- The case of $x \notin L$ is similar.

$\Rightarrow L \in ZPP$. $\square$

<u>Why 2/3? Prob. amplification</u>

- The $(2/3)$-rd in the defn. of prob. classes is arbitrary. In fact, we can use any fraction that is <u>inverse-polynomial</u> away from $1/2$.

<u>Theorem</u>: Let a PTM M be deciding L s.t. $\forall x$, $x \in L$ iff $\Pr[M \text{ accepts } x] \geq \left(\frac{1}{2} + |x|^{-c}\right)$.

Then, $\forall d$, $\exists$ PTM M' s.t. $\forall x$, $x \in L$ iff $\Pr[M' \text{ accepts } x] \geq \left(1 - 2^{-|x|^d}\right)$.

<u>Pf sketch:</u>

- <u>Idea:</u> Run M k times on x, and output the <u>majority</u> value. Apply the Chernoff bound on error prob.

• The PTM M' is: $(\text{Fix } k = 8 \cdot |x|^{d+2c})$

On input x, run $M(x)$ k times.

Let the outputs be $y_1, \ldots, y_k \in \{0,1\}$.

Output Majority$(y_1, \ldots, y_k)$.

• For $i \in [k]$, let $\underline{X_i}$ be the random variable $\begin{cases} 0, & \text{if } y_i \text{ is } \underline{\text{wrong}} \\ 1, & \text{otherwise.} \end{cases}$

Chernoff's bound: Let $X_1, \ldots, X_k$ be independent identically distributed (i.i.d.) boolean random variables. Let $\Pr[X_i = 1] =: p$ for $i \in [k]$ & $\delta \in (0,1)$. Then,

$$\Pr\left[\left|\frac{\sum_{i \in [k]} X_i}{k} - p\right| > \delta\right] < e^{-\delta^2 pk/4}.$$

$$\Rightarrow \Pr[M' \text{ is wrong}] = \Pr\left[\sum_{i=1}^{k} X_i < k/2\right]$$

$p := \Pr[M(x) \text{ is correct}]$

$$= \Pr\left[p - \frac{\sum X_i}{k} > p - \frac{1}{2}\right] = \Pr\left[\left|p - \frac{\sum X_i}{k}\right| > n^{-c}\right]$$

$$< \exp\left(-\frac{1}{4}\cdot n^{-2c}\cdot\left(\frac{1}{2}+n^{-c}\right)\cdot 8n^{d+2c}\right)$$

$$= \exp\left(-n^{d}\cdot(1+2n^{-c})\right)$$

$$< e^{-n^d} < 2^{-n^d}. \qquad \square$$

Exercise: The Chernoff bound has a neat proof using $\mathrm{Exp}\left[e^{t\cdot\sum_i X_i}\right]$ & the Markov's bound.

BPP & the PH

- $BPP \overset{?}{\subseteq} NP$ is not known, but $BPP \subseteq \Sigma_2 \cap \Pi_2$ is!

Theorem (Sipser-Gács 1983): $BPP \subseteq \Sigma_2 \cap \Pi_2$.

Pf:

- It suffices to show $BPP \subseteq \Sigma_2$.

- Let $L \in BPP$, and M be a poly-time TM $(m := n^c)$ s.t. $\forall x \in \{0,1\}^n$,

$$x \in L \Rightarrow \Pr_{r \in \{0,1\}^m}[M(x,r) = 1] \geq (1 - 2^{-n})$$

$$x \notin L \Rightarrow \Pr_{r}[M(x,r) = 1] \leq 2^{-n}.$$

- Denote $S := \{r \in \{0,1\}^m \mid M(x,r) = 1\}$. Then, as before,

$$|S| \geq (1-2^{-n})\, 2^m \quad \text{if } x \in L,$$
$$|S| \leq 2^{m-n} \quad \text{if } x \notin L.$$

- The idea is to check the "largeness" of this S in Σ_2. (Use "expansion" in a graph.)

- For $U = \{u_1, \ldots, u_k\} \subseteq \{0,1\}^m$, define an undirected graph $\underline{G_U}$ with:

  $\{0,1\}^m$ as <u>vertices</u>, and

  <u>edges</u> (s, s'), where $s \oplus s' = u_i$ for some i.

- Note that G_U is <u>regular</u> with $\deg = k$.

- Fix $k := \lfloor \frac{m}{n} \rfloor + 1$.

- For any $S \subseteq \{0,1\}^m$, define $\underline{\Gamma_u(S)}$ to be the neighbours of S in G_u.

<u>Claim 1</u>: $|S| \leq 2^{m-n} \Rightarrow \forall u, |u|=k, |\Gamma_u(S)| < 2^m$.

<u>Pf</u>:

- $|\Gamma_u(S)| \leq k \cdot |S| \leq \frac{k}{2^n} \cdot 2^m < 2^m$. □

<u>Claim 2</u>: $|S| \geq (1-2^{-n}) 2^m \Rightarrow \exists u, |u|=k, \Gamma_u(S) = \{0,1\}^m$.

<u>Pf</u>:

- We construct a u <u>probabilistically</u>!
- Choose $u_1, \ldots, u_k \in \{0,1\}^m$ randomly.

- Let $\underline{E_r}$ be the event that $r \notin \Gamma_u(S)$ & $\underline{E_{r,i}}$ " " " " $r \notin S \oplus u_i$.

• Clearly,

$$\Pr_u[E_{r,i}] = 1 - \frac{|r \oplus S|}{2^m} \leq 2^{-n}.$$

• So,

$$\Pr_u[E_r] \leq \prod_{i=1}^{k} \Pr_u[E_{r,i}] \leq 2^{-nk} < 2^{-m}.$$

$$\Rightarrow \Pr_u[\exists r, E_r] < 1.$$

$$\Rightarrow \Pr_u[\forall r, \neg E_r] > 0.$$

$$\Rightarrow \exists u, \ T_u(S) = \{0,1\}^m. \qquad \square$$

• Claims 1 & 2 imply: $\forall x \in \{0,1\}^n$,

$$x \in L \text{ iff } \exists u_1, \ldots, u_k, \forall r, \bigvee_{i \in [k]} M(x, r \oplus u_i) = 1.$$

$\in \{0,1\}^m$

$$\Rightarrow L \in \Sigma_2. \qquad \square$$