

P V

PPTs

probabilistic polynomial algorithm

$C \{0,1\}^*$ → Kleene star

$$\{1\}^* := \bigcup_{n \geq 0} \{0,1\}^n$$

$L_1 = \{\text{odd parity strings}\}$
 $x \in \{0,1\}^+$ decide if $x \in L$

A: counts the 1's.

$P \neq NP$

P is the set of languages s.t.
 $\exists \text{PPT } A: \forall x \in \{0,1\}^*: A \text{ can tell if } x \in L.$

NP " " " " " $\exists \text{PPT } A:$

$A(x,y)$



y is a witness

P V

PPTs

probabilistic polynomial algorithm

$L \subset \{0,1\}^*$ → Kleene star

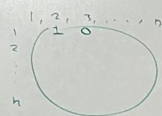
$\{0,1\}^* := \bigcup_{n \geq 0} \{0,1\}^n$

$L = \{\text{odd parity strings}\}$
 $x \in \{0,1\}^+$ decide if $x \in L$

A: counts the 1's.

$$E \in \binom{V}{2}$$

$$G = (V, E)$$



P's goal:
 $x \in L$

$$P \neq NP$$

P is the set of languages s.t.
 $\exists \text{PT } A: \forall x \in \{0,1\}^*: A \text{ can tell if } x \in L.$

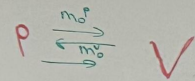
y is a witness

NP " " " " " $\exists \text{PPT } A: \exists y \in \{0,1\}^*:$
 $\rightarrow A(x,y) = 1 \text{ iff } x \in L.$ |y| is polynomial

13472



general guide
- a writing of abstract to cover
- a 1-2 page summary
- a 1-2 page abstract
- a 1-2 page introduction
- a 1-2 page conclusion
- a 1-2 page references
- a 1-2 page appendix

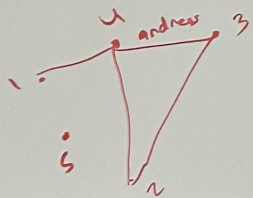
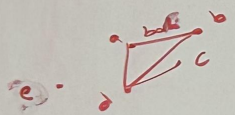


REJECT
or
ACCEPT

Graph Isomorphism Problem

$$G_1 = (V_1, E_1) \quad G_2 = (V_2, E_2)$$

$$G_1 \simeq G_2$$



$$\sigma: G_1 \rightarrow G_2$$

s.t.

$$(u, v) \in E_1 \text{ iff } (\sigma(u), \sigma(v)) \in E_2.$$

σ bijective.

①

Suppose
Then, P can only send

$$\sigma \pi(G_1)$$

$$\pi(G_2)$$

$$\begin{matrix} \tau(G_1) \\ \tau(G_2) \\ \pi(G_1) \end{matrix}$$

b=2

sample
 $b \in \{1, 2\}$

$$\begin{matrix} \text{if } b=1, \pi \\ \text{if } b=2, \sigma \pi^{-1} \end{matrix}$$

$$G'$$

① (completeness) If $x \in L$, P has a correct witness w , and (P,V) play honestly, V should ACCEPT.

② (soundness) If $x \notin L$, for any prover P, V will reject with probability at least $1/2$.

③ (zero knowledge)

Commitment Scheme

Natul is cool
 m_1

① Commit
② Decommit