

## Theorem

For any set  $A$ ,  $\nexists f: A \xrightarrow{\text{onto}} \mathcal{P}(A)$ .

### Proof

Let  $f: A \xrightarrow{\text{onto}} \mathcal{P}(A)$ , where  $A$  is arbitrary.

Then consider the set

$$S = \{ i \in A \mid i \notin f(i) \}$$

Then note that for any  $j \in \mathbb{N}$ ,  $j \in S \Rightarrow j \notin f(j)$

and  $j \notin S \Rightarrow j \in f(j)$ . Hence,  $S$  cannot be  $f(j)$ .

Since this holds for all  $j \in S$ , we conclude that  $S \notin \text{range}(f)$ .  $\square$

e.g. When  $A = \mathbb{N}$

let  $f: \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N})$ .

For any subset  $B \subseteq \mathbb{N}$ ,

represent it as a "bitmap"

$i^{\text{th}}$  bit is 1 if  $i \in B$

0 o/w.

e.g.  $B = \{2, 3, 4\}$

|   |   |   |   |   |   |   |     |
|---|---|---|---|---|---|---|-----|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | ... |
| 0 | 0 | 1 | 1 | 1 | 0 | 0 | ... |

Suppose  $f: \mathbb{N} \xrightarrow{\text{onto}} \mathcal{P}(\mathbb{N})$

|        |                                                               |                                                               |                                                               |   |   |     |   |     |
|--------|---------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------|---|---|-----|---|-----|
| $f(0)$ | <span style="border: 1px solid black; padding: 2px;">0</span> | 1                                                             | 1                                                             | 1 | 0 | 0   | 0 | ... |
| $f(1)$ | 0                                                             | <span style="border: 1px solid black; padding: 2px;">1</span> | 0                                                             | 1 | 0 | ... |   |     |
| $f(2)$ | 1                                                             | 0                                                             | <span style="border: 1px solid black; padding: 2px;">0</span> | 1 | 0 | ... |   |     |

Consider the set  $\{0, 2, \dots\}$

i.e.  $i$  is in the above set iff  $i$  is not in  $f(i)$  - i.e.  $i^{\text{th}}$  bit is 0 in  $f(i)$ .

$|P(\mathbb{R})|$

$|P(\mathbb{N})| \neq |\mathbb{R}|$

$|\mathbb{N}|$

What about

$P \neq NP$ ?

Unfortunately,

Baker, Gill, Solovay '75:

$\exists A \subseteq \mathbb{N}$  such that

$\exists B \subseteq \mathbb{N}$

such that

$P^A \neq NP^A$

$P^B = NP^B$ .

# Turing Computability

A Turing Machine  $M$  is a 7 tuple  $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$

where

$Q$  : finite set of states

$\Sigma$  : finite set of letters. (input alphabet)

$\Gamma \supsetneq \Sigma$  : finite set of letters, containing  $B \notin \Sigma$ , (tape alphabet)

$\delta: \Gamma \times Q \xrightarrow{\{q_a, q_r\}} \Gamma^* \times Q \times \{L, R\}$

$q_0 \in Q$  : initial state

$q_a \in Q$  : accept state

$q_r \in Q$  : reject state.

A language  $L$  is a set of strings.

$$L \subseteq \{0,1\}^*$$

$L$  is <sup>(Turing)</sup>acceptable if  $\exists$  Turing Machine  $M$  such that  $\forall x \in L$   $M(x)$  enters

$q_a$  & halts,  $\forall x \notin L$ ,  $M(x)$  does not enter  $q_a$ .

$L$  is decidable if  $L$ , and  $\{0,1\}^* \setminus L$  are acceptable.