P V

PPTs

probabilistic polynomial algorithm

$\in \{0,1\}^* \rightarrow$ Kleene star

$\{0,1\}^* := \bigcup_{n \in \mathbb{N}} \{0,1\}^n$

ex $L := \{$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.

$\exists$ PPT A: $\forall x \in \{0,1\}^*$: A can tell if $x \in L$.

y is a witness

NP " " " " " $\exists$ PPT A:

A(x,y)

P V

PPTs

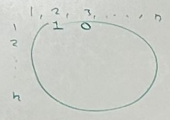
probabilistic polynomial algorithm

$L \subset \{0,1\}^*$ → Kleene star

$\{0,1\}^* := \bigcup_{n \in \mathbb{N}} \{0,1\}^n$

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

$G = (V, E)$



n^2

ex $L_1 := \{$ odd parity strings $\}$

$x \in \{0,1\}^+$ decide if $x \in L$

A: counts the 1's.

P's goal:

$x \in L$

13472

$P \neq NP$

P is the set of languages s.t.

$\exists$ PPT A: $\forall x \in \{0,1\}^*$: A can tell if $x \in L$.

y is a witness

$\exists$ PPT A: $\exists y \in \{0,1\}^*$:

NP " " " " "

$|y|$ is polynomial

$A(x,y) = 1$ iff $x \in L$.

13 7


P
V
REJECT
or ACCEPT
Graph Isomorphism Problem
$G_1 = (V_1, E_1)$
$G_2 = (V_2, E_2)$
$G_1 \simeq G_2$
$\sigma : G_1 \to G_2$
σ bijective.
s.t.
$(u,v) \in E_1$ iff $(\sigma(u), \sigma(v)) \in E_2$.
Suppose
Then, P can only send
$\sigma\pi(G_1)$
$\pi(G_2)$
G_1
G_2
$\pi(G_1)$
sample $b \in \{1,2\}$
if $b=1$, π
if $b=2$, $\sigma\circ\pi^{-1}$
σ'
(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
with probability at
(3) (zero knowledge)
Commitment Scheme
Natal is cool
m_1
(1) Commit
(2) Decommit
address