

**Proposition:** If  $\Pi_k^P \in \Sigma_k^P$  then  $PH = \Sigma_k^P$ .

Similarly, if  $\Sigma_k^P \in \Pi_k^P$  then  $PH = \Pi_k^P$ .

**Theorem (Karp-Lipton):**  $NP \in P/poly \Rightarrow PH = \Sigma_2^P$ .

**Proof:** By above proposition, enough to prove that

$$NP \in P/poly \Rightarrow \Pi_2^P \in \Sigma_2^P.$$

In particular, suffices to show  $\Pi_2 SAT \in \Sigma_2^P$

$$\Pi_2 SAT := \left\{ \langle \phi \rangle \text{ 3CNF} \mid \forall u \in \{0,1\}^n \exists v \in \{0,1\}^n \text{ s.t. } \phi(u,v) = 1 \right\}$$

inputs  $\{0,1\}^{2n}$

$NP \in P/poly \Rightarrow \exists c \in \mathbb{N}$  and a circuit family  $C := \{C_n\}_{n \geq 0}$  in  $SIZE(n^c)$  s.t. for every 3CNF  $\phi$  and  $u \in \{0,1\}^n$   $C_n(\phi, u) = 1$  iff  $\exists v \in \{0,1\}^n$  s.t.  $\phi(u,v) = 1$ .

From the family  $C$ , we can construct <sup>multi-output</sup> circuit family  $\Gamma := \{\Gamma_n\}_{n \geq 0}$  in  $SIZE(n^{2c})$  s.t.  $\Gamma_n(\phi, u)$  outputs a satisfying assignment  $v$  in case one exists.

Note that  $NP \in P/poly$  simply guarantees the existence of  $\Gamma$

... can use the  $\exists$  quantifier

Note that  $NP \subseteq P_{poly}$  simply guarantees the existence of  $\Gamma$  in  $SIZE(n^{2c})$ . However we can use the  $\exists$  quantifier in  $\Sigma_2^P$  to "guess"  $\Gamma$  as follows:

Let  $\gamma \in \mathbb{N}$  be s.t.  $s_{\Gamma}(n) \leq \gamma \cdot n^{2c} \quad \forall n \in \mathbb{N}$ .

Then, consider the following language in  $\Sigma_2^P$ :

$$L := \left\{ \left\langle \phi \right\rangle_{\substack{3CNF \\ m \\ 2n \text{ inputs}}} \mid \exists w \in \{0,1\}^{\gamma n^{2c}} \forall u \in \{0,1\}^n \text{ } w \text{ encodes a circuit } \tilde{c} \text{ and } \phi(u, \tilde{c}(\phi, u)) = 1 \right\}$$

Note that  $\phi \in \Pi_2SAT \Rightarrow \phi \in L$ , as we can take  $w = \Gamma_n$  and  $\Gamma_n(\phi, u)$  always outputs a satisfying assignment to  $\phi(u, -)$ .

Now, if  $\phi \notin \Pi_2SAT$  then  $\exists u \in \{0,1\}^n$  s.t. no  $v \in \{0,1\}^n$  satisfies  $\phi(u, -) \Rightarrow \phi \notin L$ .

$$\therefore \Pi_2SAT \leq_P L \Rightarrow \Pi_2^P = \Sigma_2^P. \quad \square$$