Circuit Size for a Function

• Theorem: ∃ a Boolean function on n bits (in fact, most such functions) that requires circuit size $\Omega(2^{n/n})$.

• Proof: By counting. The # of functions $f: \{0,1\}^n \rightarrow \{0,1\}$ is $2^{2^n}$.

• The # of circuits with size $T$ is at most $(3T^2)^T$.

• We need $(3T^2)^T \geq 2^{2^n}$. Thus $T=\Omega(2^{n/n})$. 
Circuit Size for a Function

• Theorem: ∃ a Boolean function on n bits (in fact, most such functions) that requires circuit size $\Omega(2^n/n)$.

• Was a possible approach to prove $P \neq NP$, if one can show a language in NP that requires super-polynomial circuit size.

• However, the best known circuit lower bound for an explicit function/language is only about $3n$.

• Still very far from proving $P \neq NP$. 
Non-Uniform Size Hierarchy Theorem

• Intuition: a circuit family of larger size should be able to compute more functions.

• Theorem: \( \forall \) functions \( T, T': N\rightarrow N \) with \( n < T(n) < T'(n) < 2^n/(100 \ n) \) and \( T(n) \log^2 T(n)=o(T'(n)) \), we have \( \text{SIZE}(T(n)) \subset \text{SIZE}(T'(n)) \).

• Proof: let \( l = \log T(n) + \log \log T(n) + C \) for a large enough constant \( C>1 \).

• By counting, \( \exists \) a function \( f:\{0,1\}^l\rightarrow\{0,1\} \) that requires circuit size \( \Omega(2^l/l) > T(n) \), so \( f \notin \text{SIZE}(T(n)) \).
Non-Uniform Size Hierarchy Theorem

• \( l = \log T(n) + \log \log T(n) + C \) and \( f: \{0,1\}^l \rightarrow \{0,1\} \).

• \( f \notin \text{SIZE}(T(n)) \).

• On the other hand, \( f \) can be computed by a circuit of size \( l2^l = O(T(n) \log^2 T(n)) = o(T'(n)) \).

• So \( f \in \text{SIZE}(T'(n)) \).
Circuit Size of SAT

• SAT is NP-complete.

• Does SAT have poly-size circuit family?

• SAT ∈ $P/_{poly}$? Equivalently, NP ⊆ $P/_{poly}$?

• Theorem (Karp-Lipton’ 80) If NP ⊆ $P/_{poly}$, then $PH=\Sigma_2^p$. 
**Karp-Lipton Theorem**

- **Theorem (Karp-Lipton’ 80)** If $\text{NP} \subseteq P/\text{poly}$, then $\text{PH}=\Sigma_2^p$.

- **Proof:** show that $\text{NP} \subseteq P/\text{poly} \Rightarrow \Pi_2 \text{SAT} \in \Sigma_2^p \Rightarrow \Pi_2^p \subseteq \Sigma_2^p \Rightarrow \text{PH}=\Sigma_2^p$.

- $\Pi_2 \text{SAT}=$\{all QBFs of the form $\forall u \exists v \Phi(u, v)$ that are true\}. 

Karp-Lipton Theorem

• $\Pi_2 \text{SAT}=$\{all QBFs of the form $\forall u \exists v \Phi(u, v)$ that are true\}.

• To show $\Pi_2 \text{SAT} \in \Sigma_2^p$ means, to show $\exists$ a polynomial time TM $M$ and a polynomial function $q$ s.t. $\forall$ QBF $\psi = \forall u \exists v \Phi(u, v)$

  $\psi$ is true iff $\exists u' \in \{0, 1\}^{q(|x|)} \forall v' \in \{0, 1\}^{q(|x|)} M(\psi, u', v') = 1$

• The language $L=$\{$<\Phi, u>$: $\exists v \Phi(u, v)=1$\} $\in \text{NP}$.
Karp-Lipton Theorem

• The language $L = \{ <\Phi, u> : \exists v \Phi(u, v) = 1 \} \in NP$.

• Since $NP \subseteq P/poly$, there is a poly size circuit family \{C_n\} deciding $L$, i.e., $\forall <\Phi, u>$,  
\[ \exists v \Phi(u, v) = 1 \iff C_n(\Phi, u) = 1 \]

• Using search to decision reduction, there is another poly size circuit family \{C'_n\} that outputs such a $v$. That is, $\forall <\Phi, u>$,  
\[ \exists v \Phi(u, v) = 1 \iff C'_n(\Phi, u) = v \text{ and } \Phi(u, v) = 1 \]
Karp-Lipton Theorem

- Using search to decision reduction, there is another poly size circuit family \{C'_n\} that outputs such a \(v\). That is, \(\forall <\Phi, u>,\)

\[
\exists v \Phi(u, v) = 1 \iff C'_n(\Phi, u) = v \text{ and } \Phi(u, v) = 1
\]

- Note that \{C'_n\} does not depend on \(\Phi, u, v\). We don’t know what \{C'_n\} is, but we know it exists.

- Let \(w\) be the description of \(C'_n\) which has poly size.

- So, \(\psi\) is true \(\iff \forall u \exists v \Phi(u, v) = 1 \iff \exists w\) that describes \(C'_n \forall u \Phi(u, C'_n(\Phi, u)) = 1\).
Karp-Lipton Theorem

• $\psi$ is true iff $\forall u \exists v \Phi(u, v)=1$ iff $\exists w$ that describes $C'_n \forall u \Phi(u, C'_n(\Phi, u))=1$.

• Note that $\Phi$ is part of $\psi$, so this also implies $\psi$ is true iff $\exists w \forall u M'(\psi, w, u)=1$.

• $M'$ is a poly time TM that computes $\Phi(u, C'_n(\Phi, u))$ based on $w, \psi, u$.

• Therefore, $\Pi_2 \text{SAT} \in \Sigma_2^p$. 


Karp-Lipton Theorem

• What does this mean?

• If PH does not collapse to $\Sigma_2^p$, then NP (in particular, SAT) does not have poly size circuits.

• Is this an evidence for $P \neq NP$ (since $P \subseteq P/poly$)?

• NO! Because the assumption that PH $\neq \Sigma_2^p$ is already stronger than $P \neq NP$. 
Depth of Circuits

• The depth of a circuit is related to the ability to compute the function in parallel.

• Definition: a function is said to have efficient parallel algorithms if inputs of size $n$ can be solved using a parallel computer with $\text{poly}(n)$ processors and in time $\text{poly} \log(n)$.

• Corresponds to uniform circuits of size $\text{poly}(n)$ and depth $\text{poly} \log(n)$ (each gate can be viewed as a processor).
Depth of Circuits

• Definition: A language is in the class $\text{NC}^i$ if $\exists$ a constant $c>0$ s.t. it can be decided by a log space uniform family of circuits of size $O(n^c)$ and depth $O(\log^i n)$.

• Definition: A language is in the class $\text{AC}^i$ if $\exists$ a constant $c>0$ s.t. it can be decided by a log space uniform family of circuits of size $O(n^c)$ and depth $O(\log^i n)$, where the AND/OR gate can have unbounded fan-in.

• Definition: $\text{NC}= \bigcup_{i=1}^\infty \text{NC}^i$. $\text{AC}= \bigcup_{i=1}^\infty \text{AC}^i$. 
Depth of Circuits

• Relation between NC and AC classes.

• For any $i \geq 0$, $NC^i \subseteq AC^i \subseteq NC^{i+1}$.

• We know $NC^0 \subset AC^0 \subset NC^1$ but do not know if the other relations are proper subsets.