CSC 240

3 – CANTOR'S THEOREM

SET MEMBERSHIP

- Sets are referred to by uppercase letters (A, B, S, etc…)
- Elements are usually referred to by lowercase letters (x, a, z, etc…)
- Given a set S and an element x, if x is an element of S, we would write:

$$x \in S$$

  otherwise, we would write:

$$x \notin S$$

- Given ANY set S and ANY element x, either $x \in S$ or $x \notin S$.

the symbol for the empty set

$\{ \ \}$ $\varnothing$

the empty set contains no elements

WHAT IS A SET?

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

this is the empty set
a set which contains nothing

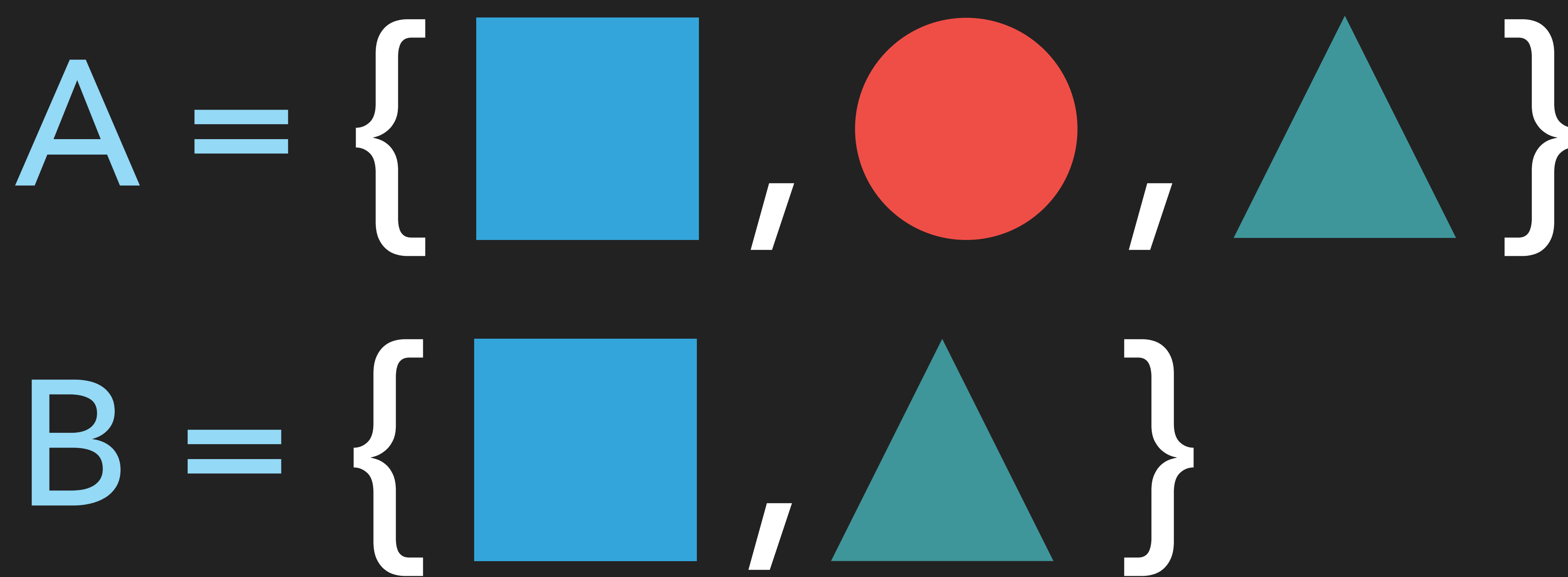
this is a set that contains one element. That element is the empty set.

FAMOUS SETS

- The set of natural numbers, $\mathbb{N}^+$ {1, 2, 3, …}
- The *other* set of natural numbers, $\mathbb{N}$ {0, 1, 2, 3, …}
- The set of integers, $\mathbb{Z}$ {…, -2, -1, 0, 1, 2, …}
- The set of all real numbers, $\mathbb{R}$

these are all *infinite* sets

SUBSETS



$B \subseteq A$ $\qquad\qquad$ $A \supseteq B$

"…is a subset of…" $\qquad$ "…is a superset of…"

SUBSETS

If A and B are sets, and every element of B is also an element of A , then B is a *subset* of A, written as:

$$B \subseteq A$$

and A is a *superset* of B, written as:

$$A \supseteq B$$

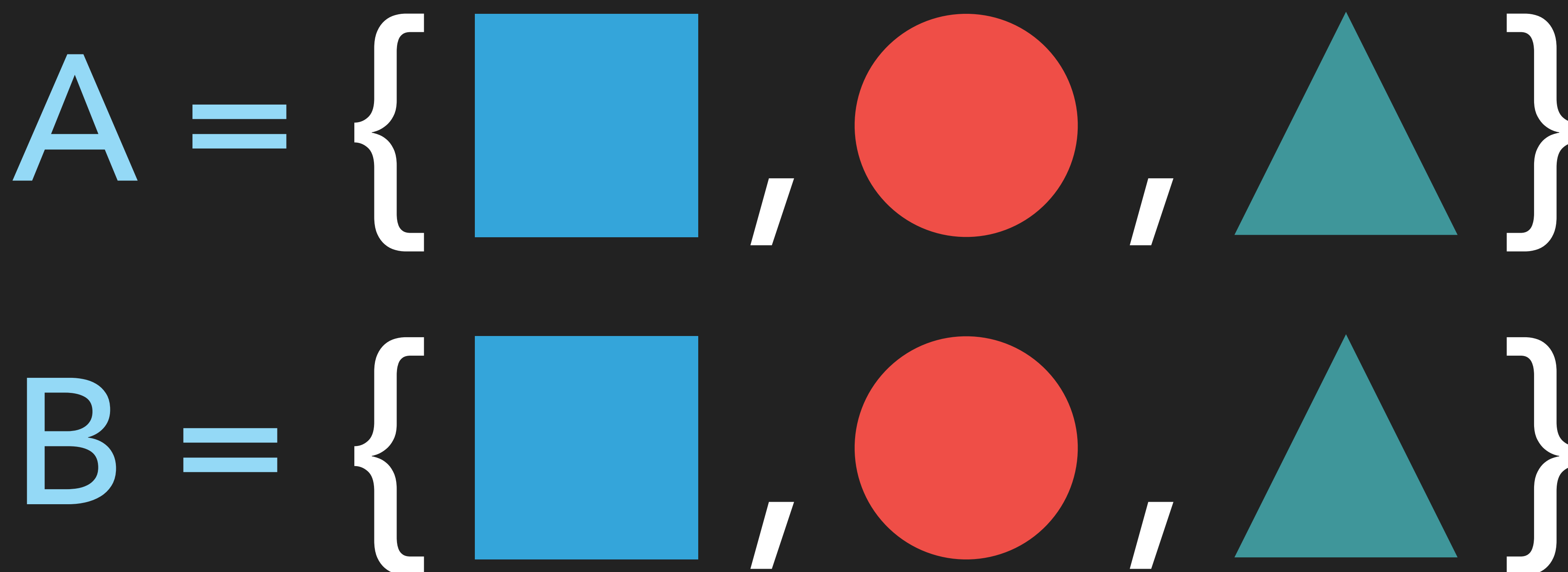
SUBSETS

If A and B are sets, and every element of B is also an element of A , then B is a *subset* of A, written as:

$$B \subseteq A$$

and A is a *superset* of B, written as:

$$A \supseteq B$$



$$B \subseteq A \qquad A \supseteq B$$

SUBSETS

$$A = \{\blacksquare, \bullet, \blacktriangle\}$$

$$B = \{\blacksquare, \bullet, \blacktriangle\}$$

$$C = \{\blacksquare, \bullet\}$$

$B \subseteq A \qquad A \supseteq B$

$C \subsetneq A \qquad A \supsetneq C$

Alt. Symbol: $\subset$

"…is a proper subset of…"

Alt. Symbol: $\supset$

"…is a proper superset of…"

- If A and B are sets, and every element of B is also an element of A , then B is a *subset* of A, written as:

  $$B \subseteq A$$

  and A is a *superset* of B, written as:

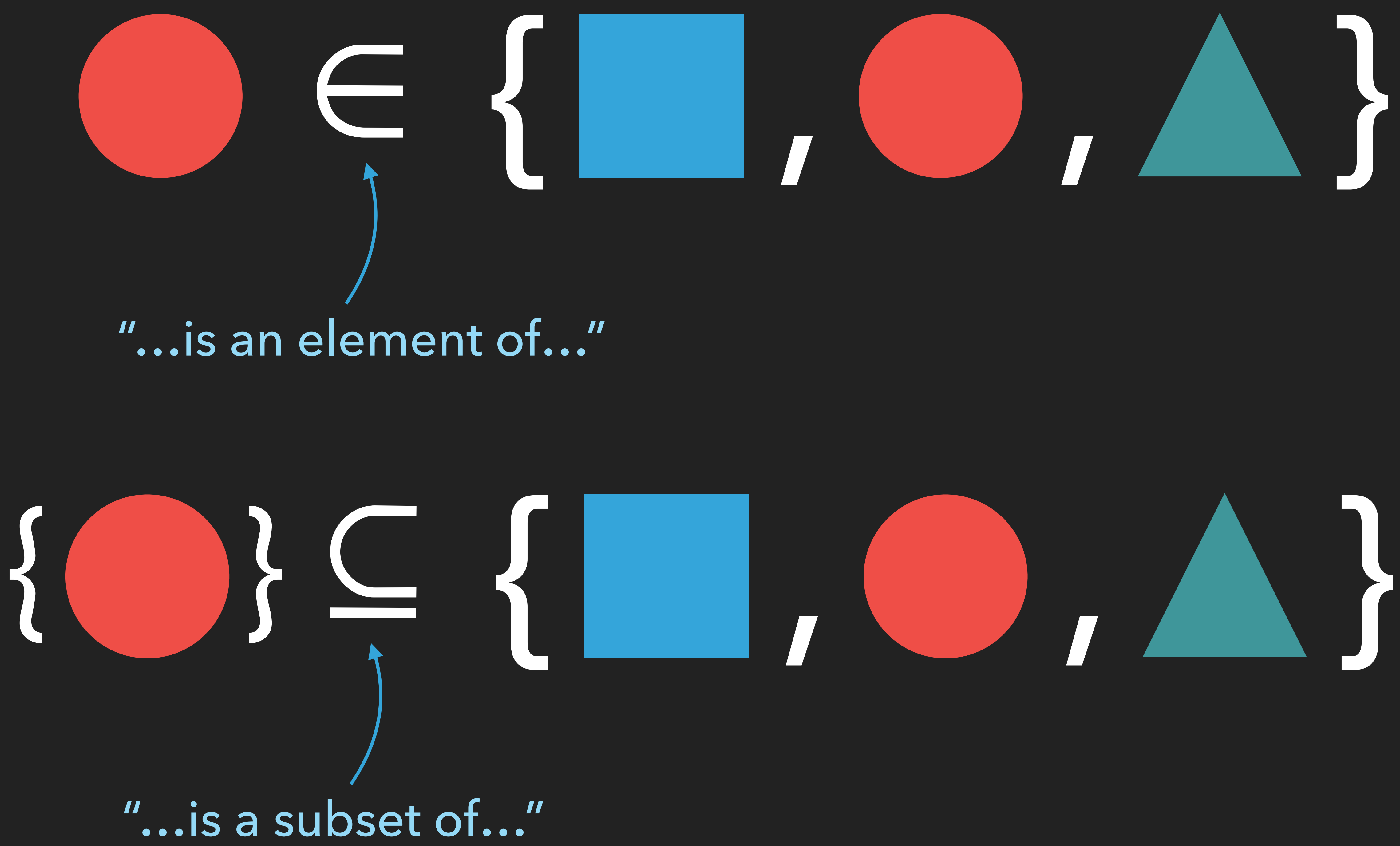
  $$A \supseteq B$$

- If A is a subset of B, but A is not equal to B, then B is a *proper subset* of A, written as:

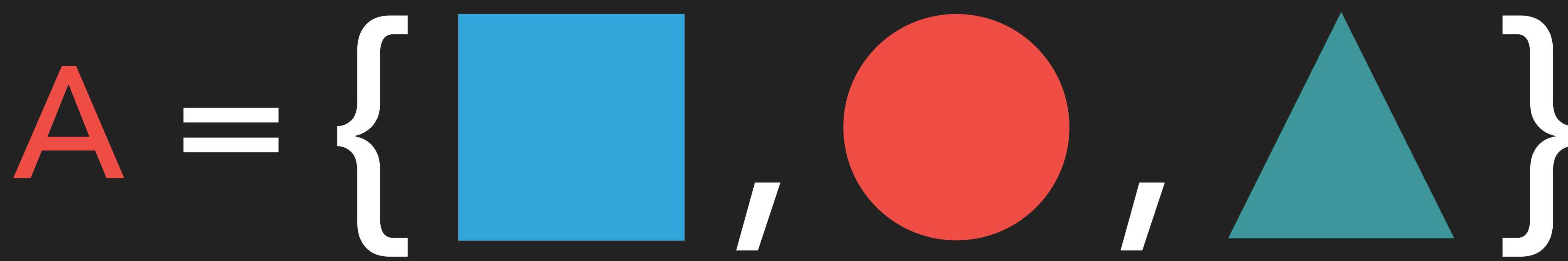
  $$B \subsetneq A$$

  and A is a *proper superset* of B, written as:

  $$A \supsetneq B$$


∈
“…is an element of…”
⊆
“…is a subset of…”

If A and B are sets, and every element of B is also an element of A , then B is a *subset* of A.



$\varnothing$? A

Is the empty set a subset of this set?
(or of any set)

Is this statement true?
"All elements of $\varnothing$ are also elements of set A"

VACUOUS TRUTH

Are these statements true or false?

“All unicorns are pink.”

“All flying whales have blue eyes.”

“All Microsoft iPods have good battery life.”

“All Microsoft iPods have poor battery life.”

These are ALL true statements!

- A statement is *vacuously true* if it is of the form:

$$\{x \in \varnothing\} \subseteq A$$

in other words:

$$P(x) \Rightarrow Q(x) \text{ where } P = \varnothing$$

- Vacuously true statements are automatically true.

"if x is a member of P, then it is also a member of Q"

"But P has no members"

SUBSETS

If A and B are sets, and every element of B is also an element of A , then B is a *subset* of A.

$$A = \{ \blacksquare , \bullet , \blacktriangle \}$$

$$\varnothing \overset{?}{\subseteq} A$$

Is the empty set a subset of this set?
(or of any set)

Is this statement true?
"All elements of ∅ are also elements of set A"

YES! Because this statement is vacuously true!

- The power set of A is the set of all subsets of A, and is written as:

$$\wp(A)$$

Different texts use different "fancy letter p's" for this. This one is called the "Weierstrass p".

- The power set of A is the set of all subsets of A, and is written as:

$$\wp(A)$$

- or, more formally:

$$\wp(A) = \{ B : B \subseteq A \}$$

Different texts use different "fancy letter p's" for this. This one is called the "Weierstrass p".

$$A = \{x, y\}$$

$$\wp(A) = \{\ \varnothing, \{x\}, \{y\}, \{x, y\}\ \}$$

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

$$\wp(B) = \{\ \varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\ \}$$

- The *cardinality* of a set is the number of elements contained in that set. It is written as:

$$|A|$$

$$A = \{\blacksquare, \bullet, \blacktriangle\}$$

$$|A| = 3$$

$$B = \{\blacksquare, \blacktriangle\}$$

$$|B| = 2$$

$$C = \{ x \in \mathbb{N}^{+} : x < 10 \}$$

$$|C| = 9$$

CARDINALITY

$$|\mathbb{N}| = ?$$

CARDINALITY

WARNING: THINGS ARE ABOUT TO GET WEIRD!

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

“aleph (alef) zero”
“aleph naught”
“aleph null”

- Two sets have the same cardinality if there is a way to pair off their elements without leaving any elements out of the pairing.

these sets have the same cardinalities

$\{1, 2, 3\}$

$\{a, b, c\}$

these sets do not have the same cardinalities

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

$\{a, b, c\}$

$$\mathbb{N} = \{\ 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6, \ldots\ \}$$

$$A = \{\ 0,\ 2,\ 4,\ 6, \ldots\ \}$$

$$A = \{\ x \in \mathbb{N} : x \text{ is even }\}$$

do $\mathbb{N}$ and A have the same cardinality?

$$
\begin{array}{lllllllll}
\mathbb{N} = \{ & 0, & 1, & 2, & 3, & 4, & 5, & 6, & \ldots \} \\
 & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & \\
A = \{ & 0, & & 2, & & 4, & & 6, & \ldots \}
\end{array}
$$

Two sets have the same cardinality if there is a way to pair off their elements without leaving any elements out of the pairing.

$$\mathbb{N} = \{\ 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ \dots\ \}$$

$$\updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow$$

$$A = \{\ 0,\ 2,\ 4,\ 6,\ 8,\ 10,\ 12,\ \dots\ \}$$

$$n \longleftrightarrow 2n$$

$$|\,\mathbb{N}\,| = |\,A\,| = \aleph_0$$

Two sets have the same cardinality if there is a way to pair off their elements without leaving any elements out of the pairing.

$$\mathbb{N} = \{\, 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ \ldots \,\}$$

$$\mathbb{Z} = \{\, \ldots,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \ldots \,\}$$

Two sets have the same cardinality if there is a way to pair off their elements without leaving any elements out of the pairing.

$$\mathbb{N} = \{\ 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ \ldots\ \}$$

$$\mathbb{Z} = \{\ 0,\ -1,\ 1,\ -2,\ 2,\ -3,\ 3,\ \ldots\ \}$$

Pair off negative integers with odd naturals

Pair off non-negative integers with even naturals

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

Two sets have the same cardinality if **there is a way** to pair off their elements without leaving any elements out of the pairing.

Does every infinite set have the same cardinality?

$$A = \{x, y\}$$

$$\wp(A) = \{\ \varnothing, \{x\}, \{y\}, \{x, y\}\ \}$$

$$|\,A\,| < |\,\wp(A)\,|$$

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

$$\wp(B) = \{\ \varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\ \}$$

$$|\,B\,| < |\,\wp(B)\,|$$

If A is in infinite set, then what is the relationship between $|A|$ and $|\wp(A)|$?

1. Two sets have the same cardinality if there is a way to pair off their elements without leaving any elements out of the pairing.

2. $|A| = |\wp(A)|$ if there is a way to pair off the elements of A with the elements of $\wp(A)$ without leaving any elements out of the pairing.

3. $|A| = |\wp(A)|$ if there is a way to pair off the elements of A with the the subsets of A without leaving any elements out of the pairing.

Can we do this?

CARDINALITY

$$X = \{x_0, x_1, x_2, x_3, \ldots\}$$

$$x_0 \longleftrightarrow \{x_0, x_2, x_3, \ldots\}$$

$$x_1 \longleftrightarrow \{x_1, x_2, x_3, \ldots\}$$

$$x_2 \longleftrightarrow \{x_0, x_1, \ldots\}$$

$$x_3 \longleftrightarrow \{x_2, \ldots\}$$

$\ldots$

$$X = \{x_0, x_1, x_2, x_3, \ldots\}$$

	x_0	x_1	x_2	x_3	...
x_0	Y	N	Y	Y	...
x_1	N	Y	Y	Y	...
x_2	Y	Y	N	N	...
x_3	N	N	Y	N	...
...	...	...	...	...	...

CARDINALITY

$$X = \{x_0, x_1, x_2, x_3, \ldots\}$$

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

Y	**Y**	**N**	**N**	…

does this row have a pairing?

CARDINALITY

$$X = \{x_0, x_1, x_2, x_3, \ldots\}$$

	x_0	x_1	x_2	x_3	…
x_0	Y	N	Y	Y	…
x_1	N	Y	Y	Y	…
x_2	Y	Y	N	N	…
x_3	N	N	Y	N	…
…	…	…	…	…	…

generate the complement of the row by flipping its Y's and N's.

N	N	Y	Y	…

does this row have a pairing?

- No matter how the elements of A and $\wp$(A) are paired up, the complemented diagonal won't have a match.
- No matter how the elements of A and the subsets of A are paired up, there will always be at least one subset that won't have a match.
- Cantor's Theorem: Every set A is strictly smaller than its power set, $\wp$(A):

$$|A| < |\wp(A)|$$

- This means that

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

- And that:

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

- And:

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

- Therefore, not all infinite sets have the same size
- There is no biggest infinity
- There are infinitely many infinities

The set of all computer programs

The set of all problems

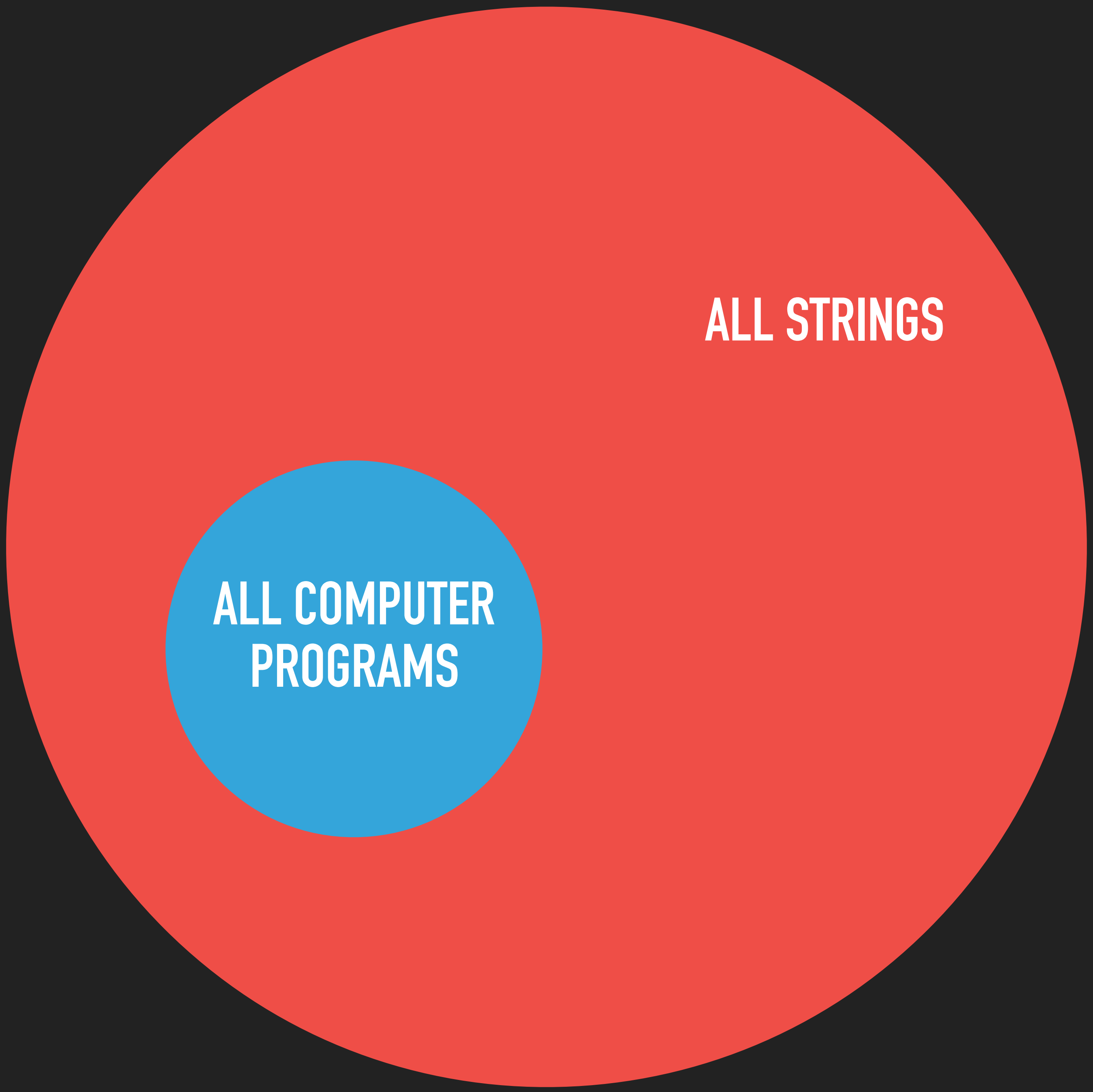
- A *string* is a sequence of characters.
- Two important facts:
  - There are *at most* as many programs as there are strings.
  - There are *at least* as many problems as there are sets of strings.

- The source code of any computer program is just a long string of text.
- All programs are strings, but are all strings programs?

```
int main() {
   cout << "Hello";
}
```

```
int main(){cout<<"Hello";}
```

CANTOR'S THEOREM AND COMPUTABILITY



$$|\text{Programs}| \leq |\text{Strings}|$$

- Is there a connection between the number of sets of strings and the number of problems to solve?
- Let S be any set of strings. Given a string w, determine if $w \in S$.

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

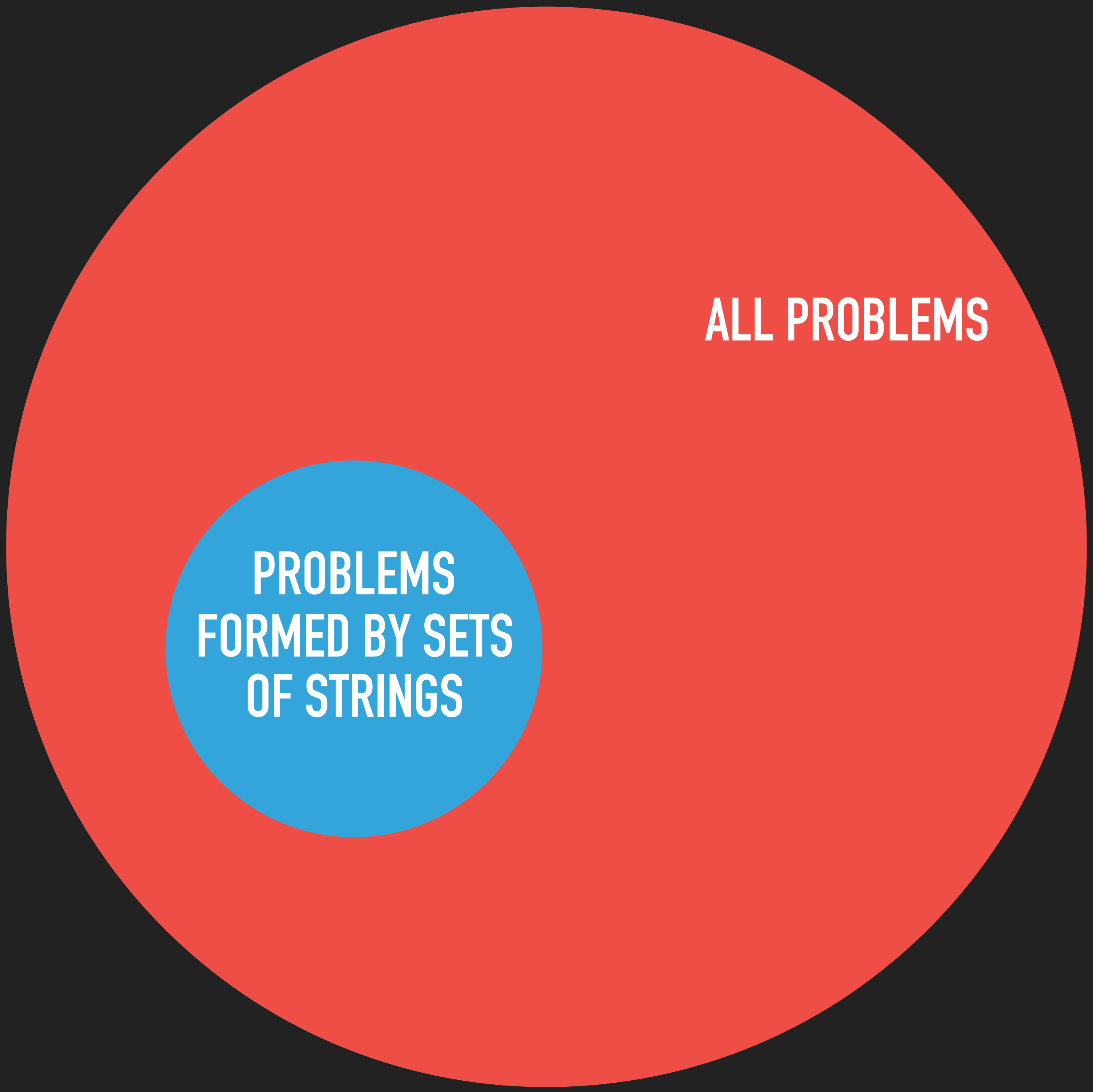
Given a string w, determine whether w is a single lower-case English letter.

$$S = \{ \text{"1"}, \text{"2"}, \text{"3"}, \ldots \}$$

Given a string w, determine whether w represents a positive integer.

- Every set of strings corresponds to at least one unique problem to solve.
- Other problems also exist.

CANTOR'S THEOREM AND COMPUTABILITY



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

- Every computer program is a *string*.
  - There are *at most* as many programs as there are strings.
  - There are *at least* as many problems as there are sets of strings.
- Cantor's Theorem tells us that there are more sets of strings than there are strings.

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

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

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

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

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

If you choose a problem at random from the set of all problems, the probability that it is solvable by a computer program is zero.

How can you prove whether or not the problem you're trying to solve with your computer program is actually solvable by a computer program?