

Recap

$L \in BPP$ iff there is a PPTM M s.t. $\forall x \in \Sigma^*$

$$x \in L \Rightarrow \Pr(M(x) \text{ accepts}) \geq 2/3$$

$$x \notin L \Leftarrow \Pr(M(x) \text{ accepts}) \leq 1/3$$

$L \in RP$ iff there is a PPTM M s.t. $\forall x \in \Sigma^*$

$$x \in L \Rightarrow \Pr(M(x) \text{ accepts}) \geq 1/2$$

$$x \notin L \Leftarrow \Pr(M(x) \text{ accepts}) = 0$$

Theorem: $BPP \subseteq \Sigma_2^P = NP^{NP}$

Proof. Let M be a PPTM for some L . Fix input x , $n = |x|$. The error of M is then 2^{-n} .

Now construct a TM $M(x, r)$, $|r| = p(n) = p(|x|)$, that corresponds to the r -th instance of the probabilistic machine. (i.e., the r -th coin toss)

Claim: $x \in L \Leftrightarrow \exists z_1, z_2, \dots, z_m, |z_i| = m, \forall y, |y| = m, \exists i$ s.t. $M(x, y \oplus z_i)$ accepts.

Proof of the theorem uses probabilistic method. We first prove the \Rightarrow part.

We pick z_1, z_2, \dots, z_m at random, and fix a y . Then we have for all i that

$$\Pr(M(x, y \oplus z_i) \text{ accepts}) \geq 1 - 2^{-n}$$

thus

$$\Pr(M(x, y \oplus z_i) \text{ rejects}) \leq 2^{-n}$$

therefore

$$\Pr(\forall i, M(x, y \oplus z_i) \text{ rejects}) \leq 2^{-nm}$$

Now make y random, we have

$$\Pr(\exists y, \forall i, M(x, y \oplus z_i) \text{ rejects}) \leq \sum_{y \in \Sigma^*} 2^{-nm} = 2^m 2^{-nm} = 2^{-(n-1)m} \ll \frac{1}{2}$$

therefore

$$\Pr(\forall y, \exists i, M(x, y \oplus z_i) \text{ accepts}) \geq \frac{1}{2} > 0$$

which is equivalent to say that

$$\exists z_1, \dots, z_m, \forall y, \exists i, M(x, y \oplus z_i) \text{ accepts}$$

Next we prove the \Leftarrow part. Let $x \notin L$, we fix z_1, \dots, z_m and pick y at random, we have

$$\Pr(M(x, y \oplus z_i) \text{ accepts}) \leq 2^{-n} \quad \forall i$$

therefore

$$\Pr(\exists i, M(x, y \oplus z_i) \text{ accepts}) \leq m 2^{-n} = \frac{p(n)}{2^n} < \frac{1}{2} \quad \text{for large } n$$

thus

$$\Pr(\forall i, M(x, y \oplus z_i) \text{ rejects}) \geq \frac{1}{2}$$

which is equivalent to say that

$$\forall z_1, \dots, z_m, \exists y, \forall i, M(x, y \oplus z_i) \text{ rejects}$$

Hence, the claim is proved.

Obviously, to check $\exists z_1, z_2, \dots, z_m, |z_i| = m, \forall y, |y| = m, \exists i \text{ s.t. } M(x, y \oplus z_i)$, we need an oracle TM that guesses z_1, \dots, z_m and ask if $\exists y \text{ s.t. } M(x, y \oplus z \text{ rejects}) \forall i$ and accepts if the answer is no. This routine is NP^{NP} .

The proof is complete. □