$\# \text{ functions } \underset{}{\overset{f:\{0,1\}^n \to \{0,1\}}{}} \gg \# \text{ circuits of size } 2^n/3n$

$\# \text{ functions } \overset{f:\{0,1\}^* \to \{0,1\}}{} \gg \# \text{ Turing machines}$

(not - countable) (countable)

$\mathbb{N}$: $\{1, 2, 3, \dots\}$ natural

$\mathbb{Z}$: $\{0, \pm 1, \pm 2, \dots\}$ integers $\mathbb{Z} \times \mathbb{Z}$

$\mathbb{Q}$: $\{p/q : p, q \in \mathbb{Z}\}$ rationals $2^{\mathbb{N}} = \{A : A \subseteq \mathbb{N}\}$

$\mathbb{R}$ reals

Def: $\phi : D \to R$ is surjective if $\forall\, y \in R$, $\exists\, x \in D$ s.t. $\phi(x) = y$.

Def: S is countable if $\exists\, \phi : \mathbb{N} \to S$ with ϕ surjective.

$\phi(1), \phi(2), \phi(3), \dots$

S is countable if every $y \in S$ occurs in this list.

$2^{\mathbb{N}} = \{A : A \subseteq \mathbb{N}\}$

Thm: $2^{\mathbb{N}}$ is not countable.

Pf:

	1	2	3	4	5	...
A_1	0	1	0	0	1	
A_2	1	1	1	1	1	
A_3	0	0	0	1	0	
$\vdots$				1		
T	1	0	1	0		

Diagonalization

$T = \{i : i \notin A_i\}$

$T \neq A_j$ since

if $j \in A_j$, $j \notin T$

if $j \notin A_j$, $j \in T$.

Thm: The set of functions $f : \{0,1\}^* \to \{0,1\}$ is not countable.

	x_1	x_2	x_3 ← all elements of $\{0,1\}^*$
f_1	$f_1(x_1)$	$f_1(x_2)$	$\cdots$
f_2	$\vdots$	$f_2(x_2)$	
f_3			
f	$1-f_1(x_1)$	$1-f_2(x_2)$	$\cdots$

Thm 8. There is a function that cannot be computed by a Turing machine.

Pf: Given program α, write M_α to denote the corresponding machine

$$f(\alpha) = \begin{cases} 1 & \text{if } M_\alpha(\alpha) = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Suppose f is computed by M_γ.

Then $M_\gamma(\gamma) \neq f(\gamma)$ by the choice of f.

$$\text{HALT}(\alpha, x) = \begin{cases} 1 & \text{if } M_\alpha(x) \text{ halts} \\ 0 & \text{otherwise.} \end{cases}$$

Thm: HALT cannot be computed by a Turing machine.

Pf: Suppose HALT can be computed.

$\underline{M(\alpha)}$

1. Run $\text{HALT}(\alpha,\alpha)$.
2. If $\text{HALT}(\alpha,\alpha) = 1$, run $M_\alpha(\alpha)$, if $M_\alpha(\alpha) = 0$, output 1. Else output 0.

$M(\alpha) = f(\alpha) \implies$ HALT is not computable.

Thm: There is a Turing machine M, s.t. given code α and input x if $M_\alpha(x)$ halts in T steps, then $M(\alpha, x)$ halts in $O(C\,T \log T)$ steps with output $M_\alpha(x)$.
Here C depends only on α.

X ——————— Y

Gödel's Incompleteness Theorem

" There is a truth that cannot be proved."

1111111111111111111111
0101010101010101010101
0101110100000011111001

$K(x)$ = length of shortest program that outputs x.

$$S_{x,N} : \quad K(x) > N$$

FACT: $\forall N$, there is an x s.t. $S_{x,N}$ is true.

Pf: # choices for x is infinite.

Proof system

machine M s.t. $M(\overset{\text{theorem}}{\tau}, \overset{\text{proof}}{\pi}) = 1$ only if τ is true.

Thm: $\exists\ x, N$ s.t.
- $S_{x,N}$ is true
- $\forall\ \pi \quad M(S_{x,N}, \pi) \neq 1$.

Pf: $\underline{M_N}$

- Enumerate all pairs (x, π) length $O(\log N)$
  if $M(S_{x,N}, \pi) = 1$ output x.

If $S_{x,N}$ has a proof whenever its true,

M_N will output x s.t $S_{x,N}$ holds.

Contradiction.