FGC Lecture 11

Theorem 0.1. If Circuit-SAT $\in \mathsf{P}$, then EXP has hard functions ($\text{Size}(f) \geq 2^n/n$).

Proof. If Circuit-SAT(which is NP-complete) is in P, then PH collapses to P. Therefore EH collapses to EXP. Then $\mathsf{EXP} = \Sigma_3^{\mathsf{EXP}}$, which contains hard problems (by Kannan's Theorem). $\square$

Theorem 0.2. If Circuit-SAT $\in \mathsf{TIME}[2^{n^{o(1)}}]$, then $\mathsf{NEXP} \not\subseteq \mathsf{P/poly}$.

Proof. If $\mathsf{EXP} \not\subseteq \mathsf{P/poly}$, then we've done.

If $\mathsf{EXP} \subseteq \mathsf{P/poly}$, by Meyer's Theorem, $\mathsf{EXP} = \Sigma_2^{\mathsf{P}}$.

For $L \in \mathsf{EXP}$, $x \in L \Leftrightarrow \exists y_1 \forall y_2 R(x, y_1, y_2)$.

By assumption, $\exists y_1 \forall y_2 R(x, y_1, y_2)$ is in time $2^{n^{o(1)}}$. So $L \in \mathsf{NTIME}[2^{n^{o(1)}}]$. So $\Sigma_3^{\mathsf{P}} \subseteq \mathsf{EXP} \subseteq \mathsf{NTIME}[2^{n^{o(1)}}]$.

Scaling up, $\exists T(n) = n^{\omega(1)}$, s.t. $\Sigma_3^{T(n)} \subseteq \mathsf{NEXP}$.

$\Sigma_3^{T(n)} \not\subseteq \mathsf{P/poly}$, thus $\mathsf{NEXP} \not\subseteq \mathsf{P/poly}$. $\square$

❧ ❧ ❧

Theorem 0.3 (Williams)**.** If Circuit-SAT $\in \mathsf{TIME}[|C| \cdot 2^n/n^{\omega(1)}]$, then $\mathsf{NEXP} \not\subseteq \mathsf{P/poly}$.

We prove the nondeterministic version of this theorem: If Circuit-TAUT $\in \mathsf{NTIME}[|C| \cdot 2^n/n^{\omega(1)}]$, then $\mathsf{NEXP} \not\subseteq \mathsf{P/poly}$.

Proof. Assume $\mathsf{NEXP} \subseteq \mathsf{P/poly}$, and Circuit-TAUT $\in \mathsf{NTIME}[|C| \cdot 2^n/n^{\omega(1)}]$.

Let $L \in \mathsf{NTIME}[2^n]$. We are going to save time in solving L, thus contradicting the nondeterministic time hierarchy theorem.

$x \in L \Leftrightarrow \exists y, |y| = 2^n, R(x, y)$. R is computable in time 2^n.

Let C_R be a locally computable circuit that computes R. By Fischer-Pippenger's Theorem, $|C_R| = O(2^n \cdot n)$. Then,

$x \in L \iff \exists(y, g_1, \dots, g_{2^n \cdot n})$, each gate is correct from its inputs, and output is 1.

This new relation has succinct witness if $x \in L$:

$x \in L \iff \exists C'' \forall i, [(op_i(C''(x, j(i)), C''(x, k(i))) = C''(x, i)) \wedge (C''(x, \text{output}) = \text{True})]$

Circuit C'' is a succinct witness.

Let $T_{C''}(i)$ be the problem to check C'' on i. Then

$x \in L \iff \exists C'', T_{C''}(i)$ is a tautology.

By assumption, "$T_{C''}(i)$ is a tautology" is in $\mathsf{NTIME}[2^{n'}/n'^{\omega(1)}]$, where $n' = n + \log n$, equals $\mathsf{NTIME}[2^n/n^{\omega(1)}]$.

So $L \in \mathsf{NTIME}[2^n/n^{\omega(1)}]$. Thus $\mathsf{NTIME}[2^n] \subseteq \mathsf{NTIME}[2^n/n^{\omega(1)}]$, contradicting Time Hierarchy Theorem. $\square$

❧ ❧ ❧

Theorem 0.4 (Williams). $\forall$ depth d, $\exists \epsilon$, s.t. ACC_6-SAT $\in \mathsf{TIME}[2^{n-n^\epsilon}]$.

Lemma 0.5. If $\mathscr{C}$ is a class of circuits so that $\mathscr{C}$-TAUT $\in \mathsf{NTIME}[2^n/n^{\omega(1)}]$ and $\mathsf{P} \subseteq \mathscr{C}$, then Circuit-TAUT $\in \mathsf{NTIME}[2^n/n^{\omega(1)}]$.

If we have a circuit class $\mathscr{C}$ so that $\mathsf{P} \subseteq \mathscr{C}$, then it's not so easy, so it's good.

If $\mathsf{P} \nsubseteq \mathscr{C}$, then the result for Circuit-TAUT applies to $\mathscr{C}$-TAUT.

Corollary. If $\mathscr{C}$-TAUT $\in \mathsf{NTIME}[2^n/n^{\omega(1)}]$, then $\mathsf{NEXP} \nsubseteq \mathscr{C}$.

Corollary. $\mathsf{NEXP} \nsubseteq \mathsf{ACC}_6$.

Proof of Lemma 0.5. If $\mathsf{P} \subseteq \mathscr{C}$, then $\mathsf{P/poly} \subseteq \mathscr{C}$.

Let D be an instance of Circuit-TAUT, and let $g_1, \dots, g_m$ be its gates. Each g_i defines a subcircuit of D, i.e. for each g_i, $\exists C_i \in \mathscr{C}$ s.t. $\forall x, g_i(x) = C_i(x)$.

Our algorithm first non-deterministically guesses each C_i for $i = 1, \dots, m$. Then, it verifies

$$\forall x, \left[C_i(x) = op_i(C_{j(i)}(x), C_{k(i)}(x))\right]$$

Because C_i, $C_{j(i)}$ and $C_{k(i)}$ are all in $\mathscr{C}$ ($\mathscr{C}$ is closed), the verification can be done by $\mathscr{C}$-TAUT.

We do the verification once per gate i, thus it is polynomial in input size.

Finally we verify $C_{\text{output}}(x)$ is tautology. $\square$