Theorem(Karp-Lipton-Sipser): *If NP $\subseteq$ P/poly then PH $= \Sigma_2^p$.*

Note that if NP $\subseteq$ P/*poly* then SAT has a polynomial-size circuit family. Namely, for some $c > 0$ there is a sequence of circuits $W_1, W_2, W_3, \ldots$, where W_n is a circuit of size n^k that decides satisfiability of all boolean formulae whose encoding size is $\leq n$. Of course, NP $\subseteq$ P/*poly* merely implies the *existence* of such a family; there may be no easy way to construct the circuits.

Lemma (Self-reducibility of SAT) There is a polynomial-time computable function h such that if $\{W_n\}_{n\geq 1}$ is a circuit family that solves SAT, then for all boolean formulae φ:

$$\varphi \in SAT \qquad \textit{iff} \qquad h(\varphi, W_{|\varphi|}) \textit{ is a satisfying assignment for } \varphi. \tag{1}$$

Proof: The main idea is to use the circuit to generate a satisfying assignment as follows. Ask the circuit if φ is satisfiable. If so, ask it if $\varphi(x_1 = T)$ (i.e., φ with the first variable assigned True) is satisfiable. The circuit's answer allows us to reduce the size of the formula. If the circuit says no, we can conclude that $\varphi(x_1 = F)$ is true, and have thus reduced the number of variables by 1. If the circuit says yes, we can substitute $x_1 = T$ and again reduced the number of variables by 1. Continuing this way, we can generate a satisfying assignment. This proves the Lemma. (Aside: The formal name for the above property of SAT is *downward self-reducibility*. All NP-complete languages have this property.) QED

Now we prove the Theorem. We show NP $\subseteq$ P/*poly* implies $\Pi_2^p \subseteq \Sigma_2^p$.

Let $L \in \Pi_2^p$. Then there is a language $L_1 \in$ NP and $c > 0$ such that

$$L = \left\{x \in \{0,1\}^* : \forall\ y, |y| \leq |x|^c, (x,y) \in L_1\right\}. \tag{2}$$

Since $L_1 \in NP$, there is a polynomial-time reduction, say g, from L_1 to SAT. Thus

$$\forall\ z \in \{0,1\}^* : z \in L_1 \qquad \text{iff} \qquad g(z) \in \text{SAT}.$$

Suppose further that $d > 0$ is such that $|g(z)| \leq |z|^d$.

Now we can rewrite (2) as

$$L = \left\{x \in \{0,1\}^* : \forall\ y, |y| \leq |x|_1^c, g(x,y) \in \text{SAT}\right\}.$$

Note that $|g(x,y)| \leq (|x| + |y|)^d$. Let us simplify this as $|x|^{cd}$. Thus if $W_{n\geq 1}$ is a n^k-sized circuit family for SAT, then by (1) we have

$$L = \left\{x : \forall\ y, |y| \leq |x|_1^c, h(g(x,y), W_{|x|^{cd}}) \text{ is a satisfying assignment for } g(x,y)\right\}.$$

Now we are almost done. Even though there may be no way for us to construct the circuit for SAT, we can just try to "guess" it. Namely, an input x is in L iff

$$\exists W, \text{ a circuit with } |x|^{cd} \text{ inputs and size } |x|^{cdk} \text{ such that}$$
$$\forall\ y, |y| \leq |x|_1^c, h(g(x,y), W) \text{ is a satisfying assignment for } g(x,y).$$

Since h is computable in polynomial time , we have thus shown $L \in \Sigma_2^p$. QED