Math 268
BFNW 93

19. If EXP\textsc{time} cannot be approximated by poly size circuits, BPP admits weakly subexp simulation.

The goal is to weaken the hypothesis.

BFNW EXP\textsc{time} \nsubseteq P/\textsc{poly} \implies BPP admits weakly subexp time simulation.

A little clarification: \( \Sigma^* \equiv \{0,1\}^* \)

**Def.** Let machine \( M \) weakly compute \( L \) if, for infinitely many \( n \), \( L \cap \Sigma^n = L(M) \cap \Sigma^n \).

**Def.** Let \( L \) admit a weakly subexp time simulation if \( \forall e \geq 0 \exists 2^{en^2} \) time bound machine \( M \) s.t. \( M \) weakly computes \( L \).

**Claim.** Explicitly, EXP\textsc{time} cannot be simulated approximately.

Let \( f: \Sigma^n \rightarrow \Sigma. \) \( f \) cannot be approximated by poly size circuits if \( \forall k \forall n \) size circuit families \( \{f_n\} \) \( \exists \epsilon > 0 \) \( \sum_{n \geq 1} 2^{-k/\epsilon} \) of BFNW. We go by contraposition.

Suppose BPP does not admit weakly subexp time simulation. We'll show EXP\textsc{time} \nsubseteq P/\textsc{poly}.

Let \( L \) be an EXP\textsc{time}-complete language, \( L = \{f_n\} \) boolean functions.

Take \( p \) prime \( \equiv 3 \mod 4 \) \( g_n: \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p \) unique multilinear extensions of \( f_n \). We want to make circuits poly-size circuit family \( \{g_n\} \) that computes \( g_n \) s.t. \( \Pr_{x \in \mathbb{Z}_p^n} (g_n(x) \equiv f_n(x)) > \epsilon \).

**Step 1:** Let \( (x_1, \ldots, x_n) \in \mathbb{Z}_p^n \). Consider

\[ g_n(a_1 x_1 + x_1) = \hat{g} (a_1 x_1) \]

with degree \( 2n \). We can interpolate \( \hat{g} (a_1 x_1) \) if we can find \( n+1 \) distinct points.

**Interpolation algorithm:**

Select \( b_1, \ldots, b_n \in \mathbb{Z}_p \) at random.

\[ \text{Compute } c_n(a_1 b_1 + x_1) = \hat{g} (b_1) \]

This gives a probabilistic circuit, with probability of incorrectness at most \( (n+1)(\frac{2n}{3^n}) = \frac{kn}{2^n} < \epsilon/5 \).

By repeating computation, we can take the majority of answers and make probability of incorrectness as small as we like.
Step 3. We assume APP does not admit weakly subexp simulation, and WTS, \( f \) does not approximate \( g_n \).

Again contraposition. Suppose \( \forall n \forall u_k \text{ size } |f_u| \) for infinitely many \( n \), \( \Pr \left( g_n(x) \neq u(x) \right) \geq \frac{1}{3n} \).

**XOR Lemma.** Let \( G: \{0,1\}^n \rightarrow \{0,1\} \). Define \( H: \{0,1\}^n \rightarrow \{0,1\} \) \( H(x_1, \ldots, x_n, y_1, \ldots, y_n, \ldots) = G(x_1, \ldots, x_n) \oplus \cdots \oplus G(x_{2k}, \ldots, x_{2k}) \). If \( \exists C_1 \text{ such that } \) computes \( H \) with probability \( \frac{1}{2 \pm (1-\epsilon)^k}+\delta \), then \( \exists C_2 \text{ such that } \) computes \( G \) with prob \( > 1-\epsilon \).