Discrete Mathematics (for Computer Science)

Part II: Computability

Zeyu Mi

2021-11-26

Adapted From:
Stanford CS103 Introduction to Set Theory
《数理逻辑与集合论》9.6-9.7,12.2-12.6

Review

- **Computational Problems**
  - Well-defined Input, output constrain
- **Set Theory Basics**
  - Definition, representation, operation, set identities
- **Formal Language**
  - A language is a set of string
  - Convert a problem solving into language recognizing

How we investigate computability?

《数理逻辑与集合论》9.6-9.7,12.2-12.6

2.1 Discussion on Problems

Part1. Intro & Set theory(I) : Basics & Formal Language.

Part2. Set Theory(II): Axiom system & Cardinality.

Part3. Capture Structures: Binary Relation & Function

2.2 Discussion on Computation

Part1. Turing Machine Basics.

Part2. Variants of Turing Machine. Church-Turing Thesis.

2.3 Discussion on computability

Part1. The Language of Turing Machine. R & RE

Part2. Undecidability.

Recap: Solving Decision Problem

For any decision problem, we can define a predicate P:

$$P(x): (x\ is\ a\ valid\ input) \wedge (x\ has\ the\ property\ the\ problem\ asks)$$

Then we can build the set:

$$\boxed{S = \{x | P(x)\}}$$

内涵表示法

Then the decision problem can be converted to:

Take x as input and decide whether $x \in S$, that S is a known set.

Naïve Set Theory

Intuitive formulation of sets is called naive set theory – goes back to German mathematician George Cantor (1800's)

In naive set theory, $\{\boldsymbol{x}|\boldsymbol{P}(\boldsymbol{x})\}$ is a set, for any predicate $\boldsymbol{P}$

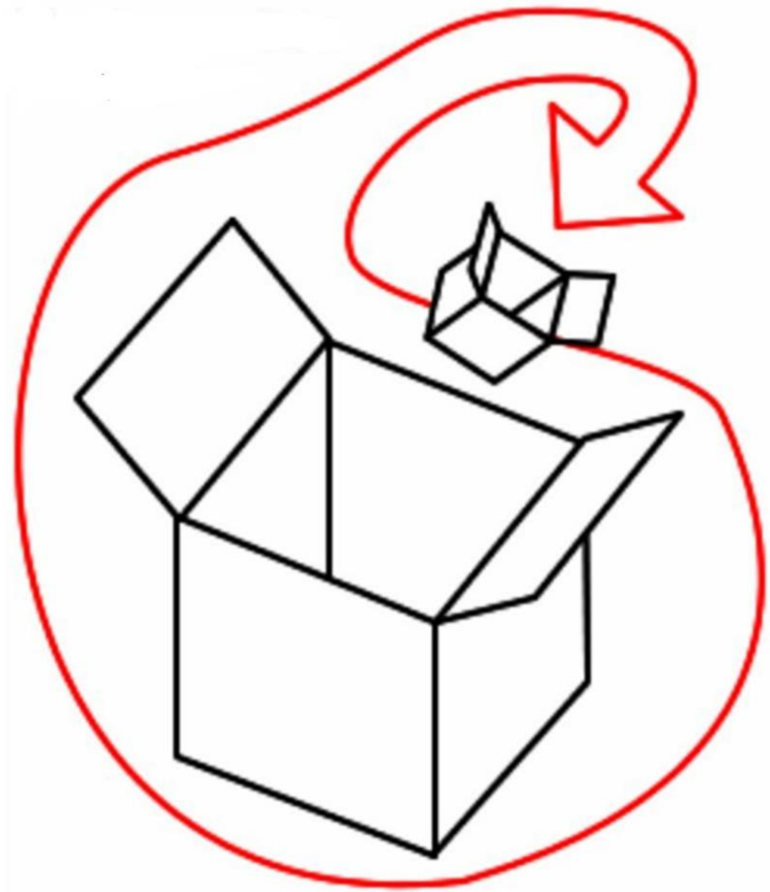
Set of objects that doesn't contain itself

So we can build a set S with predicate $\boldsymbol{P(x)}$: $\boldsymbol{x} \notin \boldsymbol{x}$, that is the set which doesn't contain itself:

$$\boldsymbol{S} = \{\boldsymbol{x} | \boldsymbol{x} \notin \boldsymbol{x}\}$$

Also recall that for any set $\boldsymbol{A}$ and any object $\boldsymbol{a}$, either $\boldsymbol{a} \in \boldsymbol{A}$ or $\boldsymbol{a} \notin \boldsymbol{A}$

$\boldsymbol{S} \in \boldsymbol{S}$ or $\boldsymbol{S} \notin \boldsymbol{S}$?



$\boldsymbol{S = \{x | x \notin x\}}$

If $\boldsymbol{S} \in \boldsymbol{S}$, according to the set construction process, $\boldsymbol{P(S)}$: $\boldsymbol{x} \notin \boldsymbol{x}$ is true, which means $\boldsymbol{S} \notin \boldsymbol{S}$, so we get:

$$\boldsymbol{S} \in \boldsymbol{S} \Rightarrow \boldsymbol{S} \notin \boldsymbol{S}$$

$S = \{x|x \notin x\}$

If $S \in S$, according to the set construction process, $P(S)\colon x \notin x$ is true, which means $S \notin S$, so we get:

$$S \in S \Rightarrow S \notin S$$

If $S \notin S$, then the predicate $P(S)\colon x \notin x$ is true, then we can assert that $S \in S$, so we get:

$$S \notin S \Rightarrow S \in S$$

$\boldsymbol{S = \{x | x \notin x\}}$

If $\boldsymbol{S} \in \boldsymbol{S}$, according to the set construction process, $\boldsymbol{P}(\boldsymbol{S})$: $\boldsymbol{x} \notin \boldsymbol{x}$ is true, which means $\boldsymbol{S} \notin \boldsymbol{S}$, so we get:

$$\boldsymbol{S} \in \boldsymbol{S} \Rightarrow \boldsymbol{S} \notin \boldsymbol{S}$$

If $\boldsymbol{S} \notin \boldsymbol{S}$, then the predicate $\boldsymbol{P}(\boldsymbol{S})$: $\boldsymbol{x} \notin \boldsymbol{x}$ is true, then we can assert that $\boldsymbol{S} \in \boldsymbol{S}$, so we get:

$$\boldsymbol{S} \notin \boldsymbol{S} \Rightarrow \boldsymbol{S} \in \boldsymbol{S}$$

The results above lead to :

$$\boldsymbol{S} \notin \boldsymbol{S} \Leftrightarrow \boldsymbol{S} \in \boldsymbol{S}$$

$\boldsymbol{S} = \{\boldsymbol{x} | \boldsymbol{x} \notin \boldsymbol{x}\}$

If $\boldsymbol{S} \in \boldsymbol{S}$, according to the set construction process, $\boldsymbol{P}(\boldsymbol{S})$: $\boldsymbol{x} \notin \boldsymbol{x}$ is true, which means $\boldsymbol{S} \notin \boldsymbol{S}$, so we get:

$$\boldsymbol{S} \in \boldsymbol{S} \Rightarrow \boldsymbol{S} \notin \boldsymbol{S}$$

If $\boldsymbol{S} \notin \boldsymbol{S}$, then the predicate $\boldsymbol{P}(\boldsymbol{S})$: $\boldsymbol{x} \notin \boldsymbol{x}$ is true, then we can assert that $\boldsymbol{S} \in \boldsymbol{S}$, so we get:

$$\boldsymbol{S} \notin \boldsymbol{S} \Rightarrow \boldsymbol{S} \in \boldsymbol{S}$$

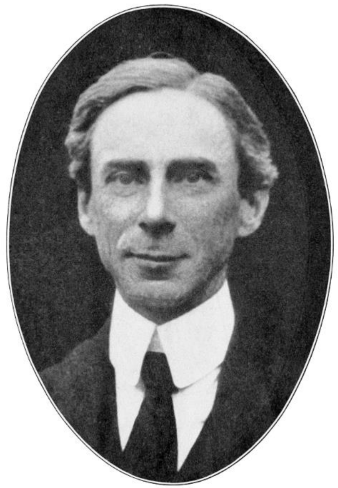
The results above lead to :

$$\boldsymbol{S} \notin \boldsymbol{S} \Leftrightarrow \boldsymbol{S} \in \boldsymbol{S}$$

It's a logic paradox!!Can't be true!!

Russell's Paradox

This paradox is call Russell's paradox, discovered by Bertrand Russell in 1901, showed that some attempted formalizations of the naïve set theory created by Georg Cantor led to a contradiction.

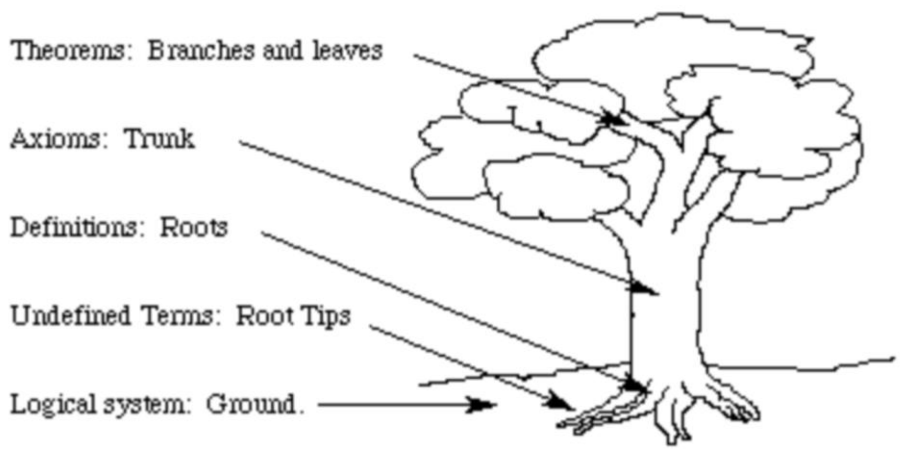


Russell in 1916

Russell’s Paradox: Solution

To solve this paradox, Ernst Zermelo and Abraham Fraenkel proposed an axiomatization of set theory called ZF axioms that avoided the paradoxes of naïve set theory.

ZF set theory is the most general accepted axiom system of set theory now.

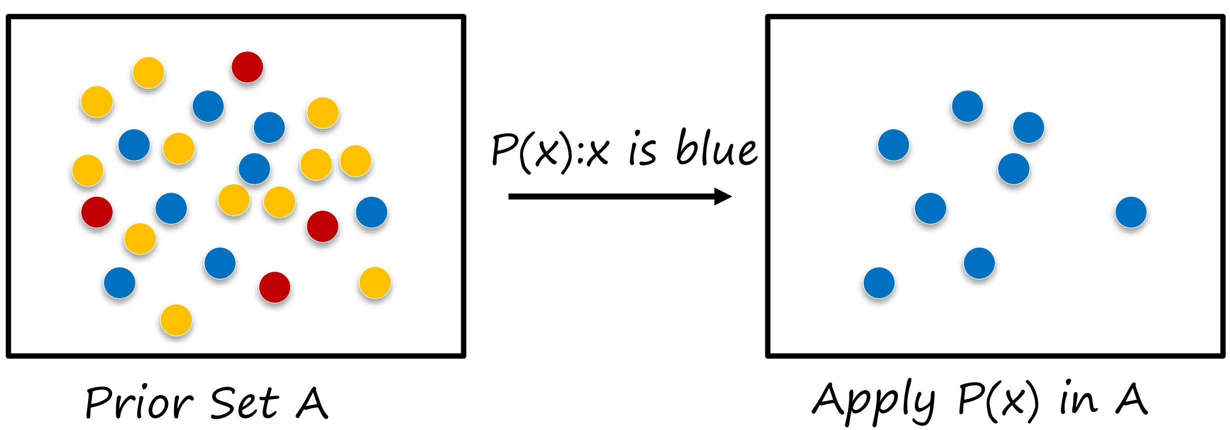


ZF Axiom System

- ZF.1 Axiom of extensionality（外延公理）
- ZF.2 Axiom of the empty set （空集合存在公理）
- ZF.3 Axiom of pairing （无序对集合存在公理）
- ZF.4 Axiom of union （并集合公理）
- ZF.5 Subset axiom schema(子集公理模式)
- ZF.6 Axiom of power set （幂集合公理）
- ZF.7 Axiom of regularity (正则公理)
- ZF.8 Axiom of infinity（无穷公理）
- ZF.9 Axiom of replacement （替换公理）
- ZF.10 Axiom of choice（选择公理）

ZF.5 Subset Axiom Schema（子集公理模式）

- Russell's paradox can be excluded by ZF.5 subset axiom schema and ZF.7 axiom of regularity.
- ZF.5 subset axiom scheme states that for any predicate $P(x)$, you can build a new set whose elements satisfy P **but in a given set**.



ZF.5 Subset Axiom Schema（子集公理模式）

- In other words, for a set $\boldsymbol{A}$, and predicate $\boldsymbol{P}(\boldsymbol{x})$, set $\{\boldsymbol{x} \mid \boldsymbol{x} \in \boldsymbol{A} \wedge \boldsymbol{P}(\boldsymbol{x})\}$ is valid under ZF axiom.
- From set $\boldsymbol{A}$ and predicate $\boldsymbol{x} \in \boldsymbol{B}$:
  - $\boldsymbol{A_0} = \{\boldsymbol{x} \mid \boldsymbol{x} \in \boldsymbol{A} \wedge \boldsymbol{x} \in \boldsymbol{B}\} = \boldsymbol{A} \cap \boldsymbol{B}$
- From set $\boldsymbol{A}$ and predicate $\boldsymbol{x} \notin \boldsymbol{B}$:
  - $\boldsymbol{A_0} = \{\boldsymbol{x} \mid \boldsymbol{x} \in \boldsymbol{A} \wedge \boldsymbol{x} \notin \boldsymbol{B}\} = \boldsymbol{A} - \boldsymbol{B}$
- From a non-empty set $\boldsymbol{A}$ and predicate $(\forall \boldsymbol{y})(\boldsymbol{y} \in \boldsymbol{A} \rightarrow \boldsymbol{x} \in \boldsymbol{y})$:
  - $As\ A\ is\ non-empty, so\ there\ exists\ a\ set\ \boldsymbol{A_1} \in \boldsymbol{A}$
  - $\boldsymbol{A_0} = \{\boldsymbol{x} \mid \boldsymbol{x} \in \boldsymbol{A_1} \wedge (\forall \boldsymbol{y})(\boldsymbol{y} \in \boldsymbol{A} \rightarrow \boldsymbol{x} \in \boldsymbol{y})\} = \bigcap \boldsymbol{A}$

ZF.5 & Russell's Paradox

- But Russell's construction $S = \{x |\ x \notin x\}$ lacks the prior set A.

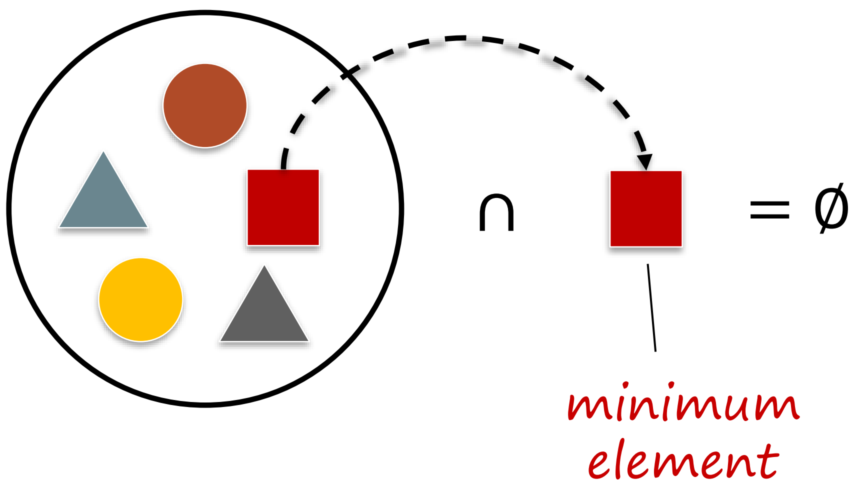
ZF.5 & Russell's Paradox

- But Russell's construction $S = \{x |\ x \notin x\}$ lacks the prior set A.

What if there exists a set **U** *contains all the sets, so that*
$S=\{x|x\in U\land x\notin x\}$ *satisfies subset axiom scheme?*

ZF.7 Axiom of regularity （正则公理）

- ZF.7 Axiom of regularity states that every non-empty set x contains a member y such that x and y are disjoint sets.
  - y is called the minimum element of x



Every set has a minimum element

ZF.7 Axiom of regularity (正则公理)

- **For any set A, can $A \in A$?**
  - Assume that $\boldsymbol{A} \in \boldsymbol{A}$.
  - We can build a new set $\boldsymbol{A}_0 = \{\boldsymbol{A}\}$.
  - According to the ZF.7 axiom of regularity, set $\boldsymbol{A_0}$ contains an element which is disjointed with $\boldsymbol{A_0}$. As $\boldsymbol{A_0}$ contains only one element $\boldsymbol{A}$, so $\boldsymbol{A_0}$ is disjointed with $\boldsymbol{A}$.
  - But $\boldsymbol{A} \in \boldsymbol{A}$, and $\boldsymbol{A} \in \boldsymbol{A_0}$, so $\boldsymbol{A} \cap \boldsymbol{A_0} \neq \emptyset$, this violates the axiom of regularity
  - So $\boldsymbol{A} \notin \boldsymbol{A}$ for any set $\boldsymbol{A}$.

ZF.7 & Russell's Paradox

What if there exists a set U contains all the sets, so that $S=\{x|x\in U \wedge x\notin x\}$ *satisfies subset axiom scheme?*

- If such universal set $\boldsymbol{U}$ exists, as $\boldsymbol{U}$ is also a set, so we have $\boldsymbol{U} \in \boldsymbol{U}$.
- But we know for any set x, we have $x \notin x$
- This means that $\boldsymbol{U}$ doesn't exists.

Russell's paradox doesn't exist in ZF set theory.

Does $\cap\emptyset$ *exist?*

ZF Axiom System

ZF.1 Axiom of extensionality

Two sets are equal (are the same set) if they have the same elements.

$$(\forall x)(\forall y)(x = y \leftrightarrow (\forall z)(z \in x \leftrightarrow z \in y))$$

ZF.2 Axiom of the empty set

There exists a set contains no elements.

$$(\exists x)(\forall y)(y \notin x)$$

ZF.3 Axiom of pairing

If x and y are sets, then there exists a set which contains x and y as elements.

$$(\forall x)(\forall y)(\exists z)(\forall u)(u \in z \leftrightarrow ((u = x) \vee (u = y)))$$

ZF Axiom System

ZF.4 Axiom of union

The union over the elements of a set exists.

$$(\forall x)(\exists y)(\forall z)(z \in y \leftrightarrow (\exists u)(z \in u \wedge u \in x))$$

ZF.5 Subset axiom schema

For any predicate $P(z)$,for any set x, then there exists a set y such that the element of y is also the element of x and $P(z)$ holds.

$$(\forall x)(\exists z)(\forall y)(z \in y \leftrightarrow (z \in x \wedge P(z)))$$

ZF.6 Axiom of power set

For any set x, there exists a set y such that the element of y is subset of x.

$$(\forall x)(\exists y)(\forall z)(z \in y \leftrightarrow (\forall u)(u \in z \to u \in x))$$

ZF Axiom System

ZF.7 Axiom of regularity (Axiom of foundation)

Every non-empty set x contains a member y such that x and y are disjoint sets.

$$(\forall x)(x \neq \varnothing \rightarrow (\exists y)(y \in x \wedge (y \cap x = \varnothing))$$

ZF.8 Axiom of infinity

There exists a set containing all the natural numbers.(First infinite set.)

$$(\exists x)(\varnothing \in x \wedge (\forall y)(y \in x \rightarrow (y \cup \{y\}) \in x))$$

ZF Axiom System

ZF.9 Axiom of replacement (替换公理模式)

For any predicate $P(x, y)$, if for any x there exists a unique y such that $P(x, y)$ holds. Then for all set t there exist a set s, such that the element y in s is exact the the corresponding y($P(x, y) holds$) of x in t.

$$(\forall x)(\exists y)(P(x, y) \wedge (\forall z)(P(x, y) \rightarrow z = y)) \rightarrow$$
$$(\forall t)(\exists s)(\forall u)(u \in s \leftrightarrow (\exists z)(z \in t \wedge P(z, u)))$$

ZF.10 Axiom of choice(选择公理)

For any relation R, there exists a function F, such that F is a subset of R and the domain of F and R are equal.

$$(\forall \text{ Relation } R)(\exists \text{ Function } F)(F \subseteq R \wedge dom(R) = dom(F))$$

Size of “The set of all computer programs”

and

Size of “The set of all problems to solve”

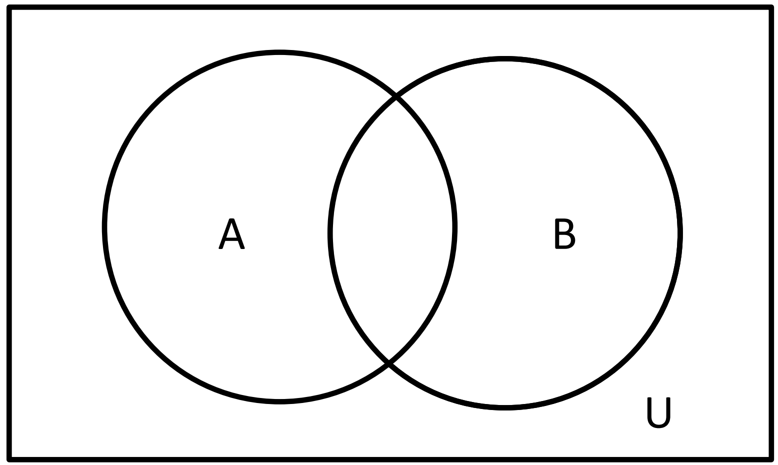
Cardinality of finite set

- The cardinality of a set is the number of elements it contains.
- If $|A|$ is a set, we denote its cardinality by writing $|A|$ or $card(A)$
- **Examples:**
  - $|\emptyset| = card(\emptyset) = 0$
  - $|\{17,23\}| = card(\{17,23\}) = 2$
  - $|\{x|x \in N \land x < 157\}| = card(\{x|x \in N \land x < 157\}) = 157$
- Only finite set’s cardinality is a specific number

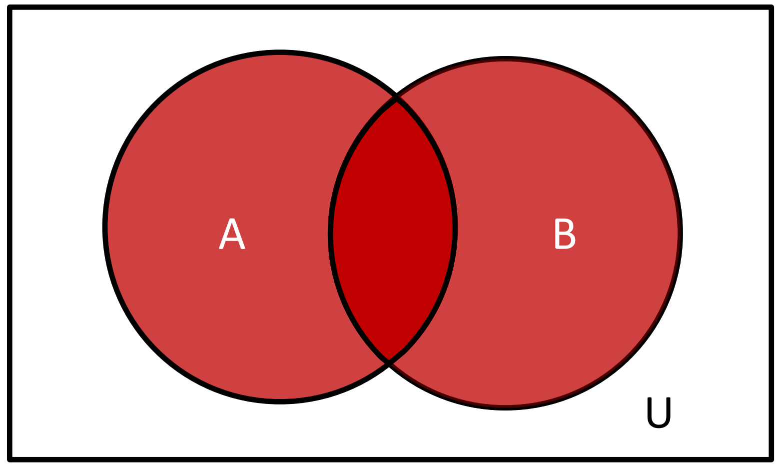
Cardinality with Set Operation

- $|A_1 \cup A_2| \leq |A_1| + |A_2|$
- $|A_1 \cap A_2| \leq \min(|A_1|, |A_2|)$
- $|A_1 - A_2| \geq |A_1| - |A_2|$
- $|A_1 \oplus A_2| = |A_1| + |A_2| - 2|A_1 \cap A_2|$
- $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

Cardinality of Union

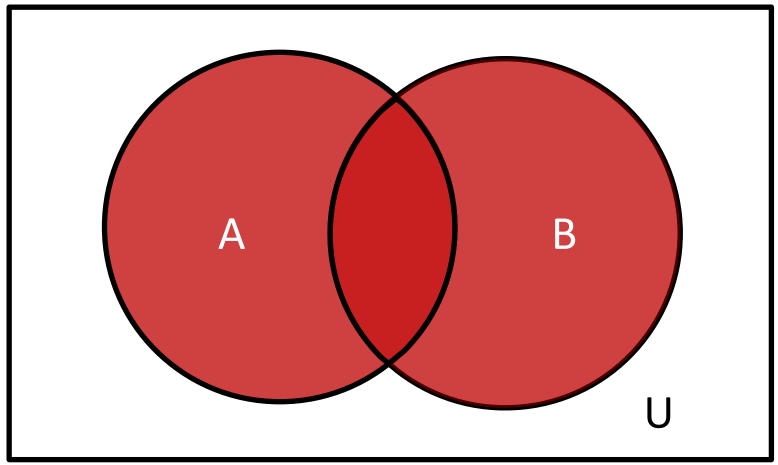


Cardinality of Union



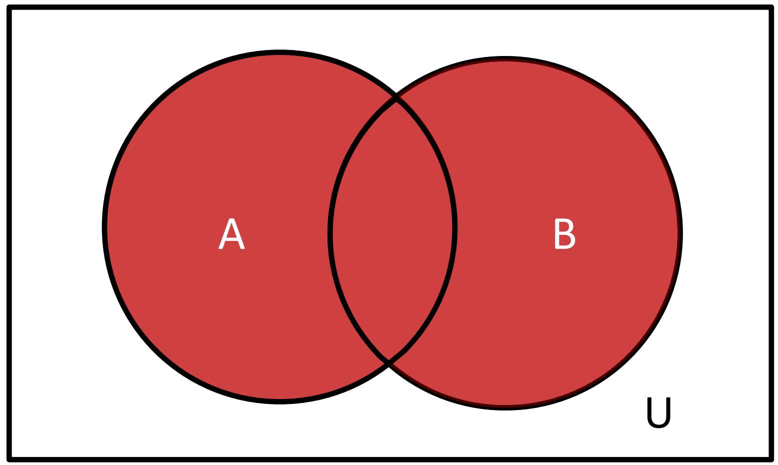
$$|A| + |B|$$

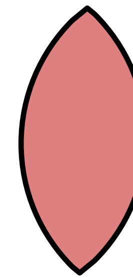
Cardinality of Union



$$|A| + |B| - |A \cap B|$$

Cardinality of Union





$$|A \cup B| = |A| + |B| - |A \cap B|$$

A Problem

- **Question:** Find the number of positive integers not exceeding 100 that are not divisible by 5 or 7.

A Problem

- **Question:** Find the number of positive integers not exceeding 100 that are not divisible by 5 or 7.
- **Answer:**

$d|n$ means that n is divisible by d

Universe $U = \{n|n \leq 100\}, A_5 = \{n|n \leq 100 \wedge 5|n\}, A_7 = \{n|n \leq 100 \wedge 7|n\}$

Numbers divisible by 5 or 7 = $A_5 \cup A_7$

So results = $|U| - |A_5 \cup A_7|$

A Problem

- **Question:** Find the number of positive integers not exceeding 100 that are not divisible by 5 or 7.
- **Answer:**

d|n means that n is divisible by d

Universe $U = \{n | n \leq 100\}, A_5 = \{n | n \leq 100 \wedge 5|n\}, A_7 = \{n | n \leq 100 \wedge 7|n\}$

Numbers divisible by 5 or 7 = $A_5 \cup A_7$

So results = $|U| - |A_5 \cup A_7|$

$$|A_5 \cup A_7| = |A_5| + |A_7| - |A_5 \cap A_7| = \frac{100}{5} + \frac{100}{7} - \frac{100}{5 * 7} = 20 + 14 - 2 = 32$$

So results = 100-32=68

Principle of Inclusion and Exclusion(容斥定理)

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| + \cdots + (-1)^{n-1} |A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n|$$

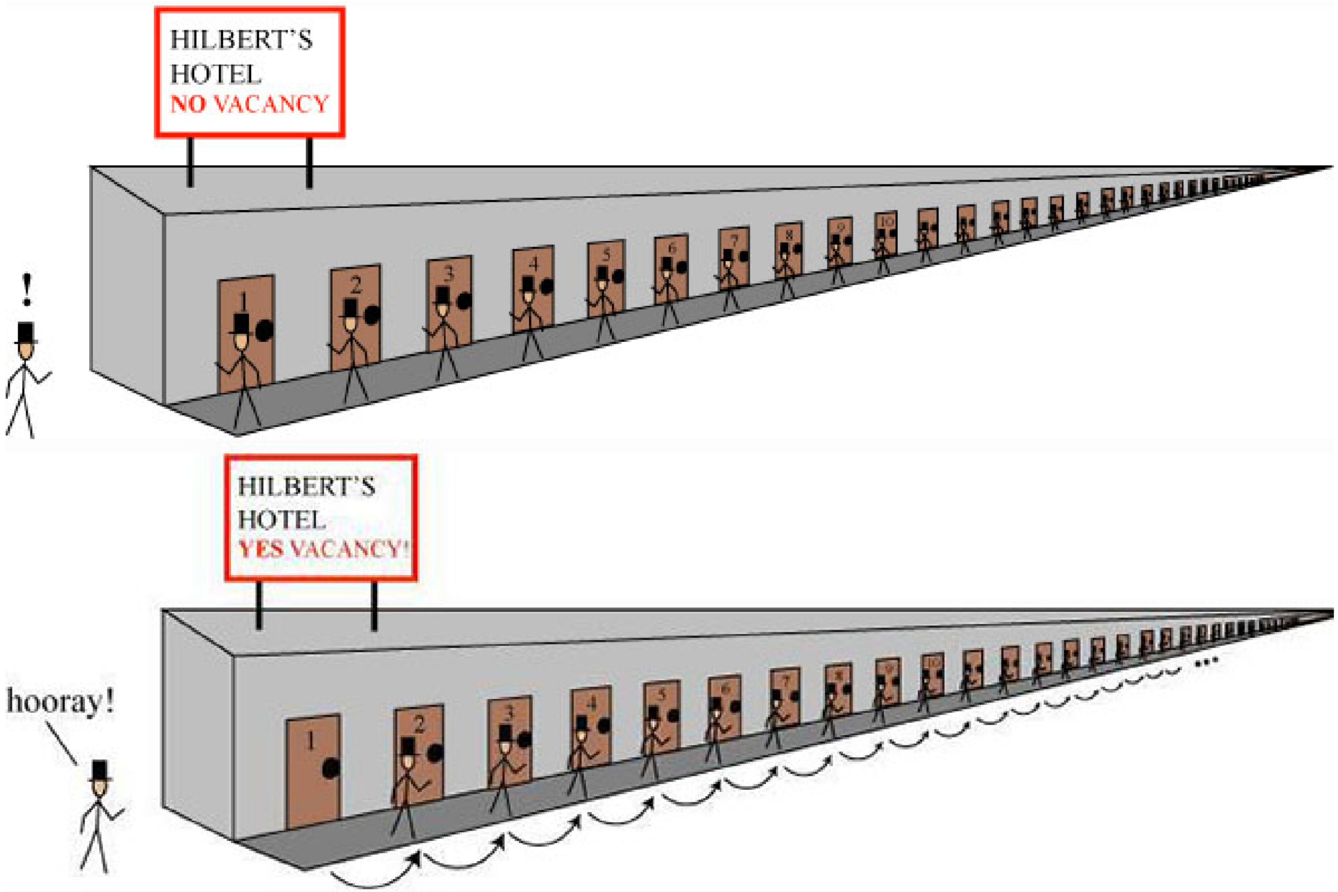
n=2: $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

n=3: $|A_1 \cup A_2 \cup A_3| =$

$$|A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

Cardinality of Infinite Set

- What is the cardinality of infinite set?
- Can we simply define the cardinality of all infinite sets as ∞?
- Or are there infinite sets of different sizes?


HILBERT'S
HOTEL
NO VACANCY
HILBERT'S
HOTEL
YES VACANCY!
hooray!

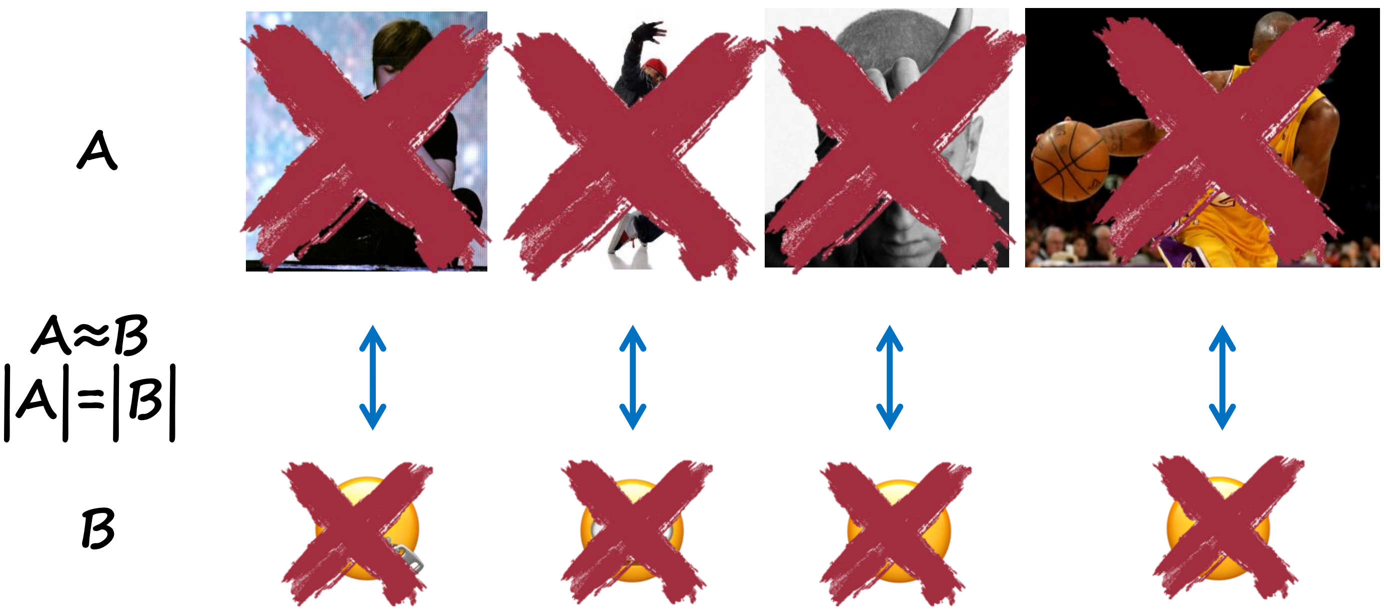
Cardinality of Infinite Set

- The cardinality of $\mathbb{N}$ can't be a natural number, since it's infinitely large.
- Let's define $\aleph_0 = |\mathbb{N}|$
  - $\aleph_0$ is pronounced "aleph-zero", "aleph-nought", or "aleph-null"（阿涅夫零）
- Now consider the set $\boldsymbol{S} = \{\boldsymbol{n} | \boldsymbol{n} \in \mathbb{N} \land \boldsymbol{n}\ \boldsymbol{is}\ \boldsymbol{even}\}$
- What is $|S|$? Is it half of $\aleph_0$?

Comparing Cardinalities

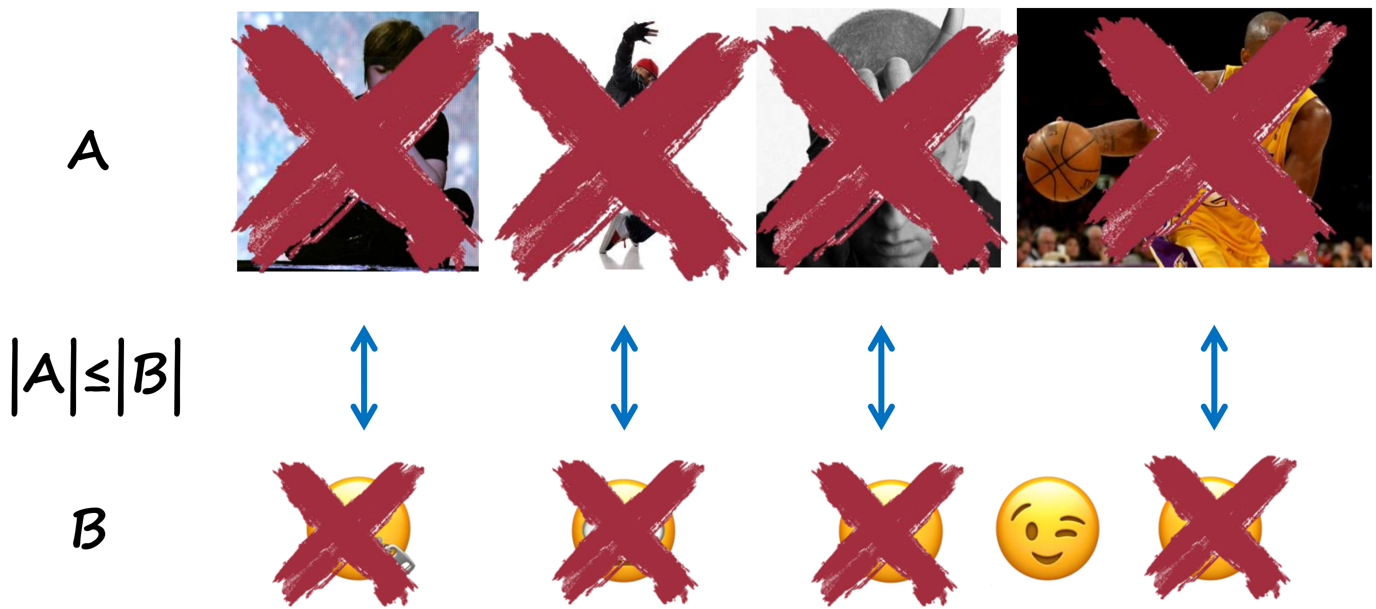
Comparing Cardinalities

For set A and B, A and B are **equianumerous (等势)** if there is a way to pair their elements off without leaving any elements uncovered, marked as $A \approx B$. Otherwise marked as $\neg A \approx B$.



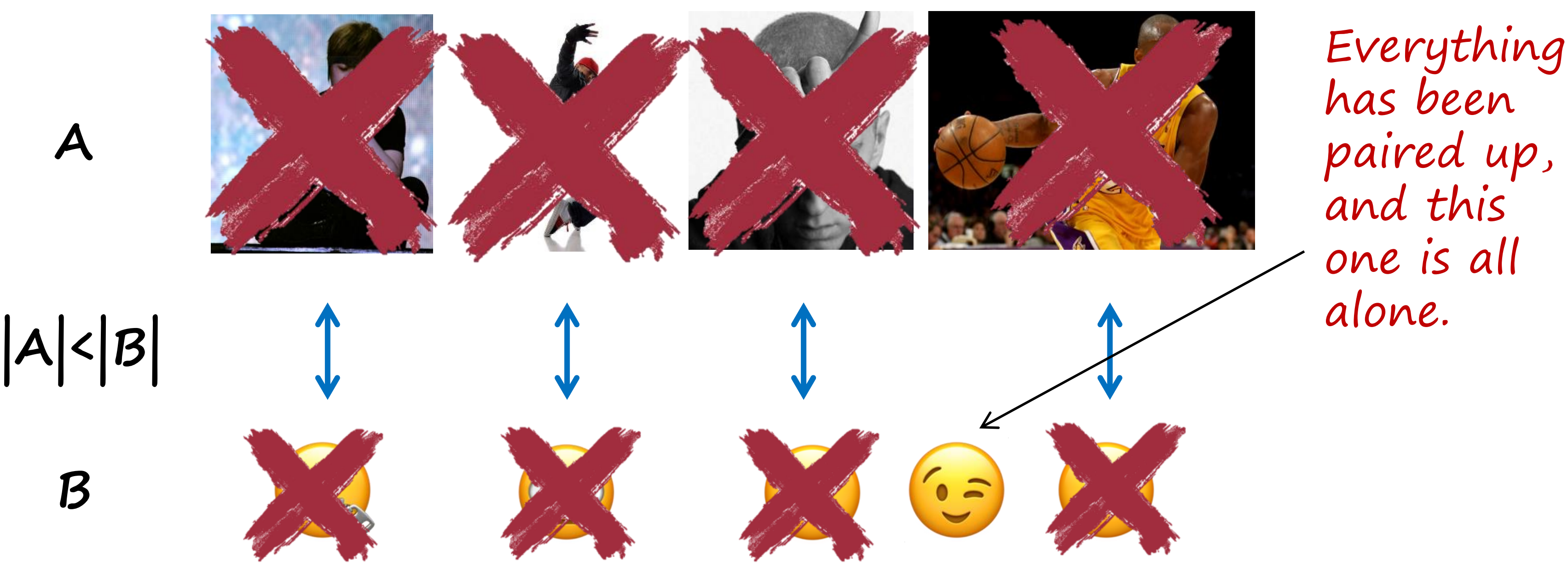
Comparing Cardinalities

For set A and B, $card(A) \leq card(B)$ if there is a way to pair their elements off without leaving **any elements of A** uncovered.



Comparing Cardinalities

For set A and B, $card(A) < card(B)$ if $card(A) \leq card(B)$ and $\neg A \approx B$.



$\mathbb{N}$ and Non-negative Even Integer

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	9	…
	$\updownarrow$		$\updownarrow$		$\updownarrow$		$\updownarrow$		$\updownarrow$		
S	0		2		4		6		8		…

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

$\mathbb{N}$ and Non-negative Even Integer

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	9	…
	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	
S	0	2	4	6	8	10	12	14	16	18	…

$$\boldsymbol{n} \boxed{\leftrightarrow} \boldsymbol{2n}$$

$$\boldsymbol{S} = \{\boldsymbol{n} | \boldsymbol{n} \in \mathbb{N} \land \boldsymbol{n}\ \boldsymbol{is}\ \boldsymbol{even}\}$$

$$|\boldsymbol{S}| = |\mathbb{N}| = \aleph_{\mathbf{0}}$$

$\mathbb{N}$ and $\mathbb{Z}$

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	9	...
$\mathbb{Z}$	...	-4	-3	-2	-1	0	1	2	3	4	...

$\mathbb{N}$ and $\mathbb{Z}$

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	9	…
$\mathbb{Z}$						0	1	2	3	4	…
	…	-4	-3	-2	-1						

ℕ and ℤ

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	9	…
$\mathbb{Z}$	0		1		2		3		4		…
	…	-4	-3	-2	-1						

$\mathbb{N}$ and $\mathbb{Z}$

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	9	…
$\mathbb{Z}$	0		1		2		3		4		…
	…	−4	−3	−2	−1						

$\mathbb{N}$ and $\mathbb{Z}$

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	9	...
$\mathbb{Z}$	0	-1	1	-2	2	-3	3	-4	4	-5	...

$\mathbb{N}$ and $\mathbb{Z}$

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	9	...
	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	
$\mathbb{Z}$	0	-1	1	-2	2	-3	3	-4	4	-5	...

$\mathbb{N}$ and $\mathbb{Z}$

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	9	…
	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	
$\mathbb{Z}$	0	-1	1	-2	2	-3	3	-4	4	-5	…

$$\boldsymbol{n} \leftrightarrow (-\mathbf{1})^{\boldsymbol{n}} \left\lceil \frac{\boldsymbol{n}}{\mathbf{2}} \right\rceil$$

$$|\mathbb{Z}| = |\mathbb{N}| = \aleph_{\mathbf{0}}$$

Countable Set

- A set is **countable** if the cardinality of which is **smaller than or equal to** that of the **set of all natural number**.
  - $\boldsymbol{A}$ is countable if $|\boldsymbol{A}| \leq \aleph_{\mathbf{0}}$
- All finite sets are countable.
- As $|\mathbb{Z}| = |\mathbb{Q}| = |\mathbb{N}|$, $\mathbb{Z}$ and $\mathbb{Q}$ are also countable sets.

Do all infinite sets have the same cardinality?

Power Set

ZF.6 Axiom of power set(幂集合公理)

For any set x, there exists a set y such that the element of y is subset of x.

$$(\forall x)(\exists y)(\forall z)(z \in y \leftrightarrow (\forall u)(u \in z \to u \in x))$$

- Donate the power set of set A as $\mathcal{P}(A)$ or 2^A
- $A = \{1,2,3\}$
  - $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$
- For finite set A with $|A| = n$, what is $|\mathcal{P}(A)|$?

Cardinality of Power Set

- For finite set $\boldsymbol{A}$ with $|\boldsymbol{A}| = n$, we can use a binary string of length n to represent its subset.

1	2	3	4	5	6	…	n
0	0	1	1	0	1	…	1

0 means the subset doesn't contain corresponding element

1 means the subset contains corresponding element

Cardinality of Power Set

- For finite set $\boldsymbol{A}$ with $|\boldsymbol{A}| = n$, we can use a binary string of length n to represent its subset.
- Every binary string represent an unique subset
  - Let $\boldsymbol{A} = \{1,2,3,4\}$, then *0101* represents $\{2,4\}$ and *0011* represents $\{3,4\}$
- There are 2^n different binary string of length n, so $\boldsymbol{A}$ has 2^n subsets.
- So $|\boldsymbol{\mathcal{P}}(\boldsymbol{A})| = 2^n = 2^{|\boldsymbol{A}|}$

Cardinality of Power Set

- As $2^n > n$ for all positive integer n, we can get
$$|\mathcal{P}(\boldsymbol{A})| = 2^{|\boldsymbol{A}|} > |\boldsymbol{A}|$$
for all finite sets $\boldsymbol{A}$
- Does $|\mathcal{P}(\boldsymbol{S})| > |\boldsymbol{S}|$ for all infinite sets $\boldsymbol{S}$?

Power Set of Infinite Set

- For an infinite set $\boldsymbol{S} = \{\boldsymbol{x_0}, \boldsymbol{x_1}, \boldsymbol{x_2}, \ldots\}$, we assume that $\mathcal{P}(\boldsymbol{S}) \approx \boldsymbol{S}$
- It means we can pair up the elements of $\boldsymbol{S}$ and the elements of $\mathcal{P}(\boldsymbol{S})$ without leaving anything out.

Power Set of Infinite Set

- For an infinite set $\boldsymbol{S} = \{\boldsymbol{x_0}, \boldsymbol{x_1}, \boldsymbol{x_2}, \dots\}$, we assume that $\boldsymbol{\mathcal{P}(S) \approx S}$
- It means we can pair up the elements of $\boldsymbol{S}$ and the **elements of $\boldsymbol{\mathcal{P}(S)}$** without leaving anything out.

subset of $\boldsymbol{S}$

Power Set of Infinite Set

- For an infinite set $\boldsymbol{S} = \{\boldsymbol{x_0}, \boldsymbol{x_1}, \boldsymbol{x_2}, \ldots\}$, we assume that $\boldsymbol{\mathcal{P}(S) \approx S}$
- It means we can pair up the elements of $\boldsymbol{S}$ and the **subset of $\boldsymbol{S}$** without leaving anything out.

What would that look like?

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

$x_1 \longleftrightarrow \{x_3, x_5, \ldots\}$

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

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

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

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

$\ldots \longleftrightarrow \{\ldots\}$

x_0	x_1	x_2	x_3	x_4	x_5	…

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

$x_1 \longleftrightarrow \{x_3, x_5, \ldots\}$

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

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

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

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

$\ldots \longleftrightarrow \{\ldots\}$

	x_0	x_1	x_2	x_3	x_4	x_5	…
$x_0 \leftrightarrow \{$	$x_0,$		$x_2,$		$x_4,$		…
$x_1 \leftrightarrow \{$				$x_3,$		$x_5,$	…
$x_2 \leftrightarrow \{$	$x_0,$		$x_2,$			$x_5,$	…
$x_3 \leftrightarrow \{$		$x_1,$			$x_4,$		…
$x_4 \leftrightarrow \{$			$x_2,$				…
$x_5 \leftrightarrow \{$	$x_0,$				$x_4,$	$x_5,$	…
… $\leftrightarrow \{$	…	…	…	…	…	…	…

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

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

Flip this set. Swap what's included and what's excluded

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

Which element is paired with this set?

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

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

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

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

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

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

$\{$		x_1,		x_3,	x_4,		... $\}$

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

{		x_1,		x_3,	x_4,		… }

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

No element can be paired with this set!!!

The Cantor's Theorem

- It's obvious that $|\boldsymbol{S}| \leq |\mathcal{P}(\boldsymbol{S})|$ as every elements of $\boldsymbol{S}$ can construct a subset of $\boldsymbol{S}$, it's easy to pair $\boldsymbol{S}$ with $\mathcal{P}(\boldsymbol{S})$ without leaving any element of $\boldsymbol{S}$.
- And we have $\neg\boldsymbol{S} \approx \mathcal{P}(\boldsymbol{S})$ from the diagonalization proof.
- So we have the **Cantor's Theorem**: Every set is strictly smaller than its power set:

$$\boxed{|\boldsymbol{S}| < |\mathcal{P}(\boldsymbol{S})| \text{ for any set } \boldsymbol{S}}$$

Infinite Cardinalities

- By Cantor's Theorem:

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$$
$$|\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))|$$
$$|\mathcal{P}(\mathcal{P}(\mathbb{N}))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))|$$
$$|\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))))|$$
$$\ldots$$

- Not all infinite sets have the same size!
- There is no biggest infinity!
- There are infinitely many infinities!

Size of "The set of all computer programs"

and

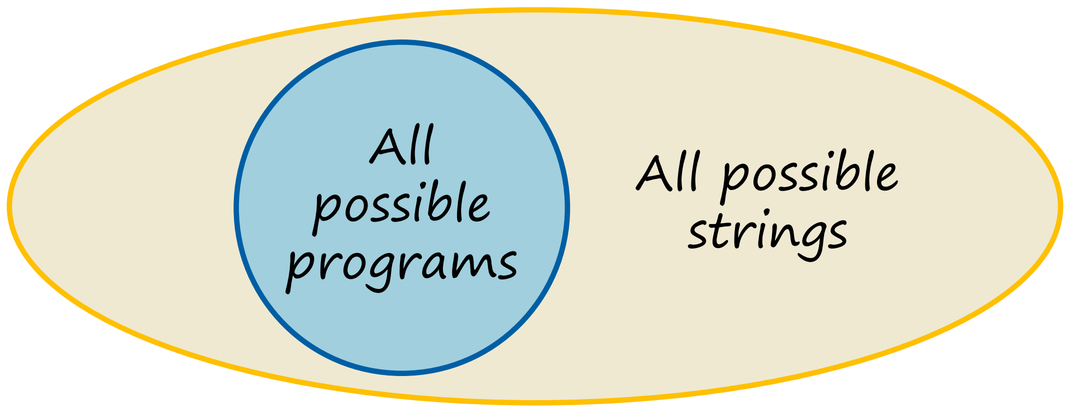
Size of "The set of all problems to solve"

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.

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|

Strings and Problems

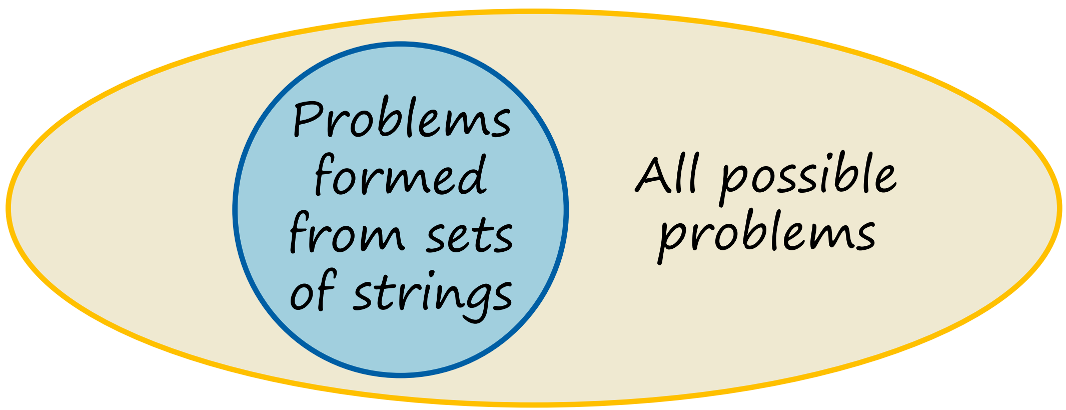
- There is a connection between the number of sets of strings and the number of problems to solve.
- Let S be any set of strings. This set S gives rise to a problem to solve:

Give a string $\boldsymbol{w}$, determine wether $\boldsymbol{w} \in \boldsymbol{S}$.

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:

Give a string w, determine wether $w \in S$.



|Set of Strings| ≤ |Problems|

Where We’re Going

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

Where We're Going

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

|Programs| ≤ |Strings|

Where We're Going

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

|Programs| ≤ |Strings|

|Set of strings| ≤ |Problems|

Where We're Going

- A string is a sequence of characters.
  - There are at most as many programs as there are strings.
  - There are at least as many problems as there are sets of strings.
- **From Cantor's Theorem, we know that there are more sets of strings than strings**

|Programs| ≤ |Strings| < |Set of strings| ≤ |Problems|

|Programs|<|Problems|!!!

Frustrating Result

- There are more problems to solve than there are programs to solve them.
  - **Some problems can not be solved by programs**
- 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.☹

Size of "The set of all computer programs"

is strictly smaller than

Size of "The set of all problems to solve"

Next

Capture the structure of a problem.

- Binary relations.

Other fundamental tools.

- Functions