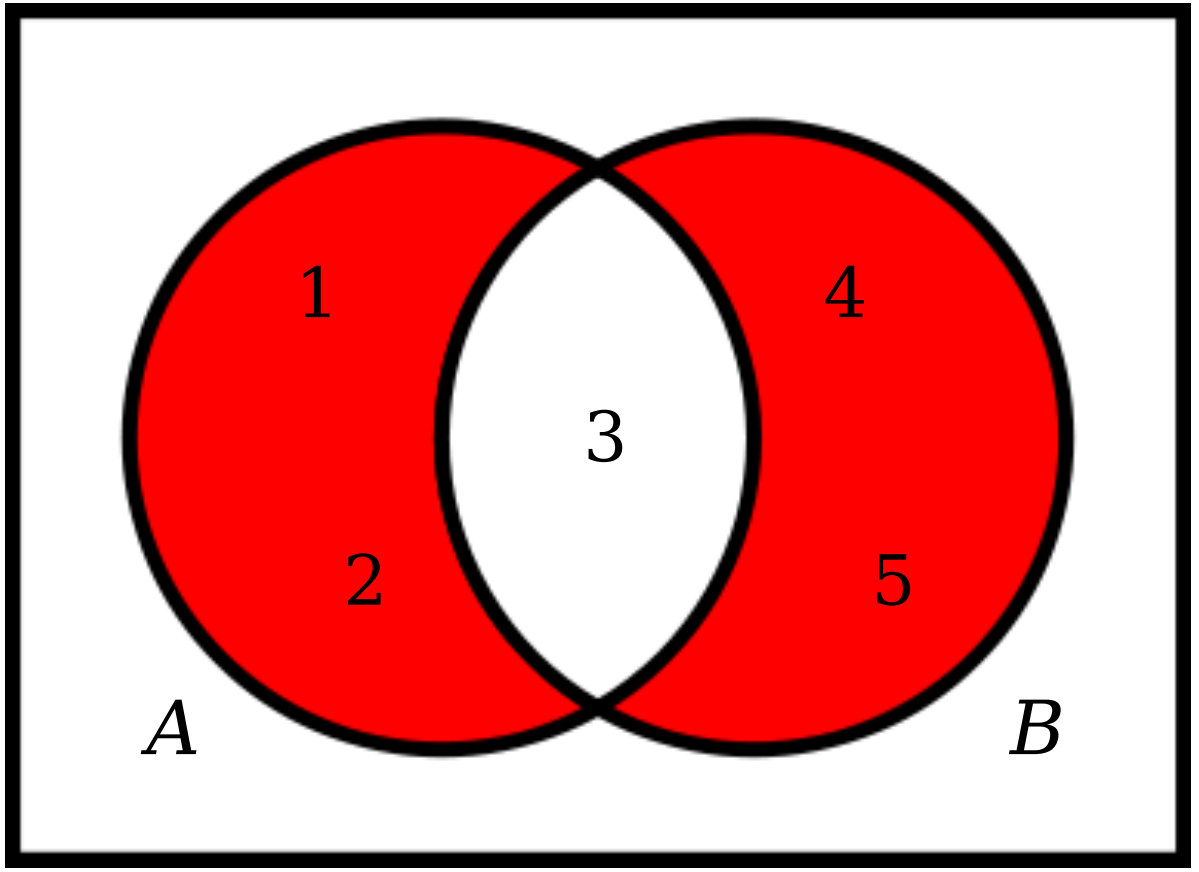
$A \setminus B$

{ 1, 2 }

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

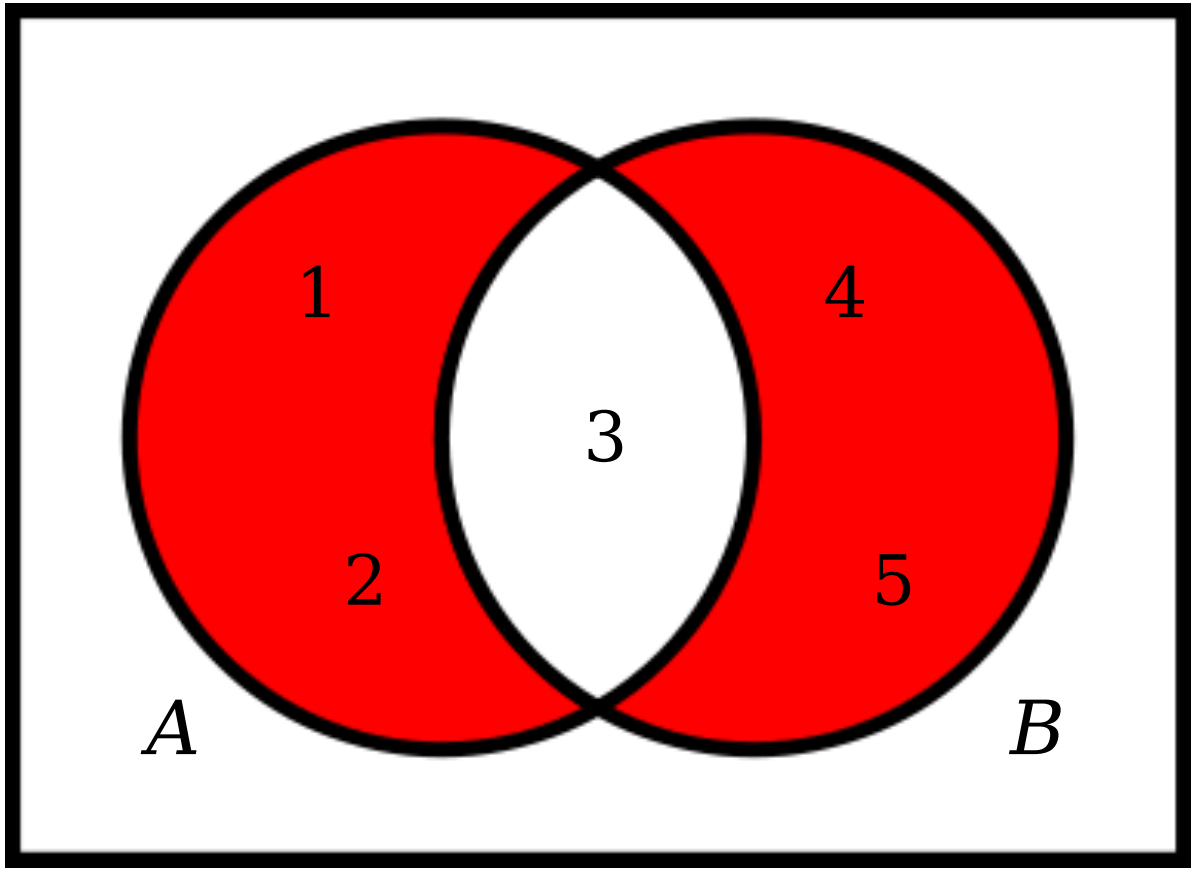
$B = \{ 3, 4, 5 \}$

Venn Diagrams



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

Venn Diagrams



Symmetric Difference

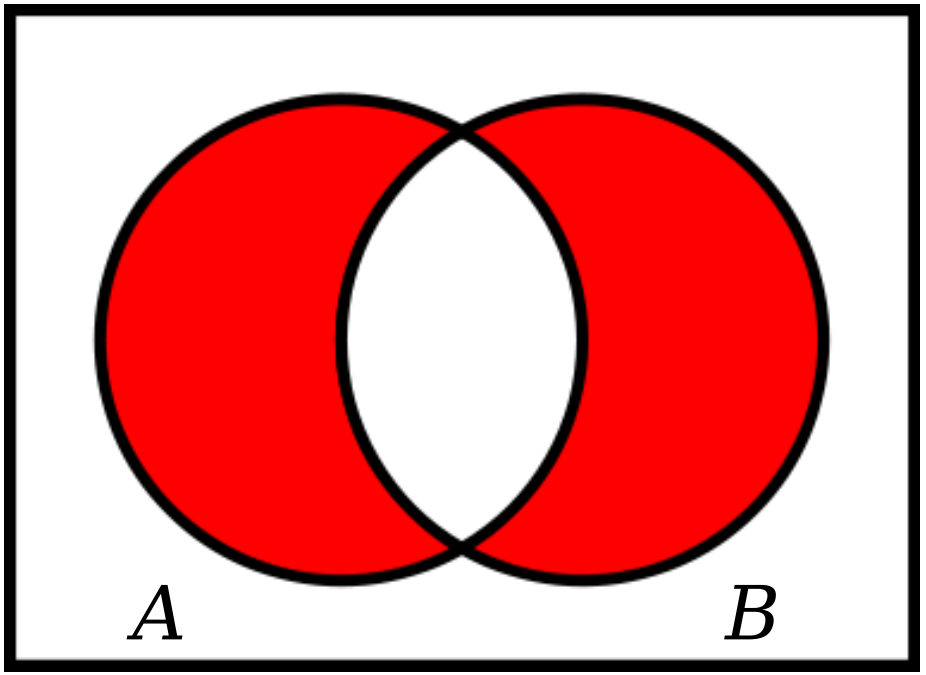
$A \Delta B$

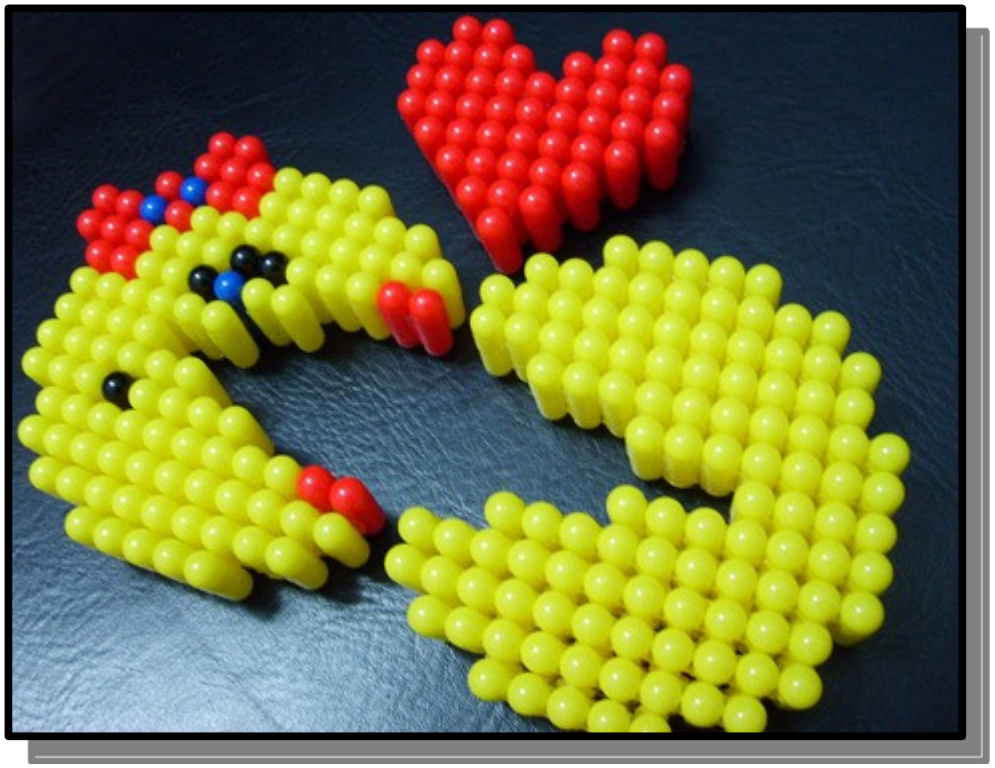
{ 1, 2, 4, 5 }

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

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

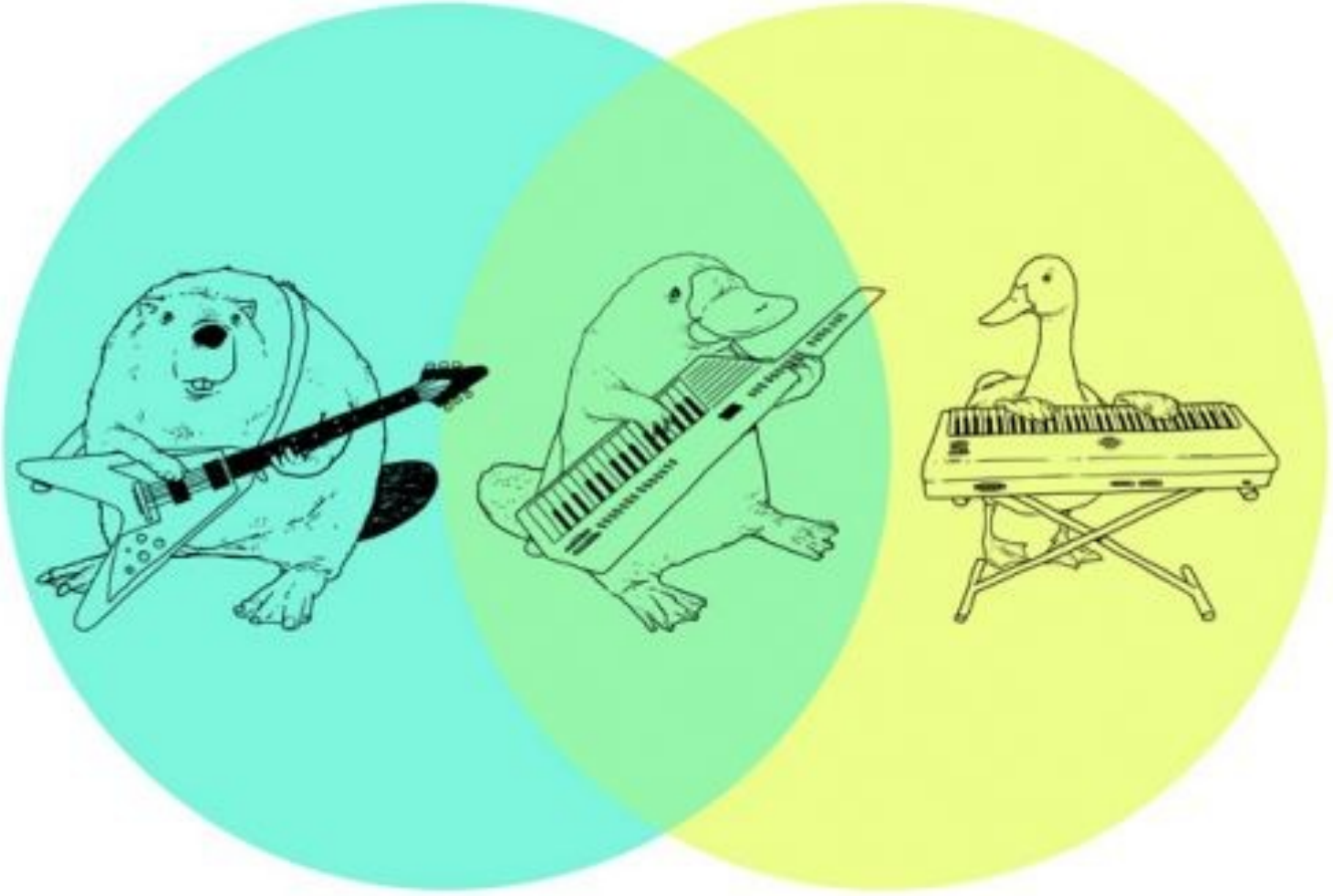
Venn Diagrams



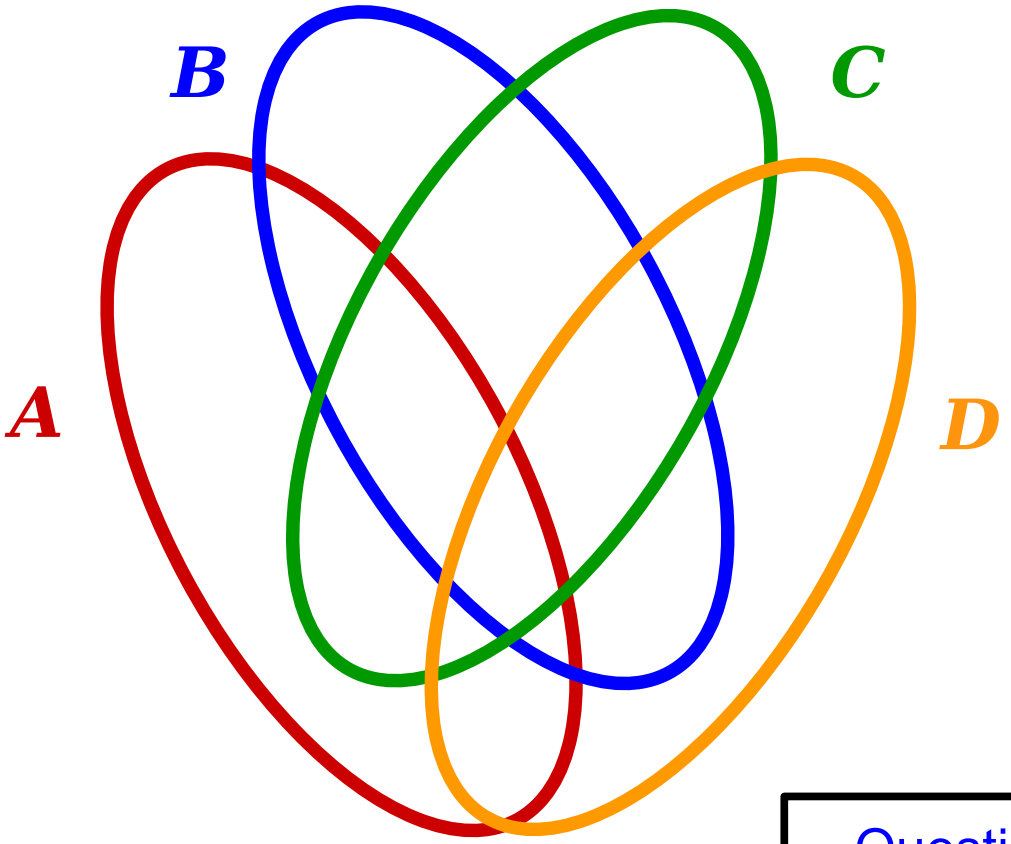


$A \Delta B$

Venn Diagrams

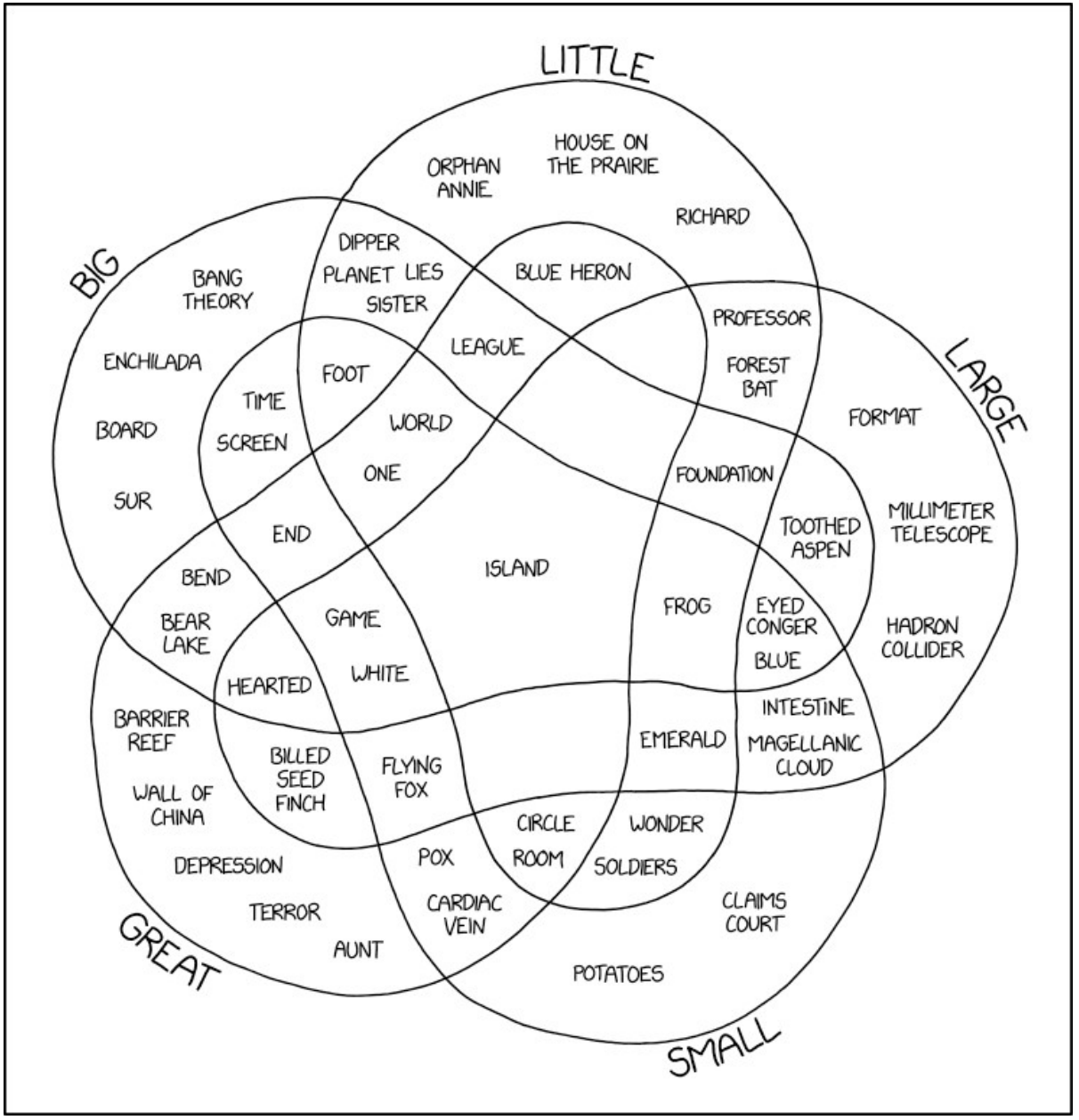


Venn Diagrams for Four Sets



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

Venn Diagrams for Five Sets



https://www.xkcd.com/2122/

Venn Diagrams for Seven Sets

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

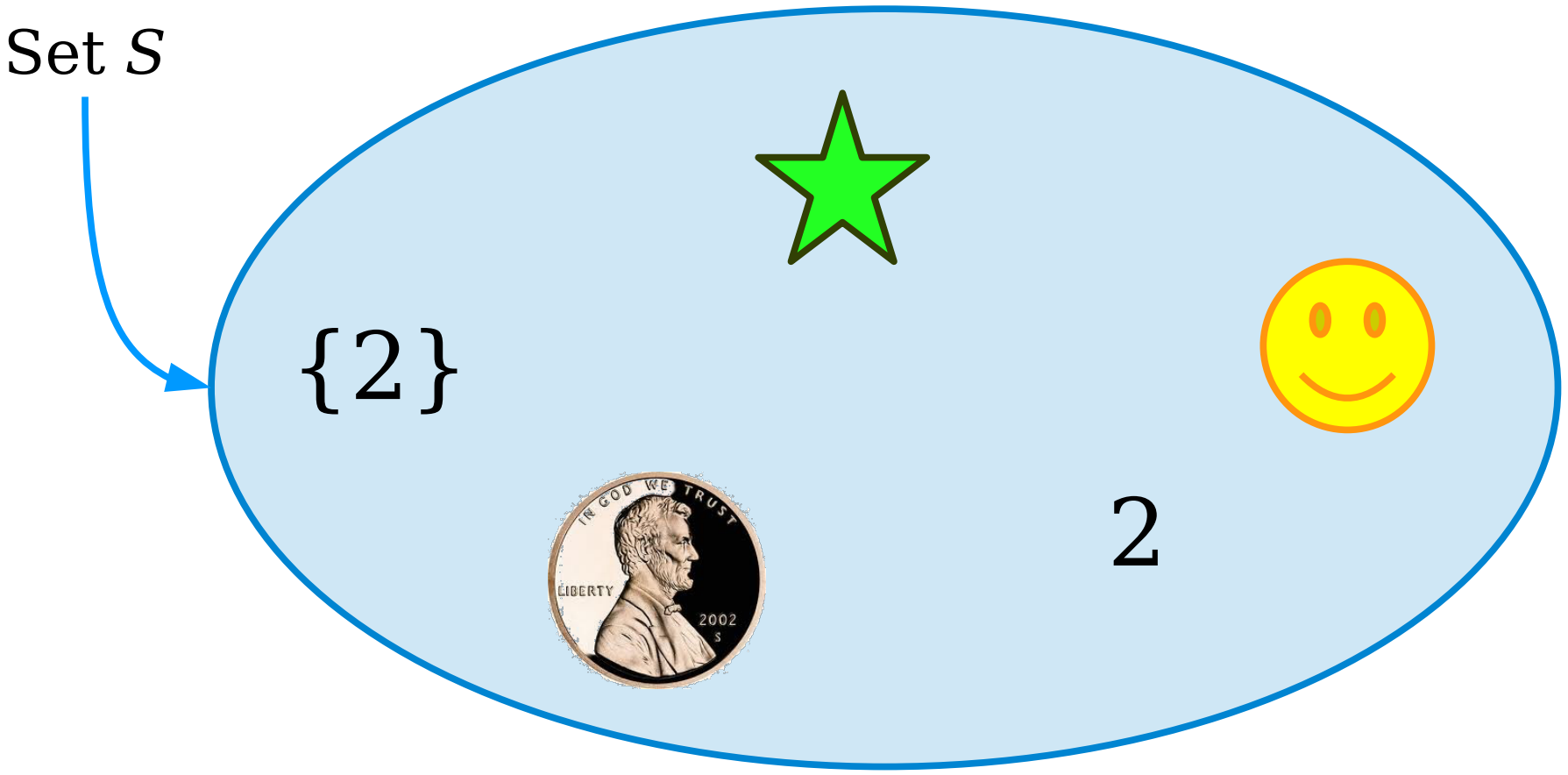
Let’s take a quick break!

Subsets and Power Sets

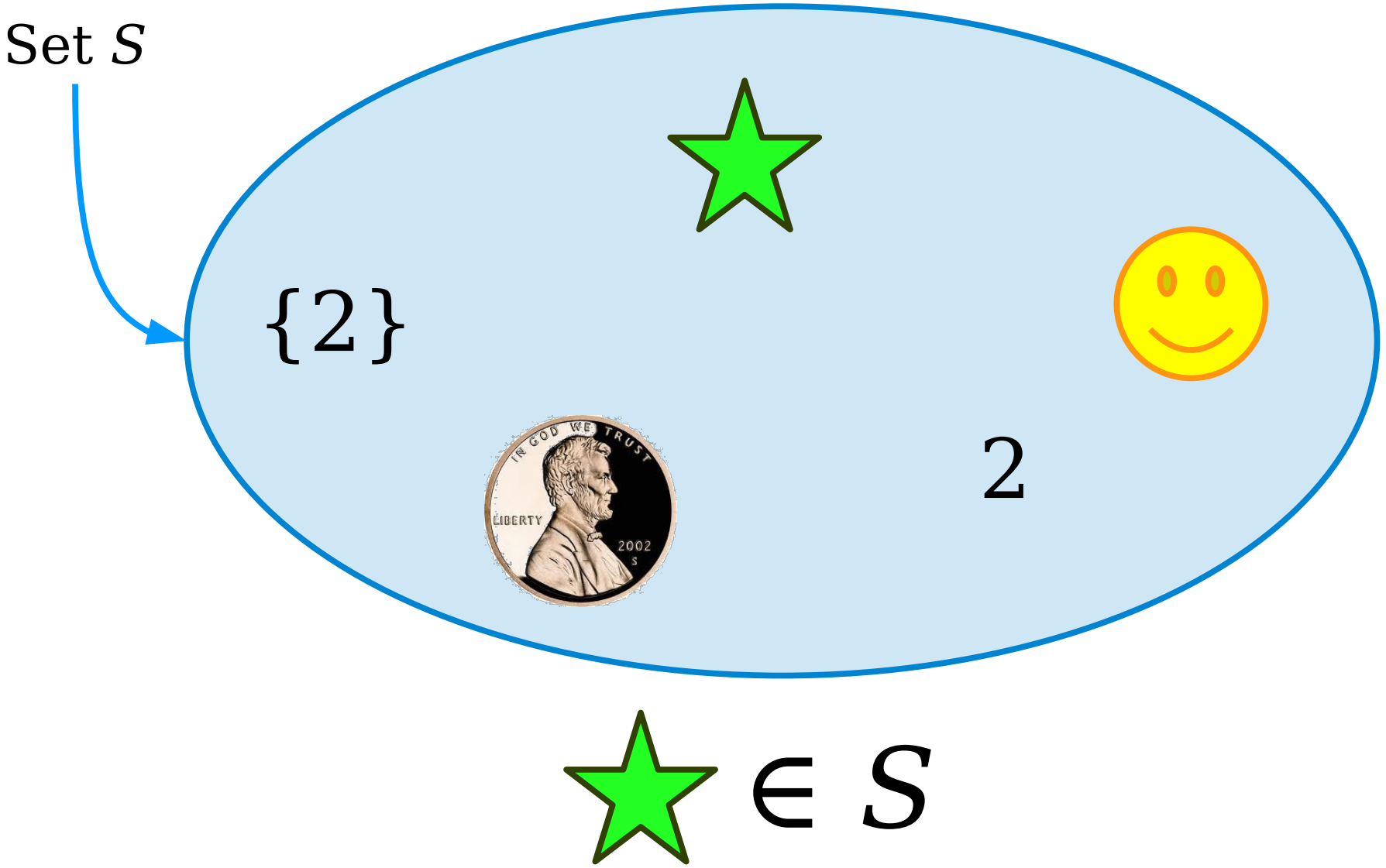
Subsets

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

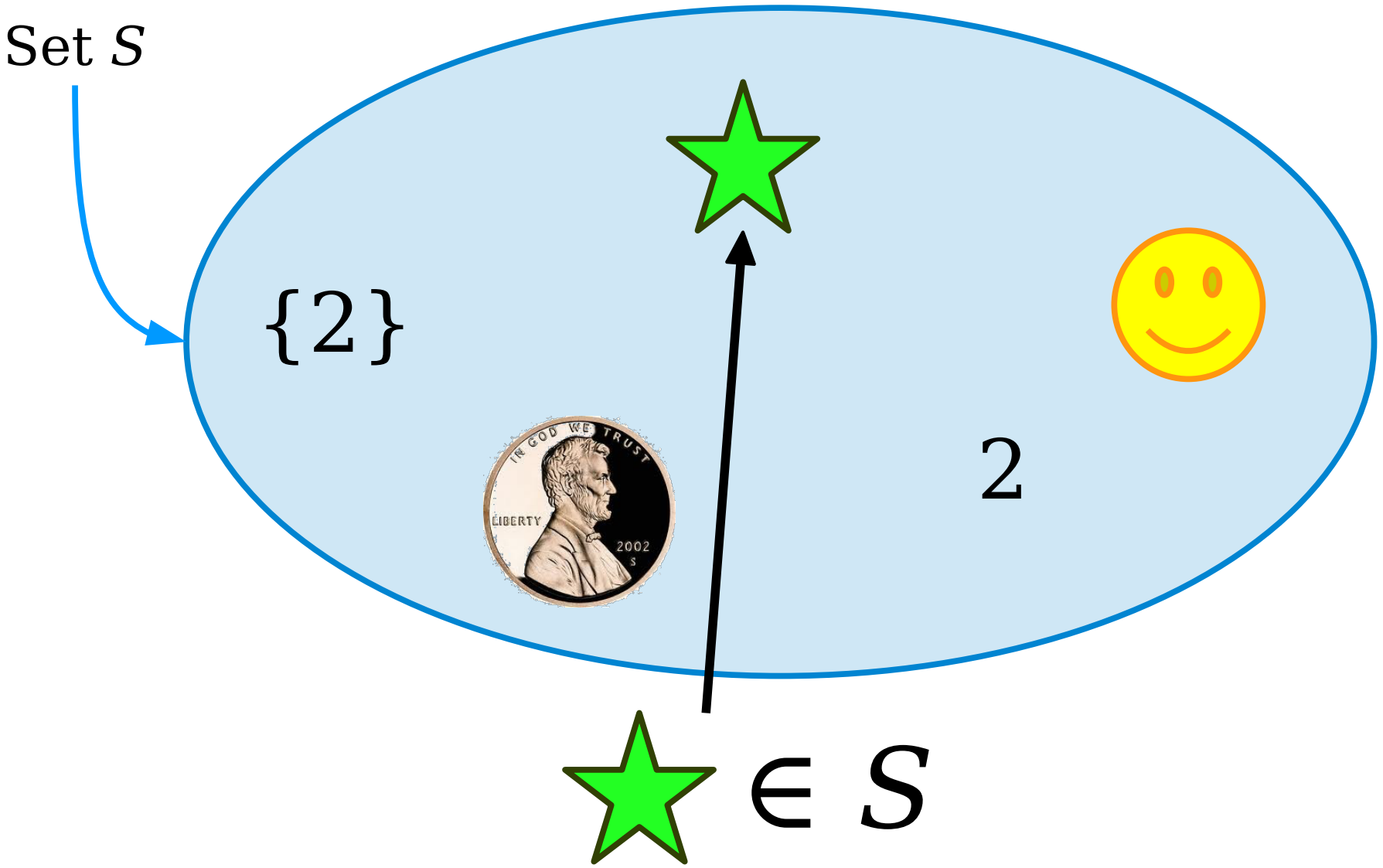
Subsets and Elements



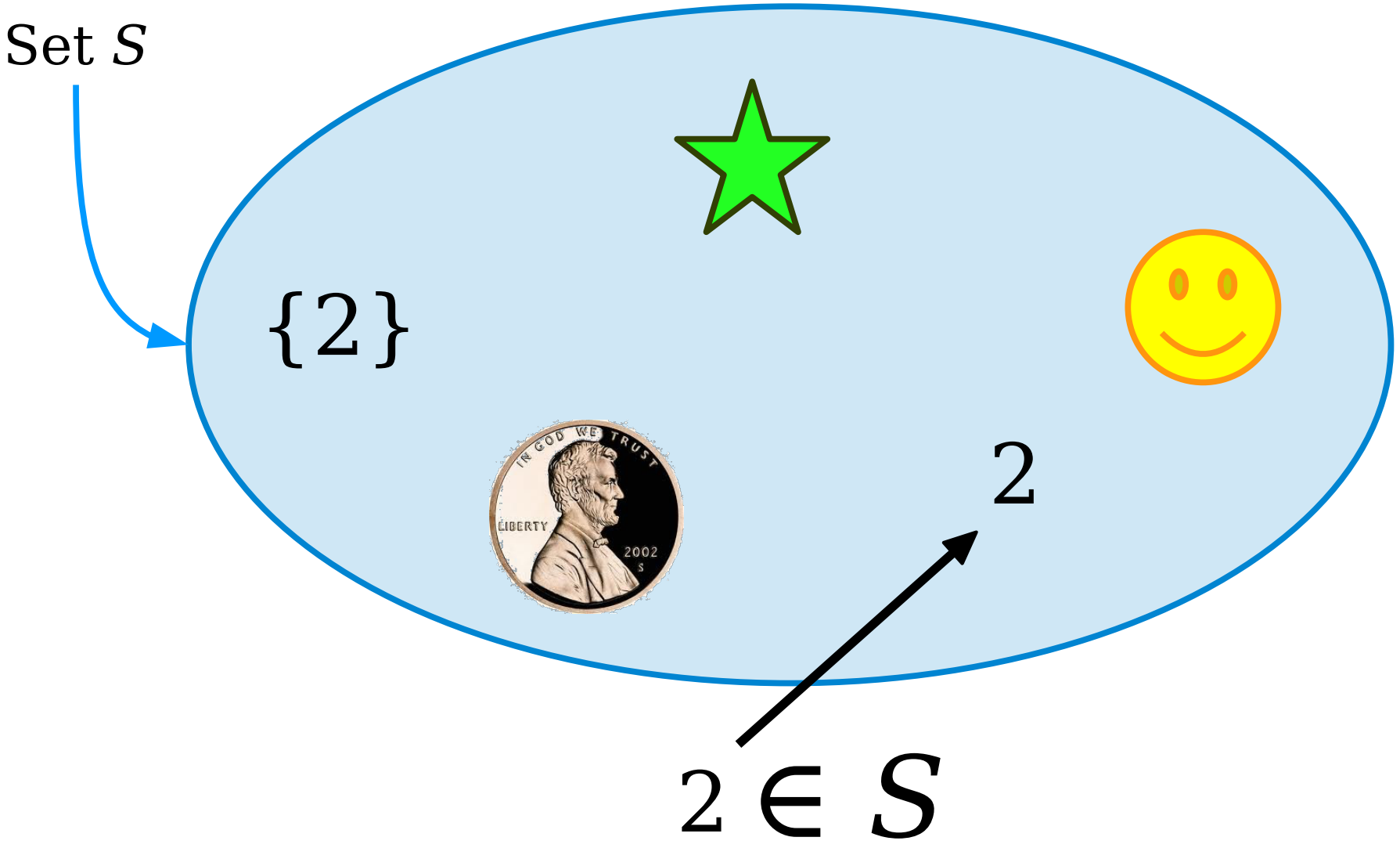
Subsets and Elements



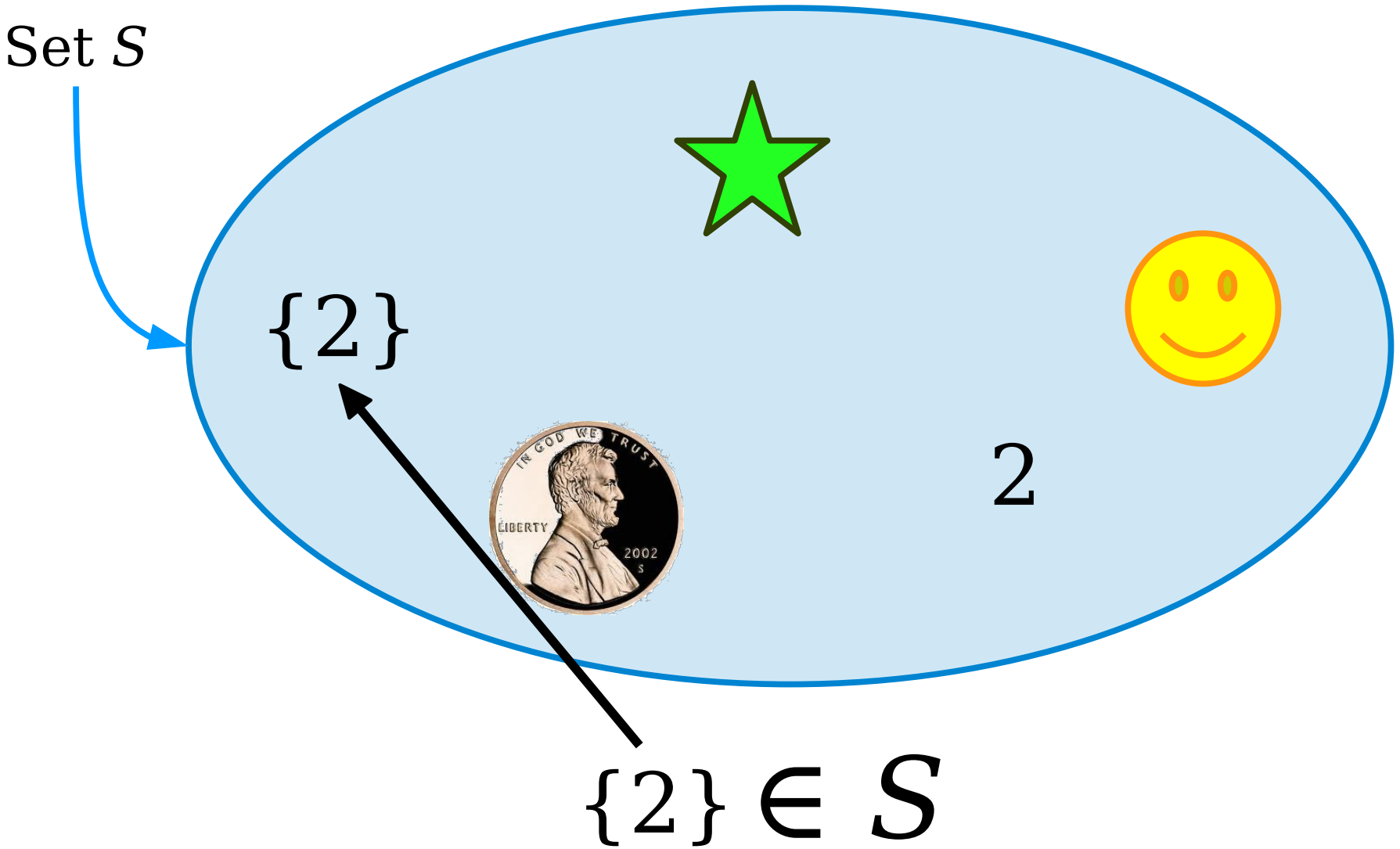
Subsets and Elements



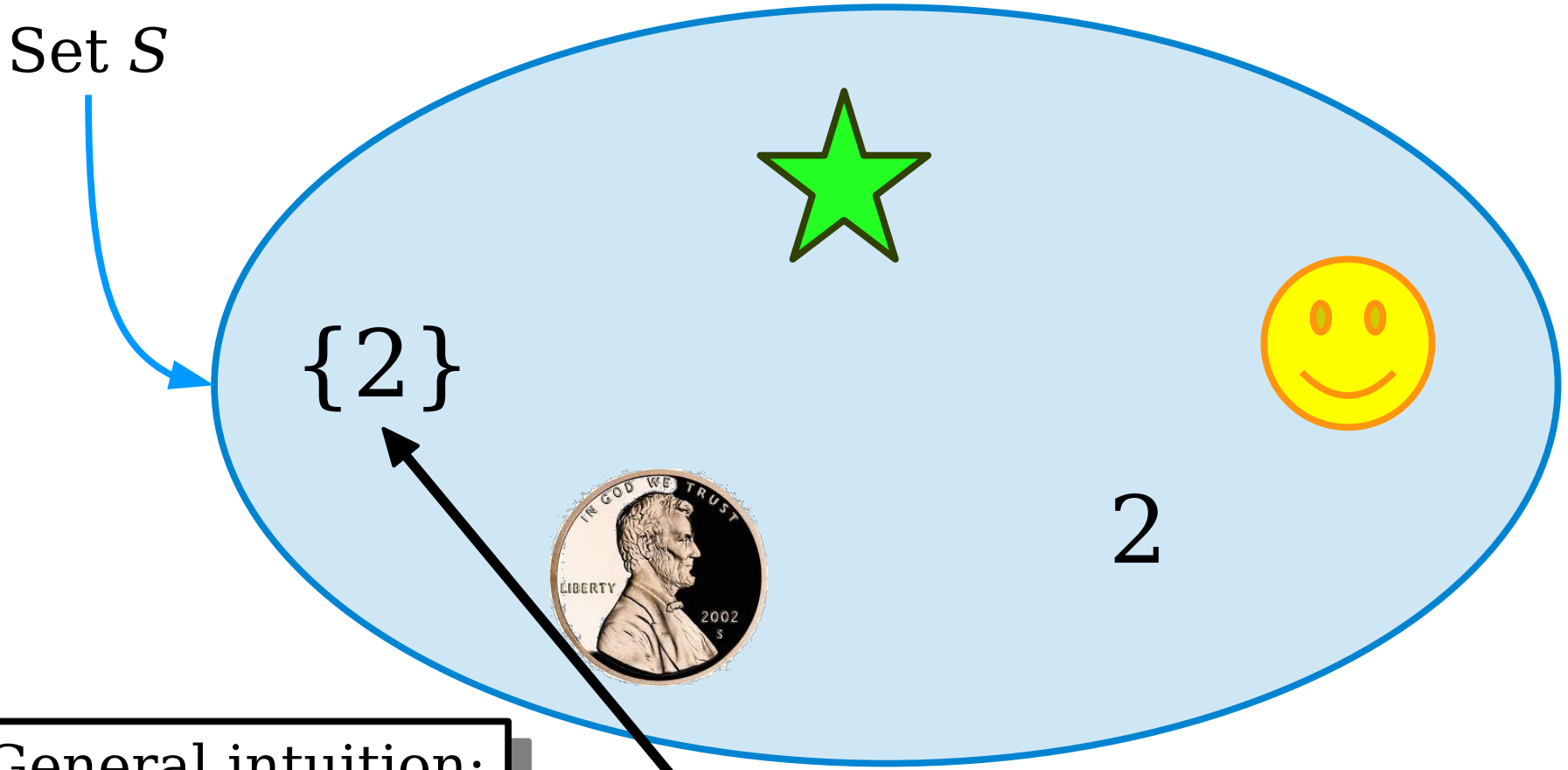
Subsets and Elements



Subsets and Elements

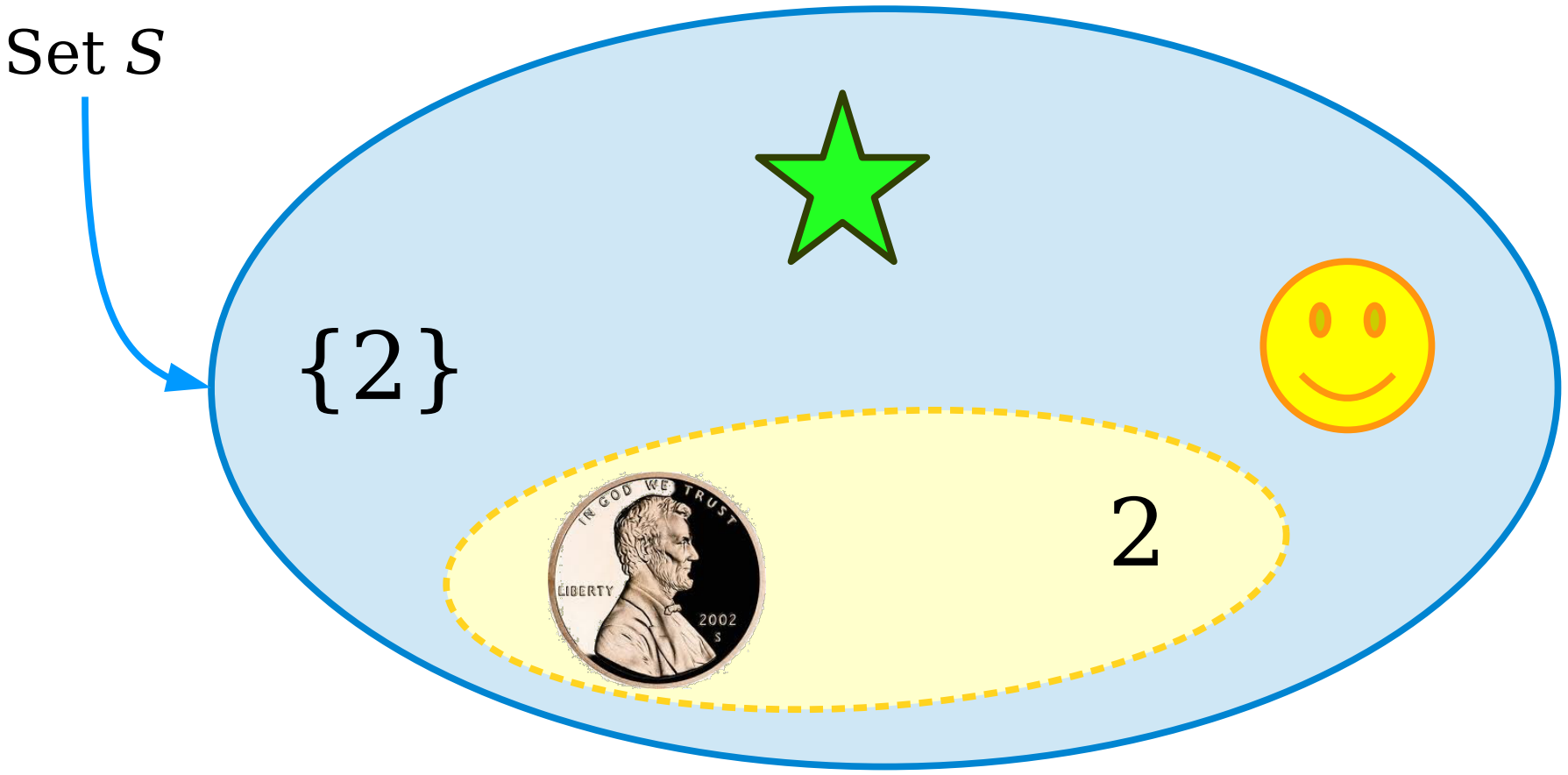


Subsets and Elements

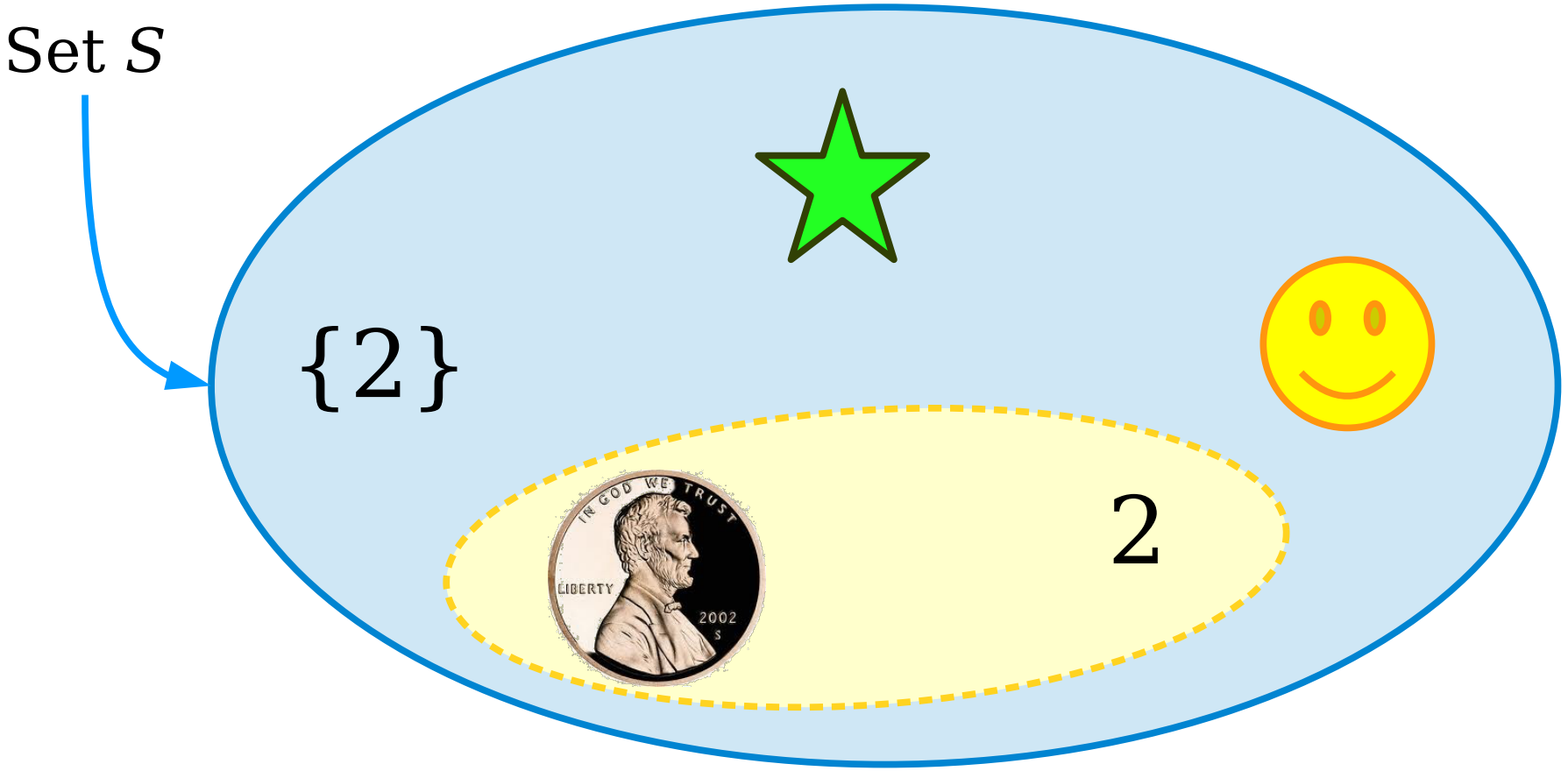


General intuition: $x \in S$ means you can ***point at x inside of S***.

Subsets and Elements

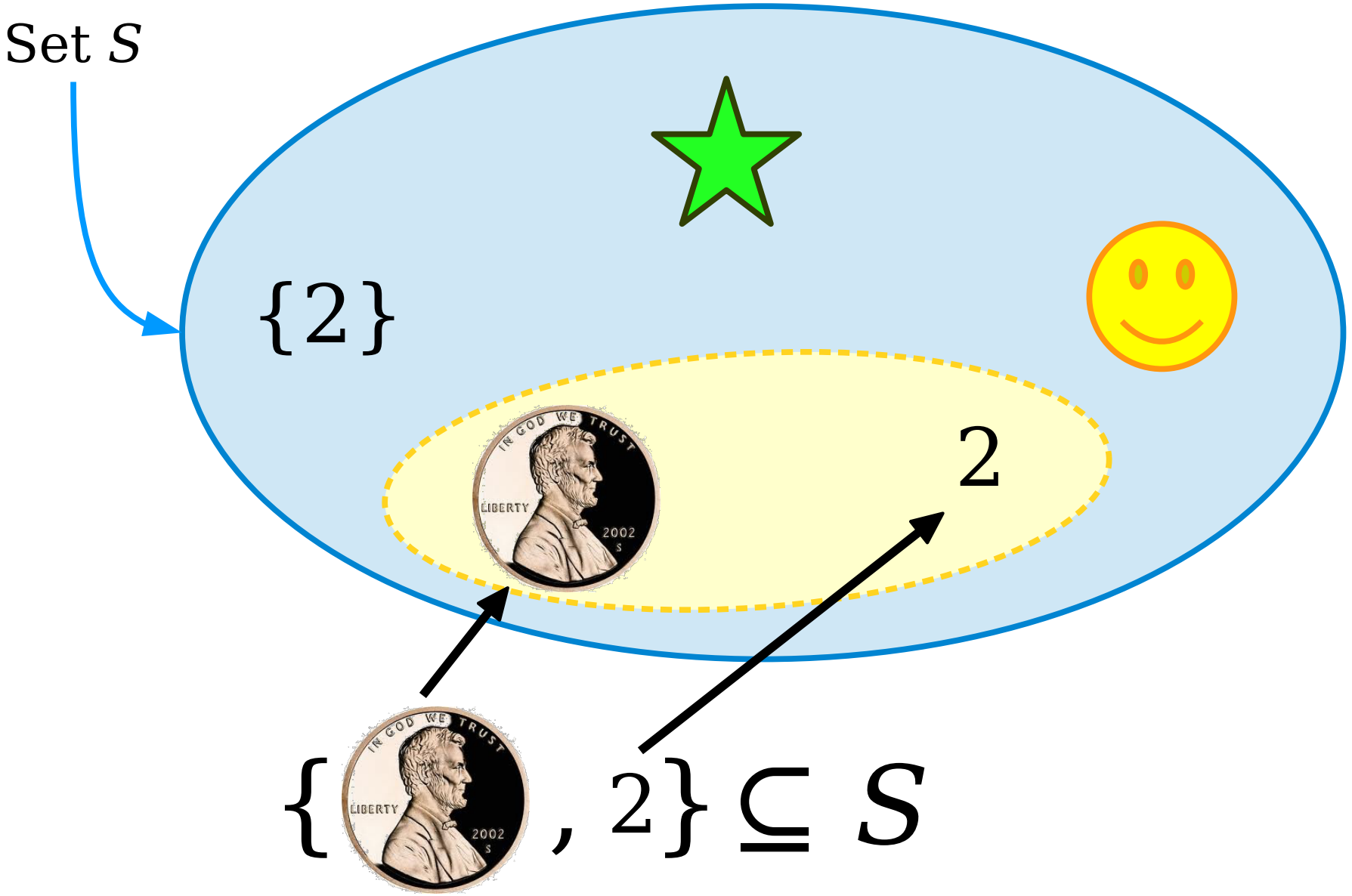


Subsets and Elements

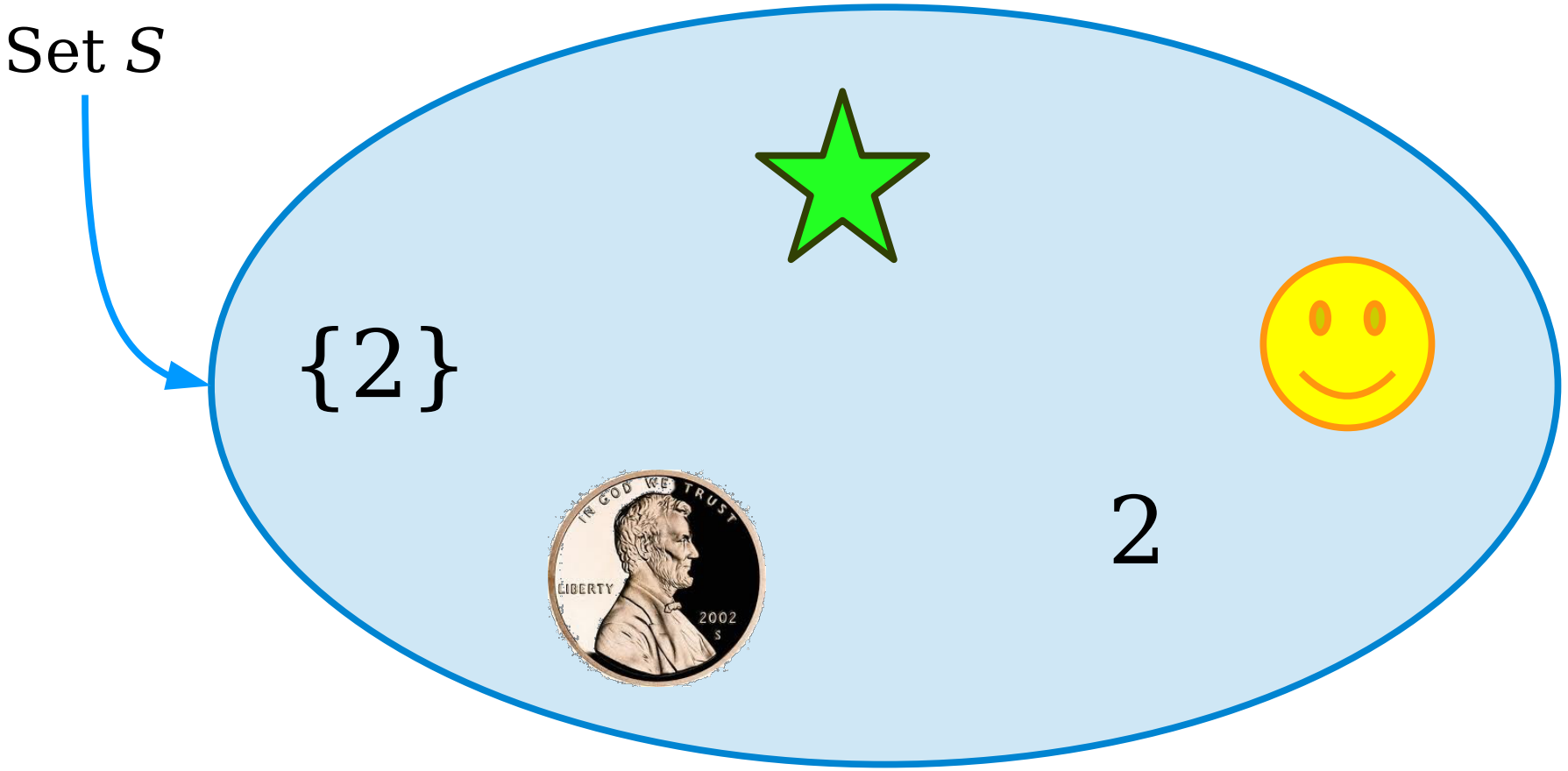


$\{$  $, 2\} \subseteq S$

Subsets and Elements

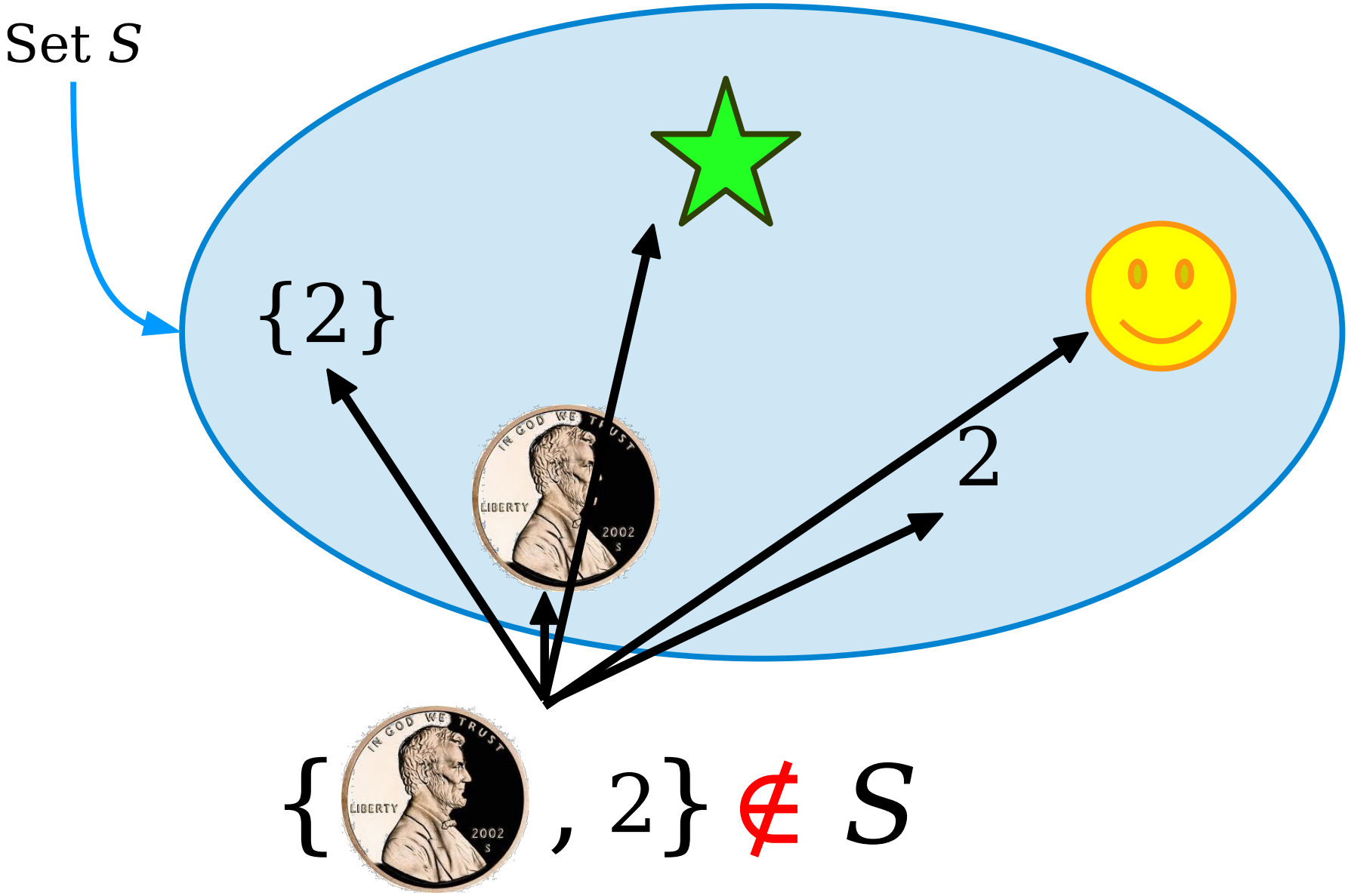


Subsets and Elements

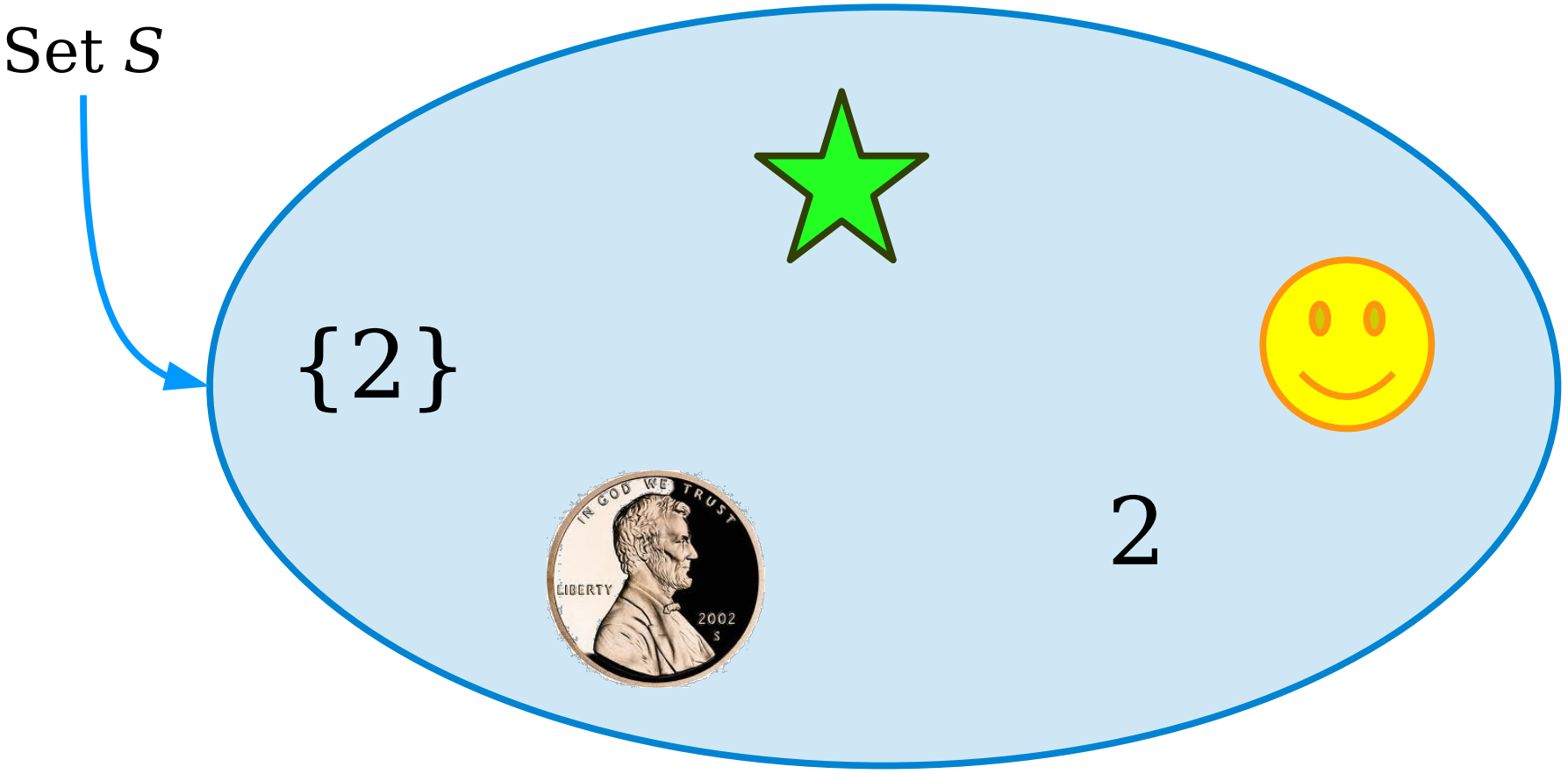


$\{$  $, 2\} \notin S$

Subsets and Elements

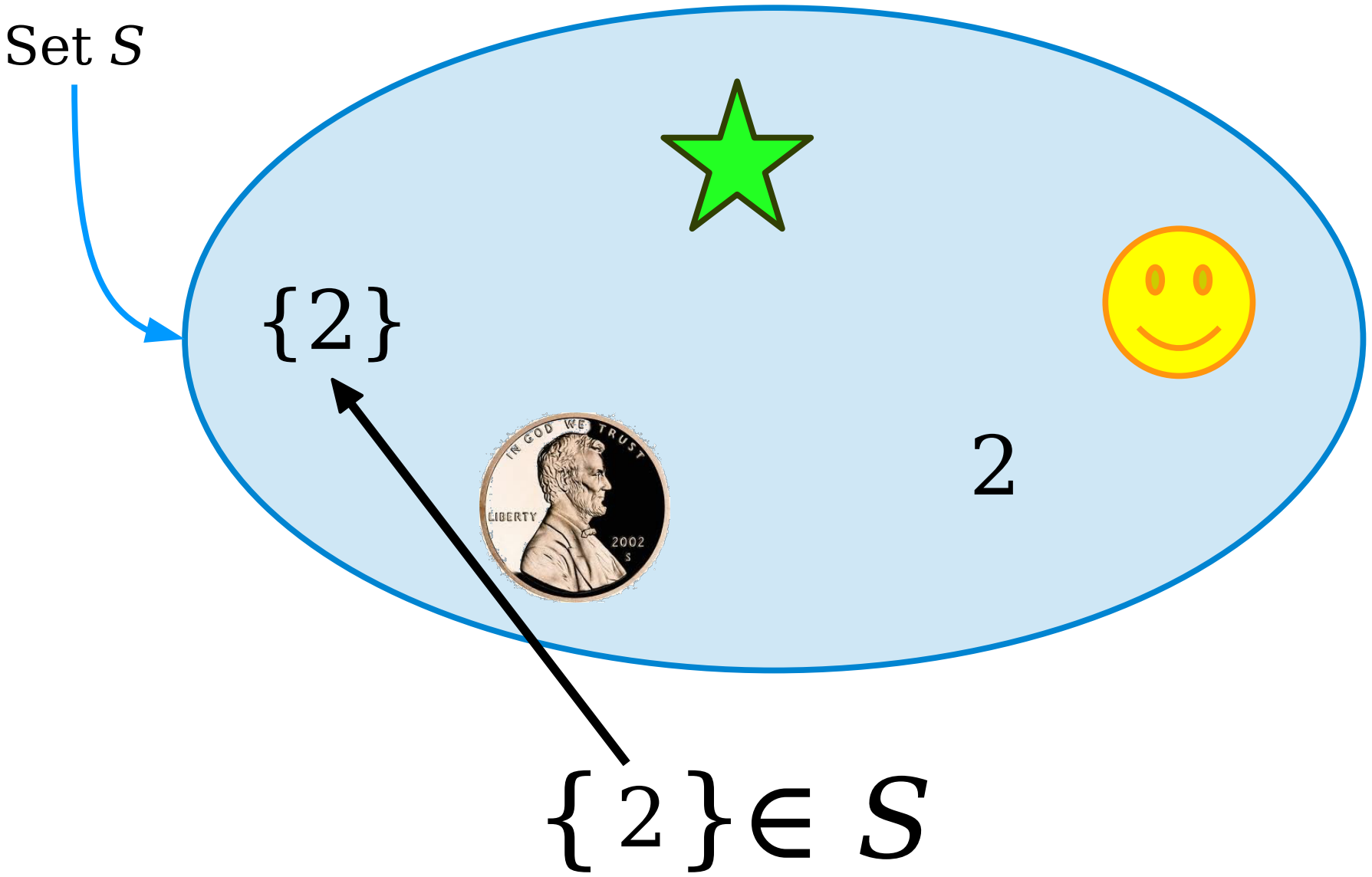


Subsets and Elements

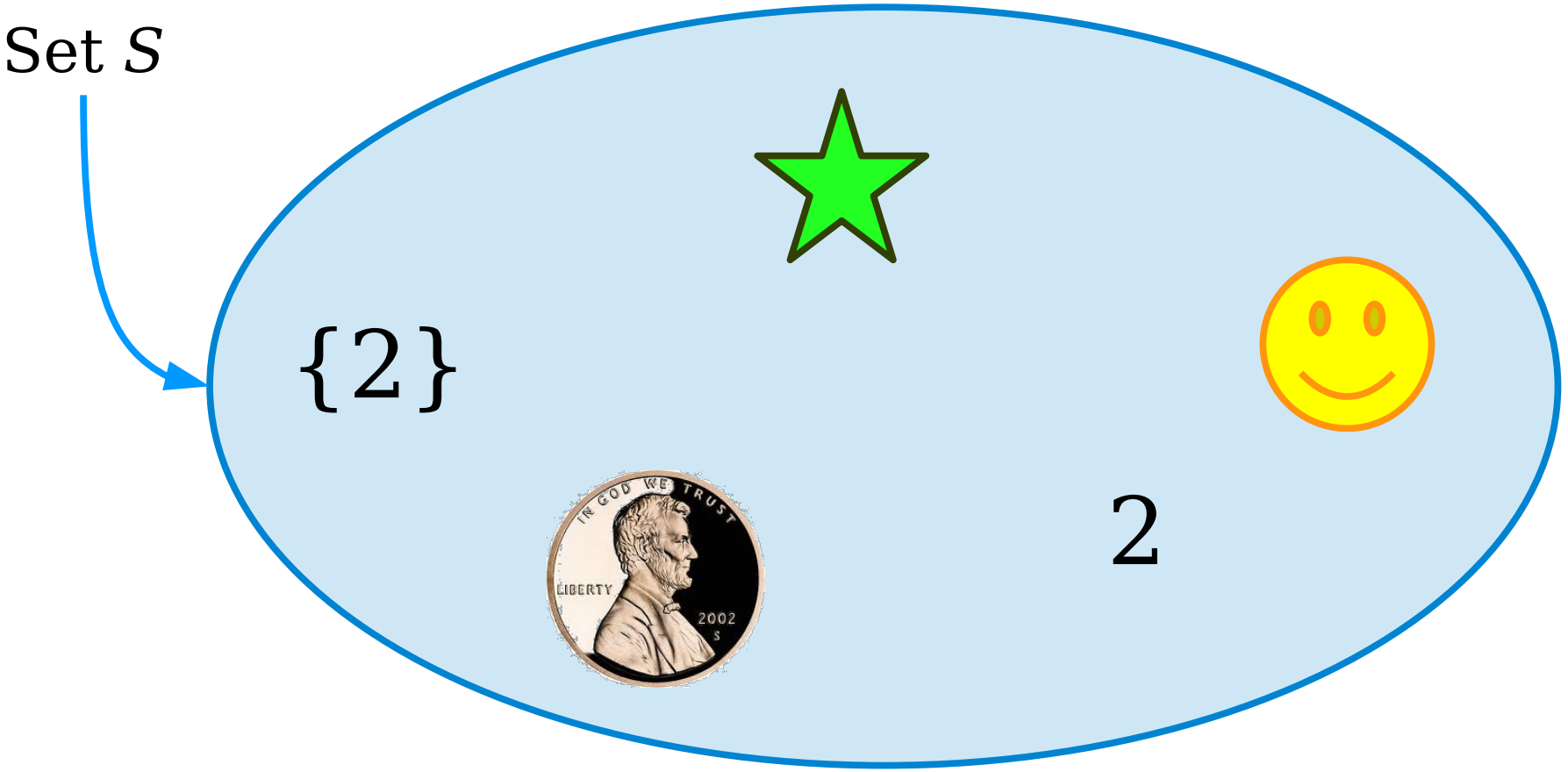


$$\{2\} \in S$$

Subsets and Elements

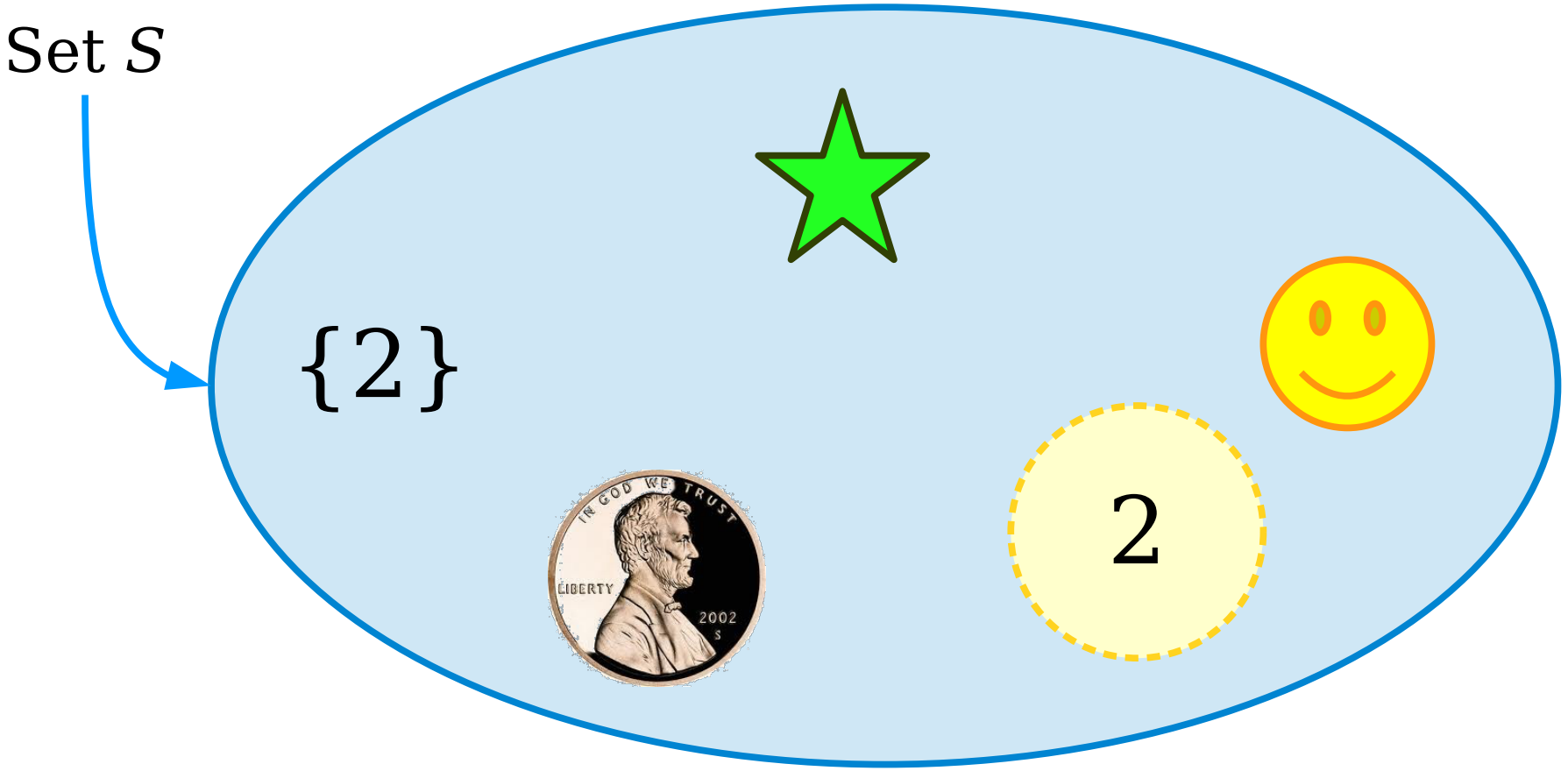


Subsets and Elements



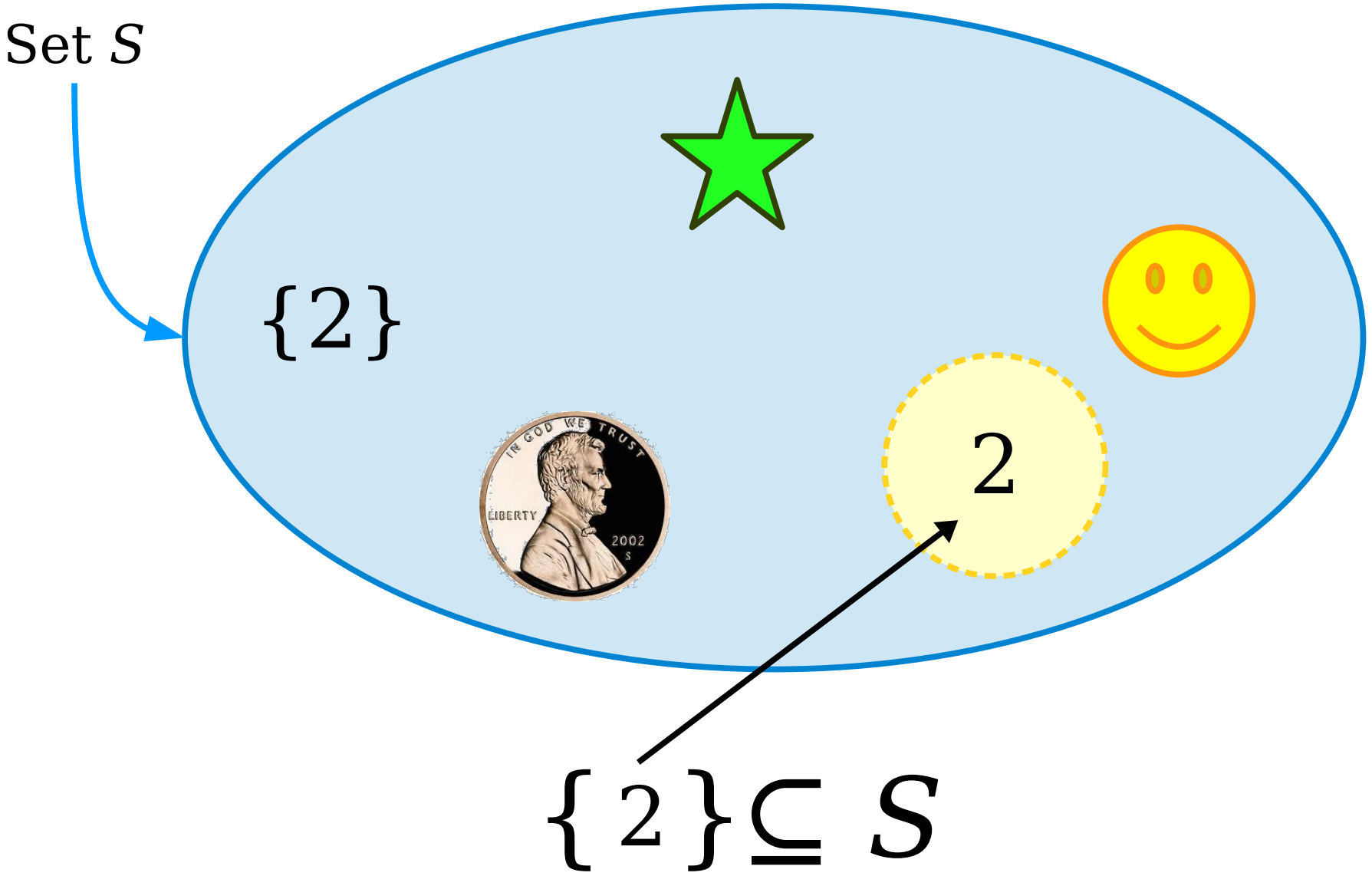
$$\{2\} \subseteq S$$

Subsets and Elements

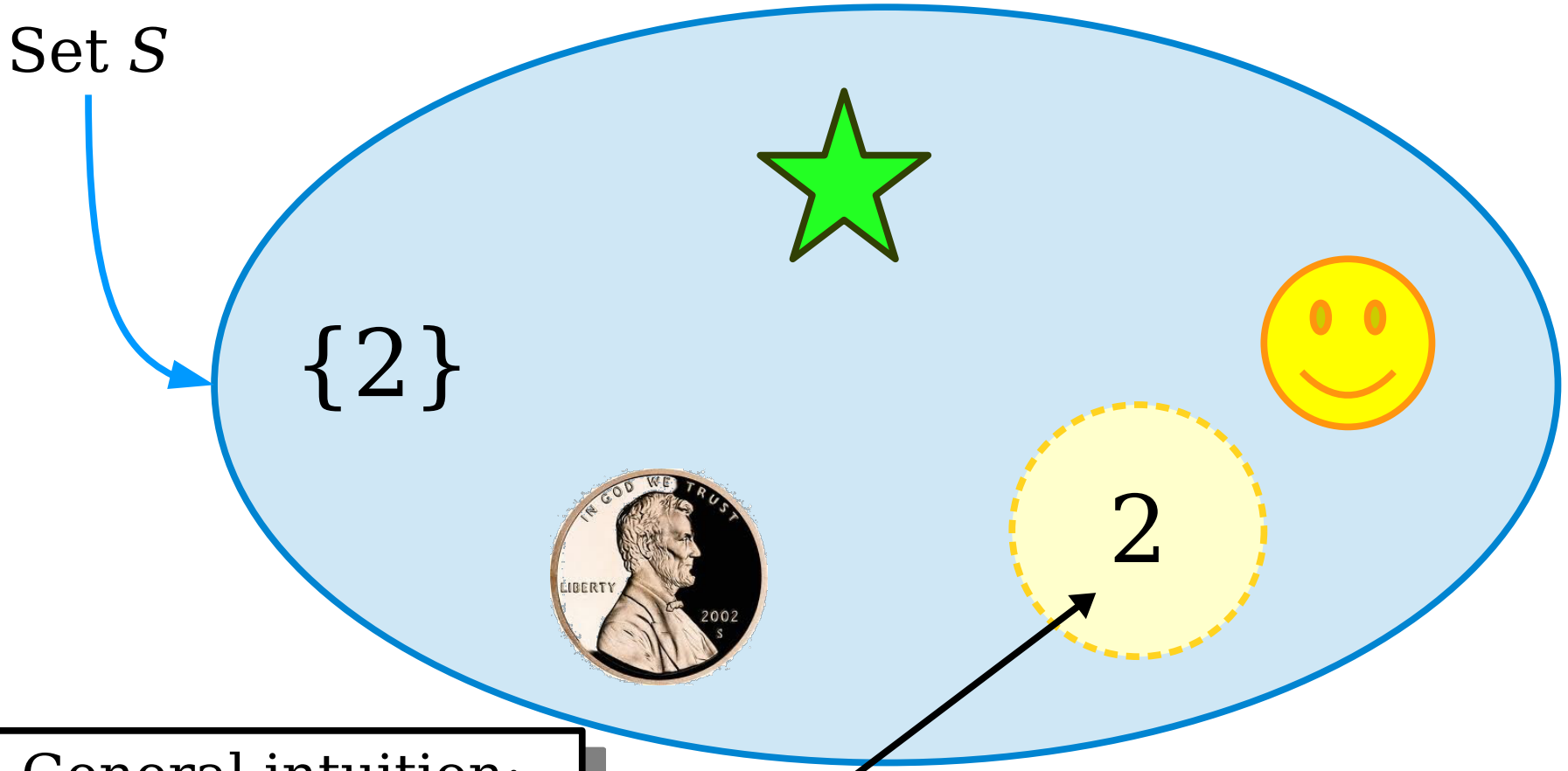


$$\{2\} \subseteq S$$

Subsets and Elements



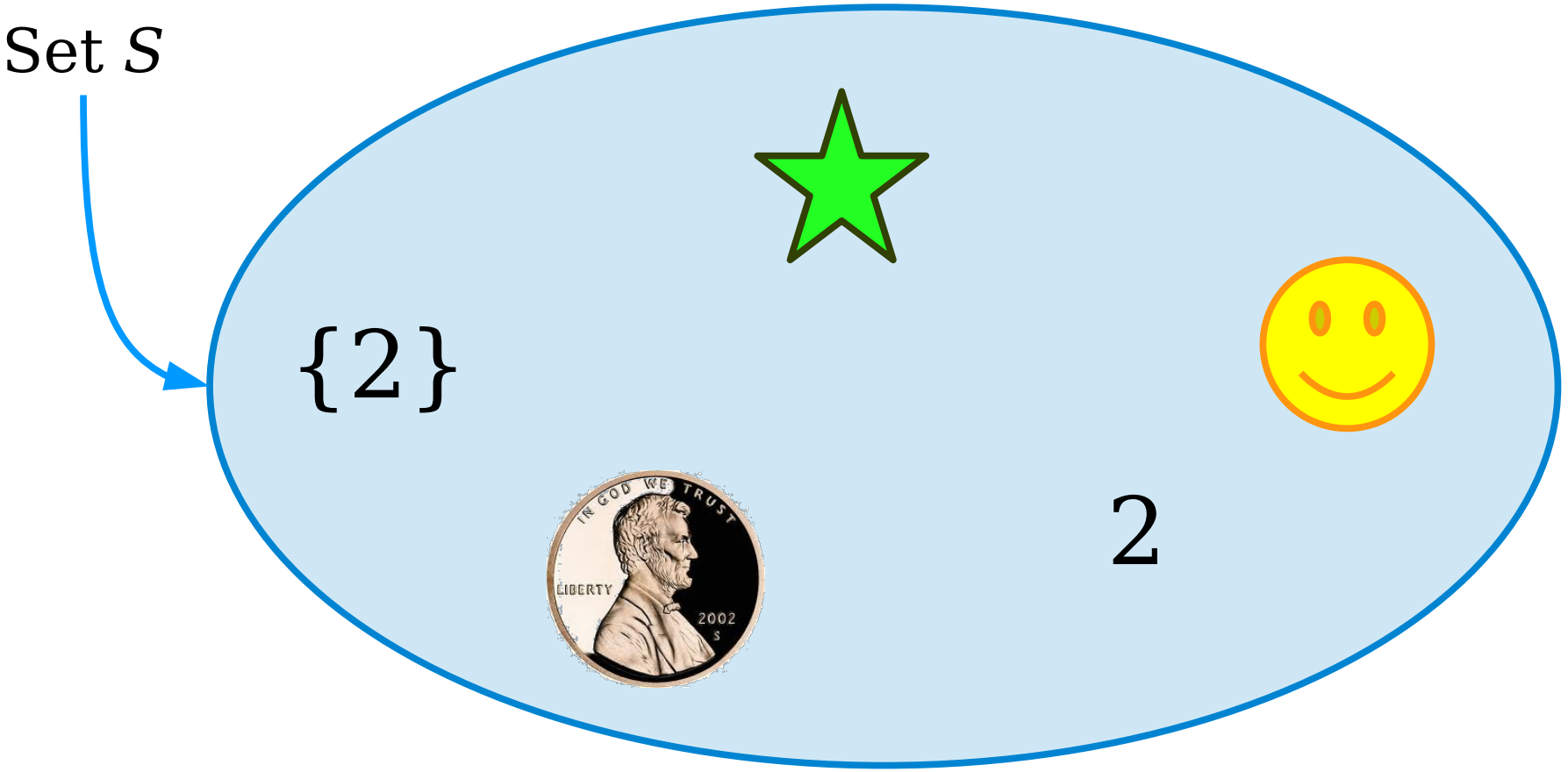
Subsets and Elements



General intuition:
$A \subseteq B$ if you can form A by ***circling elements of B***.

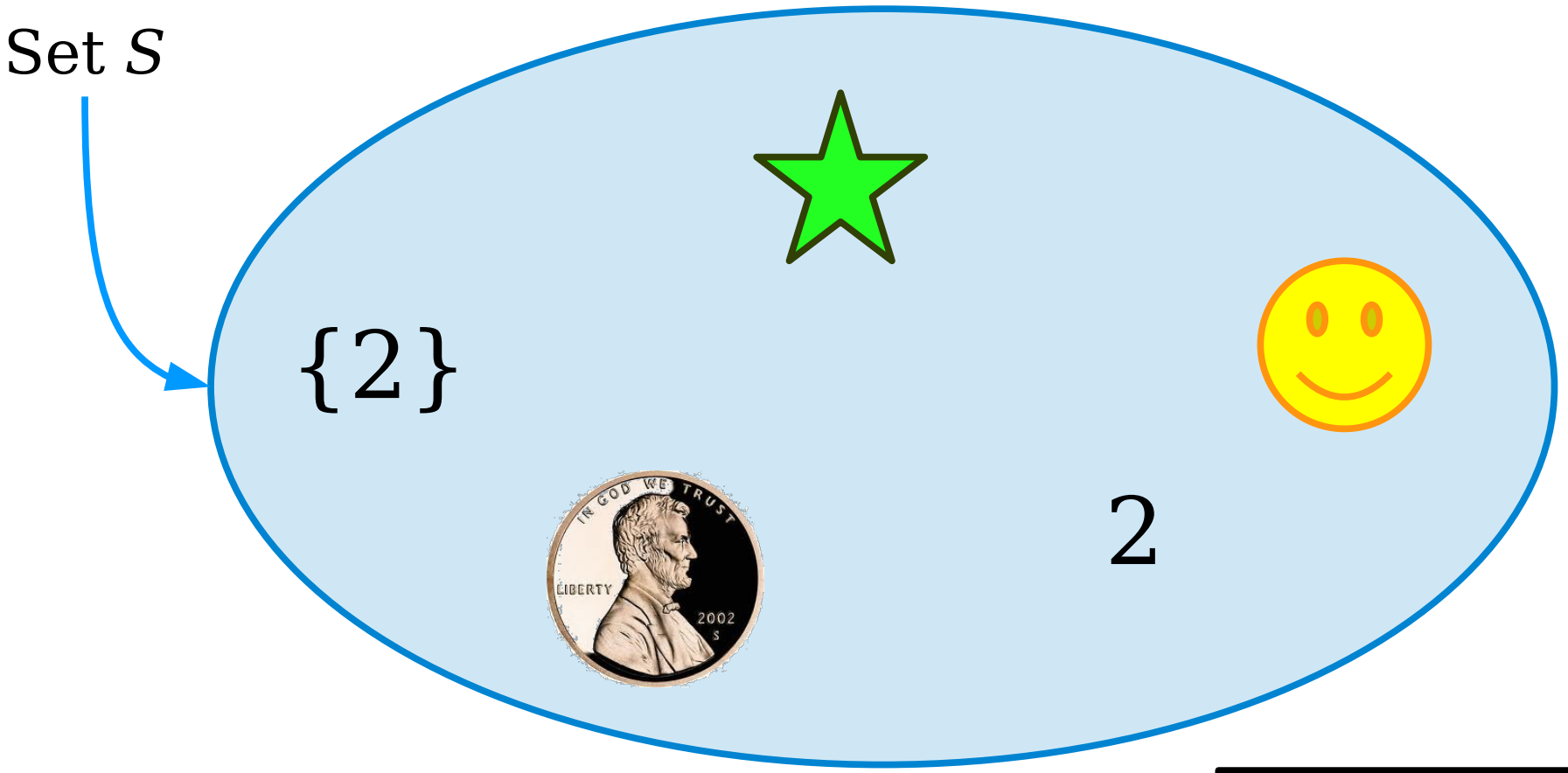
$\{2\} \subseteq S$

Subsets and Elements



$$2 \notin S$$

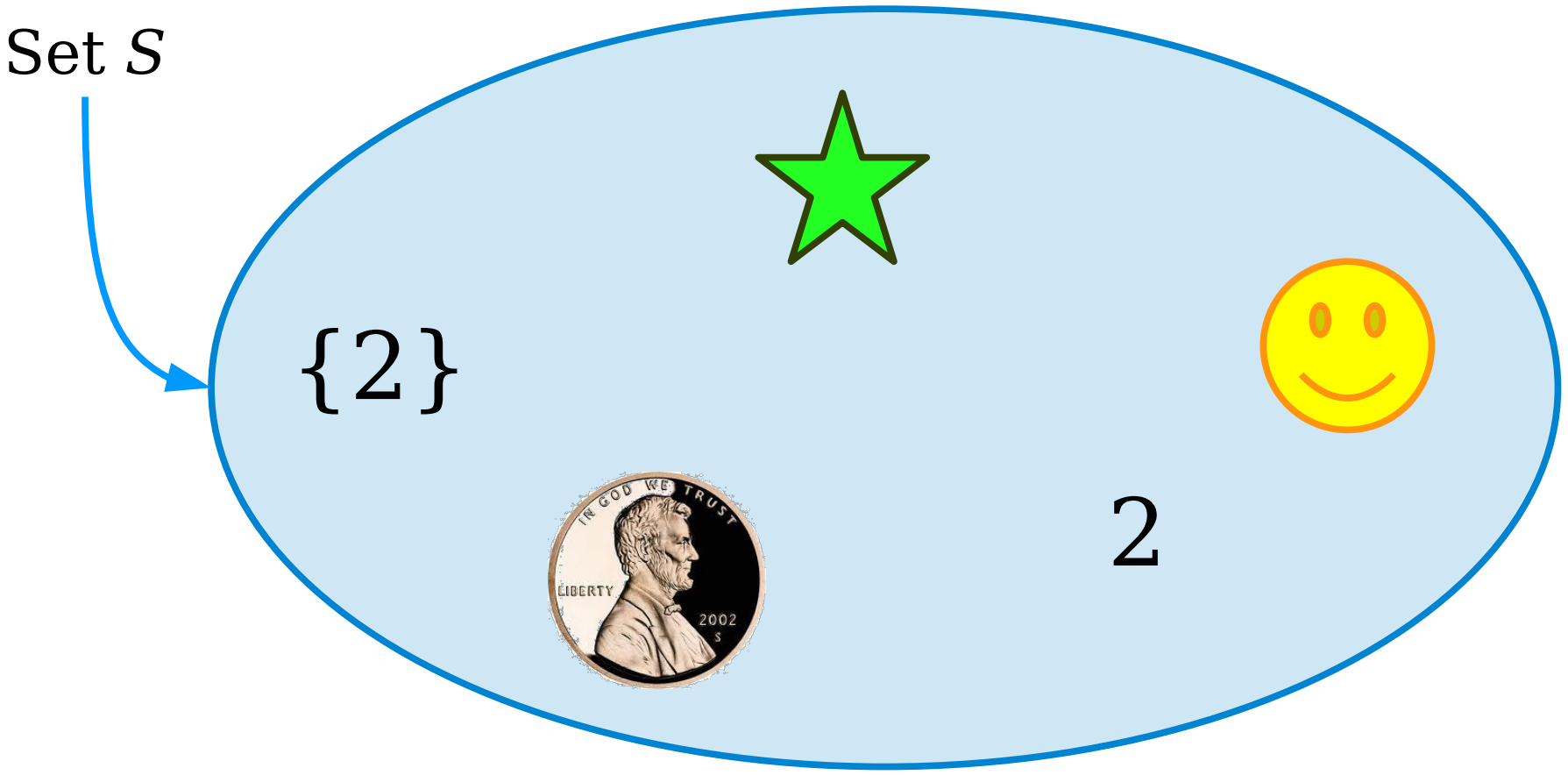
Subsets and Elements



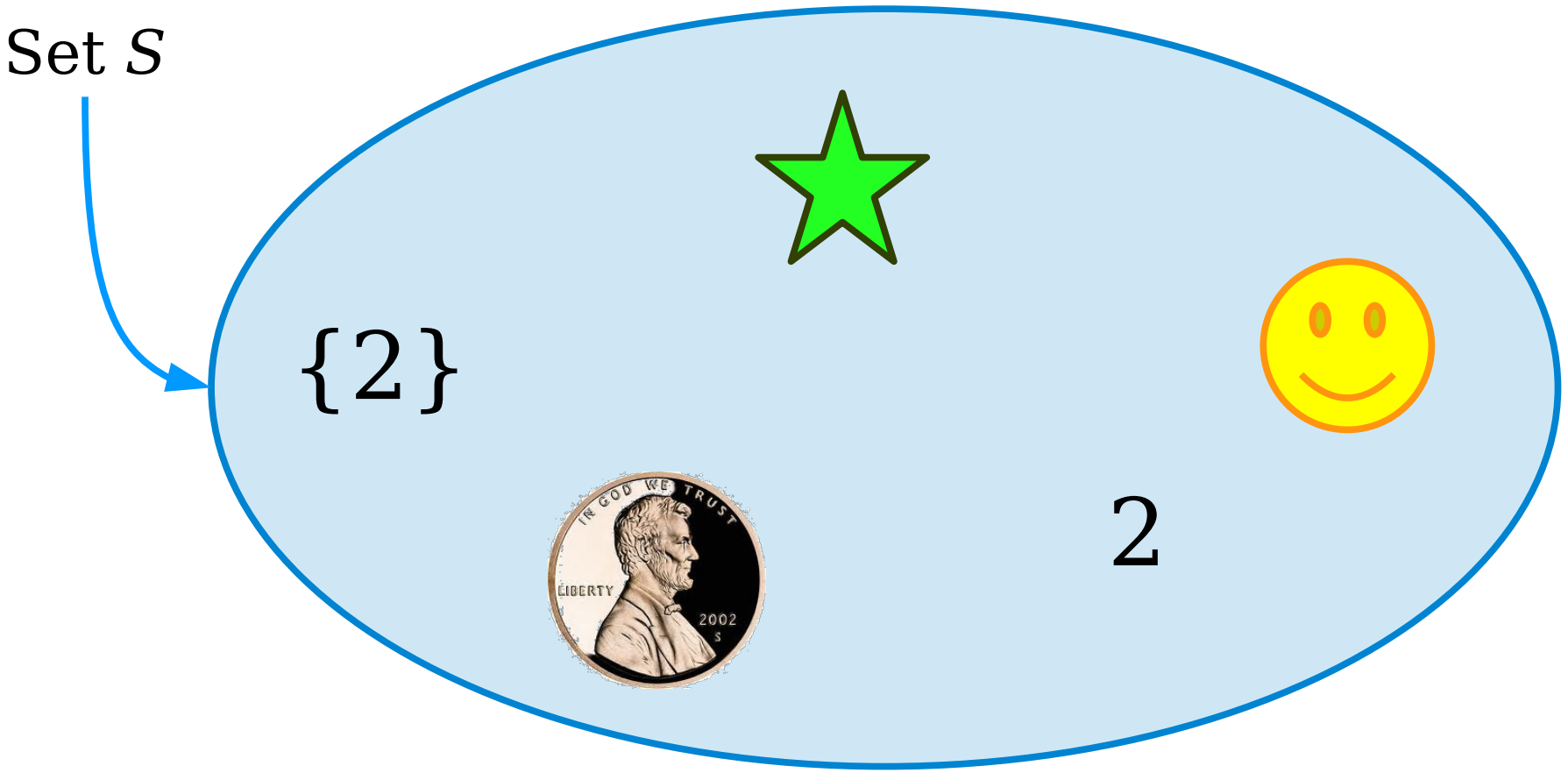
$2 \notin S$

(Since 2 isn't a set.)

Subsets and Elements

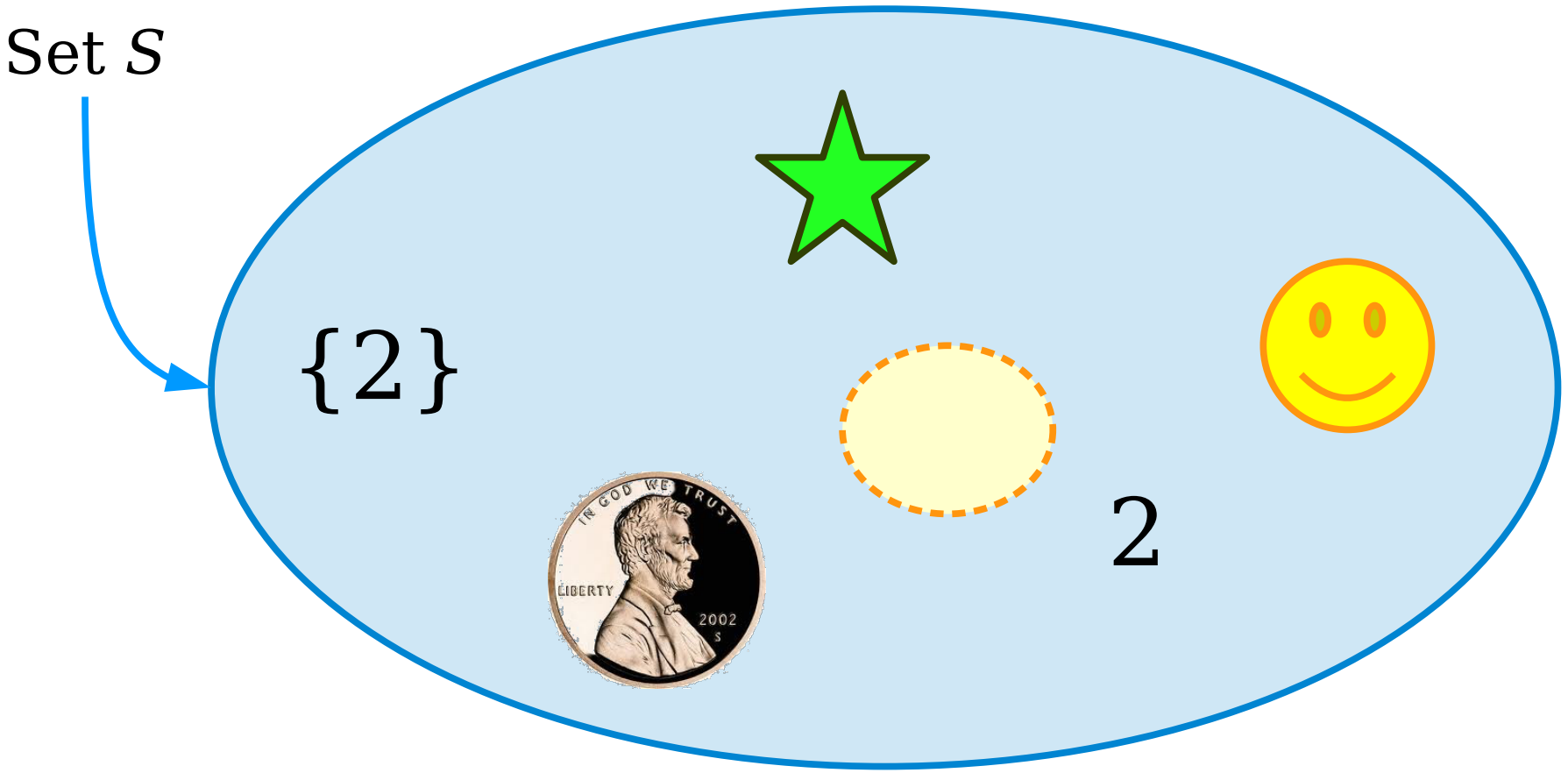


Subsets and Elements



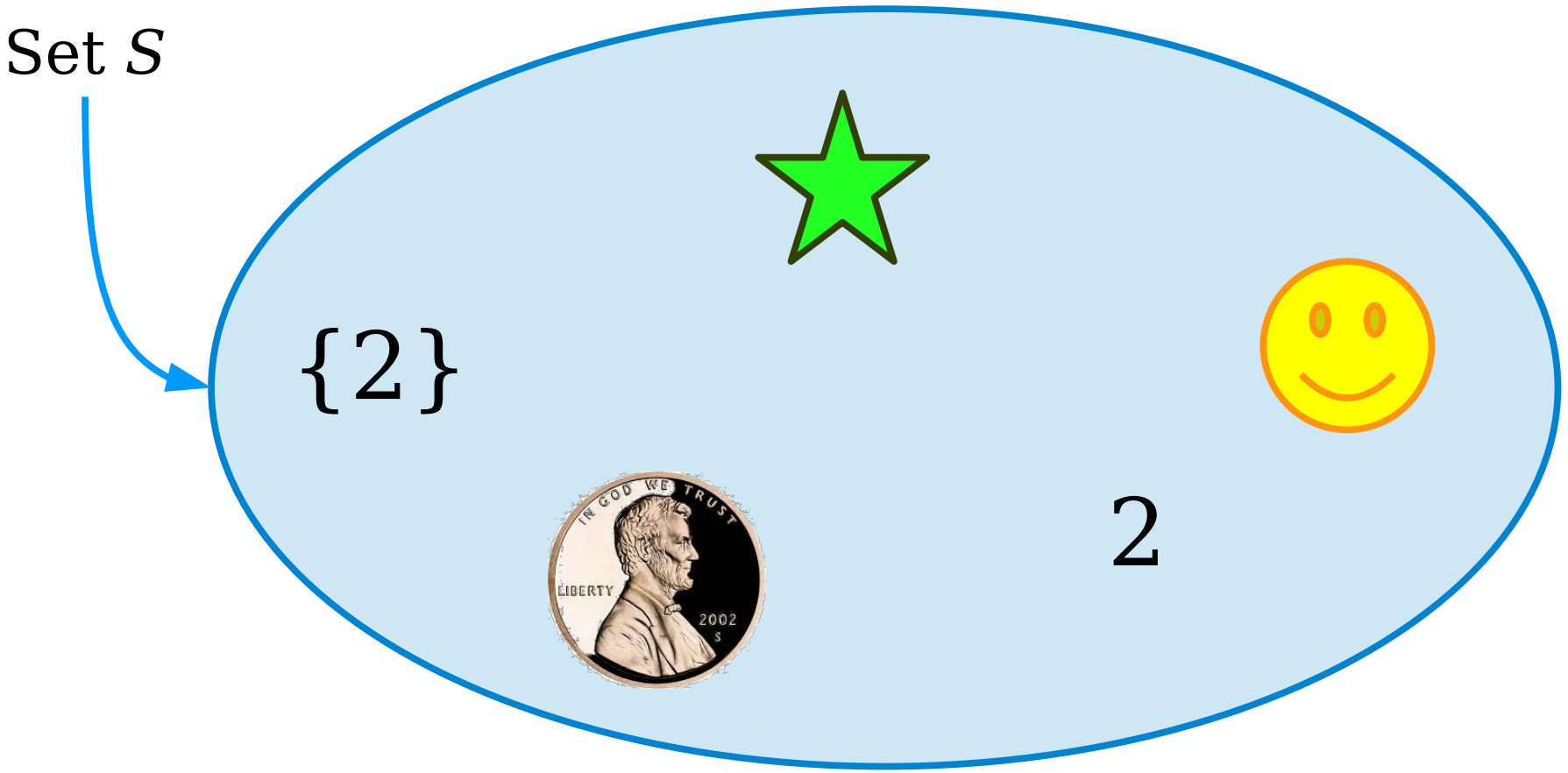
$$\emptyset \subseteq S$$

Subsets and Elements



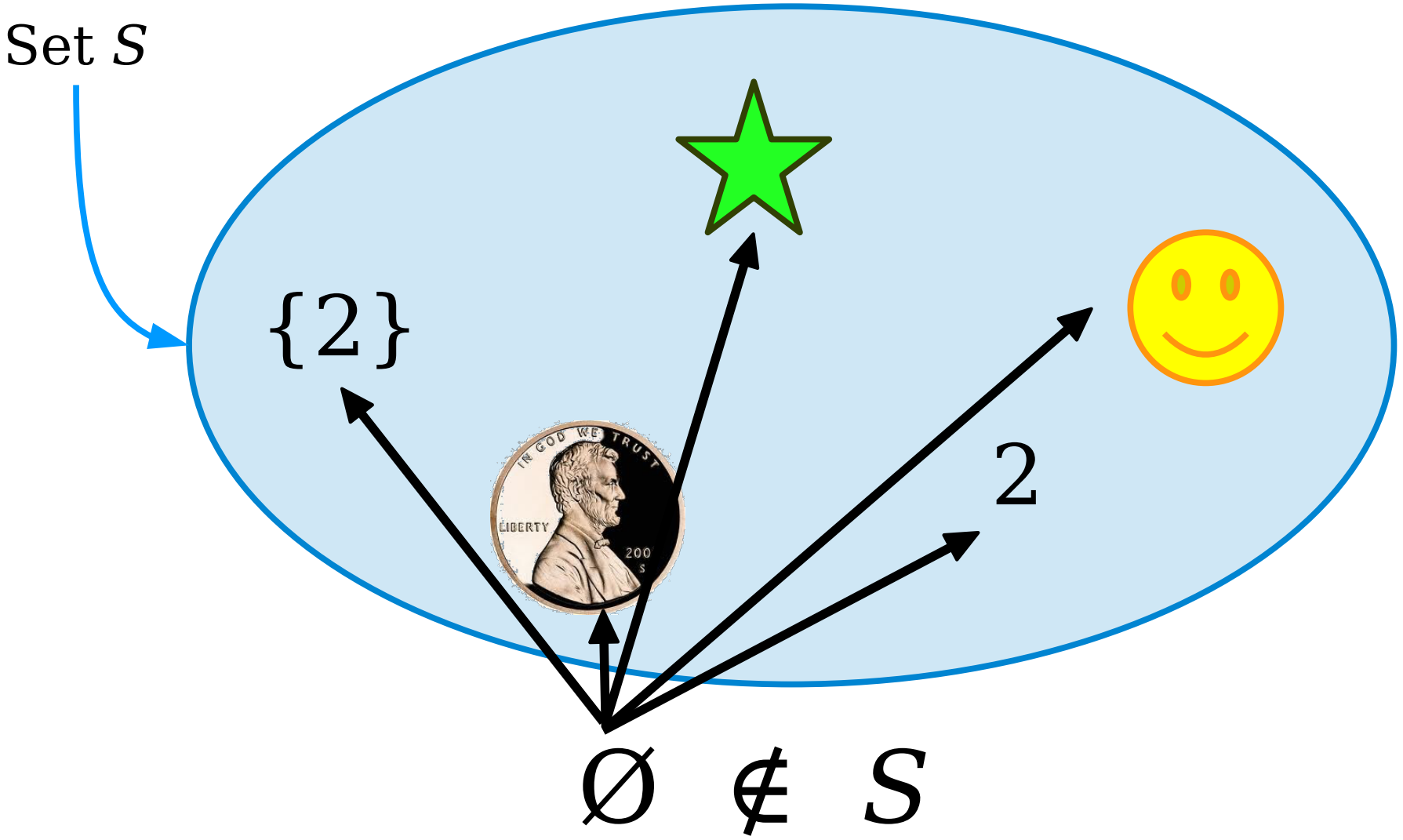
$$\emptyset \subseteq S$$

Subsets and Elements



$$\emptyset \notin S$$

Subsets and Elements



Subsets and Elements

- We say that $S \in T$ if, among the elements of T, one of them is *exactly* the object S
  - $s \in T$
- We say that $S \subseteq T$ if S is a set and every element of S is also an element of T. (S has to be a set for the statement $S \subseteq T$ to be true.)
- Although these concepts are similar, ***they are not the same!*** Not all elements of a set are subsets of that set and vice-versa.
- We have a resource on the course website, the Guide to Elements and Subsets, that explores this in more depth.

Power Sets

$$S = \{ \text{  }, \text{  } \}$$

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

This is the ***power set*** of S, the set of all subsets of S. We write the power set of S as $\wp(S)$.

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

(Do you see why?)

Question: What is $\wp(\emptyset)$?

Respond at pollev.com/robynreiss

What is $\wp(\emptyset)$?

Answer: $\{\emptyset\}$

Remember that $\emptyset \neq \{\emptyset\}$!

Cardinality

Cardinality

- The ***cardinality*** of a set is the number of elements it contains.
- If S is a set, we denote its cardinality as $\boldsymbol{|S|}$.
- Examples:
  - $|\{whimsy, mirth\}| = 2$
  - $|\{\{a, b\}, \{c, d, e, f, g\}, \{h\}\}| = 3$
  - $|\{1, 2, 3, 3, 3, 3, 3\}| = 3$
  - $|\{ n \in \mathbb{N} \mid n < 4 \}| = |\{0, 1, 2, 3\}| = 4$
  - $| \varnothing | = 0$
  - $| \{\varnothing\} | = 1$

The Cardinality of ℕ

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

The Cardinality of ℕ

- What is |ℕ|?
  - There are infinitely many natural numbers.
  - |ℕ| can't be a natural number, since it's infinitely large.
- We need to introduce a new term.
- Let's define $\aleph_0 = |\mathbb{N}|$.
  - $\aleph_0$ is pronounced “aleph-zero,” “aleph-nought,” or “aleph-null.”

Consider the set

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

What is $|S|$?

How Big Are These Sets?

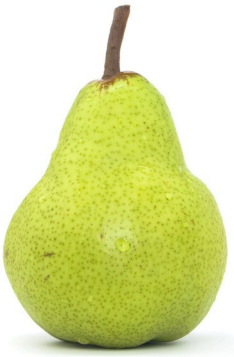
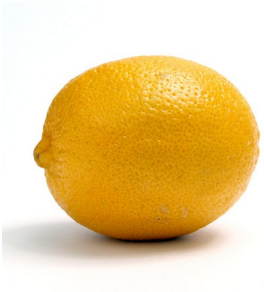
{ 

, 

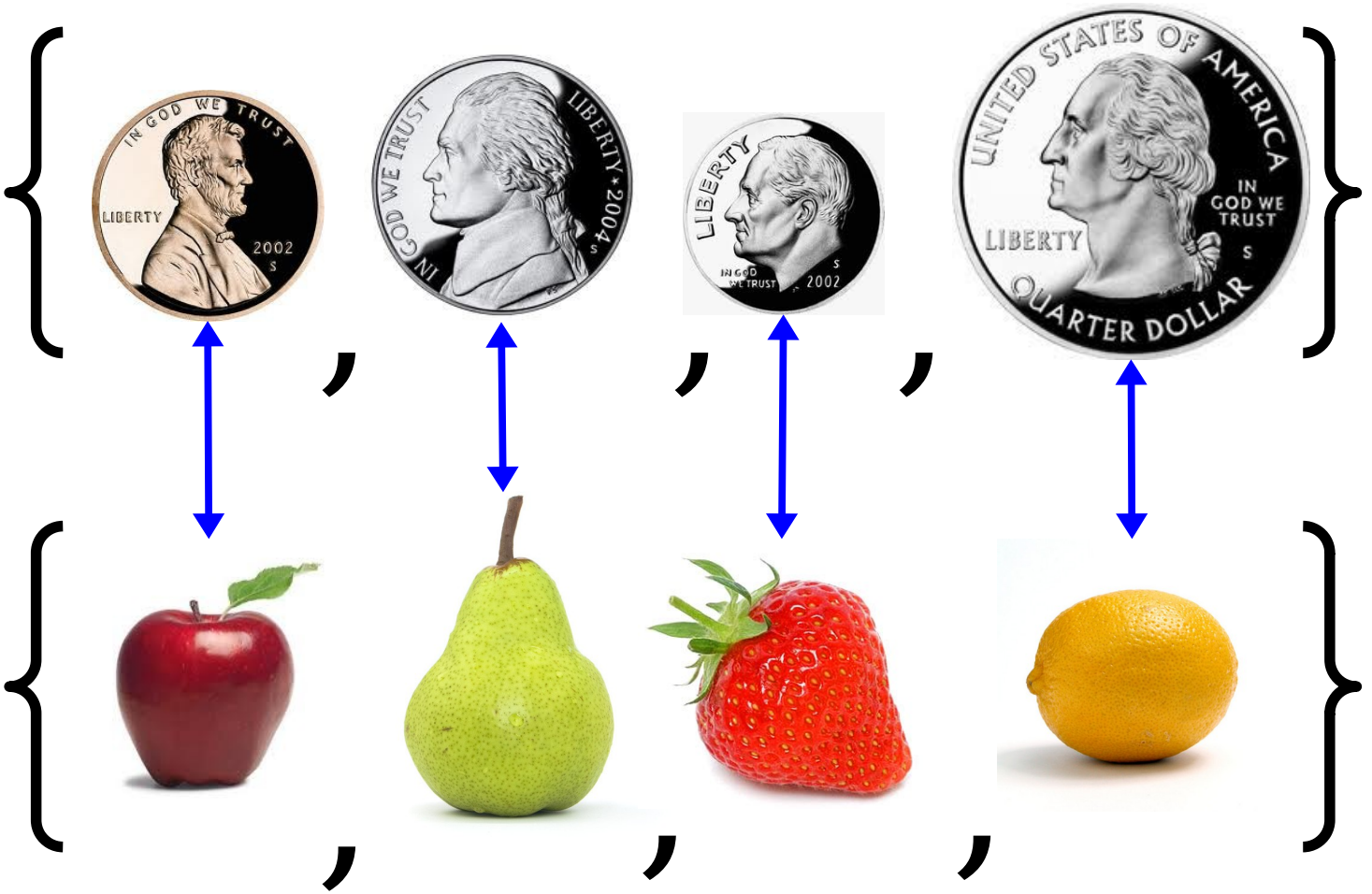
, 

, 

}

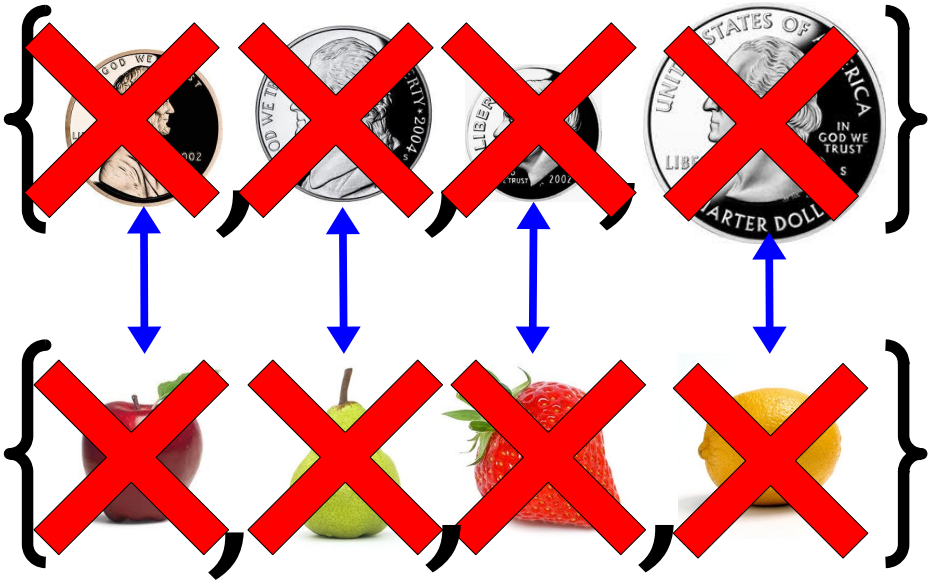
{ 
, 
, 
, 
}

How Big Are These Sets?



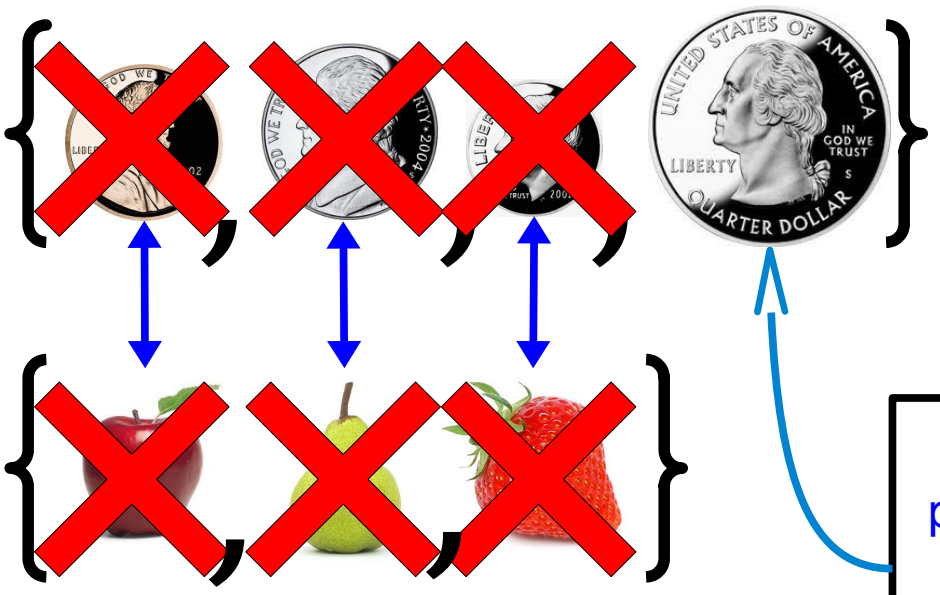
Comparing Cardinalities

- *By definition,* two sets have the same size if there is a way to pair their elements off without leaving any elements uncovered.
- The intuition:



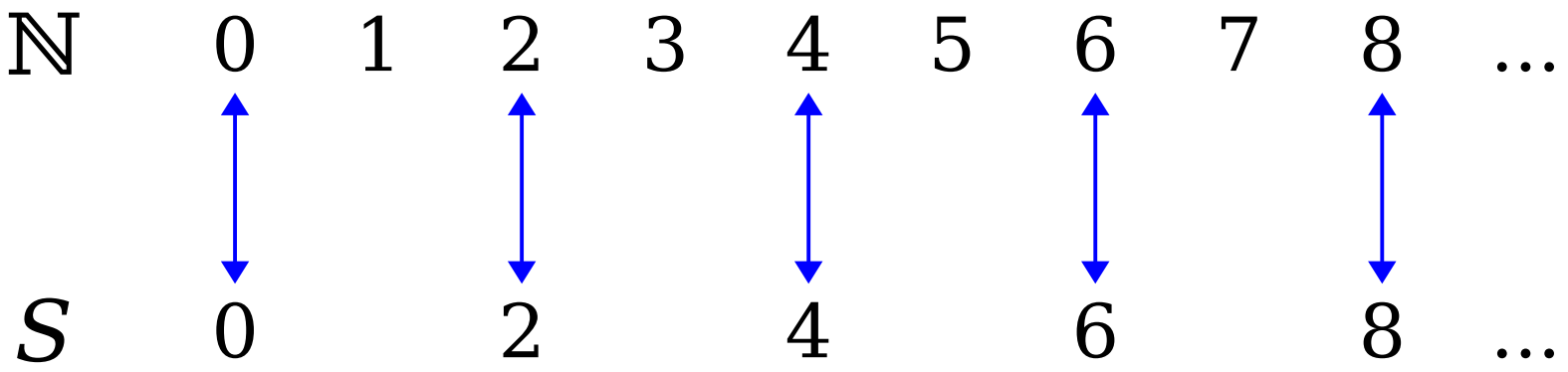
Comparing Cardinalities

- *By definition,* two sets have the same size if there is a way to pair their elements off without leaving any elements uncovered.
- The intuition:



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

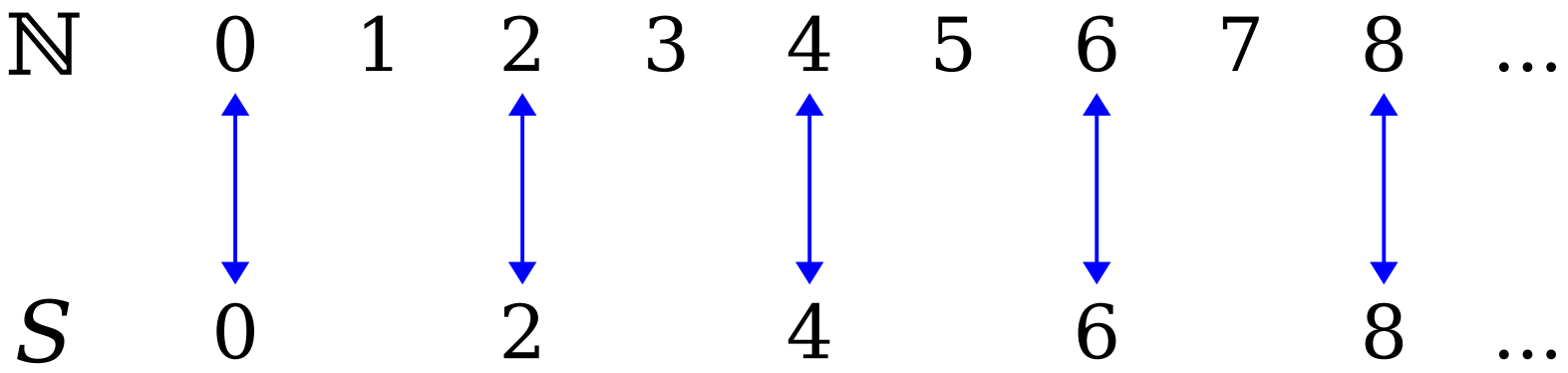
Infinite Cardinalities



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

Two sets have the same size if there is a way to pair their elements off without leaving any elements uncovered

Infinite Cardinalities



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

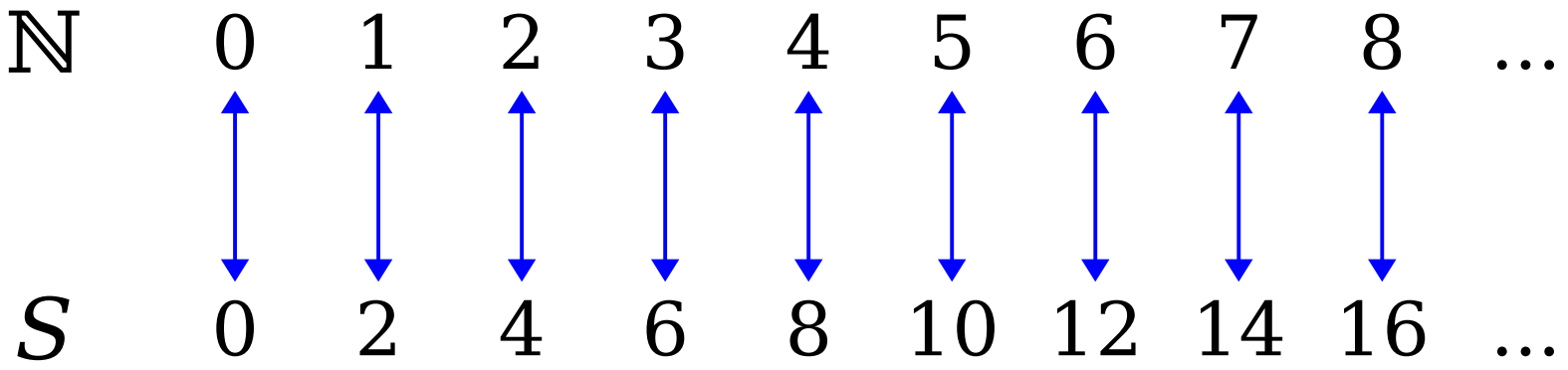
Two sets have the same size if *there is a way* to pair their elements off without leaving any elements uncovered

Infinite Cardinalities

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

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

Infinite Cardinalities



$$n \leftrightarrow 2n$$

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

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

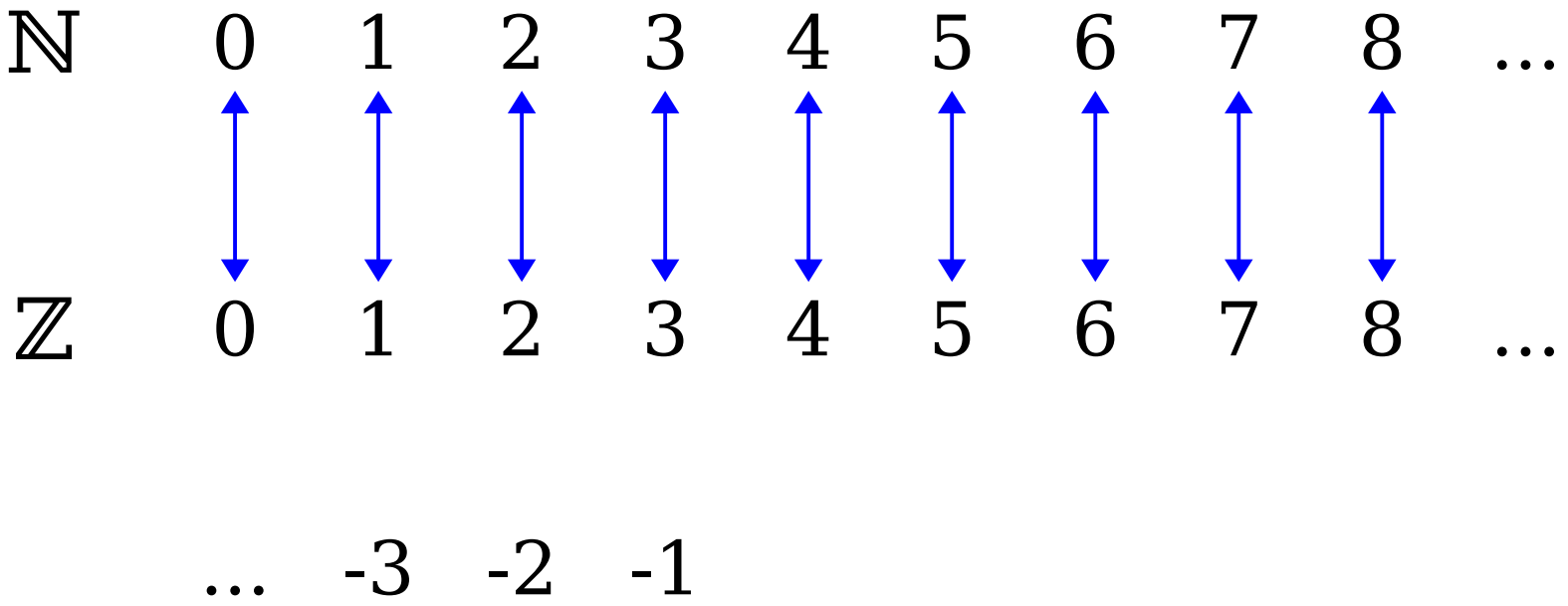
Infinite Cardinalities

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

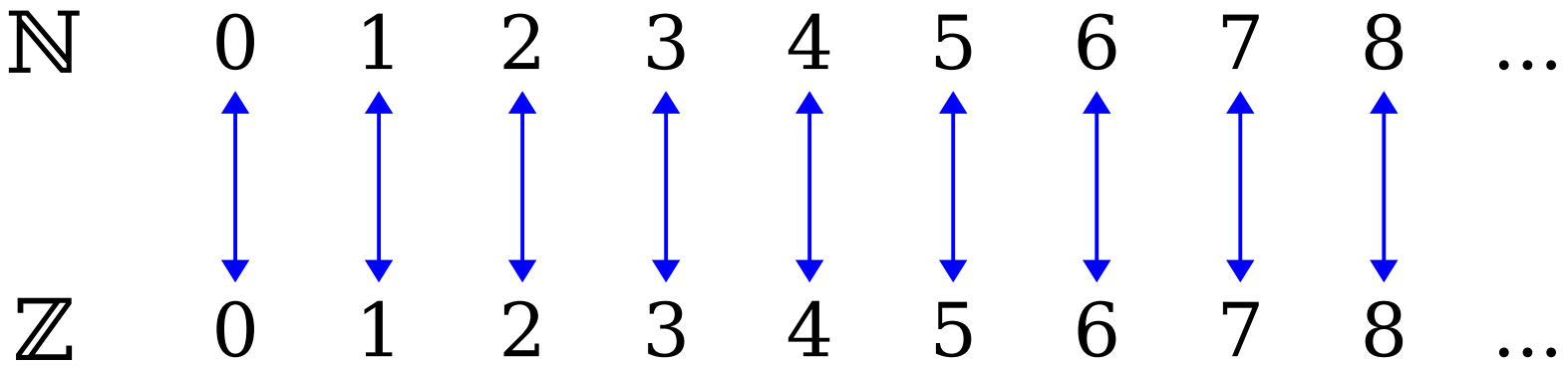
Infinite Cardinalities

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

Infinite Cardinalities



Infinite Cardinalities



Two sets have the same size if *there is a way* to pair their elements off without leaving any elements uncovered

Infinite Cardinalities

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

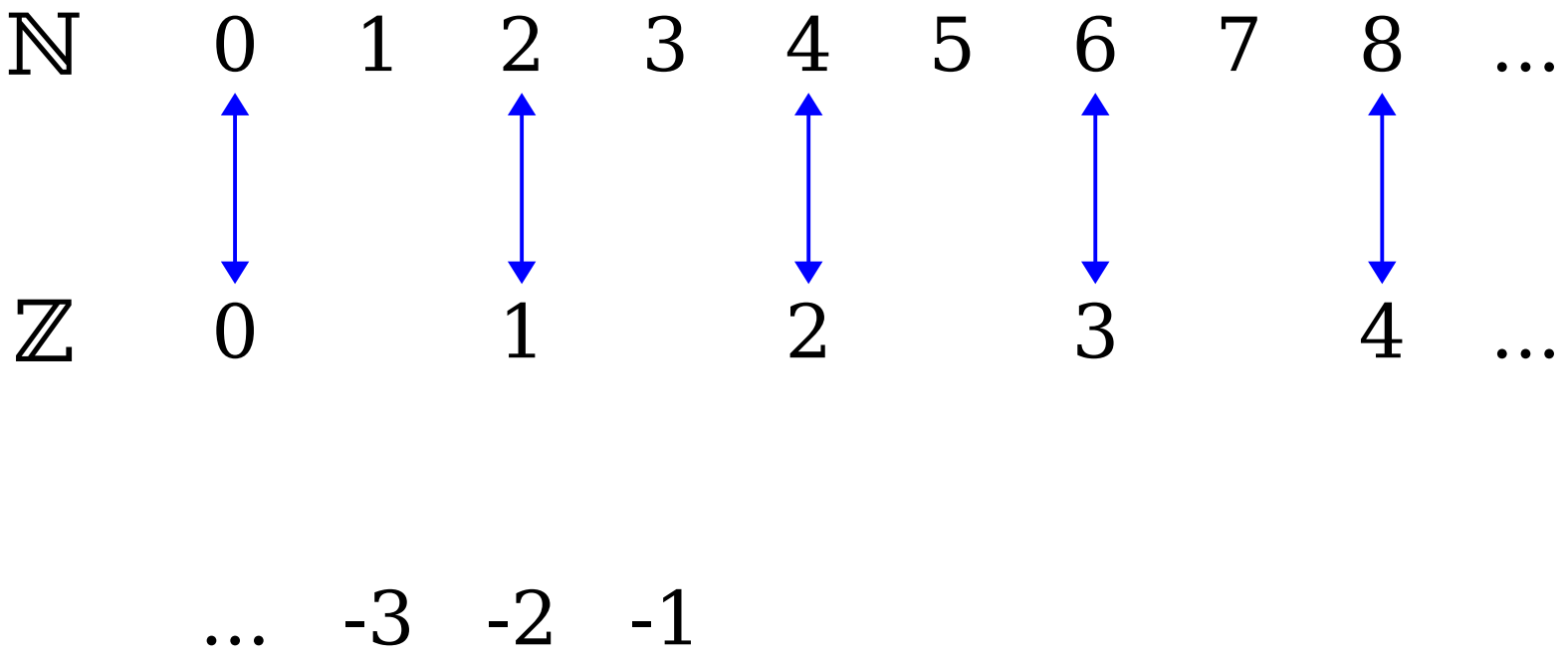
Infinite Cardinalities

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

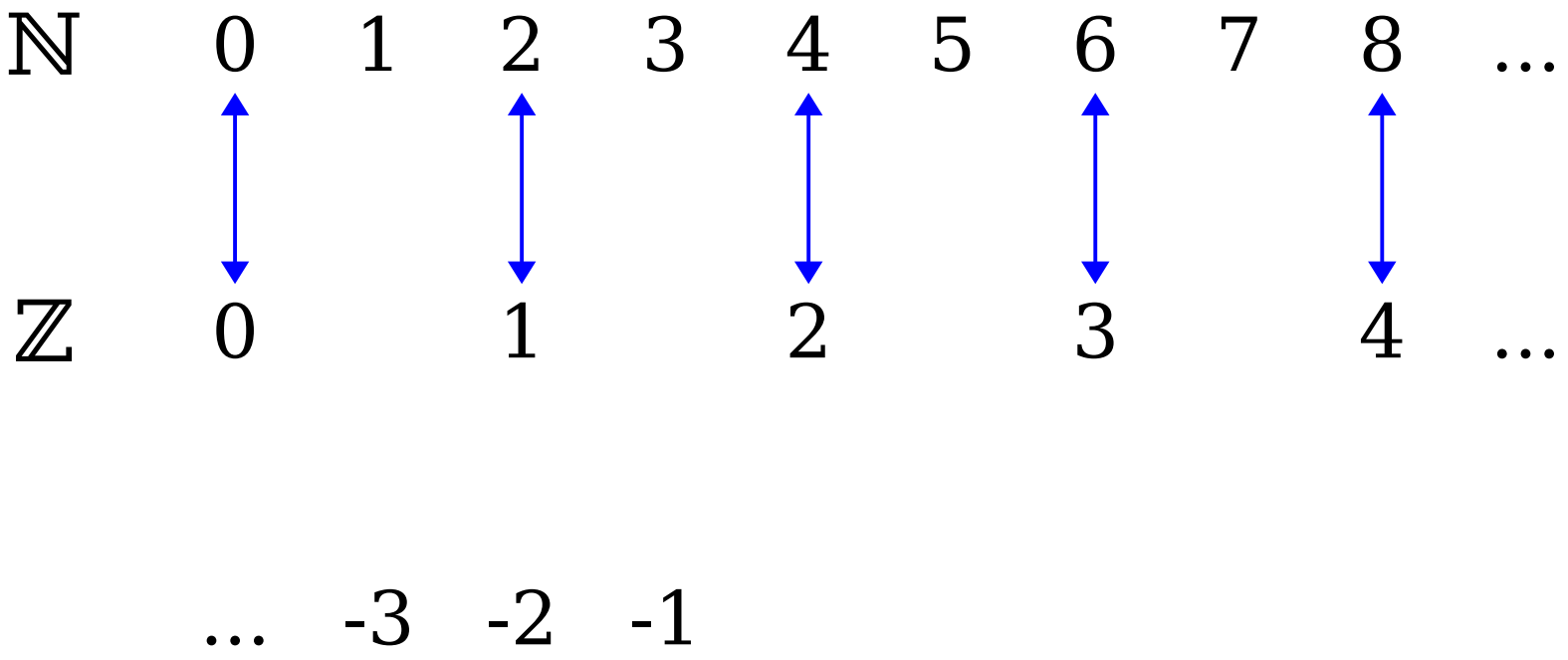
Infinite Cardinalities

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

Infinite Cardinalities

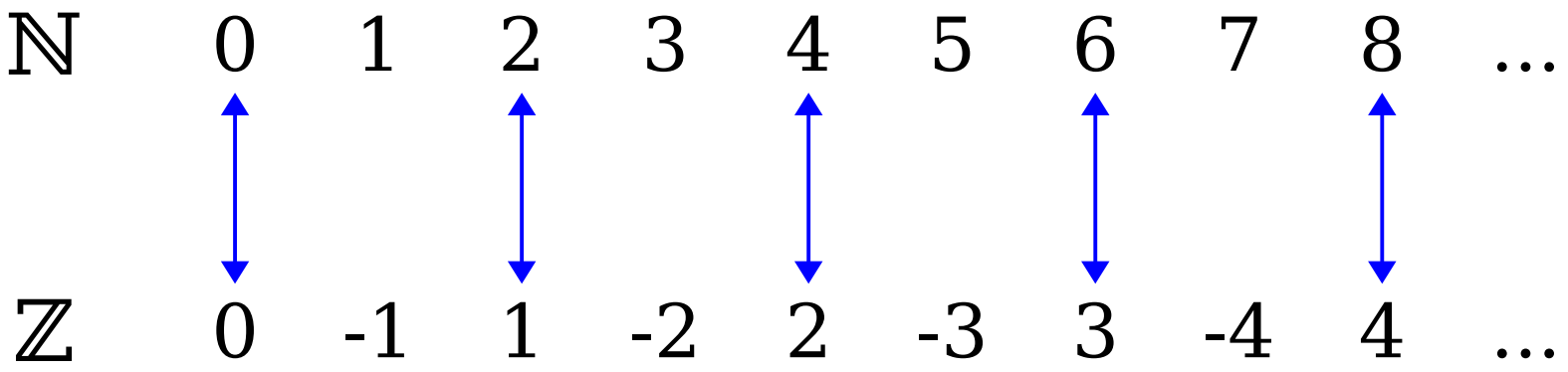


Infinite Cardinalities



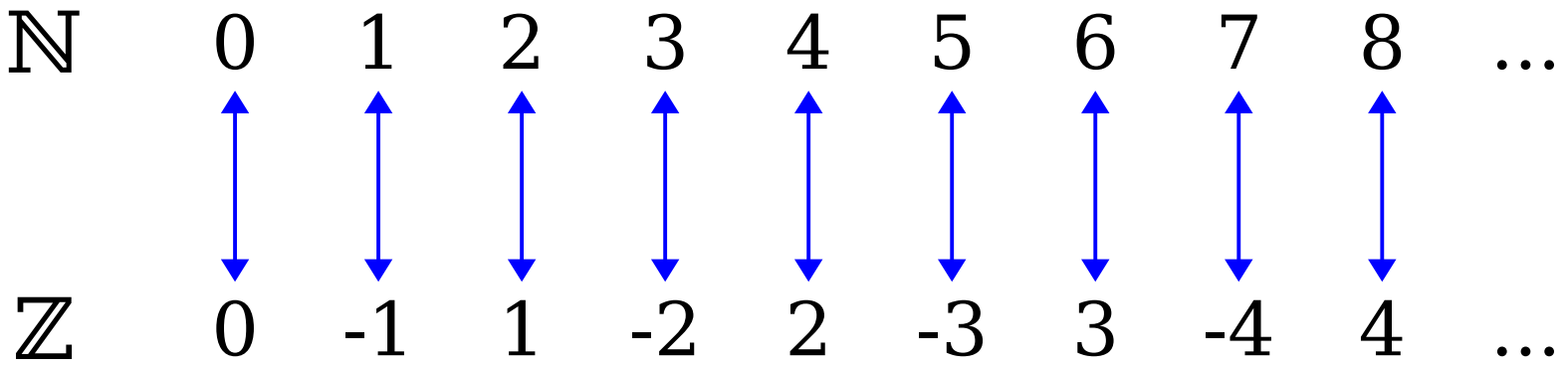
Pair nonnegative integers with even natural numbers.

Infinite Cardinalities



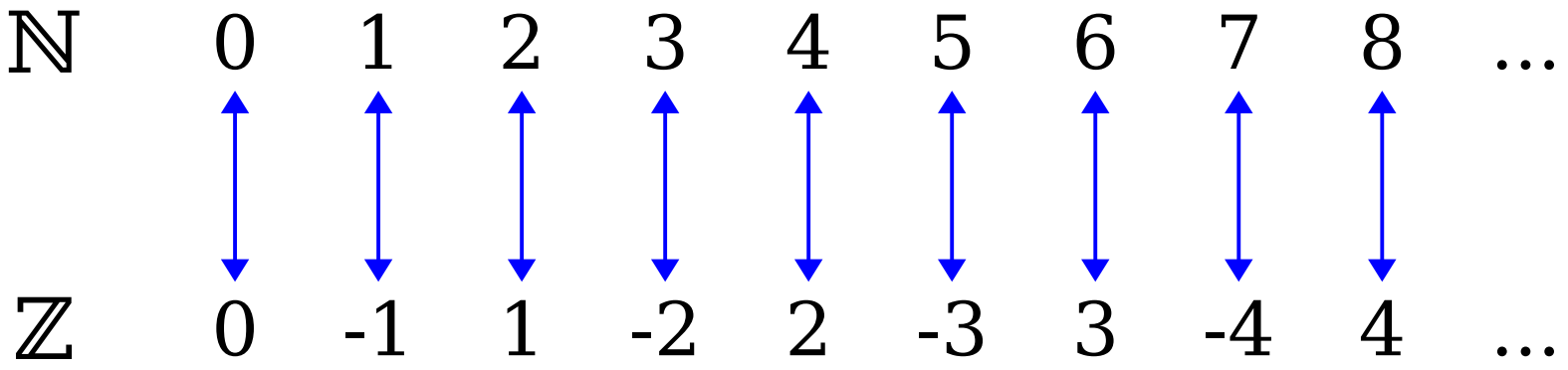
Pair nonnegative integers with even natural numbers.

Infinite Cardinalities



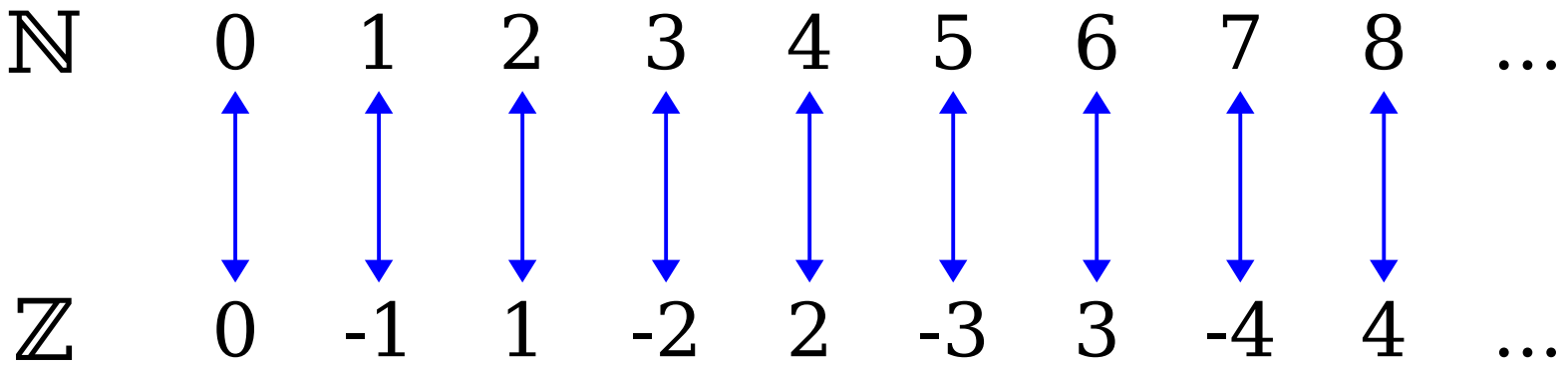
Pair nonnegative integers with even natural numbers.

Infinite Cardinalities



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

Infinite Cardinalities



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

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

Important Question:

Do all infinite sets have
the same cardinality?

$$S = \left\{ \text{  }, \text{  } \right\}$$

$$\wp(S) = \left\{ \varnothing, \left\{ \text{  } \right\}, \left\{ \text{  } \right\}, \left\{ \text{  }, \text{  } \right\} \right\}$$

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

$$S = \{ \text{penny}, \text{nickel}, \text{button} \}$$

$$\wp(S) = \{ \emptyset, \{\text{penny}\}, \{\text{nickel}\}, \{\text{button}\}, \{\text{penny}, \text{nickel}\}, \{\text{penny}, \text{button}\}, \{\text{nickel}, \text{button}\}, \{\text{penny}, \text{nickel}, \text{button}\} \}$$

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

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

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

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

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

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

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

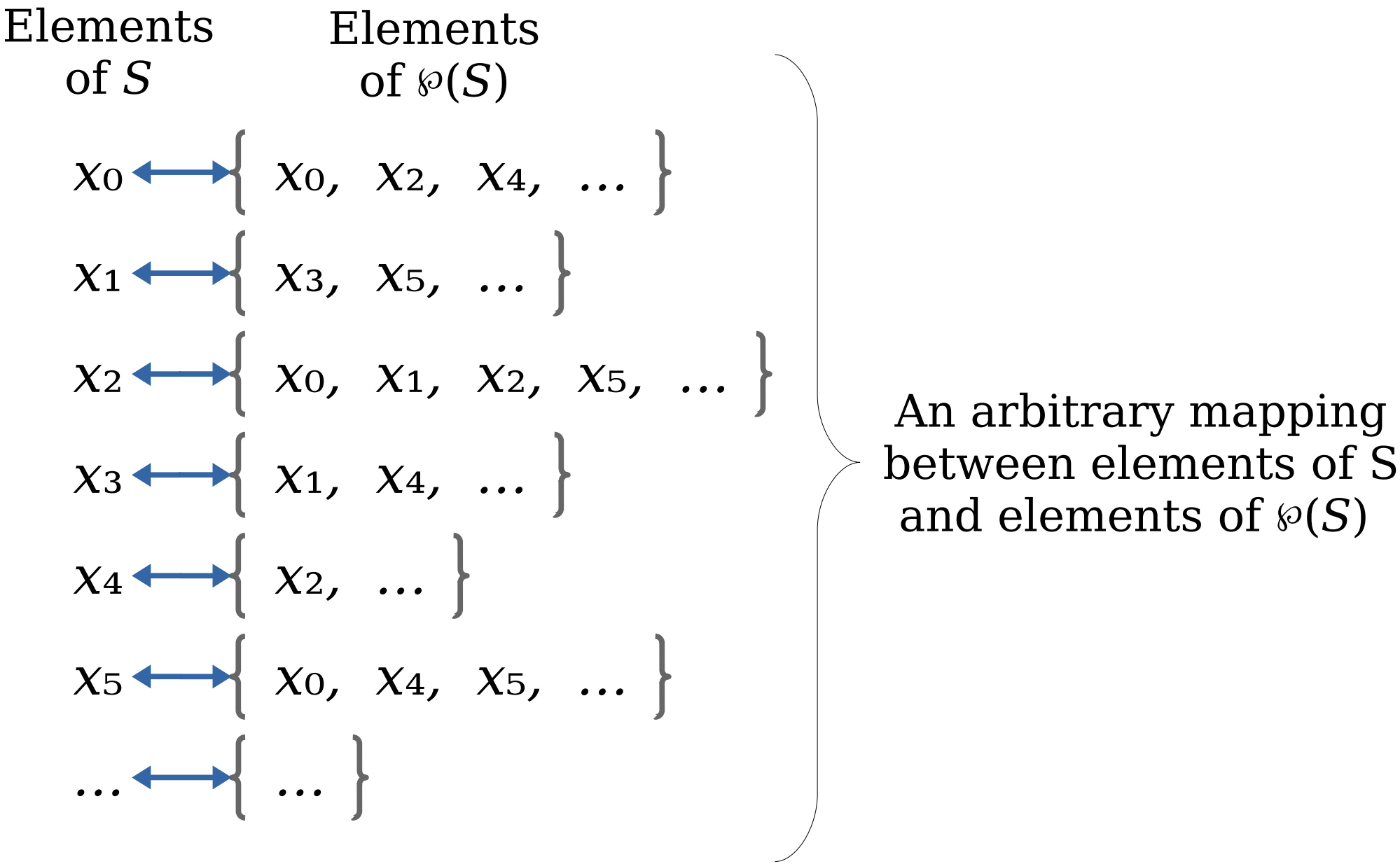
If $|S| = |\wp(S)|$, we can pair up the elements of S and the elements of $\wp(S)$ without leaving anything out.

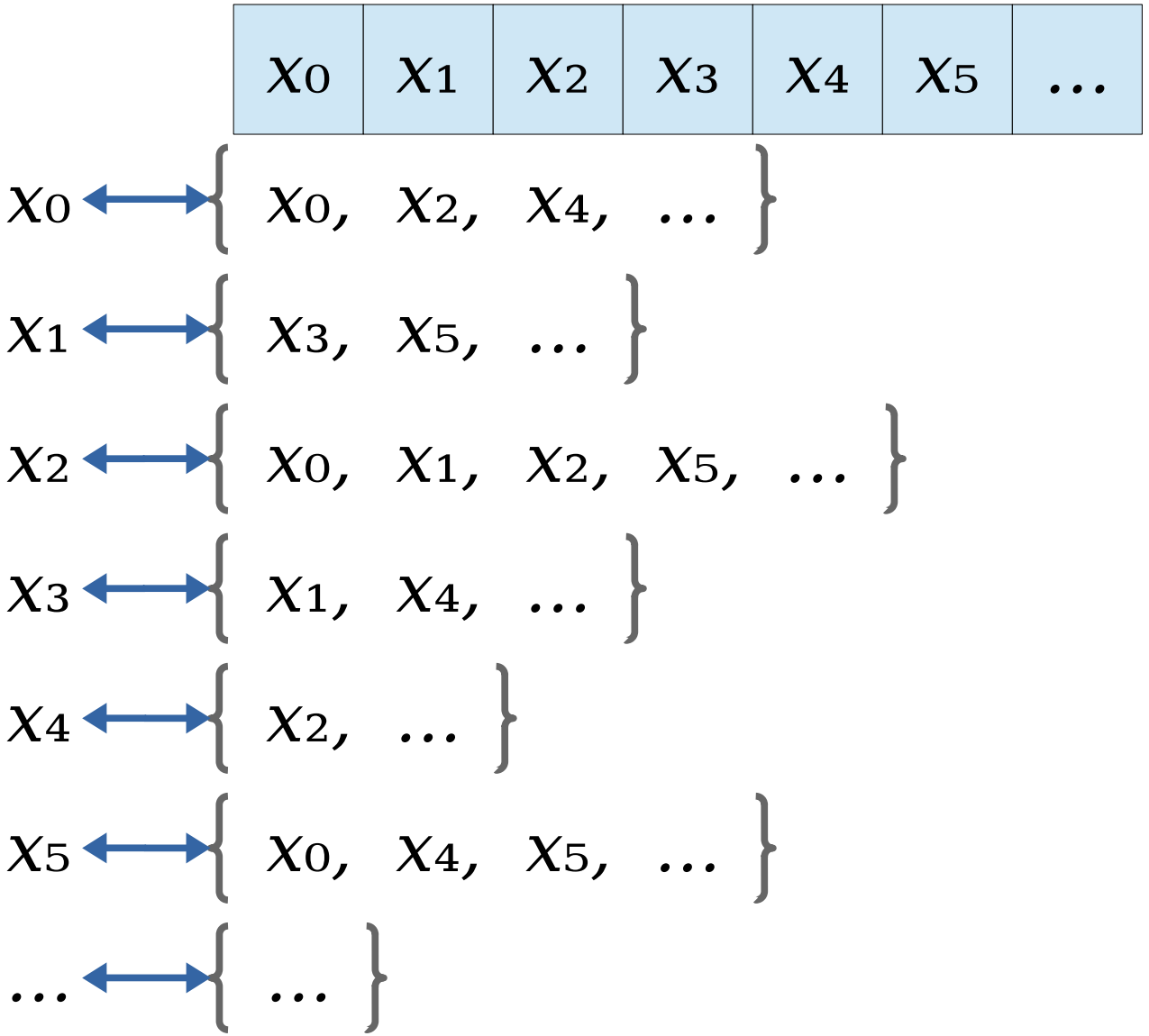
If $|S| = |\wp(S)|$, we can pair up the elements of S and the subsets of S without leaving anything out.

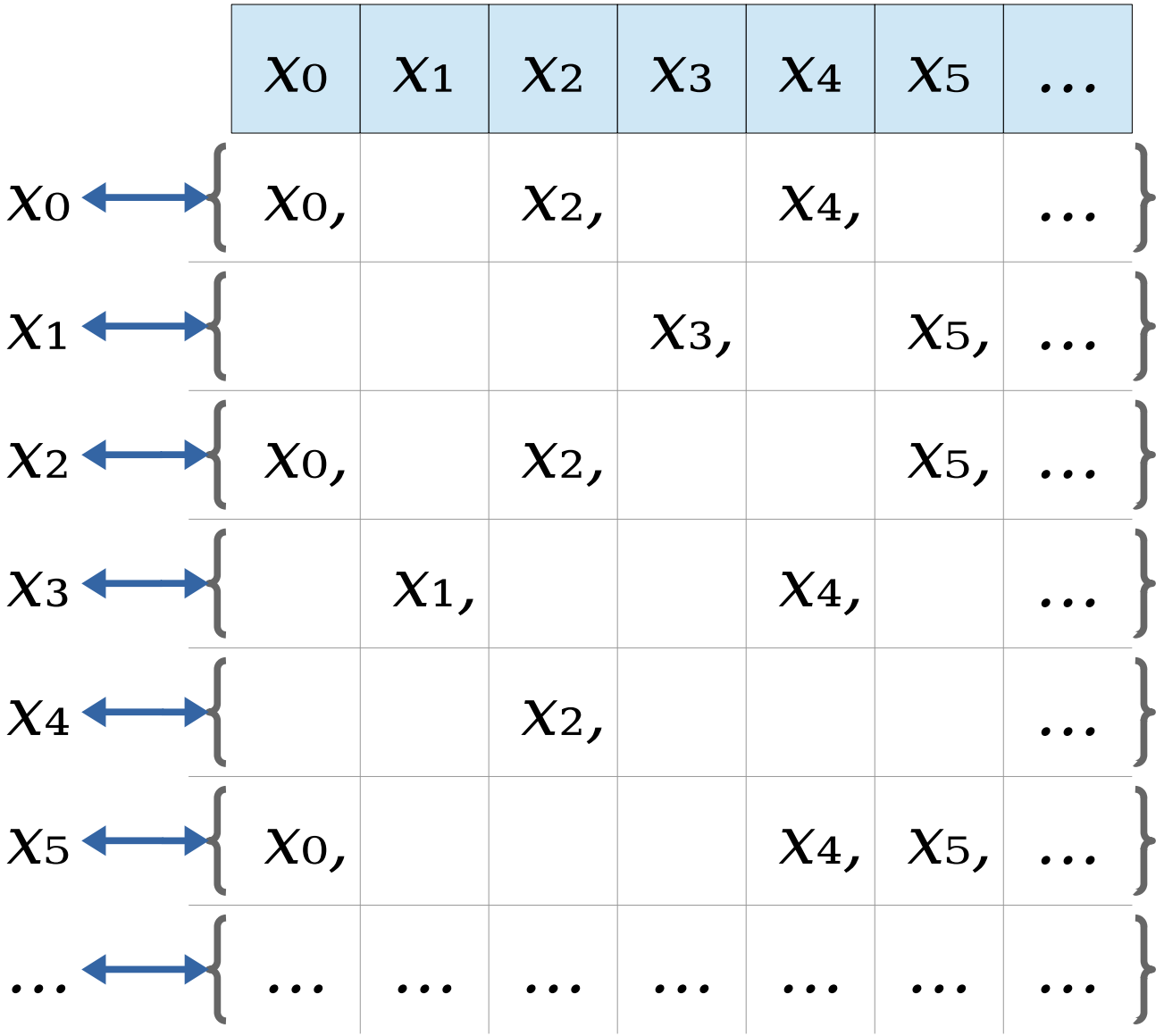
If $|S| = |\wp(S)|$, we can pair up the elements of S and the subsets of S without leaving anything out.

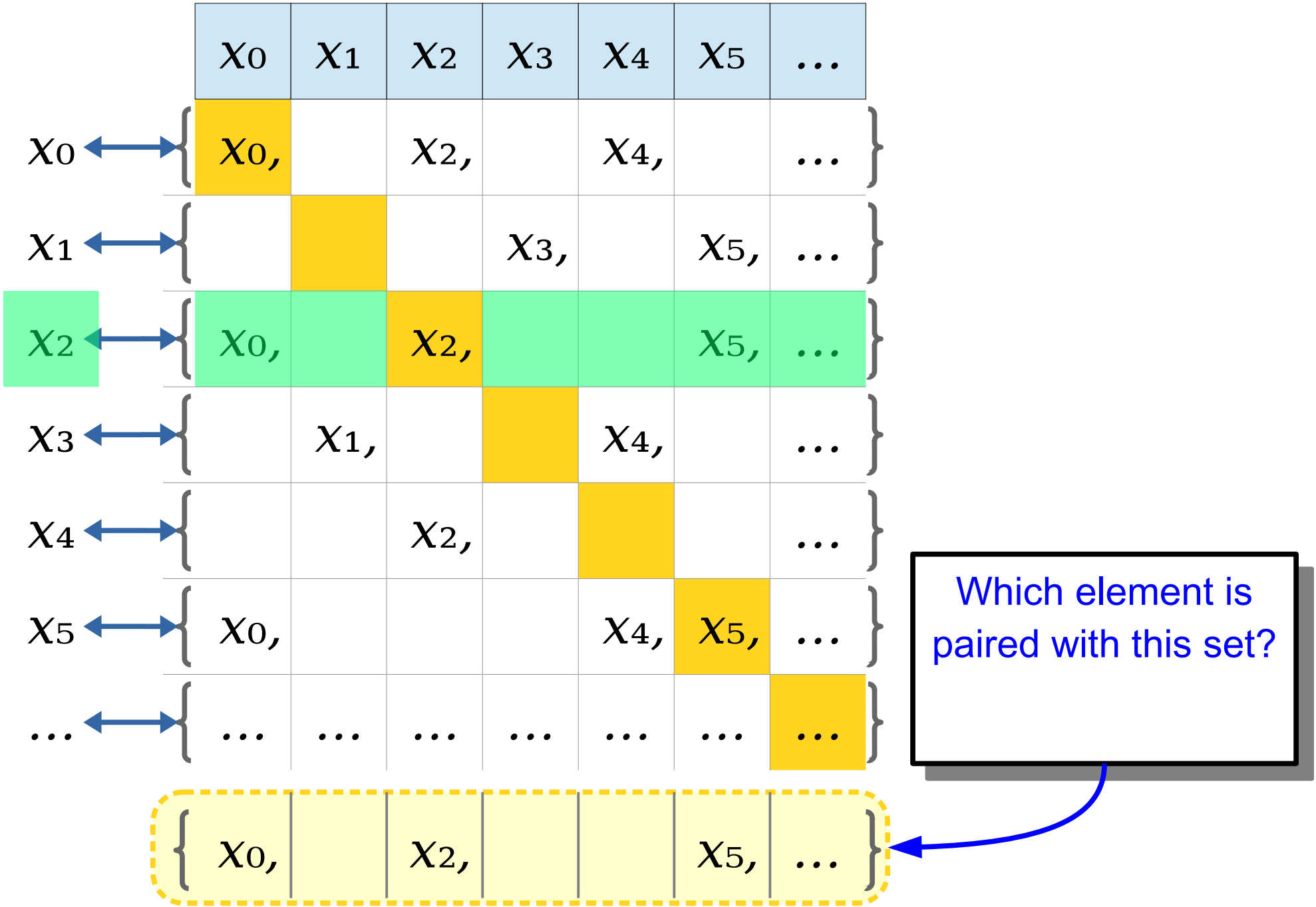
If $|S| = |\wp(S)|$, we can pair up the elements of S and the subsets of S without leaving anything out.

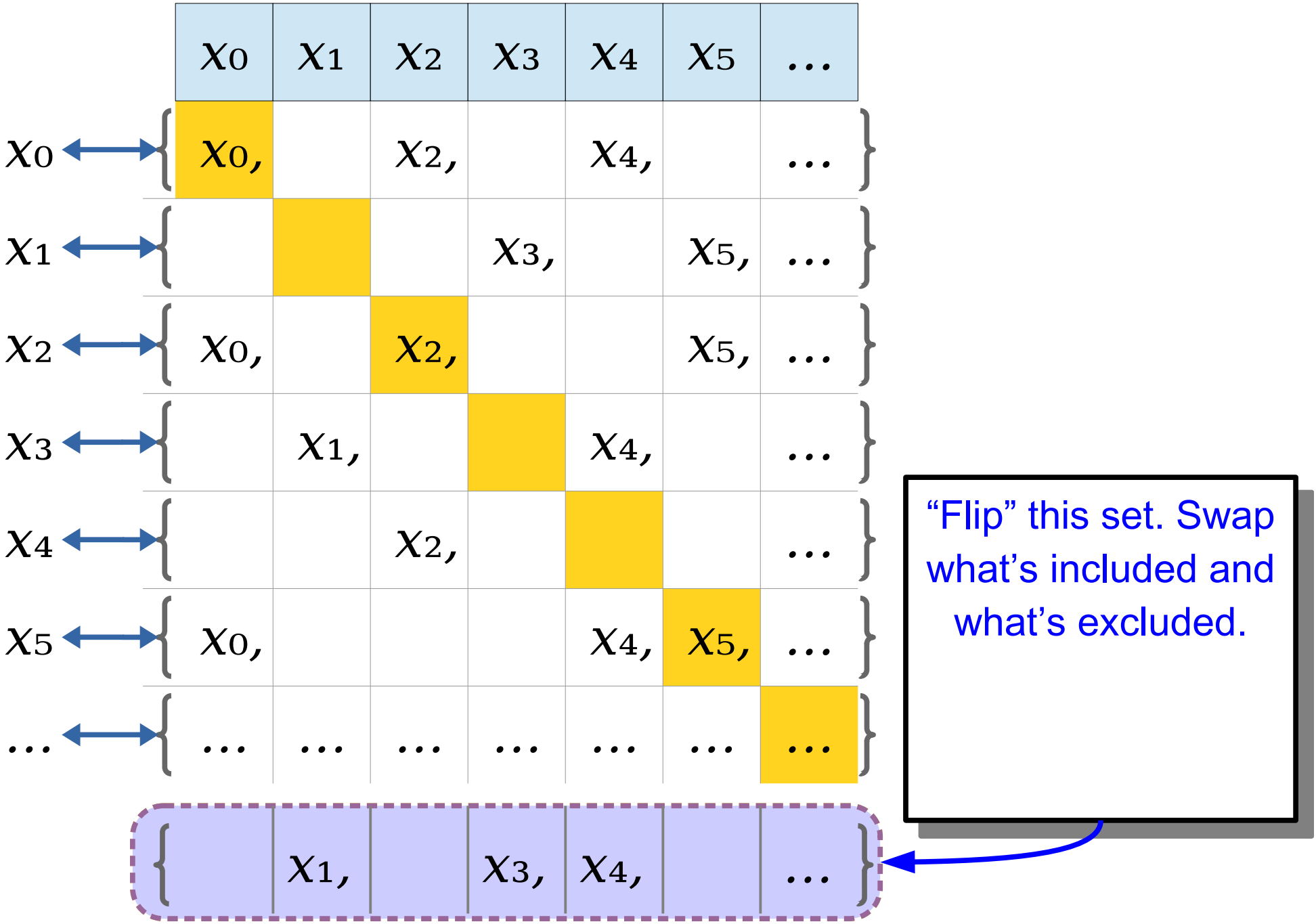
What would that look like?

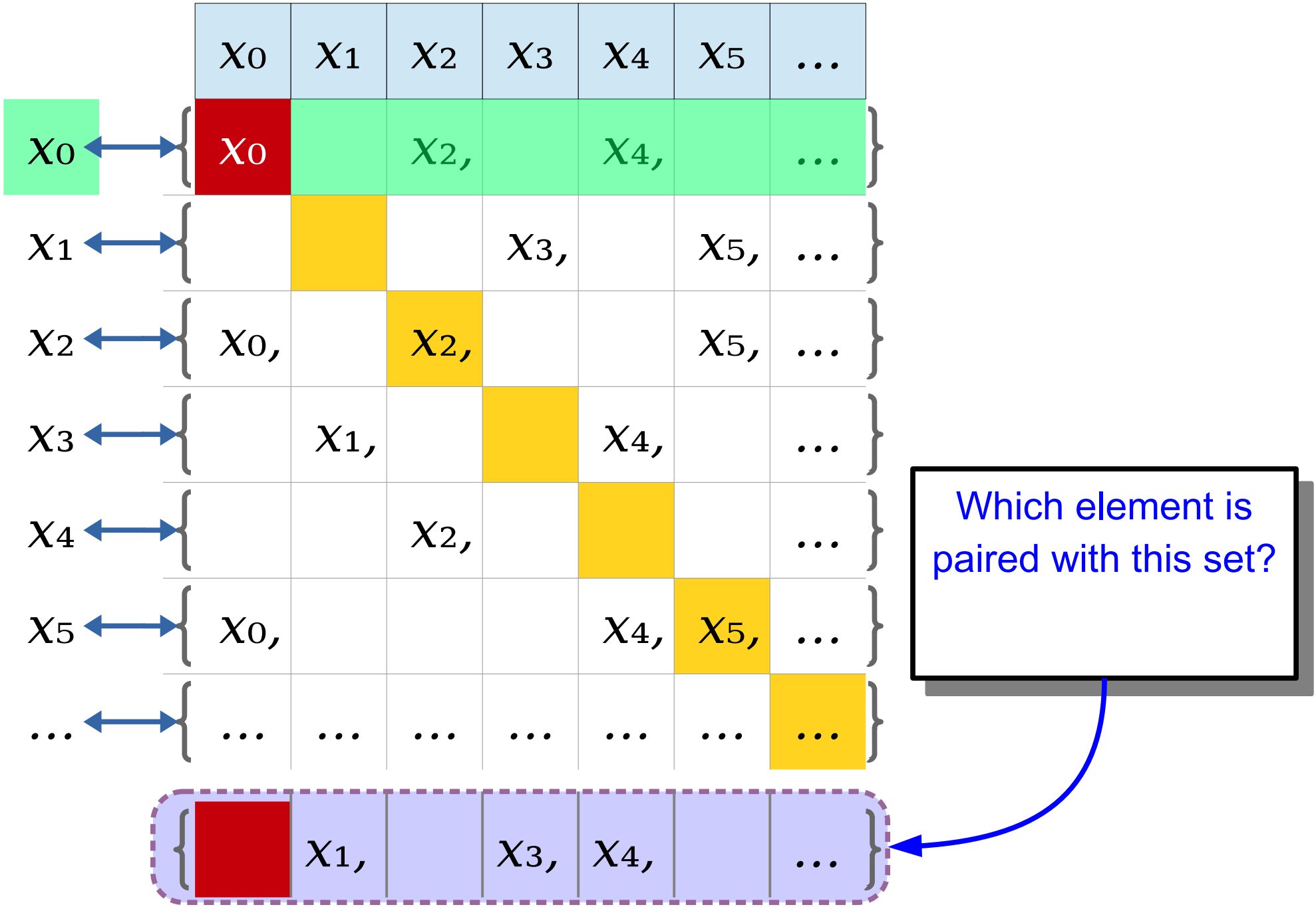

Elements of S
Elements of $\wp(S)$
$x_0 \leftrightarrow \{ x_0, x_2, x_4, \ldots \}$
$x_1 \leftrightarrow \{ x_3, x_5, \ldots \}$
$x_2 \leftrightarrow \{ x_0, x_1, x_2, x_5, \ldots \}$
$x_3 \leftrightarrow \{ x_1, x_4, \ldots \}$
$x_4 \leftrightarrow \{ x_2, \ldots \}$
$x_5 \leftrightarrow \{ x_0, x_4, x_5, \ldots \}$
$\ldots \leftrightarrow \{ \ldots \}$
An arbitrary mapping between elements of S and elements of $\wp(S)$

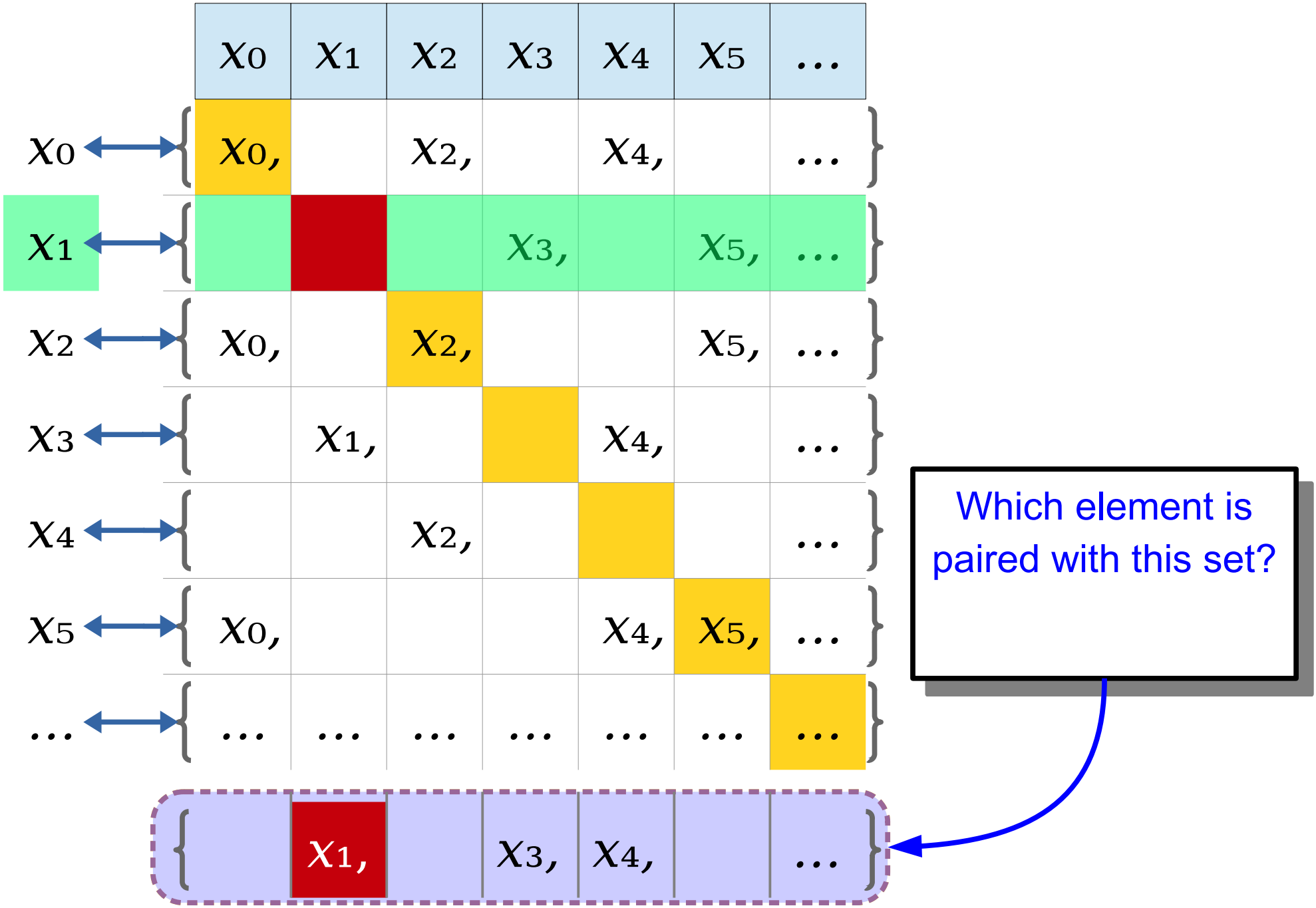

x_0 x_1 x_2 x_3 x_4 x_5 ...
x_0 { x_0, x_2, x_4, ... }
x_1 { x_3, x_5, ... }
x_2 { x_0, x_1, x_2, x_5, ... }
x_3 { x_1, x_4, ... }
x_4 { x_2, ... }
x_5 { x_0, x_4, x_5, ... }
... { ... }

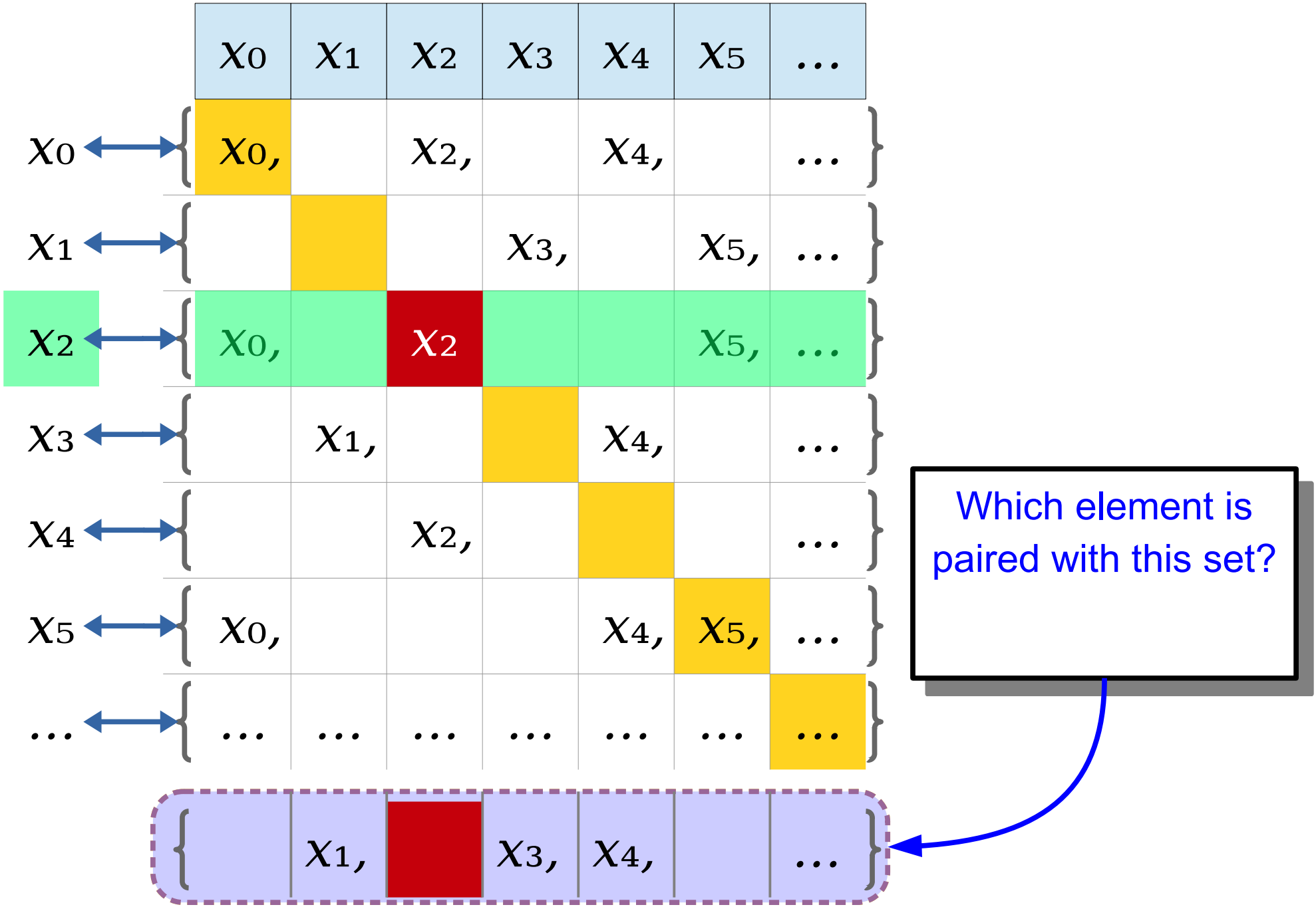

x_0 x_1 x_2 x_3 x_4 x_5 ...
x_0 x_0, x_2, x_4, ...
x_1 x_3, x_5, ...
x_2 x_0, x_2, x_5, ...
x_3 x_1, x_4, ...
x_4 x_2, ...
x_5 x_0, x_4, x_5, ...
... ...

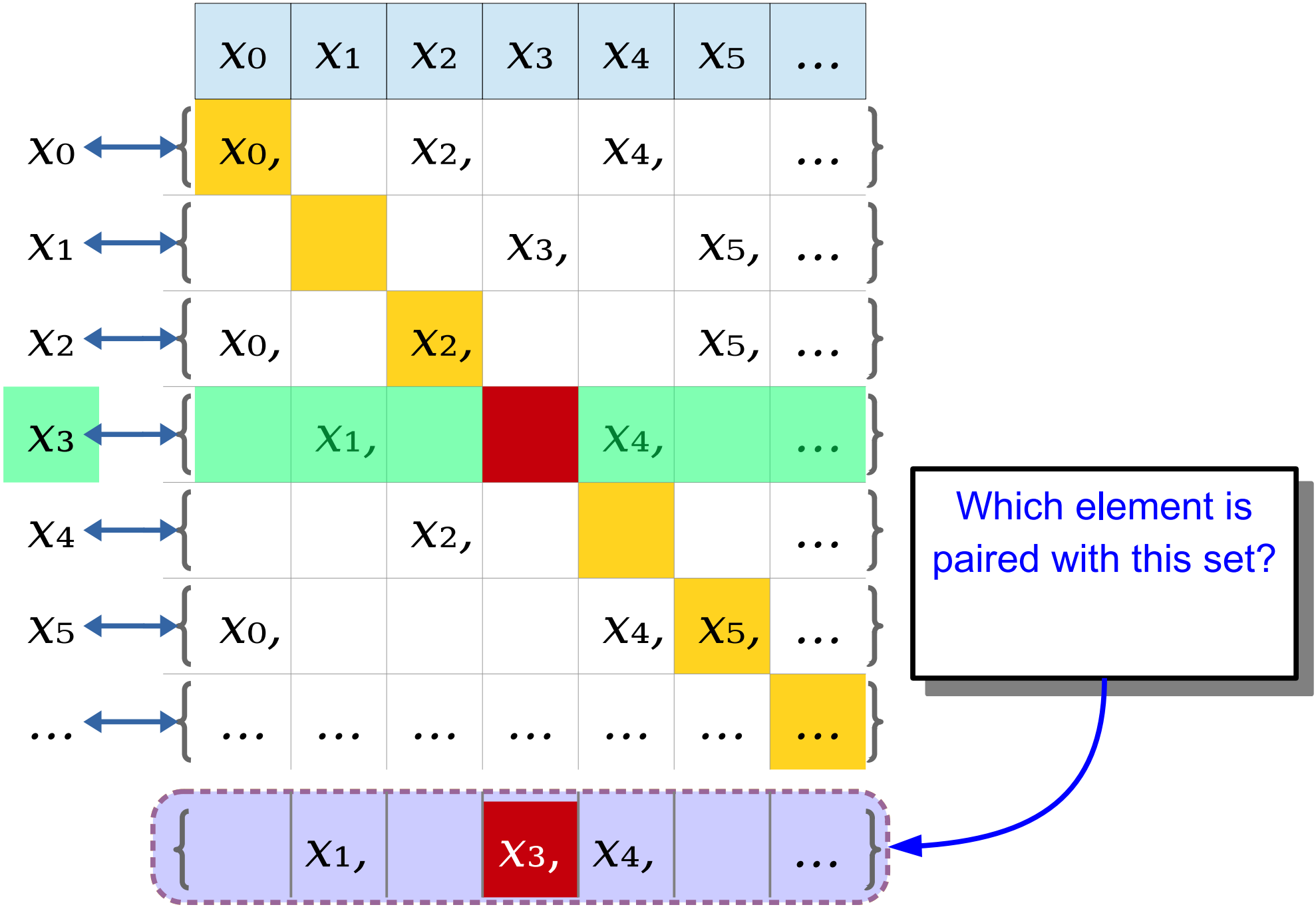

x0 x1 x2 x3 x4 x5 …
x0 x0, x2, x4, …
x1 x3, x5, …
x2 x0, x2, x5, …
x3 x1, x4, …
x4 x2, …
x5 x0, x4, x5, …
… … … … … … … …
x0, x2, x5, …
Which element is paired with this set?

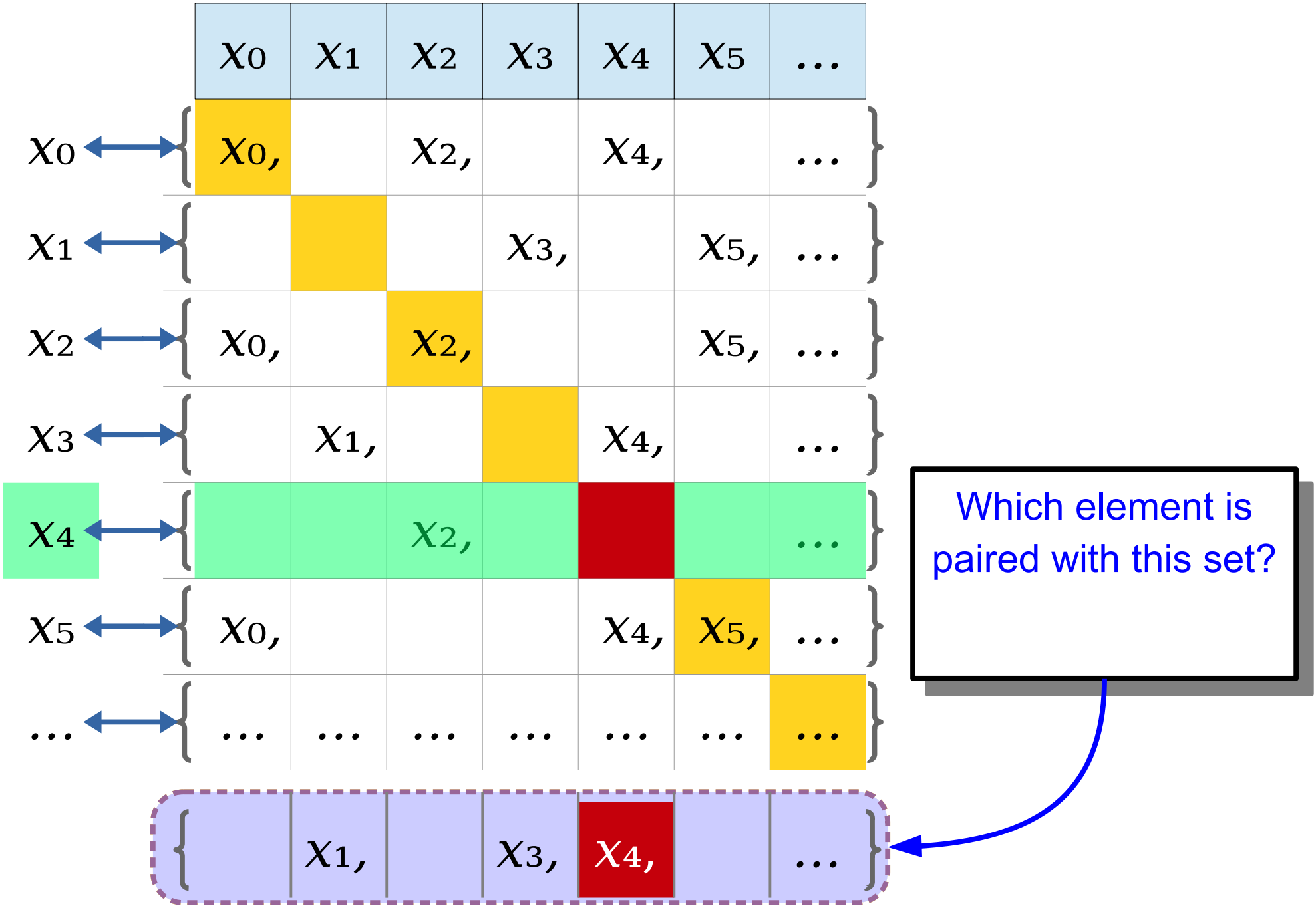

x0 x1 x2 x3 x4 x5 …
x0 x0, x2, x4, …
x1 x1, x3, x5, …
x2 x0, x2, x5, …
x3 x1, x4, …
x4 x2, …
x5 x0, x4, x5, …
… … … … … … … …
x1, x3, x4, …
“Flip” this set. Swap what’s included and what’s excluded.

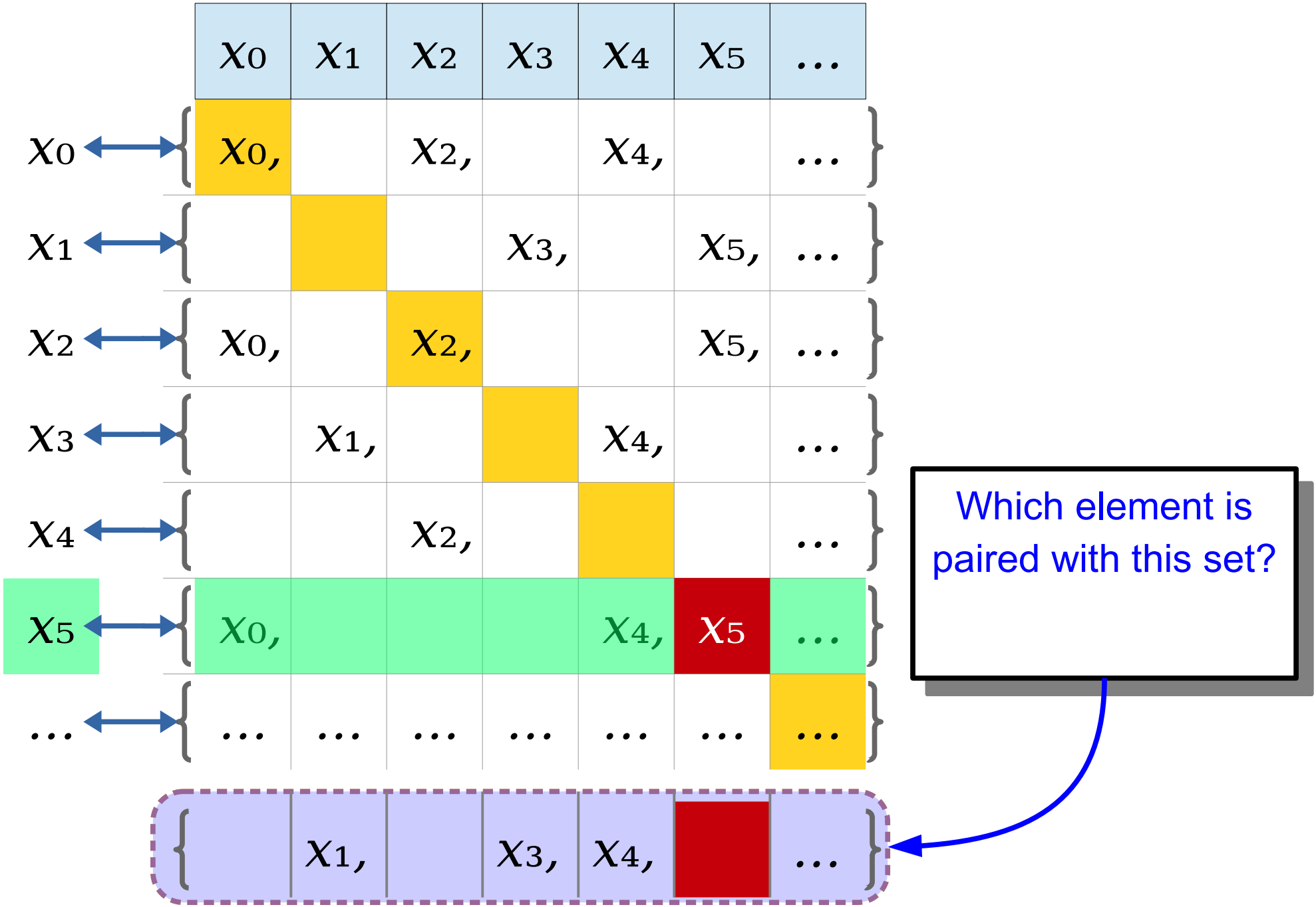

x0 x1 x2 x3 x4 x5 …
x0
x0 x2, x4, …
x1
x3, x5, …
x2
x0, x2, x5, …
x3
x1, x4, …
x4
x2, …
x5
x0, x4, x5, …
…
… … … … … … …
x1, x3, x4, …
Which element is paired with this set?

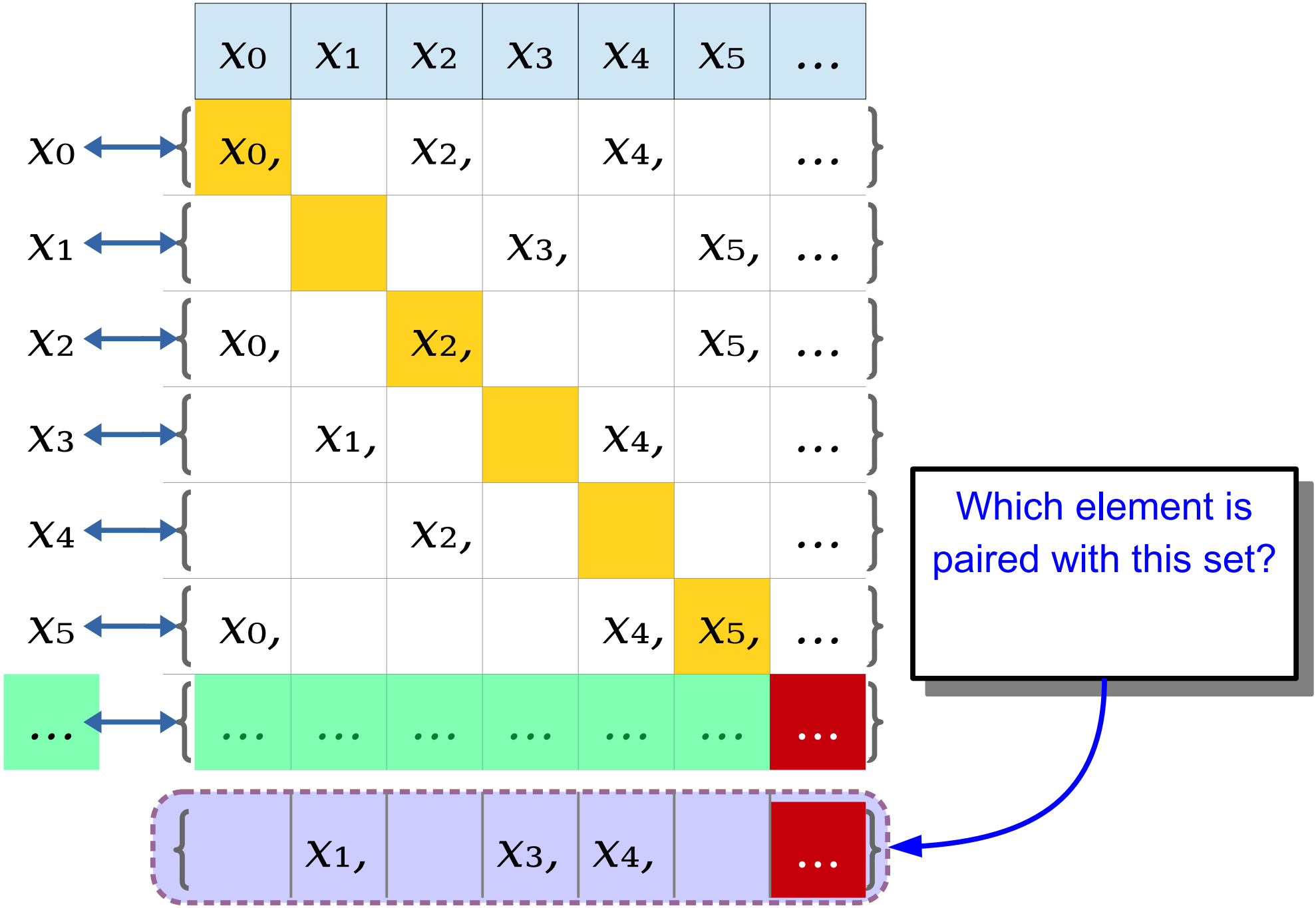

x0 x1 x2 x3 x4 x5 …
x0 x0, x2, x4, …
x1 x3, x5, …
x2 x0, x2, x5, …
x3 x1, x4, …
x4 x2, …
x5 x0, x4, x5, …
… … … … … … … …
x1, x3, x4, …
Which element is paired with this set?


x0 x1 x2 x3 x4 x5 …
x0 x0, x2, x4, …
x1 x3, x5, …
x2 x0, x2 x5, …
x3 x1, x4, …
x4 x2, …
x5 x0, x4, x5, …
… … … … … … … …
x1, x3, x4, …
Which element is paired with this set?


x0 x1 x2 x3 x4 x5 …
x0 x0, x2, x4, …
x1 x3, x5, …
x2 x0, x2, x5, …
x3 x1, x4, …
x4 x2, …
x5 x0, x4, x5, …
… … … … … … … …
x1, x3, x4, …
Which element is paired with this set?


x0 x1 x2 x3 x4 x5 …
x0 x0, x2, x4, …
x1 x1, x3, x5, …
x2 x0, x2, x5, …
x3 x1, x4, …
x4 x2, …
x5 x0, x4, x5, …
… … … … … … … …
x1, x3, x4, …
Which element is paired with this set?


x0 x1 x2 x3 x4 x5 …
x0 x0, x2, x4, …
x1 x1, x3, x5, …
x2 x0, x2, x5, …
x3 x1, x4, …
x4 x2, …
x5 x0, x4, x5 …
… … … … … … … …
x1, x3, x4, …
Which element is paired with this set?


x_0 x_1 x_2 x_3 x_4 x_5 …
x_0 x_0, x_2, x_4, …
x_1 x_3, x_5, …
x_2 x_0, x_2, x_5, …
x_3 x_1, x_4, …
x_4 x_2, …
x_5 x_0, x_4, x_5, …
… … … … … … … …
x_1, x_3, x_4, …
Which element is paired with this set?

The Diagonalization Proof

- No matter how we pair up elements of S and subsets of S, the complemented diagonal won't appear in the table.
  - In row n, the nth element must be wrong.
- No matter how we pair up elements of S and subsets of S, there is *always* at least one subset left over.
- This result is ***Cantor's theorem***: Every set is strictly smaller than its power set:

If S is a set, then $|S| < |\wp(S)|$.

Two Infinities…

- By Cantor's Theorem:

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

…And Beyond!

- 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 is no biggest infinity!***
- ***There are infinitely many infinities!***

What does this have to do with computation?

“The set of all computer programs”

“The set of all problems to solve”

Where We're Going

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

Where We're Going

A ***string*** is a sequence of characters.

We're going to prove the following results:

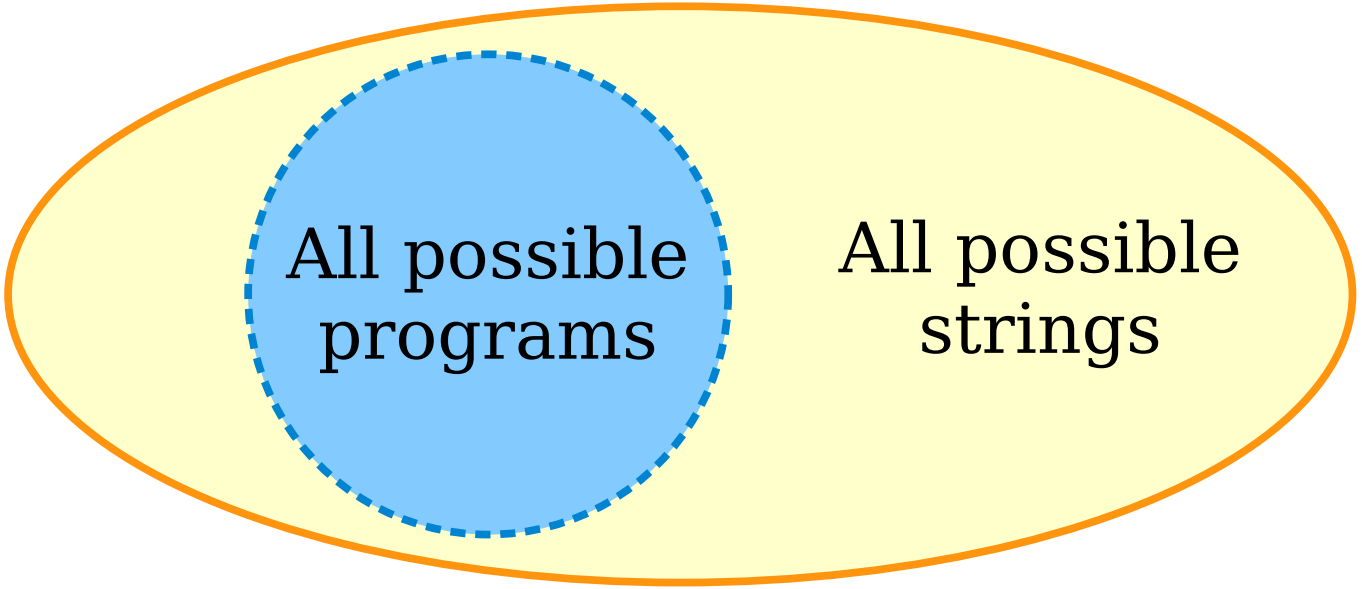
- There are ***at most*** as many programs as there are strings.

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

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

Strings and Programs

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



|Programs| ≤ |Strings|

Where We're Going

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

Where We're Going

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

Where We're Going

A ***string*** is a sequence of characters.

We're going to prove the following results:

There are ***at most*** as many programs as there are strings. ✓

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

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

Strings and Problems

- There is a connection between the number of sets of strings and the number of problems to solve.
- Let S be any set of strings. This set S gives rise to a problem to solve:

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

Strings and Problems

Given a string *w*, determine whether *w* ∈ *S*.

- Suppose that S is the set

$$S = \{ \text{"}a\text{"}, \text{"}b\text{"}, \text{"}c\text{"}, \ldots, \text{"}z\text{"} \}$$

- From this set S, we get this problem:

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

Strings and Problems

Given a string *w*, determine whether *w* ∈ *S*.

- Suppose that S is the set

  S = { "0", "1", "2", …, "9", "10", "11", … }

- From this set S, we get this problem:

Given a string *w*, determine whether *w* represents a natural number.

Strings and Problems

Given a string *w*, determine whether *w* ∈ *S*.

- Suppose that S is the set

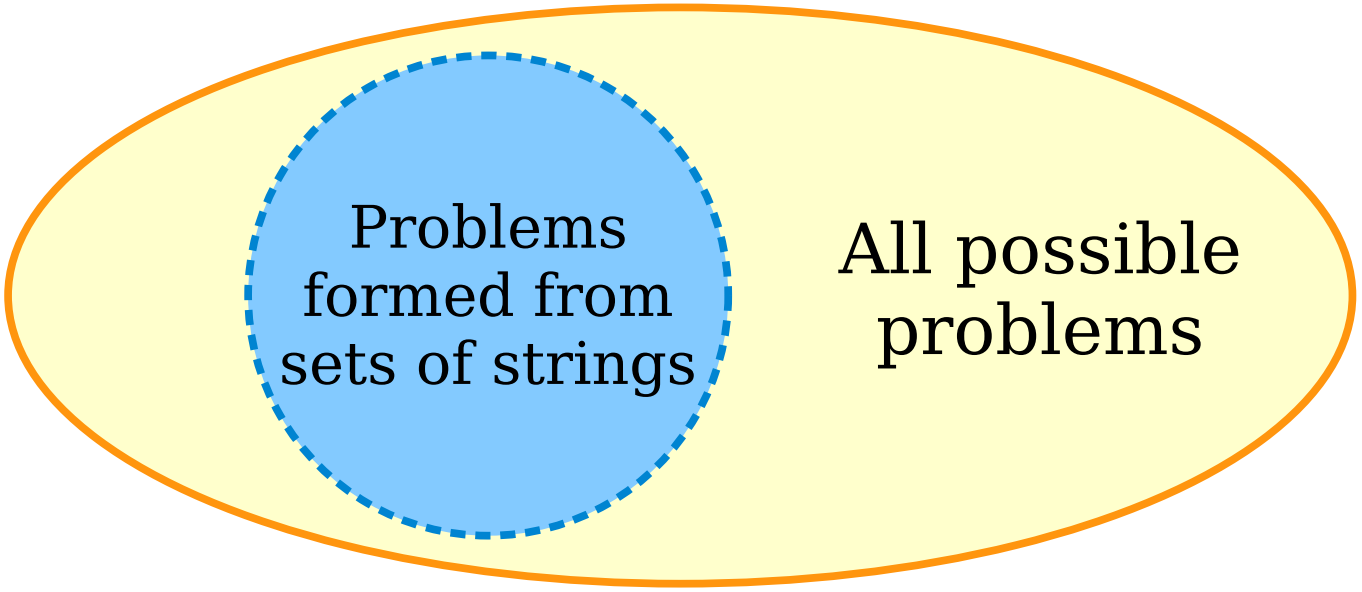
$$S = \{ p \mid p \text{ is a legal C++ program} \}$$

- From this set S, we get this problem:

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

Strings and Problems

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



|Sets of Strings| ≤ |Problems|

Where We're Going

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

Where We're Going

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

Where We're Going

A ***string*** is a sequence of characters.

We're going to prove the following results:

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

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

Where We're Going

A ***string*** is a sequence of characters.

We're going to prove the following results:

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

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

Every computer program is a string.

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

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

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

|Programs| ≤ |Strings| < |℘(Strings)| ≤ |Problems|

Every computer program is a string.

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

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

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

|Programs| < |Problems|

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

|Programs| < |Problems|

It Gets Worse

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

We need to develop a more nuanced understanding of computation.

Where We're Going

- ***What makes a problem impossible to solve with computers?***
  - Is there a deep reason why certain problems can't be solved with computers, or is it completely arbitrary?
  - How do you know when you're looking at an impossible problem?
  - Are these real-world problems, or are they highly contrived?
- ***How do we know that we're right?***
  - How can we back up our pictures with rigorous proofs?
  - How do we build a mathematical framework for studying computation?

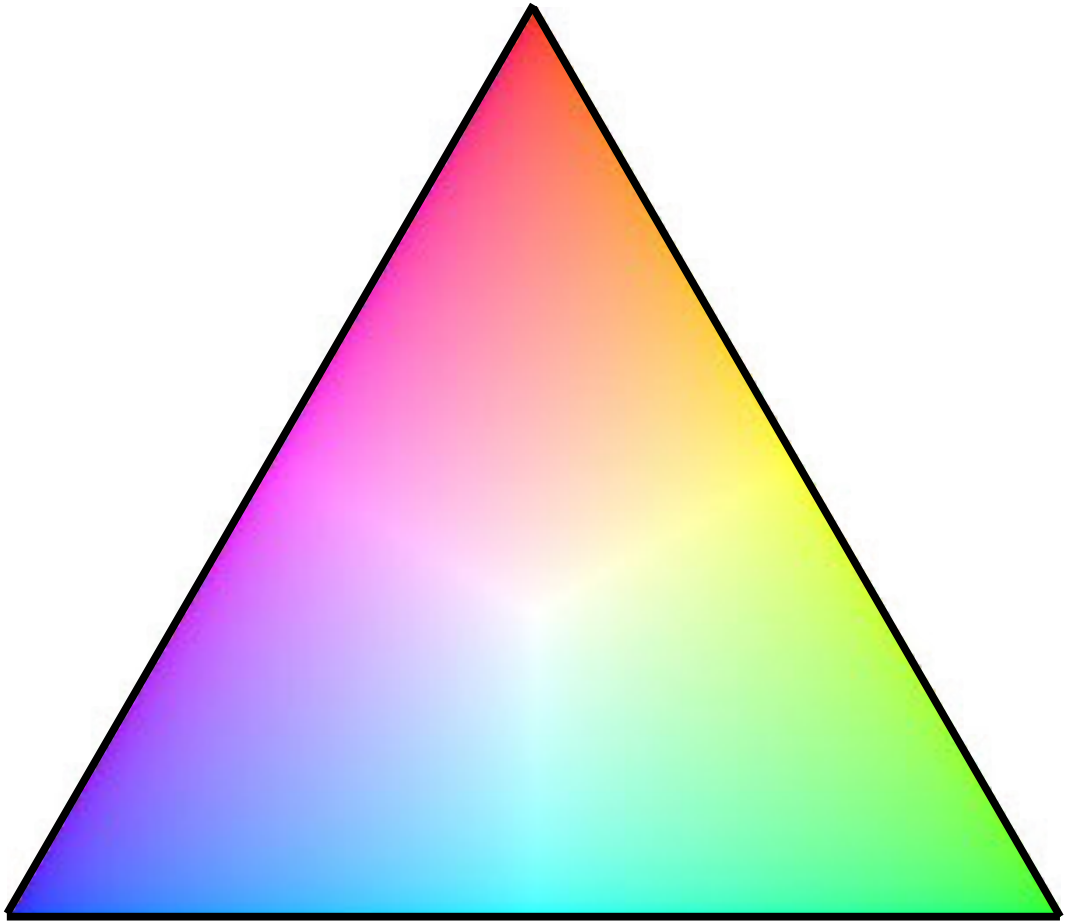
Let’s take a quick break!

Mathematical Proofs

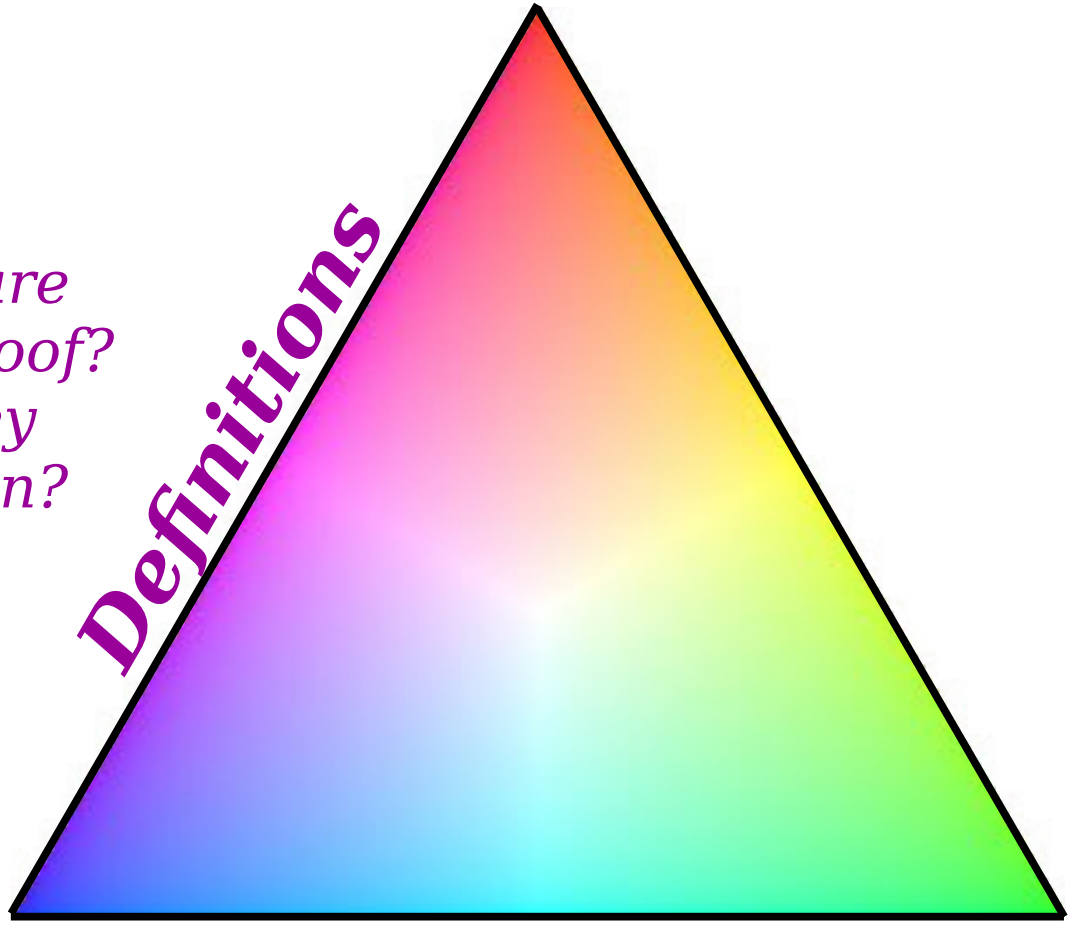
What is a Proof?

A ***proof*** is an argument that demonstrates why a conclusion is true, subject to certain standards of truth.

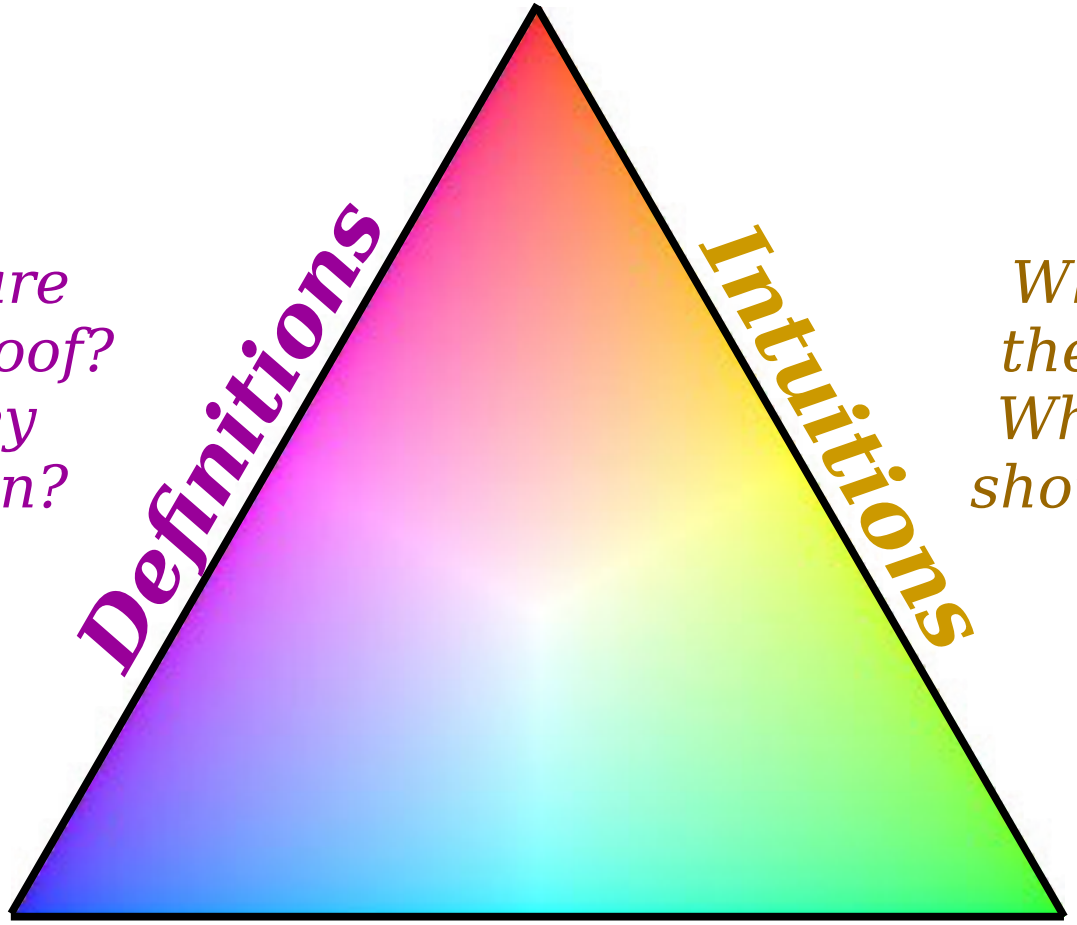
A ***mathematical proof*** is an argument that demonstrates why a mathematical statement is true, following the rules of mathematics.



What terms are used in this proof? What do they formally mean?

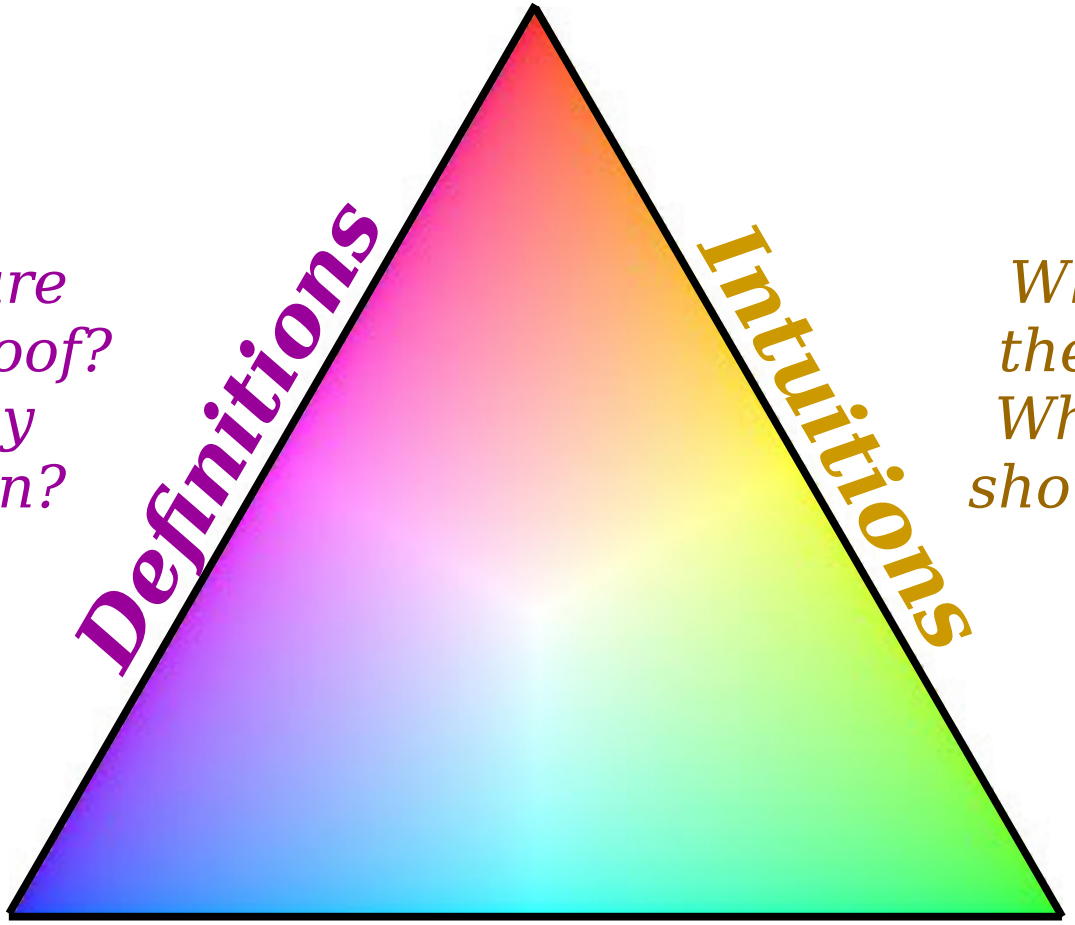


What terms are used in this proof? What do they formally mean?



What does this theorem mean? Why, intuitively, should it be true?

What terms are used in this proof? What do they formally mean?

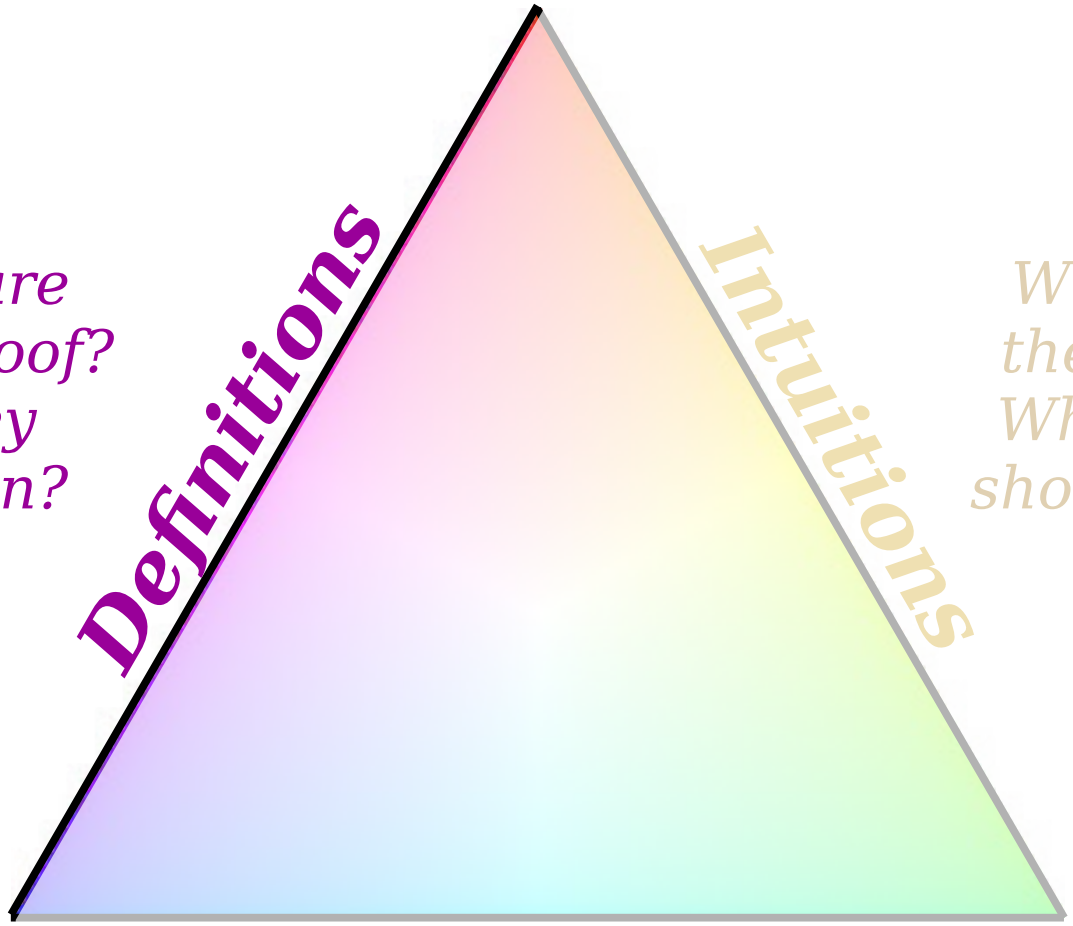


What does this theorem mean? Why, intuitively, should it be true?

What is the standard format for writing a proof? What are the techniques for doing so?

Writing our First Proof

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



What terms are used in this proof? What do they formally mean?

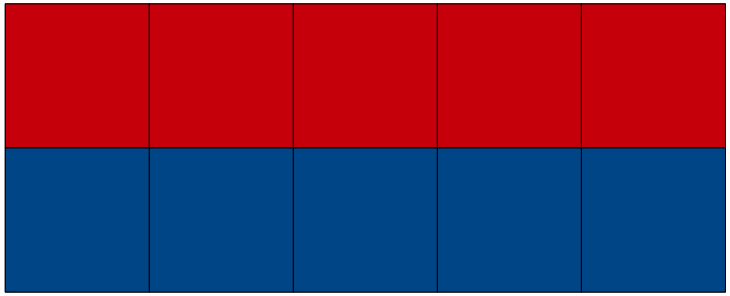
What does this theorem mean? Why, intuitively, should it be true?

What is the standard format for writing a proof? What are the techniques for doing so?

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

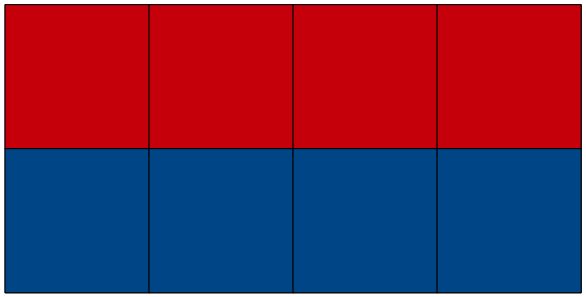
Theorem: If n is an even integer, then n^2 is even.

10



$2 \cdot \mathbf{5}$

8



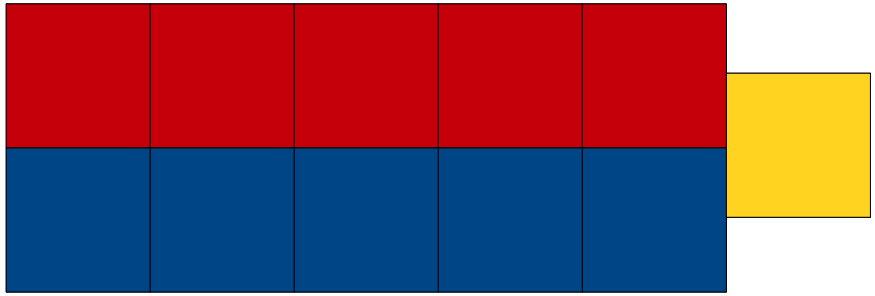
$2 \cdot \mathbf{4}$

0

$2 \cdot \mathbf{0}$

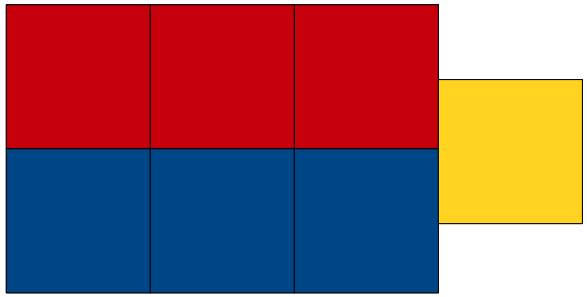
An integer n is called ***even*** if
there is an integer k where $n = 2k$.

11



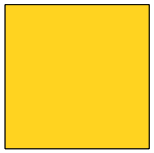
$2 \cdot \mathbf{5} + \mathbf{1}$

7



$2 \cdot \mathbf{3} + \mathbf{1}$

1



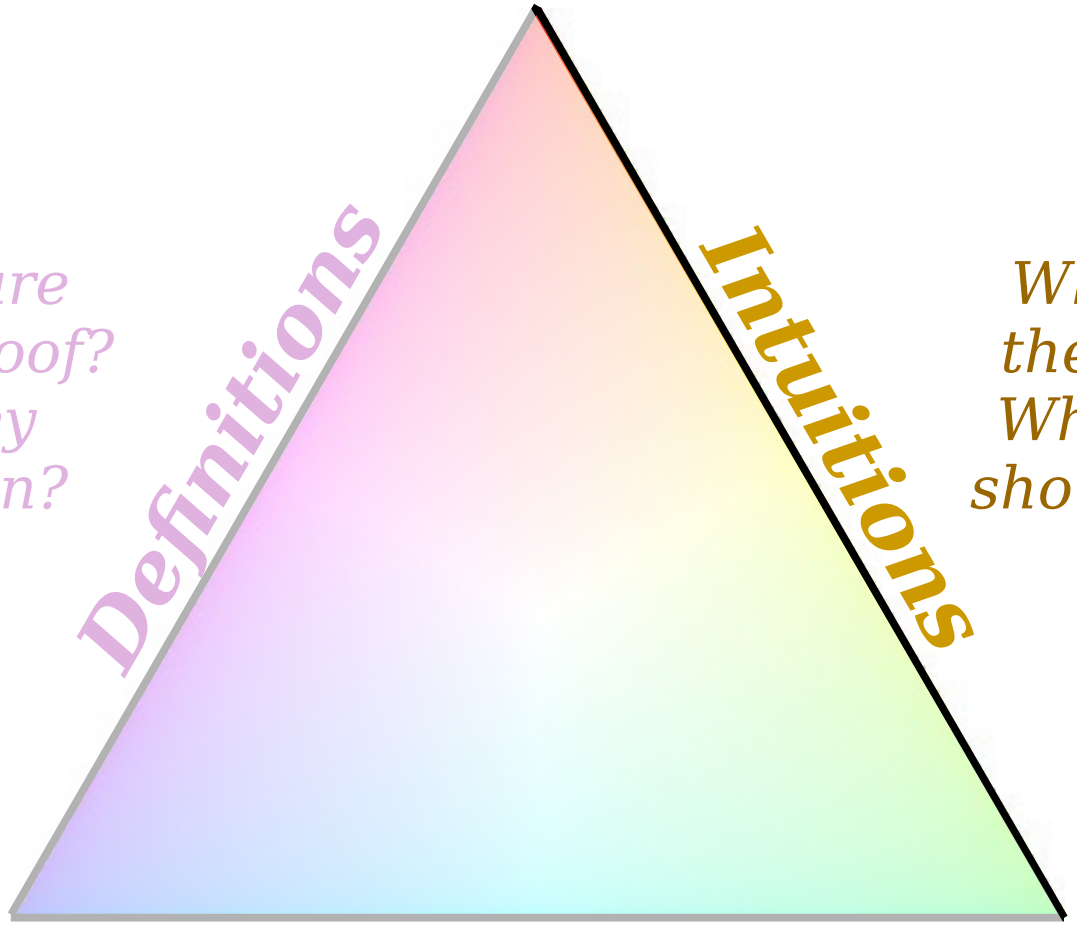
$2 \cdot \mathbf{0} + \mathbf{1}$

An integer n is called ***odd*** if
there is an integer k where $n = 2k+1$.

Going forward, we'll assume the following:

1. Every integer is either even or odd.
2. No integer is both even and odd.

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



What terms are used in this proof? What do they formally mean?

What does this theorem mean? Why, intuitively, should it be true?

What is the standard format for writing a proof? What are the techniques for doing so?

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

Let's Try Some Examples!

$$2^2 = 4 = 2 \cdot \mathbf{2}$$

$$10^2 = 100 = 2 \cdot \mathbf{50}$$

$$0^2 = 0 = 2 \cdot \mathbf{0}$$

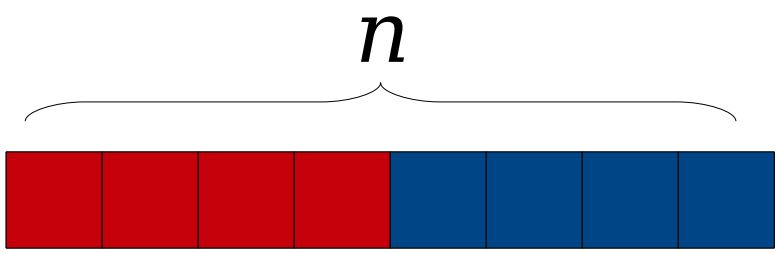
$$(-8)^2 = 64 = 2 \cdot \mathbf{32}$$

$$n^2 = 2 \cdot \mathbf{?}$$

What's the pattern? How do we predict this?

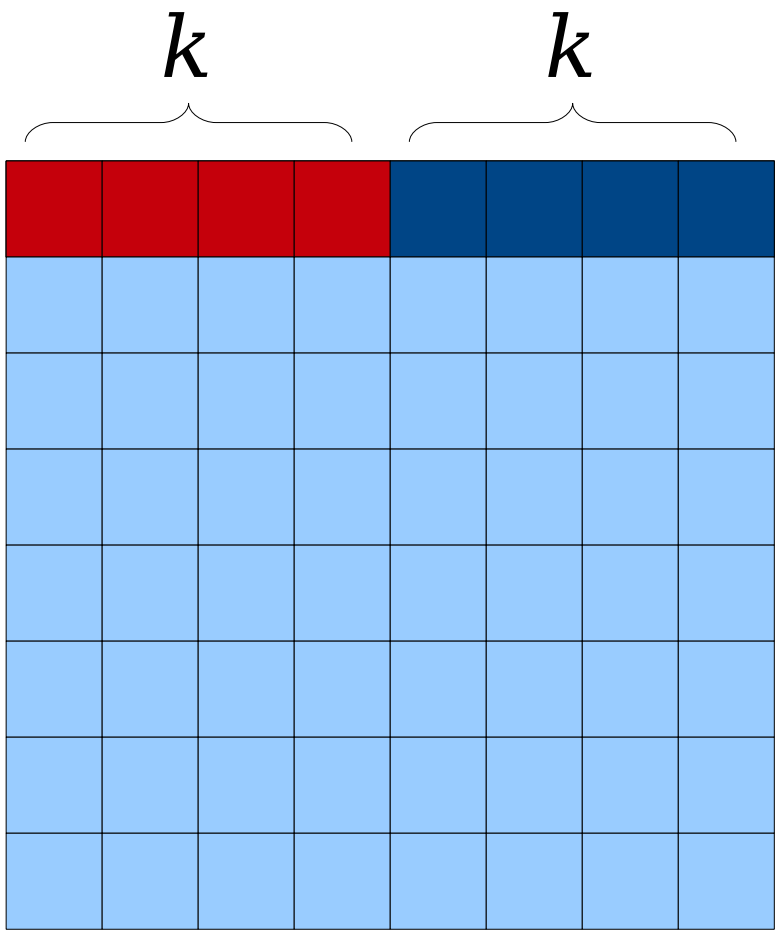
Theorem: If n is an even integer, then n^2 is even.

Let's Draw Some Pictures!



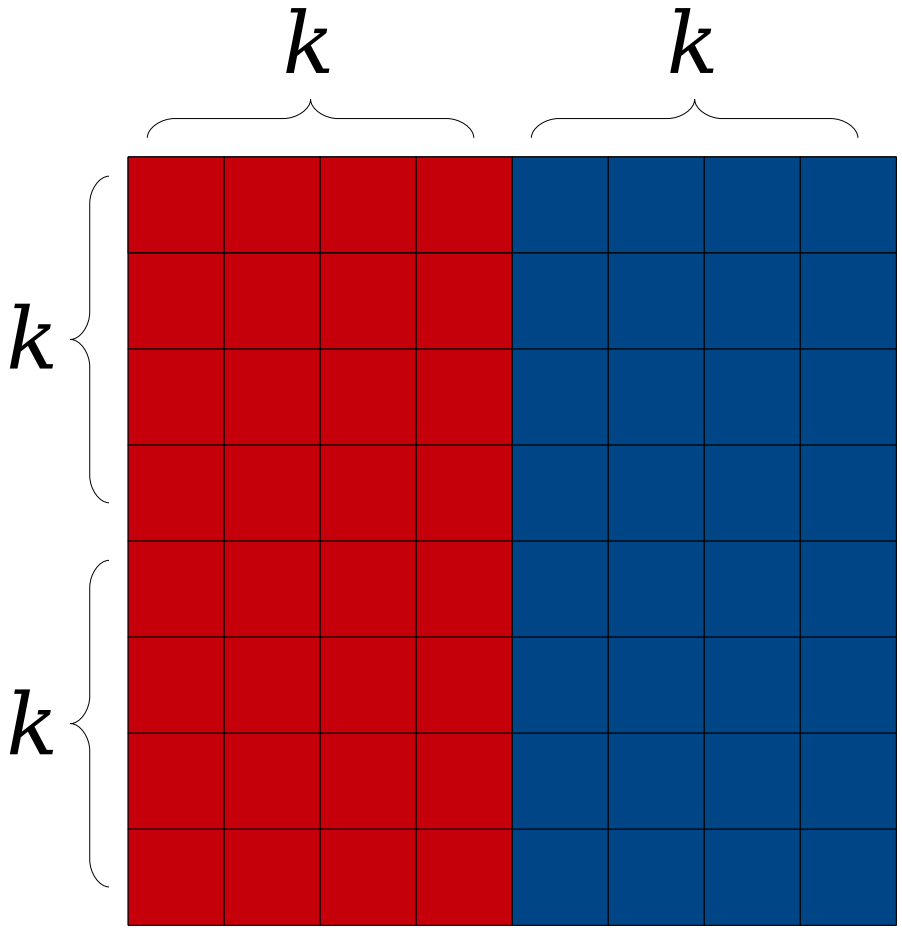
Theorem: If n is an even integer, then n^2 is even.

Let's Draw Some Pictures!



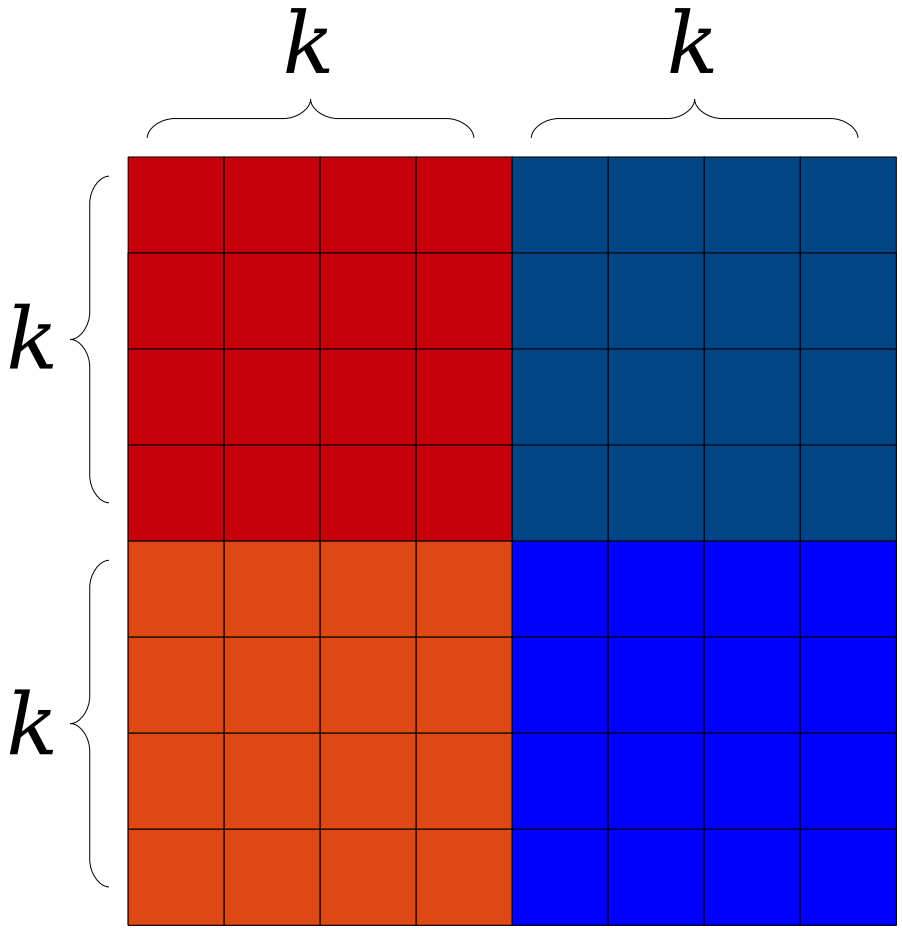
Theorem: If n is an even integer, then n^2 is even.

Let's Draw Some Pictures!



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

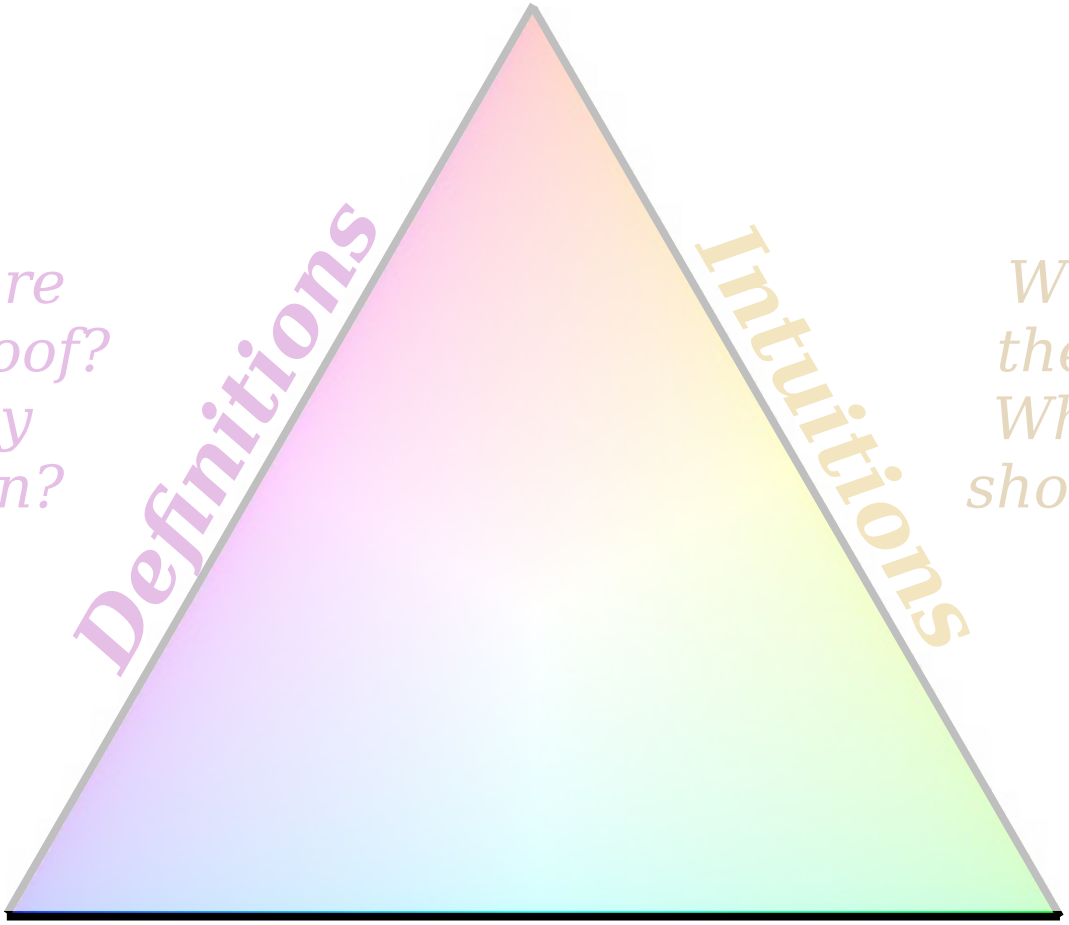
Let's Draw Some Pictures!



$$n^2 = 2(2k^2)$$

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

What terms are used in this proof? What do they formally mean?



What does this theorem mean? Why, intuitively, should it be true?

Conventions

What is the standard format for writing a proof? What are the techniques for doing so?

Our First Proof!

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

Our First Proof!

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

Proof: Let n be an even integer.

Our First Proof!

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

Proof: Let n be an even integer.

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

Our First Proof!

Theorem: If n is an even integer, 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 $n^2 = (2k)^2$

Our First Proof!

Theorem: If n is an even integer, 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 $n^2 = (2k)^2 = 4k^2$

Our First Proof!

Theorem: If n is an even integer, 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 $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Our First Proof!

Theorem: If n is an even integer, 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 $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Our First Proof!

Theorem: If n is an even integer, 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 $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even.

Our First Proof!

Theorem: If n is an even integer, 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 $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

Our First Proof!

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

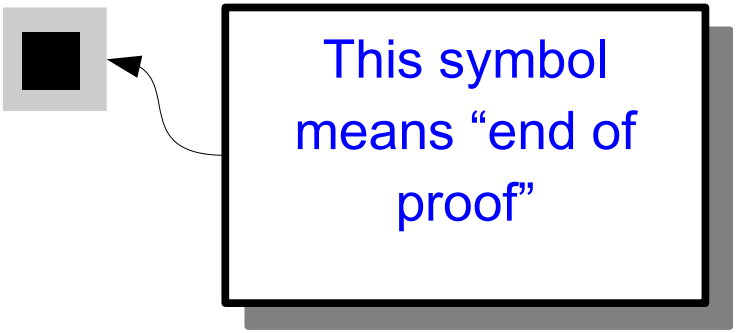
Proof: Let n be an even integer.

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

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

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■



Our First Proof!

Theorem: If n is an even integer, 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 $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

Our First Proof!

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

Proof: Let n be an even integer.

Since n i
such tha

This mea

From thi
m (name

Therefor

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.

Our First Proof!

Theorem: If n is an even integer, 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 $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

Our First Proof!

Theorem: If n is an even integer, 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 th … ^{2}).

From this, we … er m (namely, $2k$ …

Therefore, n^2 …

This is the definition of an even integer. We need to use this definition to make this proof rigorous.

Our First Proof!

Theorem: If n is an even integer, 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 $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

Our First Proof!

Theorem: If n is an even integer, 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 $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Fr
m

Th

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.

Our First Proof!

Theorem: If n is an even integer, 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 $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

Our First Proof!

Theorem: If n [illegible] en.

Proof: Let n b[illegible]

Since n [illegible]
such th[illegible]

This me[illegible]^2).

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

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

Our First Proof!

Theorem: If n is an even integer, 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 $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

Our First Proof!

Theorem: If n is an even integer, 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

From thi

m (name

Therefore, n^2 is even. ■

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

Our First Proof!

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

Proof: Let n be an even integer.

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

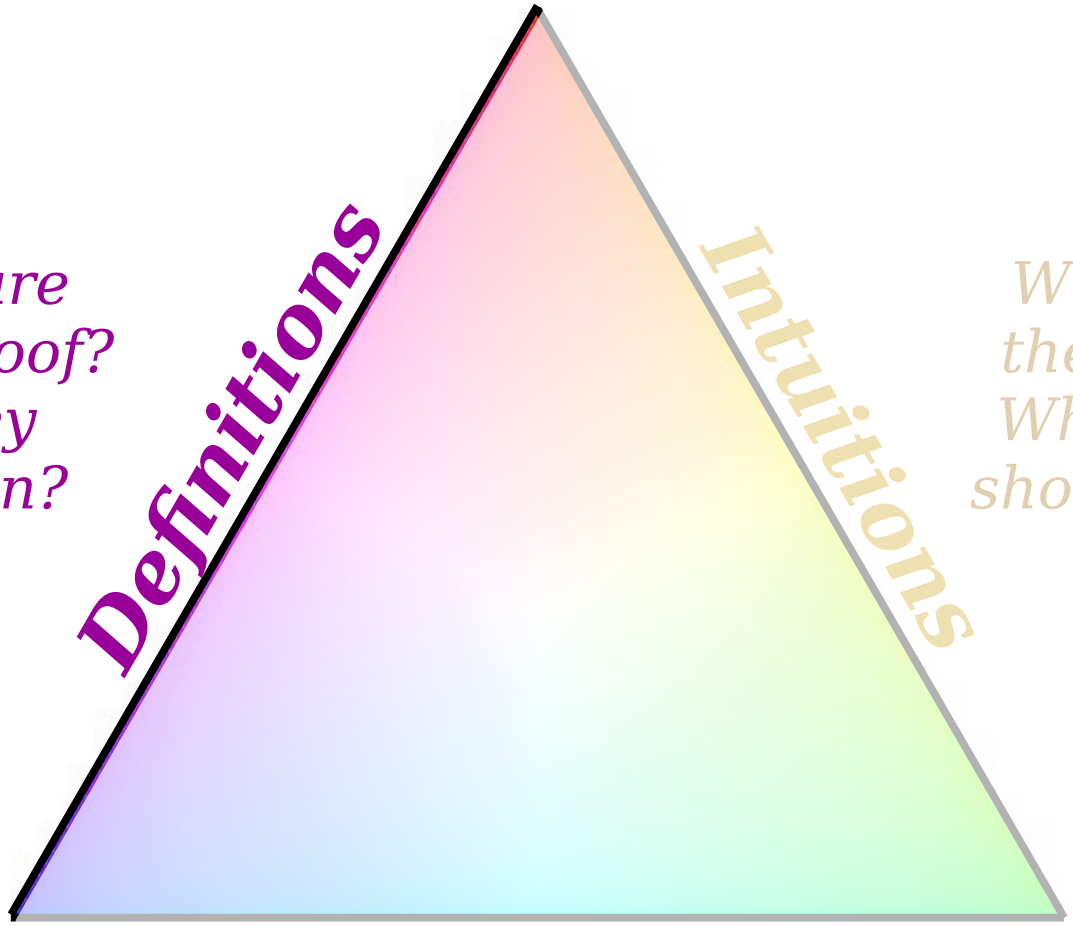
This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

Our Next Proof

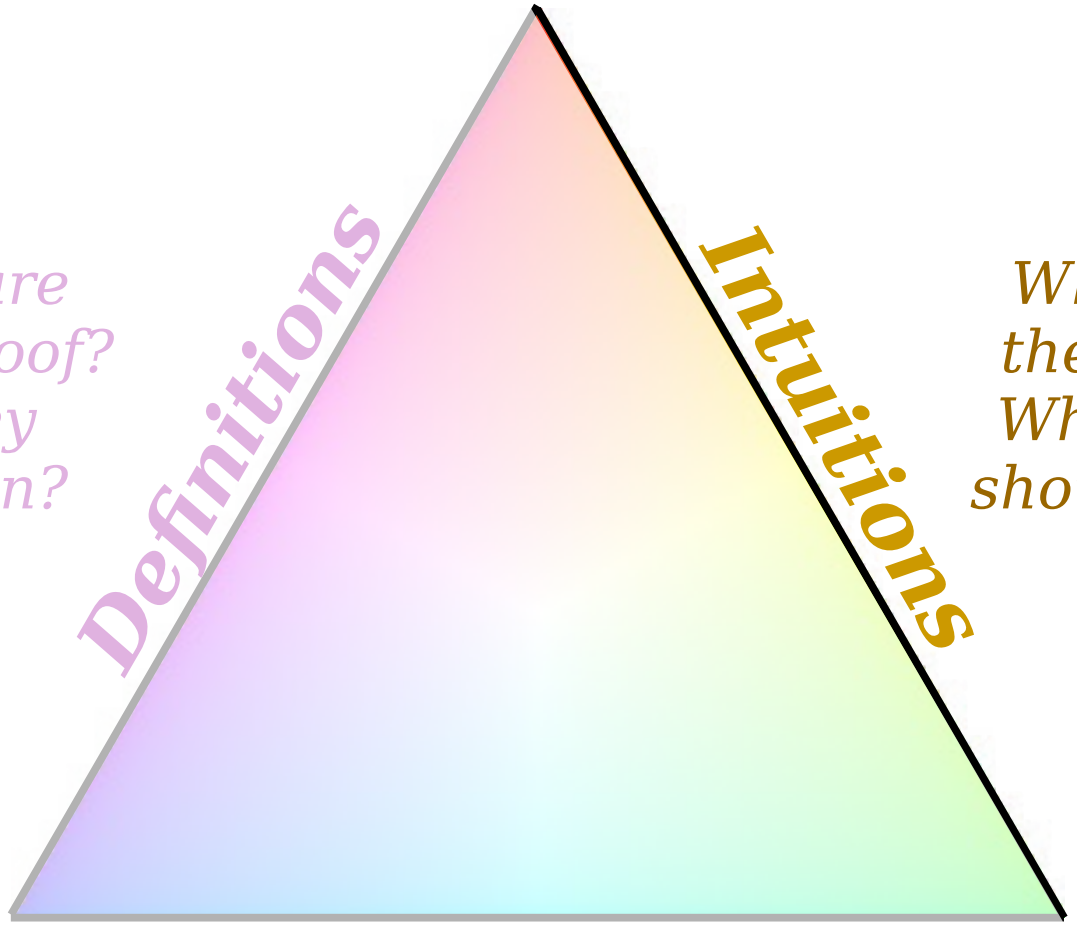
Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.



What terms are used in this proof? What do they formally mean?

What does this theorem mean? Why, intuitively, should it be true?

What is the standard format for writing a proof? What are the techniques for doing so?



What terms are used in this proof? What do they formally mean?

What does this theorem mean? Why, intuitively, should it be true?

What is the standard format for writing a proof? What are the techniques for doing so?

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Let's Try Some Examples!

$$1 + 1 = 2 = 2 \cdot \mathbf{1}$$

$$137 + 103 = 240 = 2 \cdot \mathbf{120}$$

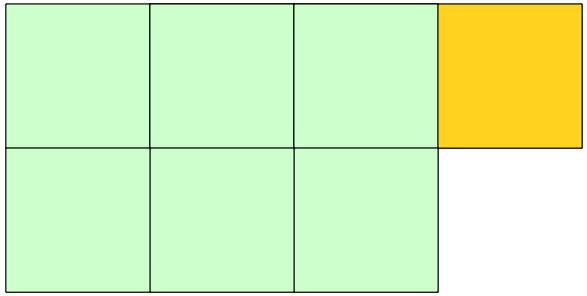
$$-5 + 5 = 0 = 2 \cdot \mathbf{0}$$

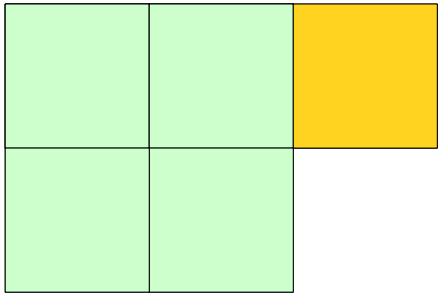
$$m + n = 2 \cdot \mathbf{?}$$

What's the pattern? How do we predict this?

Theorem: For any integers m and n, if m and n are odd, then $m+n$ is even.

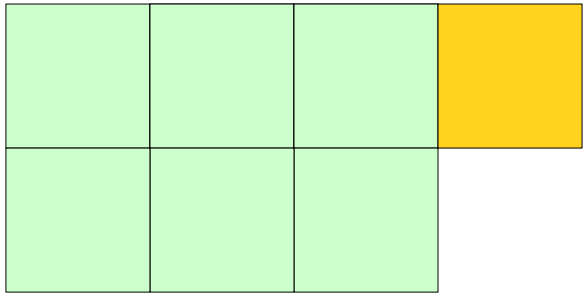
Let's Draw Some Pictures!

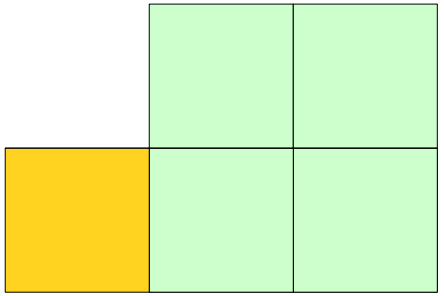




Theorem: For any integers m and n, if m and n are odd, then $m+n$ is even.

Let's Draw Some Pictures!

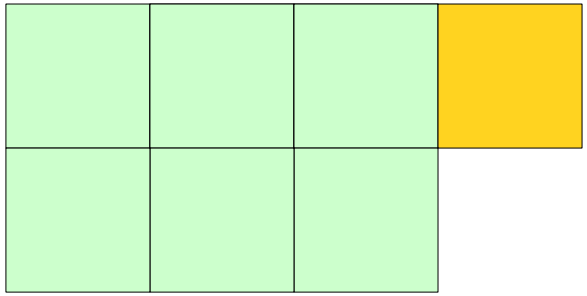


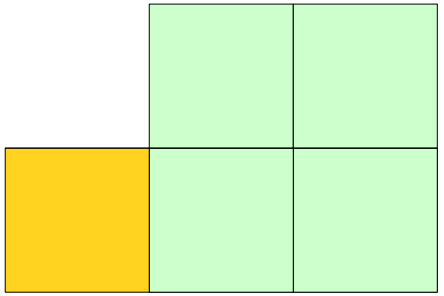


Theorem: For any integers m and n, if m and n are odd, then $m+n$ is even.

Let's Do Some Math!

$2k+1$

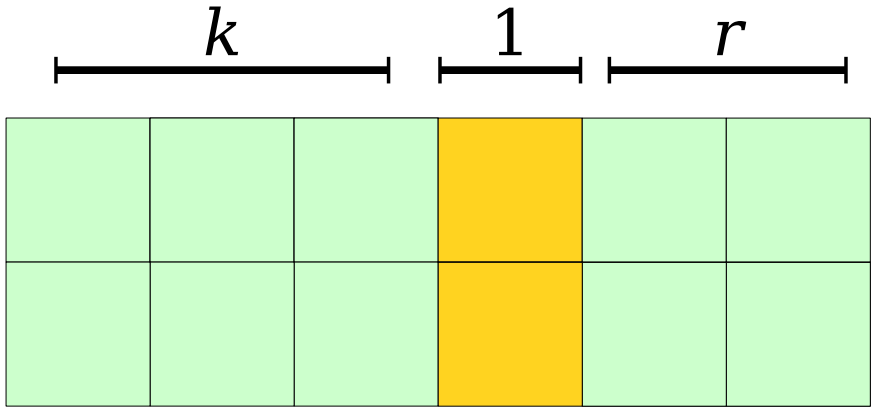




$2r+1$

Theorem: For any integers m and n,
if m and n are odd, then $m+n$ is even.

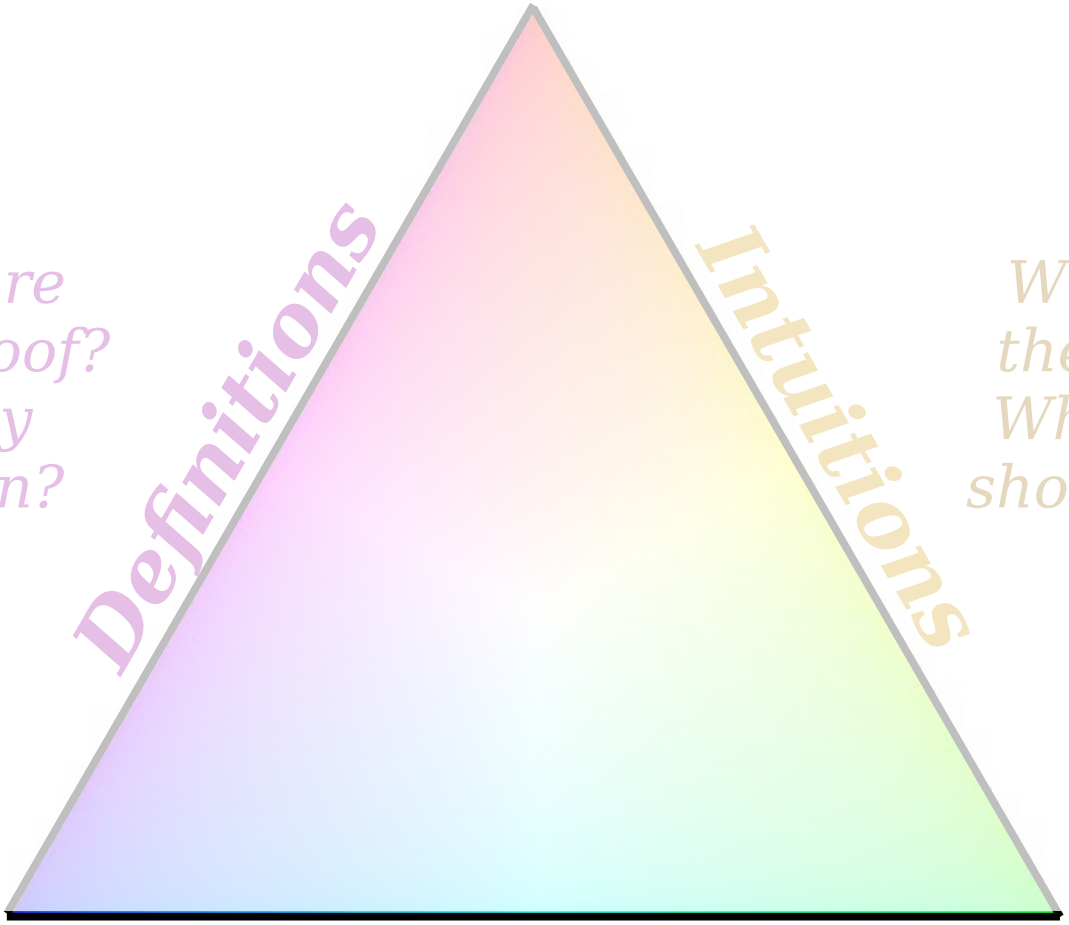
Let's Do Some Math!



$$(2k+1) + (2r+1) = 2(k + r + 1)$$

Theorem: For any integers m and n,
if m and n are odd, then $m+n$ is even.

What terms are used in this proof? What do they formally mean?



What does this theorem mean? Why, intuitively, should it be true?

Conventions

What is the standard format for writing a proof? What are the techniques for doing so?

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof:

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Consider any arbitrary integers m and n where m and n are odd.

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Consider any arbitrary integers m and n where m and n are odd. Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \qquad (1)$$

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Consider any arbitrary integers m and n where m and n are odd. Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \qquad (1)$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \qquad (2)$$

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Consider any arbitrary integers m and n where m and n are odd. Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \qquad (1)$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \qquad (2)$$

By adding equations (1) and (2) we learn that

$$m + n = 2k + 1 + 2r + 1$$

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Consider any arbitrary integers m and n where m and n are odd. Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \qquad (1)$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \qquad (2)$$

By adding equations (1) and (2) we learn that

$$\begin{aligned} m + n &= 2k + 1 + 2r + 1 \\ &= 2k + 2r + 2 \end{aligned}$$

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Consider any arbitrary integers m and n where m and n are odd. Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \tag{1}$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \tag{2}$$

By adding equations (1) and (2) we learn that

$$\begin{aligned} m + n &= 2k + 1 + 2r + 1 \\ &= 2k + 2r + 2 \\ &= 2(k + r + 1). \end{aligned} \tag{3}$$

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Consider any arbitrary integers m and n where m and n are odd. Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \tag{1}$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \tag{2}$$

By adding equations (1) and (2) we learn that

$$\begin{aligned} m + n &= 2k + 1 + 2r + 1 \\ &= 2k + 2r + 2 \\ &= 2(k + r + 1). \end{aligned} \tag{3}$$

Equation (3) tells us that there is an integer s (namely, $k + r + 1$) such that $m + n = 2s$.

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Consider any arbitrary integers m and n where m and n are odd. Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \tag{1}$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \tag{2}$$

By adding equations (1) and (2) we learn that

$$\begin{aligned} m + n &= 2k + 1 + 2r + 1 \\ &= 2k + 2r + 2 \\ &= 2(k + r + 1). \end{aligned} \tag{3}$$

Equation (3) tells us that there is an integer s (namely, $k + r + 1$) such that $m + n = 2s$. Therefore, we see that $m + n$ is even, as required.

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Consider any arbitrary integers m and n where m and n are odd. Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \tag{1}$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \tag{2}$$

By adding equations (1) and (2) we learn that

$$\begin{aligned} m + n &= 2k + 1 + 2r + 1 \\ &= 2k + 2r + 2 \\ &= 2(k + r + 1). \end{aligned} \tag{3}$$

Equation (3) tells us that there is an integer s (namely, $k + r + 1$) such that $m + n = 2s$. Therefore, we see that $m + n$ is even, as required. ■

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Consider any arbitrary integers m and n where m and n are odd. Since m is odd, we know that there is an integer k where

Similarl such that

By addi

Equatio + r + 1) such th en, as required

This is called making ***arbitrary choices***. Rather than specifying what ***m*** and ***n*** are, we're signaling to the reader that they could, in principle, supply any choices of ***m*** and ***n*** that they'd like.

By picking ***m*** and ***n*** arbitrarily, anything we prove about ***m*** and ***n*** will generalize to all possible choices we could have made.

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Consider any arbitrary integers m and n where m and n are odd. Since m is odd, we know that there is an integer k where

Similarly, bec er r such that

By adding eq

$$= 2(k + r + 1). \qquad (3)$$

Equation (3) tells us that there is an integer s (namely, $k + r + 1$) such that $m + n = 2s$. Therefore, we see that $m + n$ is even, as required. ■

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.

Numbering these equalities lets us refer back to them later on, making the flow of the proof a bit easier to understand.

Theo d n are odd, then m

Proo d n where m and n are o s an integer k where

$$m = 2k + 1. \tag{1}$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \tag{2}$$

By adding equations (1) and (2) we learn that

$$\begin{aligned} m + n &= 2k + 1 + 2r + 1 \\ &= 2k + 2r + 2 \\ &= 2(k + r + 1). \end{aligned} \tag{3}$$

Equation (3) tells us that there is an integer s (namely, $k + r + 1$) such that $m + n = 2s$. Therefore, we see that $m + n$ is even, as required. ■

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Consider any arbitrary integers m and n where m and n are odd. Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \tag{1}$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \tag{2}$$

hat

1

(3)

er s (namely, $k + r + 1$)

at $m + n$ is even, as

This is a complete sentence! Proofs are expected to be written in complete sentences, so you'll often use punctuation at the end of formulas.

We recommend using the "mugga mugga" test – if you read a proof and replace all the mathematical notation with "mugga mugga," what comes back should be a valid sentence.

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Consider any arbitrary integers m and n where m and n are odd. Since m is odd, we know that there is an integer k where

$$m = 2k + 1. \tag{1}$$

Similarly, because n is odd there must be some integer r such that

$$n = 2r + 1. \tag{2}$$

By adding equations (1) and (2) we learn that

$$\begin{aligned} m + n &= 2k + 1 + 2r + 1 \\ &= 2k + 2r + 2 \\ &= 2(k + r + 1). \end{aligned} \tag{3}$$

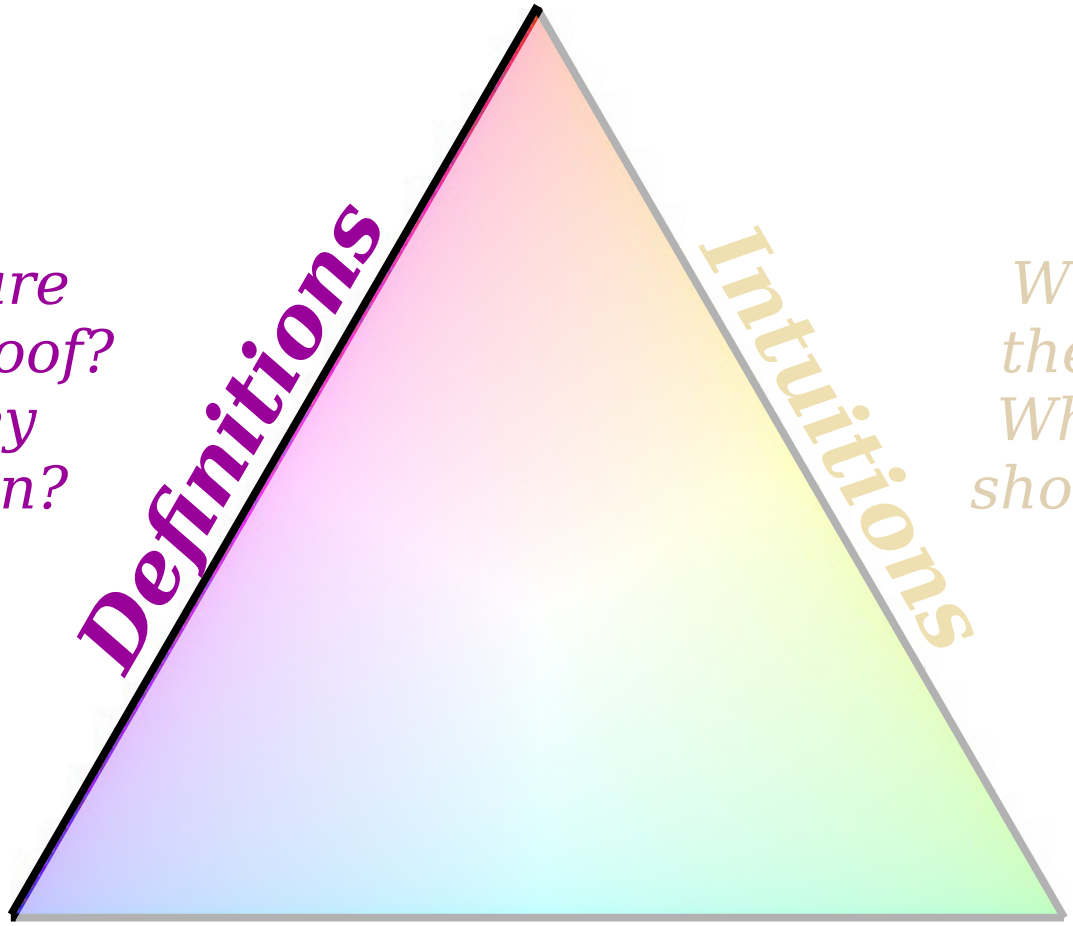
Equation (3) tells us that there is an integer s (namely, $k + r + 1$) such that $m + n = 2s$. Therefore, we see that $m + n$ is even, as required. ■

Some Little Exercises

- Here's a list of other theorems that are true about odd and even numbers:
  - ***Theorem:*** The sum and difference of any two even numbers is even.
  - ***Theorem:*** The sum and difference of an odd number and an even number is odd.
  - ***Theorem:*** The product of any integer and an even number is even.
  - ***Theorem:*** The product of any two odd numbers is odd.
- Going forward, we'll just take these results for granted. Feel free to use them in the problem sets.
- If you'd like to practice the techniques from today, try your hand at proving these results!

Universal and Existential Statements

Theorem: For any odd integer n,
there exist integers r and s where $r^2 - s^2 = n$.



What terms are used in this proof? What do they formally mean?

What does this theorem mean? Why, intuitively, should it be true?

What is the standard format for writing a proof? What are the techniques for doing so?

Theorem: For any odd integer n,
there exist integers r and s where $r^2 - s^2 = n$.

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

This result is true for every possible choice of odd integer n. It'll work for $n = 1$, $n = 137$, $n = 103$, etc.

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

We aren't saying this is true for every choice of r and s. Rather, we're saying that ***somewhere out there*** are choices of r and s where this works.

Universal vs. Existential Statements

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

  For all *x*, `[some-property]` holds for *x*.

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

  There is some *x* where `[some-property]` holds for *x*.

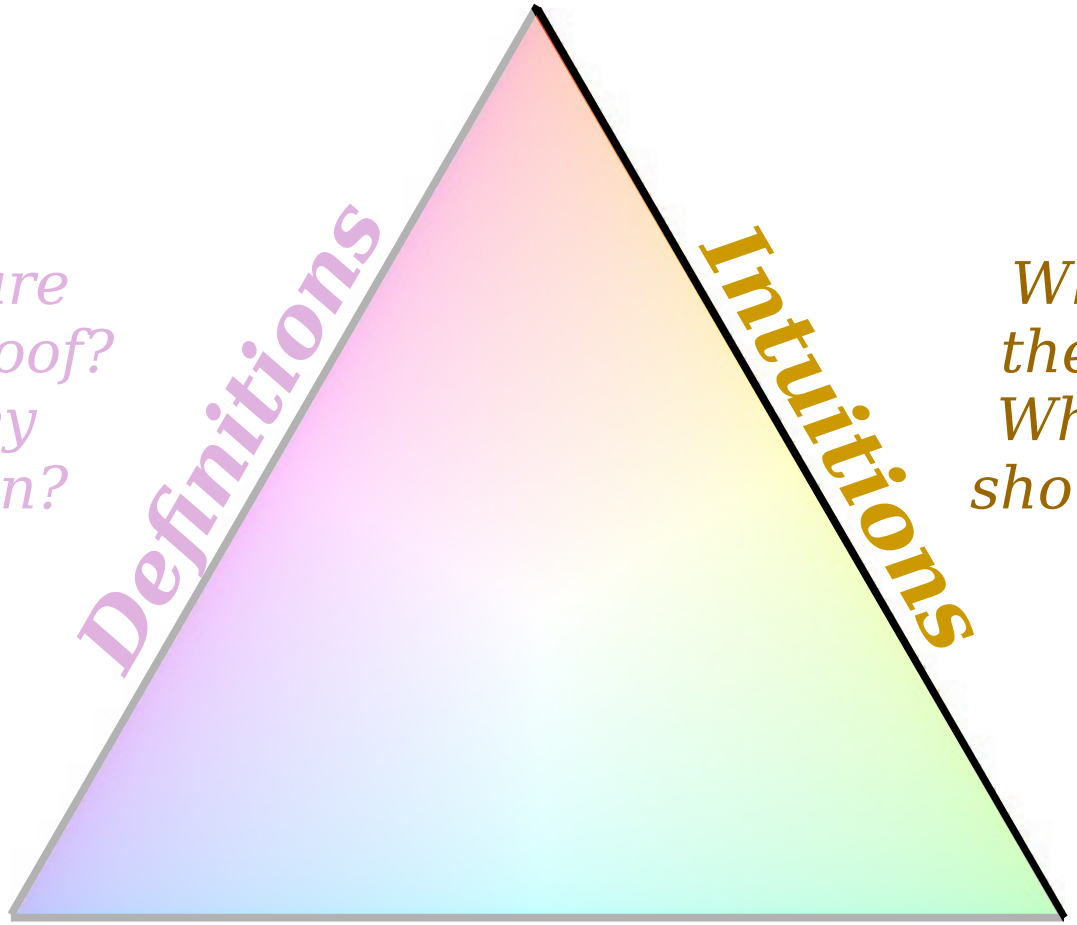
- How do you prove an existential statement?

Proving an Existential Statement

- Over the course of the quarter, we will see several different ways to prove an existential statement of the form

  There is an *x* where `[some-property]` holds for *x*.

- ***Simplest approach:*** Search far and wide, find an x that has the right property, then show why your choice is correct.



What terms are used in this proof? What do they formally mean?

What does this theorem mean? Why, intuitively, should it be true?

What is the standard format for writing a proof? What are the techniques for doing so?

Let's Try Some Examples!

$1 = \_\_^2 - \_\_^2$

$3 = \_\_^2 - \_\_^2$

$5 = \_\_^2 - \_\_^2$

$7 = \_\_^2 - \_\_^2$

$9 = \_\_^2 - \_\_^2$

Question: Fill in these blanks and see if you can come up with a pattern for why this result is true.

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Let's Try Some Examples!

$$1 = \mathbf{1}^2 - \mathbf{0}^2$$

$$3 = \mathbf{2}^2 - \mathbf{1}^2$$

$$5 = \mathbf{3}^2 - \mathbf{2}^2$$

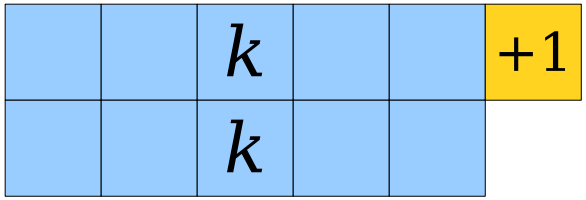
$$7 = \mathbf{4}^2 - \mathbf{3}^2$$

$$9 = \mathbf{5}^2 - \mathbf{4}^2$$

We've got a pattern – but why does this work?

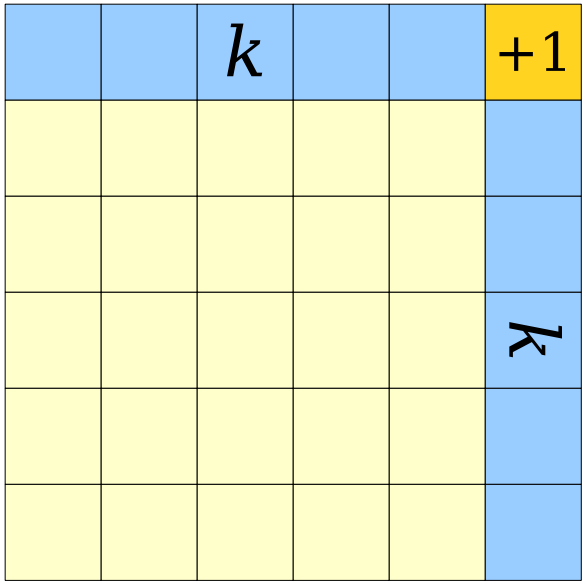
Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Let's Draw Some Pictures!



Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

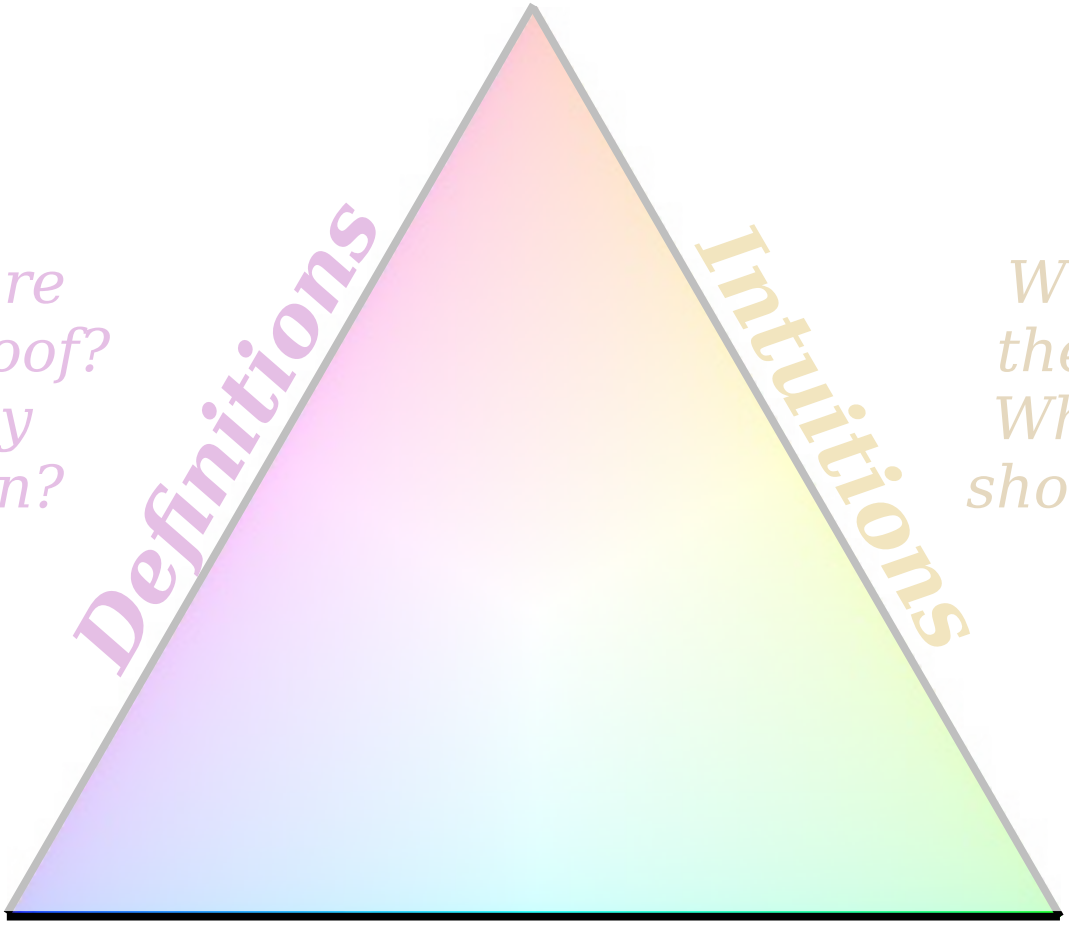
Let's Draw Some Pictures!



$(k+1)^2 - k^2 = 2k+1$

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

What terms are used in this proof? What do they formally mean?



What does this theorem mean? Why, intuitively, should it be true?

Conventions

What is the standard format for writing a proof? What are the techniques for doing so?

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n.

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.

Now, let $r = k+1$ and $s = k$.

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.

Now, let $r = k+1$ and $s = k$. Then we see that

$$r^2 - s^2 \quad = \quad (k+1)^2 - k^2$$

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.

Now, let $r = k+1$ and $s = k$. Then we see that

$$\begin{aligned} r^2 - s^2 &= (k+1)^2 - k^2 \\ &= k^2 + 2k + 1 - k^2 \end{aligned}$$

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.

Now, let $r = k+1$ and $s = k$. Then we see that

$$\begin{aligned} r^2 - s^2 &= (k+1)^2 - k^2 \\ &= k^2 + 2k + 1 - k^2 \\ &= 2k + 1 \end{aligned}$$

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.

Now, let $r = k+1$ and $s = k$. Then we see that

$$\begin{aligned} r^2 - s^2 &= (k+1)^2 - k^2 \\ &= k^2 + 2k + 1 - k^2 \\ &= 2k + 1 \\ &= n. \end{aligned}$$

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.

Now, let $r = k+1$ and $s = k$. Then we see that

$$\begin{aligned} r^2 - s^2 &= (k+1)^2 - k^2 \\ &= k^2 + 2k + 1 - k^2 \\ &= 2k + 1 \\ &= n. \end{aligned}$$

This means that $r^2 - s^2 = n$, which is what we needed to show.

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.

Now, let $r = k+1$ and $s = k$. Then we see that

$$\begin{aligned} r^2 - s^2 &= (k+1)^2 - k^2 \\ &= k^2 + 2k + 1 - k^2 \\ &= 2k + 1 \\ &= n. \end{aligned}$$

This means that $r^2 - s^2 = n$, which is what we needed to show. ■

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.

Now, l

We make an ***arbitrary choice***. Rather than specifying what ***n*** is, we're signaling to the reader that they could, in principle, supply any choice ***n*** that they'd like.

$$= \quad 2k + 1$$

$$= \quad n.$$

This means that $r^2 - s^2 = n$, which is what we needed to show. ■

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.

Now, let $r = k+1$ and $s = k$. Then we see that

$$r^2 - s^2 = (k+1)^2 - k^2$$

We're trying to prove an existential statement. The easiest way to do that is to just give concrete choices of the objects being sought out.

This mean
needed to show. ∎

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.

Now, let $r = k+1$ and $s = k$. Then we see that

$$\begin{aligned} r^2 - s^2 &= (k+1)^2 - k^2 \\ &= k^2 + 2k + 1 - k^2 \\ &= 2k + 1 \\ &= n. \end{aligned}$$

This means that $r^2 - s^2 = n$, which is what we needed to show. ■

Time-Out for Announcements!

Reading Recommendations

- We've released two handouts online that you should read over:
  - **How to Succeed in CS103**
  - **Guide to Proofs**
- Additionally, if you haven't yet read over the **Guide to Elements and Subsets**, we'd recommend doing so.