Theorem 15.1 BPP $\subseteq \Sigma_2^p \cap \Pi_2^p$

Proof: It suffices to show that BPP $\subseteq \Sigma_2^p$ because BPP $=$ co-BPP.

Let $L \in$ BPP. Let M be the BPP machine accepting L with error probabilities 2^{-n} for inputs of length n.

Fix $x \in \{0,1\}^n$ and let $S_x = \left\{r \in \{0,1\}^m \;\middle|\; M(x,r) = 1\right\}$

If $x \in L$ Then $|S_x| \geq 2^m(1-2^{-n})$

If $x \notin L$ Then $|S_x| \leq 2^{m-n}$.

We will show that we can distinguish these two cases in Σ_2^p.

Let $k = \lceil \frac{m}{n} \rceil + 1$.

For $u \in \{0,1\}^m$, let $S + u = \left\{w \oplus u \;\middle|\; w \in S\right\}$

For $u_1, \ldots, u_k \in \{0,1\}^m$, consider the event:

$$\bigcup_{i=1}^{k} (S_x + u_i) \quad = \quad \{0,1\}^m \qquad \star$$

Claim 1. If $x \notin L$ then $\forall u_1, \ldots u_k \in \{0,1\}^m$, $\star$ does not hold.

Proof: There aren't enough elements k copies of S_x to cover $\{0,1\}^m$: $k2^{m-n} < 2^m$. $\square$

Claim 2. If $x \in L$ then $\exists u_1, \ldots u_k \in \{0,1\}^m$, $\star$ holds.

Proof: We show that for $u_1, \ldots u_r$ chosen randomly and independently, Prob$(\star) > 0$.

For $r \in \{0,1\}^m$, let B_r be the event $r \notin \bigcup_{i=1}^k (S_x + u_i)$.

$B_r = \bigcap_{i=1}^k B_r^i$ where B_r^i is the event $r \notin S + u_i$, or equivalently, the event $r \oplus u_i \notin S_x$.

Prob$(B_r^i) \leq 2^{-n}$

Prob$(B_r) \leq 2^{-nk} < 2^{-m}$

Thus, Prob$(\star) > 0$ $\square$

$$\begin{aligned} x \in L \quad &\Leftrightarrow \quad \exists u_1 \ldots u_k \in \{0,1\}^m \; \forall r \in \{0,1\}^m \; r \in \bigcup_{i=1}^{k} (S_x + u_i) \\ &\Leftrightarrow \quad \exists u_1 \ldots u_k \in \{0,1\}^m \; \forall r \in \{0,1\}^m \; \bigvee_{i=1}^{k} (M(x, r \oplus + u_i) = 1) \end{aligned}$$

$\square$