February 1, 2021 9:13 AM

Randomized Complexity Classes

ZPP = all languages (i.e. decision problems) with Las Vegas alg'ms in expected polytime

"Zero-error Probabilistic Polytime"

RP = all languages L with one-sided Monte Carlo alg'ms $\mathcal{A}$ in worst-case polytime

s.t. $\forall$ input x,

$$\begin{cases} \text{if } x \in L \Rightarrow \Pr(\mathcal{A} \text{ outputs yes on } x) \geq \frac{1}{2} \\ \text{if } x \notin L \Rightarrow \Pr(\mathcal{A} \text{ outputs no on } x) = 1. \end{cases}$$

Rmk: $\frac{1}{2}$ can be changed to any const $\in (0,1)$ by repeating & taking OR of output (with t iterations, err prob $\leq \frac{1}{2^t}$).

(e.g. Miller-Rabin: COMPOSITE $\in$ RP)
Adleman-Huang: " $\in$ ZPP)
AKS: " $\in$ P)

Fact 1. $P \subseteq ZPP \subseteq RP$ (by Markov).

Fact 2. $RP \subseteq NP$.

Pf: certificate = seq of rand bits. □

Fact 3. $ZPP = RP \cap \text{co-}RP$.

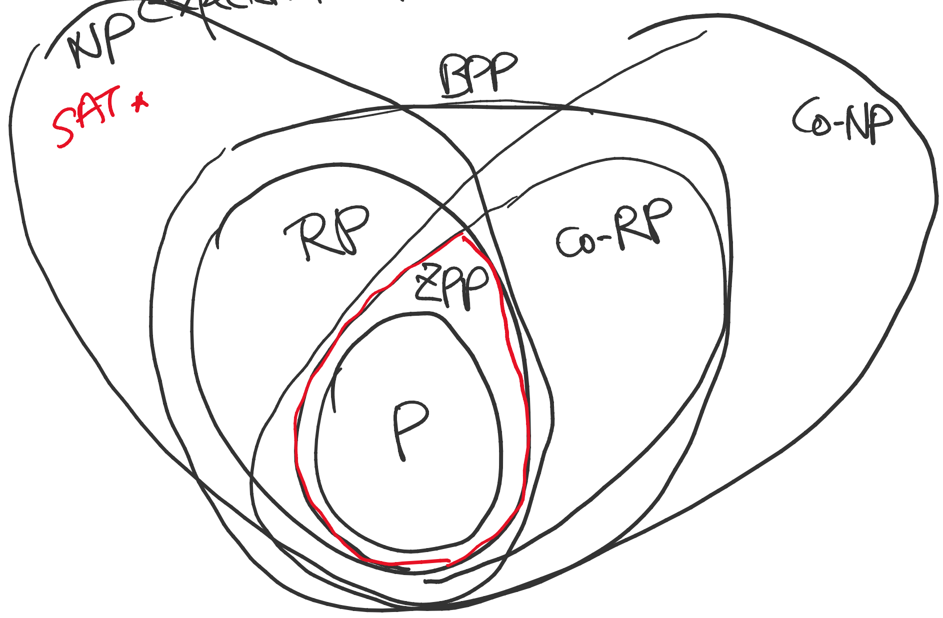
Pf. ($\subseteq$) since $ZPP = \text{co-}ZPP$.

Pf: ($\subseteq$) ... since ZPP = co-ZPP.

($\supseteq$) Suppose we have 2 one-sided Monte-Carlo alg'm $\mathcal{A}$ for L
$\mathcal{A}'$ for L^c.

run both: if $\mathcal{A}$ says no, know $x \notin L$.
if $\mathcal{A}'$ says no, know $x \in L$.
w. prob $\le \frac{1}{2}$ $\longrightarrow$ otherwise repeat

expected # iterations ≤ 2. $\square$



BPP = all languages L with 2-sided Monte-Carlo alg'ms in polytime

"Bounded-error Probabilistic Polytime"

s.t. $\forall$ input x,
if $x \in L \Rightarrow \Pr[\mathcal{A}$ outputs yes on $x] > \frac{2}{3}$
if $x \notin L \Rightarrow \Pr[\mathcal{A}$ outputs no on $x] > \frac{2}{3}$

Rmk: $\frac{2}{3}$ can be changed to any const $\in (\frac{1}{2}, 1)$.
by repeating & taking majority of output

(with t repetitions,
err prob $\le \frac{1}{2^{\Theta(t)}}$ by Chernoff bd...)

(if exactly $\frac{1}{2}$, we get different class PP)

(if exactly $\frac{1}{2}$, we get different class !!)

not relevant to us

$\frac{\frac{1}{2}+\frac{1}{p(n)}}{\cancel{\frac{1}{2}+\frac{1}{2^n}}}$

Fact 4 $RP \subseteq BPP$.

(also, $co\text{-}RP \subseteq BPP$, since $BPP = co\text{-}BPP$)

Upper bd for BPP ?

Known: (Sipser-Gacs-Lauterman '83) $BPP \subseteq NP^{NP} \cap co\text{-}NP^{NP}$

In fact, $BPP \subseteq ZPP^{NP}$

In fact, $MA \subseteq ZPP^{NP}$ (Goldreich-Zuckerman '97)

Merlin-Arthur (rand. analog of NP)

Possibility of general derandomization?

Thm (Adelman '78) $\overset{BPP}{\cancel{RP}} \subseteq P/poly$.

all languages L that can be solved by a non-uniform det. alg'm in polytime

i.e. a sequence of alg'ms $A_1, A_2, \ldots, A_n, \ldots$ one for each input size n

or equiv: polytime alg'm that is given an advice string with poly length

Or equiv. algm ... string with poly length & depending on n.

Or equiv: poly-size circuit

Pf: By repeating cn times, ← runtime $T(n)$, still poly.
get an alg'm $\mathcal{A}$ with err prob. $\leq \frac{1}{2^{cn}}$

Fix n.
Pick rand sequence r of $T(n)$ bits.
For any fixed input x of size n, in bits
$\Pr[\mathcal{A}$ is wrong on x using $r] \leq \frac{1}{2^{c(n)}}$.

By union bd,
$\Pr[\exists x$ of size n, $\mathcal{A}$ is wrong on x using $r]$
$\leq 2^n \frac{1}{2^{c(n)}} < 1$ for $c>1$.

"Probabilistic method" (prove existence of something by showing ... prob is nonzero)

there exists sequence r_n s.t.
$\forall$ input x of size n,
$\mathcal{A}$ using r_n is correct on x.
this is a nonunif. alg'm $\mathcal{A}_n$.
□

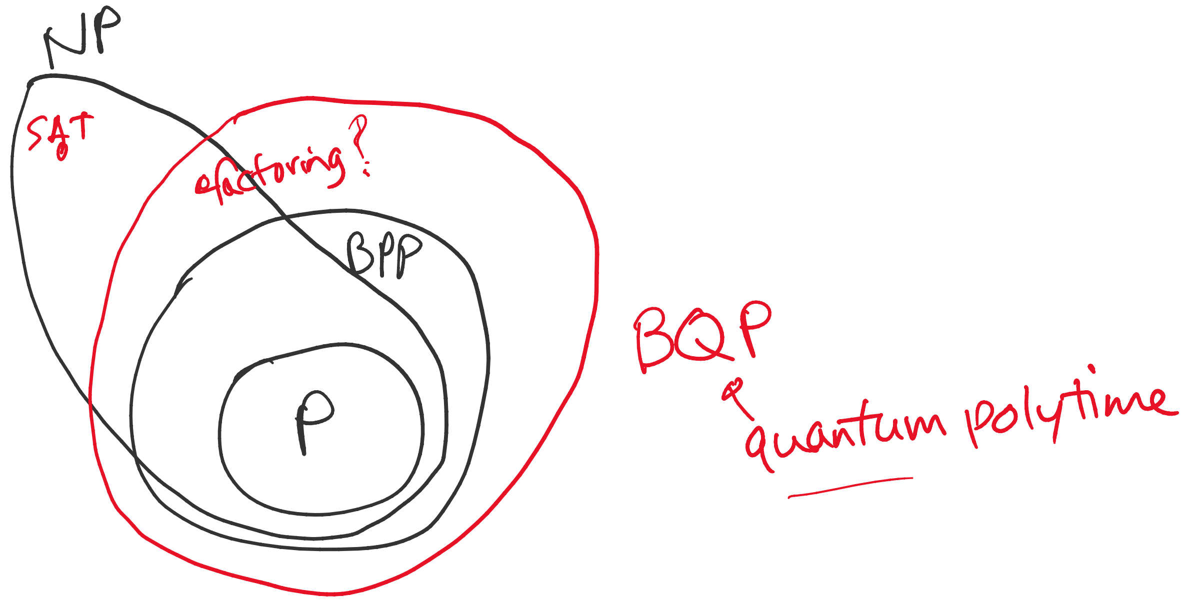
Big Open Problem Is BPP = P ?

Known: Impagliazzo & Wigderson '97 showed
BPP = P if there is a problem in $E = DTIME(2^{O(n)})$
... circuit complexity ...

BPP = P ...

in $E = DTIME(2^{...})$ that has circuit complexity $2^{\Omega(n)}$.

("hardness vs. randomness").



Random Re-Ordering

Example 0: find min of n numbers $S = \{x_1, \dots, x_n\}$

standard incremental alg'm:

RANDOMly permute $x_1, \dots, x_n$

0. ans = ∞
1. for $i = 1, \dots, n$
2. if $x_i <$ ans
3. ans = x_i (*)
4. return ans

"hiring problem"

O(n) time (n-1 comps)

How many changes (*)?

worst-case: n times ($n, n-1, \dots, 1$)

expected?

naively: list all $n!$ permutations, compute #, take avg, . . .

rewrite alg'm backwards:

min(S):

0. if $S = \phi$ return ∞
1. pick $x \in S$ randomly
2. ans = min$(S - \{x\})$
3. if $x <$ ans
4. ans $= x$ (*)
5. return ans

For any fixed S,

$$\Pr[\,(*) \text{ is done}\,] = \Pr[\,x < \min(S - \{x\})\,] = \Pr[\,x = \min(S)\,] = \frac{1}{n}.$$

$\Rightarrow$ expected total # changes

$$F(n) = F(n-1) + \frac{1}{n} \cdot 1 \cancel{+ \left(1 - \frac{1}{n}\right) \cdot 0}$$

by linearity of expectation

$$\Rightarrow F(n) = \frac{1}{n} + \frac{1}{n-1} + \frac{1}{n-2} + \ldots + \frac{1}{2} + \frac{1}{1}$$

(Harmonic numbers)

$$= \boxed{\Theta(\log n)}.$$