Math 268 2012-11-06

BFNW 93

NW. If EXPTIME cannot be approximated by poly size circuits, BPP admits weakly subexp simulations.

The goal is to weaken the hypothesis.

BFNW EXPTIME $\not\subseteq$ P/POLY $\Rightarrow$ BPP admits weakly subexp time simulation.

A little clarification: $\Sigma = \{0,1\}$ $L \subseteq \Sigma^*$

Def A machine M weakly computes L if, for infinitely many n, $L \cap \Sigma^n = L(M) \cap \Sigma^n$.

Def L admits a weakly subexp time simulation if $\forall \varepsilon > 0$ $\exists$ a 2^{n^ε} time bound machine M s.t. M weakly computes L.

Def ~~Rmk Explicitly, EXPTIME cannot be simulated approximated.~~

Let $f : \Sigma^* \to \Sigma$. f cannot be approximated by poly size circuits if $\forall k$ $\forall n^k$-size circuit families $\{c_n\}$ $\Pr_{x \in \{0,1\}^n}(C_n(x) \neq f_n(x)) > 1/2 - 1/n^k$ for infinitely many n

Pf of BFNW. We go by contraposition.

Suppose BPP does not admit weakly subexp time simulation. We'll show EXPTIME $\subseteq$ P/POLY.

Let L be an EXPTIME-complete language, $L = \{f_n\}$ boolean functions. Take p prime $p > n$. $g_n : \mathbb{Z}_p^n \to \mathbb{Z}_p$ unique multilinear extensions of f_n. We want to make ~~circuits~~ a poly-size circuit family $\{c_n\}$ that computes (polysize) g_n s.t. $\Pr_{x \in \mathbb{Z}_p^n}(g_n(x) \neq c_n(x)) \le \frac{1}{3n}$ (I). We'll then (II) construct $\{D_n\}$ from $\{c_n\}$ to compute g_n with very high certainty.

Step II. Input $x = (x_1, \cdots, x_n) \in \mathbb{Z}_p^n$. Let $a \in \mathbb{Z}_p^n$. Consider $g_n(at+x) = g(t)$, with degree $\le n$. We can interpolate $g(t)$ if we can find $n+1$ distinct points.

Interpolation algorithm:

Select $t_1, \dots, t_{n+1} \neq 0 \in \mathbb{Z}_p$ at random.

Compute $c_n(a t_i + x) =? g(t_i)$.

This gives a probabilistic circuit, with probability of incorrectness at most $(n+1)\left(\frac{1}{3n}\right) = \frac{n+1}{3n} \le 2/5$

By repeating computation, we can take the majority of answers and make probability of incorrectness as small as we like.

__Step I__. We assume BPP does not admit weakly subexp simulation, and WTS $\exists$ ckts that approximate g_n.

Again contraposition. Suppose $\forall k$ $\forall n^k$-size $\{C_n\}$ for infinitely many n $\Pr_{x \in \mathbb{Z}_p^n} (g_n(x) \neq C_n(x)) \geq \frac{1}{3n}$.

__XOR Lemma__ Let $G : \{0,1\}^n \to \{0,1\}$. Define $H : \{0,1\}^{nk} \to \{0,1\}$ $H(x_{11}, \ldots, x_{1n}, x_{21}, \ldots, x_{2n}, \ldots, x_{k1}, \ldots, x_{kn}) = G(x_{11}, \ldots, x_{1n}) \oplus \cdots \oplus G(x_{k1}, \ldots, x_{kn})$. If $\exists$ C ckt that computes H with probability $\geq \frac{1}{2} + \frac{1}{2}(1-\varepsilon)^k + \delta$, then $\exists$ C_2 ckt of size approximately $\text{size}(C_1)/\delta$, that computes G w/ prob $> 1-\varepsilon$