BPP and Polynomial Hierarchy

1 April, 2021 14:02

Error reduction for BP-type computation

Let A be a prob. algorithm with error $\le \varepsilon \le \frac{1}{3}$.

Modify A to get A':

alg. for A': on input x

run A on x k-times (k even)

if A accepts x in $\ge k/2$ of the runs $\rightarrow$ ACCEPT

o/w REJECT.

$$\Pr[A' \text{ errs on input } x] = \sum_{i=\frac{k}{2}}^{k} \varepsilon_x^i (1-\varepsilon_x)^{k-i} \binom{k}{i}$$

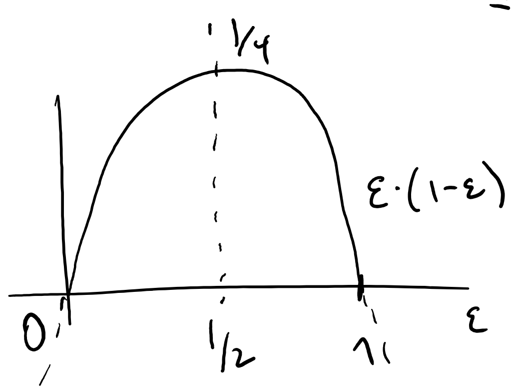
ε_x .. error of A on x

$\varepsilon_x \le \varepsilon$

$$\le \sum_{i=\frac{k}{2}}^{k} \varepsilon_x^{k/2} (1-\varepsilon_x)^{k/2} \binom{k}{i}$$

$$\le 2^k \cdot \varepsilon_x^{k/2} (1-\varepsilon_x)^{k/2}$$

$$\le 2^k \left(\varepsilon(1-\varepsilon)\right)^{k/2}$$



if $\varepsilon \le \frac{1}{3} \Rightarrow \varepsilon(1-\varepsilon) \le \frac{2}{9}$

$$\underset{\varepsilon \le \frac{1}{3}}{\le} 2^k \cdot \left(\frac{2}{9}\right)^{k/2} = \left(\frac{8}{9}\right)^{k/2}$$

$$\Rightarrow \Pr[A' \text{ errs on } x] \le \left(\frac{8}{9}\right)^{k/2} = \frac{1}{\left(\frac{9}{8}\right)^{k/2}}$$

$\Big(\frac{}{9} \quad = \quad \left(\frac{9}{8}\right)^{k/2}$

set $k = \dfrac{4n}{\lg \frac{9}{8}}$

$$\Rightarrow \Pr[A' \text{ errs on } x] \leq \frac{1}{\left(\frac{9}{8}\right)^{\frac{2n}{\lg 9/8}}} = \frac{1}{2^{2n}}$$

<u>Thm</u>: BPP $\in$ P/poly

<u>Pf</u>: Let A be a randomized alg. running in time n^c with error $\leq \varepsilon$.

Reduce its error by running it $\frac{4n}{\lg 9/8}$ - times

$\longrightarrow$ error $\leq \frac{1}{2^{2n}}$, alg A'

running time $O(n^{c+1})$.

$\Rightarrow \exists\, r \in \{0,1\}^{n^{c+1}}$ ... random string s.t. A' is correct on all inputs $x \in \{0,1\}^n$.

(only $\frac{1}{2^{2n}}$ fraction of random strings $r \in \{0,1\}^{n^{c+1}}$ gives wrong answer for a given input $x \in \{0,1\}^n$. There are 2^n inputs so in total, the fraction of random strings $r \in \{0,1\}^{n^{c+1}}$ for which A' errs on some input is $\leq 2^n \cdot \frac{1}{2^{2n}} = \frac{1}{2^n}$.

$\Rightarrow$ most random strings work correctly for all inputs $x \in \{0,1\}^n$.)

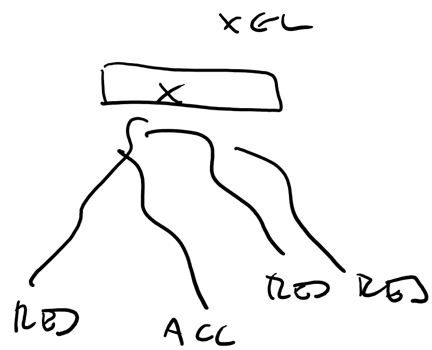
$\rightarrow$ r is the advice for the algorithm A'' on inputs, ... A'

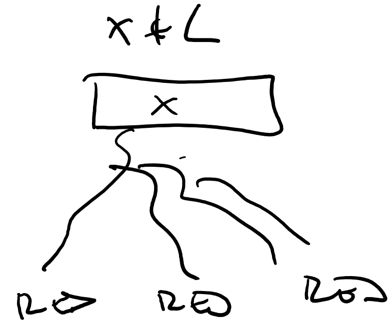
of length n, A'' uses the advice as random string for A'' & checks what it does. $\square$

Alternating Machines

$L \in NP$ ... nondet. TM N for L

$x \in \{0,1\}^n$

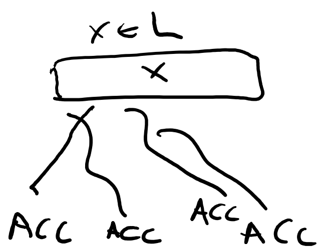


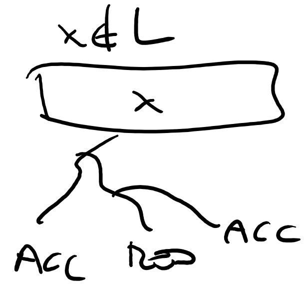


computation tree

$L \in coNP \iff \overline{L} \in NP$ ... $\exists$ co-nondeterministic TM N

$x \in \{0,1\}^n$

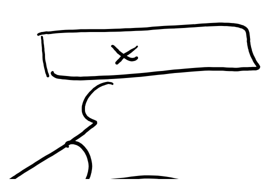




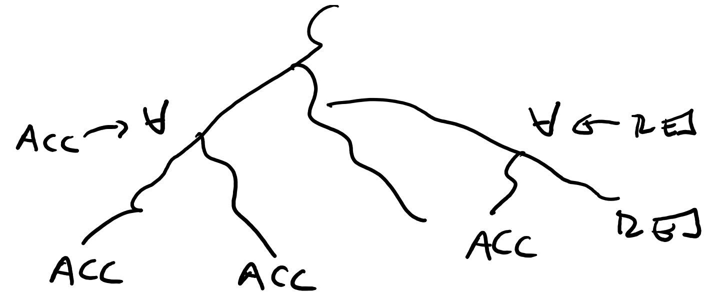
→ always accepts → must reject sometimes

→ generalization – each state of a nondet TM is designated either as existential ($\exists$) or universal ($\forall$). → alternating TM M

$x \in \{0,1\}^n$



$x \in \{0,1\}$



the computation of M on input x is evaluated bottom up. Each configuration is labelled either as ACC or REJ. Leaves are labelled in the obvious way. Config's with ∃ state is labelled as accepting if at least one of its child configuration is labelled accepting. Configuration with ∀ state is labelled accepting if both its children are labelled accepting. O/w they are rejecting.

x is accepted if the initial configuration on x is labelled as accepting.

→ ATIME$(t(n))$ ... class of problems L that can be solved by <u>alternating</u> TM running in time $O(t(n))$.

- $NP \cup coNP \subseteq \bigcup_k ATIME(n^k)$.
- $PSPACE = \bigcup_k ATIME(n^k)$

<u>Pf:</u> • $\bigcup_k ATIME(n^k) \subseteq PSPACE$:

PSPACE we can backtrack through the ... the computation tree & figure out the acceptance of ATM on ~~some~~ input x.

- $PSPACE \subseteq \bigcup_k ATIME(n^k)$:

$QBF \in ATIME(n^4)$:

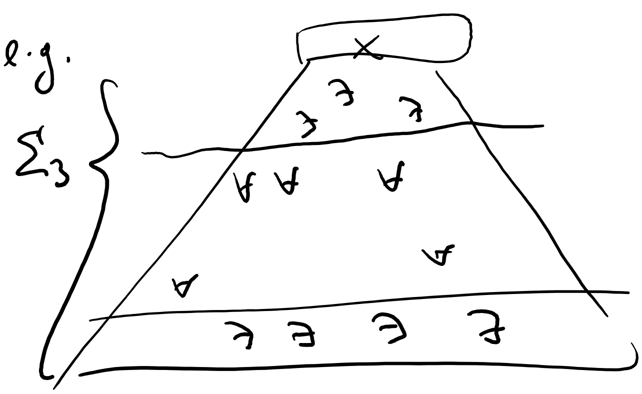
given a QBF φ of length n start evaluating it; on universally quantified variables branch using $\forall$ state, on existential quantifiers branch using $\exists$ state.

e.g. $\varphi = \exists x_1 \forall x_2 \exists x_3 \dots \varphi(x_1 \dots x_n)$

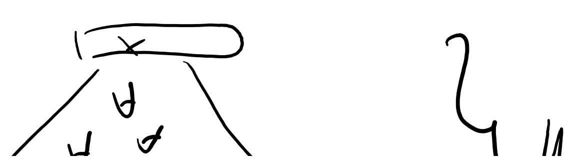
eventually accept iff the assignment satisfies the formula. ∎

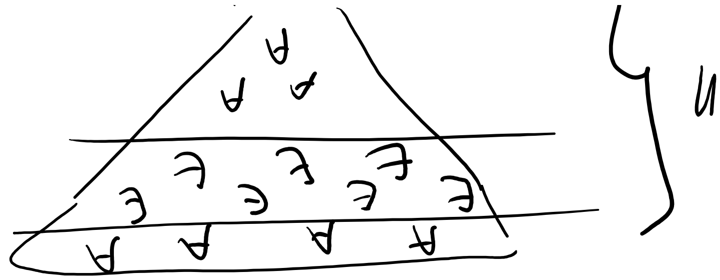
Σ_k-TIME$(t(n))$ … class of problems accepted by ATM's running in time $O(t(n))$ which switch at most $(k-1)$-times between $\exists$ & $\forall$ states. They start in $\exists$ state.

e.g.



Π_k-TIME$(t(n))$ — " — but start in $\forall$ state.





$$\Sigma_k^P = \bigcup_c \Sigma_k\text{-}\cancel{\text{TIME}}(n^c)$$

$$\Pi_k^P = \bigcup_c \Pi_k\text{-TIME}(n^c)$$

- $\Sigma_1 = NP$ $\qquad \Pi_1 = coNP$
- $BPP \subseteq \Sigma_2$

Pf: Alg A for $L \in BPP$ with error $\le \frac{1}{2^n}$.
running in time n^c

Σ_2-alg for L: on input x

1) guess existentially $a_1, a_2, \dots a_{n^c} \in \{0,1\}^{n^c}$
2) guess universally $r \in \{0,1\}^{n^c}$
check deterministically whether $\exists i \in [n]$
s.t. A accepts x with random bits
set to $r \oplus a_i$
bit-wise XOR

if such i exists $\rightarrow$ ACCEPT
o/w $\rightarrow$ REJECT

ma.

$\rightarrow \Sigma_2$ machine running in time $\simeq O(n^{\cdots})$

For $x \in \{0,1\}^n$ let $S_x = \{ r \in \{0,1\}^{n^c},$ A accepts x using random bits r $\}$

If $x \in L$ then $|S_x| \geq (1 - \frac{1}{2^n}) \cdot 2^{n^c}$

$\Rightarrow \exists a_1, \dots a_{n^c} \in \{0,1\}^{n^c}$ s.t.

$$\{0,1\}^n \subseteq \bigcup_{i=1}^{n} a_i \oplus S_x$$

$$\left(a_i \oplus S_x = \{ a_i \oplus r, \; r \in S_x \} \right)$$

Pf: for given $r \in \{0,1\}^{n^c}$, prob., that randomly chosen sequence $a_1, a_2, \dots a_{n^c}$ doesn't cover r in $\bigcup_{i=1}^{n} a_i \oplus S_x$

is at most $\left(\frac{1}{2^n}\right)^{n^c} \leq \left(\frac{1}{4}\right)^{n^c} \leq \frac{1}{2^{2n^c}}$.

Hence a random choice $a_1, \dots a_{n^c}$ covers all r with positive probability.

If $x \notin L$ then $|S_x| \leq \frac{2^{n^c}}{2^n}$

$$\Rightarrow \left| \bigcup_{i=1}^{n} a_i \oplus S_x \right| \leq \frac{2^{n^c}}{2^n} \cdot n = \frac{2^{n^c}}{n} < 2^{n^c}$$

$\Rightarrow$ it can never cover whole $\{0,1\}^{n^c}$.

Lemma: Let $S \subseteq \{0,1\}^m$ be s.t. $|S| \geq \frac{3}{4} \cdot 2^m$.

Then $\exists a_1, a_2, \ldots a_m \in \{0,1\}^m$ s.t.

$$\bigcup_{i=1}^{m} S \oplus a_i = \{0,1\}^m$$

i.e. $\forall r \in \{0,1\}^m \ \exists i \in [m]$ s.t. $r \oplus a_i \in S$

Pf: fix $r \in \{0,1\}^m$

$$\Pr_{a \in \{0,1\}^m}[r \in S \oplus a] = \Pr_a[r \oplus a \in S]$$

$$= \Pr_a[a \in S] \geq \frac{3}{4}$$

$$\Rightarrow \Pr_{a_1 \ldots a_m \in \{0,1\}^m}[\forall i \ \ r \notin S \oplus a_i] \leq \left(\frac{1}{4}\right)^m$$

$$\Rightarrow \exists a_1, \ldots a_m \in \{0,1\}^m \ \forall r \in \{0,1\}^m, \ r \in \bigcup_{i=1}^{m} S \oplus a_i$$

$\boxed{\text{QED}}$