Today we will talk about Randomized Complexity classes.

Last time we showed BPP \( \subseteq \text{P/poly} \). Today we will show BPP \( \subseteq \Sigma_2P \cap \Pi_2P \)

**BPP error amplification**

Error amplification means decreasing the probability of error. The key tool in this regard is the use of Chernoff bounds.

**Theorem 1** Let \( X_1, X_2, \ldots, X_n \) be independent, identically distributed random variables taking values in \([0,1]\). Let \( Y = \sum_{i=0}^{n} X_i \), \( \mu = E[Y] \).

Then \( \Pr[|Y - \mu| > \varepsilon \mu] < e^{-\varepsilon^2/3} \), for \( \varepsilon \in [0,1] \).

**Proof:** See handout on probability.

**Amplification Lemma:** Let \( L \) be a language such that there is a randomized polynomial-time TM \( M \) such that,

\[
\begin{align*}
  x \in L &\implies Pr[M(x)\text{accepts}] \geq C(|x|) \\
  x \notin L &\implies Pr[M(x)\text{accepts}] \leq S(|x|)
\end{align*}
\]

where \( C(n) - S(n) \geq \frac{1}{p(n)} \) for some \( p() \)

Then \( \forall b > 0, \exists a \) a random ptme TM \( M' \) such that

\[
\begin{align*}
  x \in L &\implies \Pr[M'(x)\text{accepts}] \geq 1 - 2^{-|x|^b} \\
  x \notin L &\implies \Pr[M'(x)\text{accepts}] \leq 2^{-|x|^b}
\end{align*}
\]

(Remark: This is reasonably tight)

**Proof:**\( M' \) runs \( M \) \( k = 12(p(n))^b + n^b \) times, \( n = |x| \). Accepts if \( M \) accepted more than \( k \cdot \frac{s(n)+c(n)}{2} \) times. Applying Chernoff’s bound, we get the desired behaviour of \( M' \).

**Theorem 2** (Sipser) \( BPP \subseteq \Sigma_2P \).

Note: This implies co-BPP \( \subseteq \Pi_2P \), but co-BPP = BPP since definition of BPP is symmetric.

**Proof:**

Let \( L \) be a language in BPP. We know \( \exists A \in \text{P} \) and a function \( f(n) = n^{O(1)} \) such that

If \( w \in L \) then \( \Pr_{r \leftarrow [f(n)]}[(r,w) \in A] > 1 - 2^{-n} \), and

if \( w \notin L \) then \( \Pr_{r \leftarrow [f(n)]}[(r,w) \in A] < 2^{-n} \).

where \( n = |w| \).

**Def.** Define \( R_w = \{ r : |r| = f(n) \text{ such that } (r,w) \in A \} \). Correspondingly,

If \( w \in L \) then \( |R_w| > (1 - 2^{-n})2^{f(n)} \) and

if \( w \notin L \) then \( |R_w| < 2^{-n}2^{f(n)} \).
The idea here is to take a number of translations of $R_w$, and see if they cover the entire space \{0,1\}^{f(n)}$. Each translation of $R_w$ has the same size as $R_w$, and if $R_w$ is most of the space (ie, $w \in L$) then this collection of translations would be likely to cover the space. However, if $R_w$ is very small (ie, $w \not\in L$) then this collection could never cover the space. More formally, 

**Def. (translation)** Let $S \subseteq \{0,1\}^{f(n)}$. For $t \in \{0,1\}^{f(n)}$ let the translation $S \oplus t$ be defined as

$$\{x : x \oplus t \in S\}$$

where $x \oplus t$ is defined as the XOR of the two strings (or, the bitwise sum modulo 2).

**Claim.** (1) If $|S| > (1 - 2^{-n})2^{f(n)}$ then $\exists \tau = \{t_1, \ldots, t_{f(n)}\}$ such that

$$\bigcup_{i=1}^{f(n)} (S \oplus t_i) = \{0,1\}^{f(n)}$$

(2) If $|S| < 2^{-n}2^{f(n)}$ then $\forall \tau = \{t_1, \ldots, t_{f(n)}\}$,

$$\bigcup_{i=1}^{f(n)} (S \oplus t_i) \neq \{0,1\}^{f(n)}$$

First, we show that the claim proves the theorem. If the claim is true, we can design a $\Sigma_2P$ machine $M$ to solve $L$ as follows:

1. Use $\exists$ states to generate $\tau$.
2. Use $\forall$ states to generate $r \in \{0,1\}^{f(n)}$.
3. Check if $r \in \bigcup \{R_x \oplus t_i\}$ and accept if so, otherwise, reject.

This is polynomial time, since we can check whether $r \in R_x$ in polynomial time, and $f(n)$ is polynomial in $n$. By the claim, if $x \in L$ then on any correct $\tau$ we accept. If $x \not\in L$ we reject, since there is no such $\tau$. Therefore, we only have to prove the claim.

First, we prove part (2) of the claim. If $|S| < 2^{-n}2^{f(n)}$ then

$$\left| \bigcup_{i} (S \oplus t_i) \right| \leq f(n)2^{-n}2^{f(n)}.$$ 

Since $f(n) = n^{O(1)}$, $f(n)2^{n} < 1$ for sufficiently large $n$. Therefore, this union doesn’t cover $\{0,1\}^{f(n)}$.

Note that the "sufficiently large $n$" clause here doesn’t cause a problem. If we take this into account, we need only hard-code the correct answer for all words smaller than this bound into our $\Sigma_2P$ machine.

Next, we prove part (1). Let

$$p = \Pr_{\tau}[\forall r \in \bigcup_{i=1}^{f(n)} (t_i \oplus S)]$$

$$= \Pr_{\tau}\left[\exists r \in \bigcup_{i=1}^{f(n)} (t_i \oplus S)\right]$$

$$\geq 1 - \Pr_{\tau}[r \not\in \bigcup_{i=1}^{f(n)} (t_i \oplus S)].$$

We choose the $t_i$’s independently, so we can consider them independently. Therefore,

$$p \geq 1 - \sum_{r \not\in f(n)} \prod_{i=1}^{f(n)} \Pr_{t_i}[r \not\in t_i \oplus S]$$

$$= 1 - \sum_{r \not\in f(n)} \prod_{i=1}^{f(n)} 2^{-n}$$

7-2
since \( r \in t_i \oplus S \) if and only if \( t_i \in r \oplus S \),

\[
= 1 - 2^{f(n)}(2^{-n})^f(n) = 1 - 2^{-f(n)(n-1)} > 0.
\]

Since this probability is nonzero, there must be at least some \( \tau \) for which the union of the translations determined by \( \tau \) covers \( \{0, 1\}^f(n) \). This completes the proof. ■

**Verifying Polynomial identities**

Let \( p \) be a given polynomial in \( k \) variables, \( q_1, \ldots, q_k \) given polynomials in \( m \) variables. The equation

\[
p(q_1(y_1, \ldots, y_m), \ldots, q_k(y_1, \ldots, y_m)) = 0
\]

can be difficult to check deterministically. Expanding the polynomial out would give us an exponential number of terms. However, if we use randomization there is an easy test. Choose \( x_1, \ldots, x_m \) at random and see if we get zero. If we choose \( x_i's \) in a large enough range, the probability that the test is passed but \( p \) is not identically zero becomes exponentially small. So we can check polynomial identities in co-RP.

**Lemma 3 (Schwartz's Lemma)** Let \( P(x_1, x_2, \ldots, x_n) \) be a polynomial of degree \( d \). Then if \( P \neq 0 \), then

\[
\Pr_{x_1, x_2, \ldots, x_n \in S}[P(x_1, x_2, \ldots, x_n) = 0] \leq \frac{dn}{|S|}.
\]

**Proof:** We use induction on \( n \).

**Base case** \((n = 1)\): If \( P \neq 0 \), then there are at most \( d \) zeroes in \( p \). At most \( d = d \cdot 1 \) of them are in \( S \).

**Inductive step:** Write

\[
P(x_1, x_2, \ldots, x_n) = \sum_{i=0}^{d_1} x_i^i P_i(x_2, \ldots, x_n).
\]

By hypothesis,

\[
\Pr_{x_2, \ldots, x_n}[P_i(x_2, \ldots, x_n) = 0] \leq \frac{(n-1)d}{|S|}.
\]

If \( P_{d_1}(x_2, \ldots, x_n) \neq 0 \), then \( \Pr_{x_1}[P(x_1, \ldots, x_n)] \leq \frac{d_1}{|S|} \). ■