Relation between BPP and other classes.

→ $P \subseteq BPP$ $\quad$ $BPP \subseteq P$? $\quad$ $BPP \subseteq NP$?

↖ true?

thm: $BPP \subseteq P/poly$. (P w poly-length advice).

goal: find random string that works for all inputs of size n.

proof: use error reduction to get error down to 2^{-n-1}. (poly overhead in time).

$\forall x,\ |x|=n,\ \Pr_r[M(r) \neq L(x)] \leq 2^{-n-1}$

$\Pr_y[\bigvee_{x,\,|x|=n} M(r_y) \neq L(x)] \leq \sum_{x,\,|x|=n} \Pr_y[M(r_y) \neq L(x)] \leq 2^n \cdot 2^{-n-1} = 1/2 < 1$

$\exists y$ s.t. $\bigwedge_{x,\,|x|=n} M(r_y) = L(x)$. give y as advice to a TM that simulates M. ✻

thm: $BPP \subseteq P^{\Pi_2 P}$. $BPP \subseteq \Sigma_2 P \cap \Pi_2 P$. // Gács-Lautemann-Sipser thm.

fix $L \in BPP$, error reduction → $\exists M$ correct except w/pr. 2^{-n}.

fix x, $|x|=n$, $|y|=m=poly(n)$.

$x \in L$

$\times \{\bullet, \to, \downarrow, \searrow\} =$

$x \notin L$

$\times \{\bullet, \to, \downarrow, \searrow\} =$

proof. $BPP \subseteq \Sigma_2 P$. (BPP closed under complements → $BPP \subseteq \Pi_2 P$).

fix $L \in BPP$, error reduction → $\exists M$ correct except w/pr. 2^{-n}.

fix x, $|x|=n$, $|y|=m=poly(n)$.

$S_x = \{y : M(x,y) = 1\}$. $\quad x \in L \Rightarrow |S_x| \geq 2^m \cdot (1-2^{-n})$. $\quad x \notin L \Rightarrow |S_x| \leq 2^m \cdot 2^{-n} = 2^{m-n}$.

$y \in \{0,1\}^m \sim \mathbb{F}_2^m$

$v \in \mathbb{F}_2^m$ $\quad v + S_x = \{v+y : y \in S_x\}$. $\quad v_1 \dots v_k$: $\bigcup_{v_1 \dots v_k} v_i + S_x \supseteq \mathbb{F}_2^m$.

↑ want.

find $v_1 \dots v_k$ with probabilistic method.

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

lemma: $|S_x| \leq 2^{m-n}$, $k < 2^n$ ⇒ then $\bigcup v_i + S_x \neq \mathbb{F}_2^m$.

$\bigcup v_i + S_x$: $\leq 2^{m-n}$ $\quad$ $\mathbb{F}_2^m$: $< 2^m$.

lemma: $|S_x| \geq 2^m \cdot (1-2^{-n})$, $k > \lceil \frac{m}{n} \rceil$, then $\exists v_1 \dots v_k$ s.t. $\bigcup v_i + S_x = \mathbb{F}_2^m$.

proof: show every $r \in \mathbb{F}_2^m$ is covered. fix r.

$\Pr_{v_i \text{ unif.}}[r \notin \bigcup v_i + S_x] \leq \prod^{k} 2^{-n} = 2^{-kn} < 2^{-m}$ $\quad (k > \lceil \frac{m}{n} \rceil)$

↑ $r \notin v_i + S_x$ for some i.

$r + v_i \notin S_x$ ← unif. distr.

$\Pr_v[\exists r\ r \notin \bigcup\ ] \leq \sum_{r \in \mathbb{F}_2^m} \Pr_v[\text{bad for } r] < \sum 2^{-m} = 1$.

$\exists v = v_1 \dots v_k$ $\forall r$, $r \in \bigcup$ as we wanted to show. /

$x \in L \leftrightarrow \exists v_1 \dots v_k\ \forall r \in \{0,1\}^m\ \bigvee_{i \in \{0,1\}^k} M(x, v_i + r) = 1$ → $L \in \Sigma_2 P$.

$N(x, v_1 \dots v_k, r)$

$x \notin L \rightarrow \forall v_1 \dots v_k\ \exists r\ \bigwedge_i M(x, v_i + r) = 0$ ✻

Interactive Proofs.

2 glasses of water. I claim: can distinguish between the two glasses.

You have a coin, can move glasses around. Can you verify this claim?

A?

B?

AAA BBB

111 222

def. Interactive Proofs. P, V ← prover, verifier ← functions

on input x interactive protocol

V sends string $a_1 = V(x)$

P sends " $a_2 = P(x, a_1)$

V " " $a_3 = V(x, a_1, a_2)$

⋮

V answer $a_{out} = V(x, a_1 \dots a_{out})$ ← $\{0,1\}$.

def IP[k] class of languages st:

→ P unlimited (even uncomputable ok!)

→ V randomized poly-time TM. (in x, not in a).

→ $x \in L$ $\exists P$ st $\Pr[a_{out} = 1] > 2/3$.

→ $x \notin L$ $\forall P$: $\Pr[a_{out} = 0] > 2/3$.

→ k rounds.

$IP = \bigcup_c IP[|x|^c]$.

lemma: can replace 2/3 by any number in $[1/2 + n^{-c}, 1 - 2^{-n^d}]$, get same class.

proof: repeat protocol enough times.

subtlety: prover sees messages from previous interactions.

ok because def is ∀P.

"Parallel Repetition".

can make it work even for IP[k]:

repeat k times:

1: send $a_1^1, a_1^2, a_1^3 \dots a_1^t$

2: $a_2^1, a_2^2, a_2^3 \dots a_2^t$

⋮

K+1: V takes majority of $a_{out}^1 \dots a_{out}^t$.

e.g. IP for graph isomorphism.

G_1, G_2 if $\exists \pi : V_1 \to V_2$ bijection

st $(u,v) \in E_1$ iff $(\pi(u), \pi(v)) \in E_2$.

V: say validity

P: sends π

V: check if $\pi(G_1) = G_2$.

works for every $L \in NP$: P sends certificate.

e.g. for graph non isomorphism = $\overline{GI}$

don't know if $\overline{GI}$ has short certificates.

V: pick $i \in \{1,2\}$ uniformly.

sample π permutation $V_1 \to V_2$ uniformly.

send $H = \pi(G_i)$.

P: find if $H \cong G_1$ or $H \cong G_2$, answer i'.

V: answer $[i = i']$.

if $x \in L$ then always correct.

if $x \notin L$, then $\Pr[\text{accept}] = 1/2$. (our def. says $< 1/3$, need to repeat).

assume $x \notin L \rightarrow G_1 \cong G_2$. then: i uniform. $\in \{1,2\}$

H uniform among all graphs $\cong G_1 \cong G_2$.

i \ H	1	2
1	✓	×
2	×	✓

$\Pr[i = i'] = 1/2$.