On approximate majority and probabilistic time

Emanuele Viola

Institute for advanced study

January 2007

BPP vs. POLY-TIME HIERARCHY

- Probabilistic Polynomial Time (BPP):

  for every x, Pr [M(x) errs] $\leq$ 1/3

- Strong belief: BPP = P [NW,BFNW,IW,…]
  Still open: BPP $\subseteq$ NP ?

- Theorem [SG,L; '83]: BPP $\subseteq \Sigma_2$ P

- Recall

  NP = Σ_1 P $\rightarrow$ $\exists$ y M(x,y)

  Σ_2 P $\rightarrow$ $\exists$ y $\forall$ z M(x,y,z)

The problem we study

- More precisely [SG,L] give
  $BPTime(t) \subseteq \Sigma_2 Time(t^2)$

- Question[This Talk]:
  Is quadratic slow-down necessary?

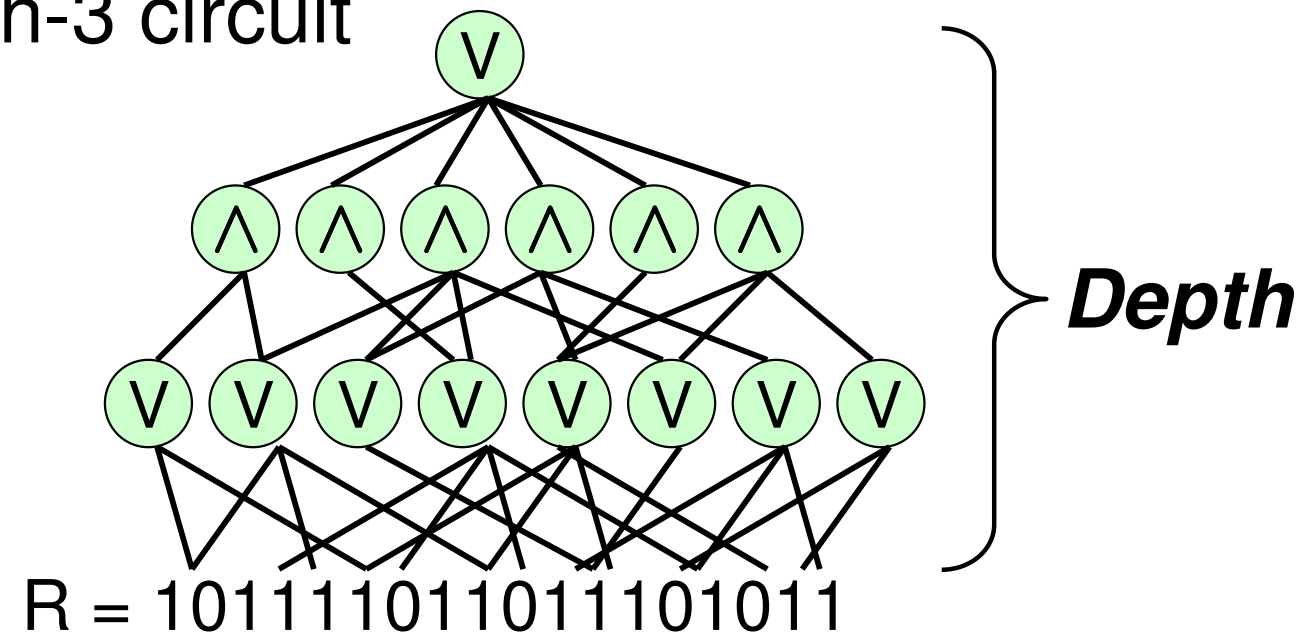
- Motivation: Lower bounds
  Know NTime ≠ Time on some models [P+,F,…]
  Technique: *speed-up* computation with quantifiers
  To prove NTime ≠ BPTime cannot afford $Time(t^2)$ [DvM]

Approximate Majority

- Input: R = 10111101101110101011
- Task: Tell $Pr_i[R_i = 1] \geq 2/3$ from $Pr_i[R_i = 1] \leq 1/3$

  Approximate: Do not care if $Pr_i[R_i = 1] \sim 1/2$

- Model: Depth-3 circuit



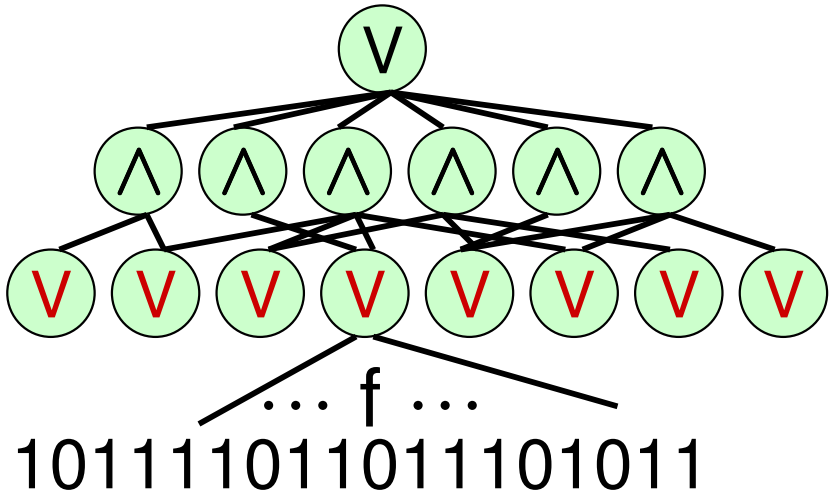
The connection [FSS]

$M(x;u) \in \text{BPTime}(t)$ ⇒ $R = 1101101111101011$, $|R| = 2^t$, $R_i = M(x;i)$

Compute M(x):

Tell $\Pr_u[M(x) = 1] \geq 2/3$ from $\Pr_u[M(x) = 1] \leq 1/3$ ⇒ Compute Appr-Maj

$\text{BPTime}(t) \subseteq \Sigma_2 \text{Time}(t') = \exists\,\forall\, \text{Time}(t')$ ⇒



Running time t'
– run M at most t'/t times

⇒ **Bottom fan-in f = t' / t**

Our Negative Result

- **Theorem[V] :** Small depth-3 circuits for Approximate Majority on N bits have bottom fan-in $\Omega(\log N)$

- **Corollary**: Quadratic slow-down necessary for relativizing techniques:

$$\text{BPTime}^{A}(t) \not\subseteq \Sigma_2\text{Time}^{A}(t^{1.99})$$

- Proof of Corollary:

  BPTime $(t) \subseteq \Sigma_2$ Time $(t') \Rightarrow$ [FSS]

  Appr-Maj on $N = 2^t$ bits $\in$ depth-3, bottom fan-in t' / t.

  By Theorem: $t' / t = \Omega(t)$.

Q.E.D.

Quasilinear-time simulation?

- Question: BPTime(t) $\subseteq \Sigma_3$ Time(t · polylog t) ?

  Related: Appr-Maj $\in$ depth-3 poly-size ?
  - arbitrary bottom fan-in

- Previous results & problems:

  [SG,L] Appr-Maj $\in$ depth-3 size $N^{\log N}$

  [A] Appr-Maj $\in$ depth-3 size poly(N) nonuniform

  [A] Appr-Maj $\in$ depth-O(1) size poly(N)

Our Positive Results

- **Theorem[V] :**
  There are uniform depth-3 poly(N)-size circuits for Approximate Majority on N bits
  - Uniform version of Ajtai's result

- **Theorem**[DvM,**V**]:
  BPTime (t) $\subseteq \Sigma_3$Time (t $\cdot$ $\log^5$ t)

Summary

	Appr-Maj on N bits	**BPTime(t)**
[SG,L]	$\in$ size $N^{\log N}$ depth 3	$\subseteq \Sigma_2 Time(t^2)$
[A]	$\in$ size poly(N) depth 3 non-uniform	----------
[A]	$\in$ size poly(N) depth O(1)	$\subseteq \Sigma_{O(1)} Time(t)$
[V]	$\notin$ size 2^{N^ε} depth 3 bottom fan-in $\varepsilon \cdot \log N$	$\not\subseteq \Sigma_2 Time(t^{1.99})$ w.r.t. oracle
[DvM,V]	$\in$ size poly(N) depth 3	$\subseteq \Sigma_3 Time(t \cdot \log^5 t)$

Rest of slides

- Proof of bottom fan-in lower bound

- Other result

  Σ_3Time (t) $\not\subseteq$ BPTime ($t^{1+o(1)}$)

  on restricted models

Our negative result

- **Theorem[V]:** $2^{N^{\varepsilon}}$-size depth-3 circuits for Approximate Majority on N bits have bottom fan-in $\Omega(\log N)$

- Switching lemmas fail
  Cannot use [H] for Approximate-Majority
  [SBI] $\Rightarrow$ bottom fan-in $\geq (\log N)^{1/2}$

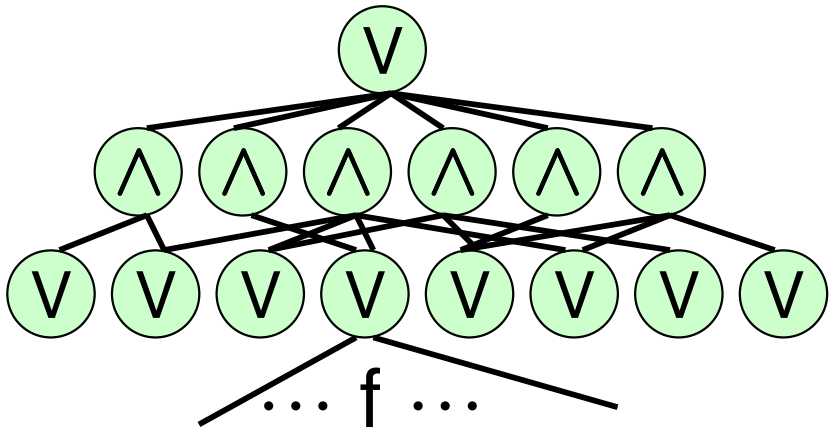
- Independently: [R] improves [SBI]
  alternative proof of theorem

- Note: No $2^{\Omega(N)}$ bound for depth-3 w/ bottom fan-in $\omega(1)$

Our Negative Result

- **Theorem[V]:** $2^{N^{\varepsilon}}$-size depth-3 circuits for Approximate Majority on N bits have bottom fan-in f = $\Omega(\log N)$

- Recall:



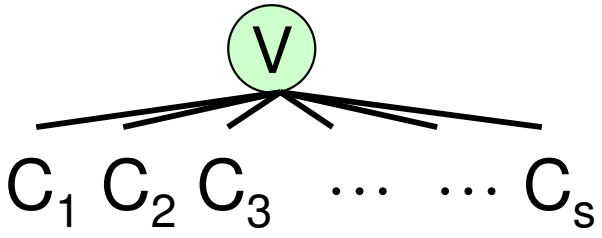
R = 10111101101110101011 |R| = N

Tells R $\in$ YES := { R : Pr_i [R_i = 1] $\geq$ 2/3 }

from R $\in$ NO := { R : Pr_i [R_i = 1] $\leq$ 1/3 }

Proof

- Circuit is OR of s depth-2 circuits



- By definition of OR :

  $R \in YES \Rightarrow$ some $C_i(R) = 1$

  $R \in NO \Rightarrow$ all $C_i(R) = 0$

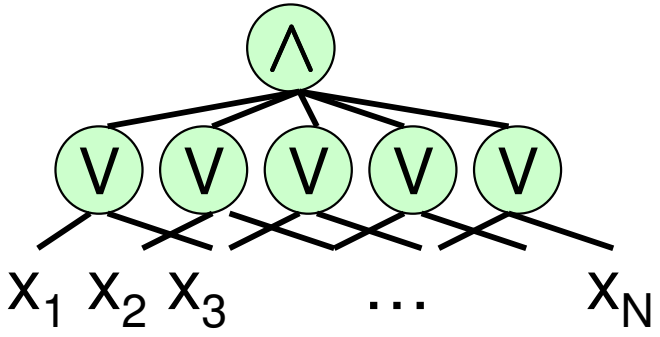
- By averaging, fix $C = C_i$ s.t.

$$\Pr_{R \in YES}[C(R) = 1] \geq 1/s$$
$$\forall R \in NO \Rightarrow C(R) = 0$$

- Claim: Impossible if C has bottom fan-in $\leq \varepsilon \log N$

CNF Claim

- Depth-2 circuit $\Rightarrow$ CNF



$(x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_4) \wedge (x_5 \vee x_3)$

bottom fan-in $\Rightarrow$ **clause** size

- **Claim:** All CNF C with clauses of size $\varepsilon \cdot \log N$

  Either $Pr_{R \in YES}[C(R) = 1] \leq 1 / 2^{N^{\varepsilon}}$
  or there is $R \in NO : C(R) = 1$

- Note: Claim $\Rightarrow$ Theorem

Either $Pr_{R \in YES}[C(R)=1] \leq 1/2^{N^{\varepsilon}}$ or $\exists R \in NO : C(R) = 1$

Proof Outline

- Definition: $S \subseteq \{x_1, x_2, \ldots, x_N\}$ is a covering if every clause has a variable in S

  E.g.: $S = \{x_3, x_4\}$ $C = (x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_4) \wedge (x_5 \vee x_3)$

- Proof idea: Consider **smallest** covering S

  Case |S| BIG : $Pr_{R \in YES}[C(R) = 1] \leq 1 / 2^{N^{\varepsilon}}$

  Case |S| tiny : Fix few variables and repeat

Either $\Pr_{R \in YES}[C(R)=1] \leq 1/2^{N^{\varepsilon}}$ or $\exists\, R \in NO : C(R) = 1$

Case |S| BIG

- $|S| \geq N^{\delta} \Rightarrow$ have $N^{\delta}/(\varepsilon \cdot \log N)$ disjoint clauses Γ_i
  - Can find Γ_i greedily

- $\Pr_{R \in YES}[C(R) = 1] \leq \Pr[\, \forall\, i, \Gamma_i(R) = 1\,]$

$$= \prod_i \Pr[\, \Gamma_i(R) = 1] \qquad \text{(independence)}$$

$$\leq \prod_i (1 - 1/3^{\varepsilon \log N}) = \prod_i \left(1 - 1/N^{O(\varepsilon)}\right)$$

$$= \left(1 - 1/N^{O(\varepsilon)}\right)^{|S|} \leq e^{-N^{\Omega(1)}}$$ ✓

Either $Pr_{R \in YES}[C(R)=1] \leq 1/2^{N^{\varepsilon}}$ or $\exists R \in NO : C(R) = 1$

Case |S| tiny

- $|S| < N^{\delta}$ $\Rightarrow$ Fix variables in S
  - Maximize $Pr_{R \in YES}[C(R)=1]$

- Note: S covering $\Rightarrow$ clauses shrink

  Example

  $(x_1 \vee x_2 \vee x_3) \wedge (\neg x_3) \wedge (x_5 \vee \neg x_4)$ $\xrightarrow{x_3 \leftarrow 0,\ x_4 \leftarrow 1}$ $(x_1 \vee x_2) \wedge (x_5)$

- Repeat

  Consider smallest covering S', etc.

Either $Pr_{R \in YES}[C(R)=1] \leq 1/2^{N^{\varepsilon}}$ or $\exists R \in NO : C(R) = 1$

Finish up

- Recall: Repeat $\Rightarrow$ shrink clauses
  So repeat at most $\varepsilon \cdot \log N$ times

- When you stop:
  Either smallest covering size $\geq N^{\delta}$ ✓
  Or C = 1
    Fixed $\leq (\varepsilon \cdot \log N)\, N^{\delta} \ll N$ vars.
    Set rest to 0 $\Rightarrow R \in NO : C(R) = 1$ ✓

Q.E.D.

Rest of slides

- Proof of bottom fan-in lower bound

- Other result

  Σ_3Time (t) $\not\subseteq$ BPTime ($t^{1+o(1)}$)

  on restricted models

The model Time_1

Input

$$(x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_4) \wedge (x_5 \vee x_3) \wedge (x_1 \vee x_6 \vee \neg x_3)$$

Random access

0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0

Sequential access work tape

Time Lower Bound for SAT

- Theorem [MS,vMR]: NTime (n) $\not\subseteq$ Time_1 ($n^{1.22}$)

- Note: ``combinatorics'' does not work
  - Palindromes $\in$ Time_1 ($n^{1+o(1)}$)

- Proof by contradiction:

  Suppose NTime(n) $\subseteq$ Time_1 ($n^{1.22}$)

  $\subseteq \Sigma_{O(1)}$ Time($n^{0.1}$) (speed-up with quantifiers)

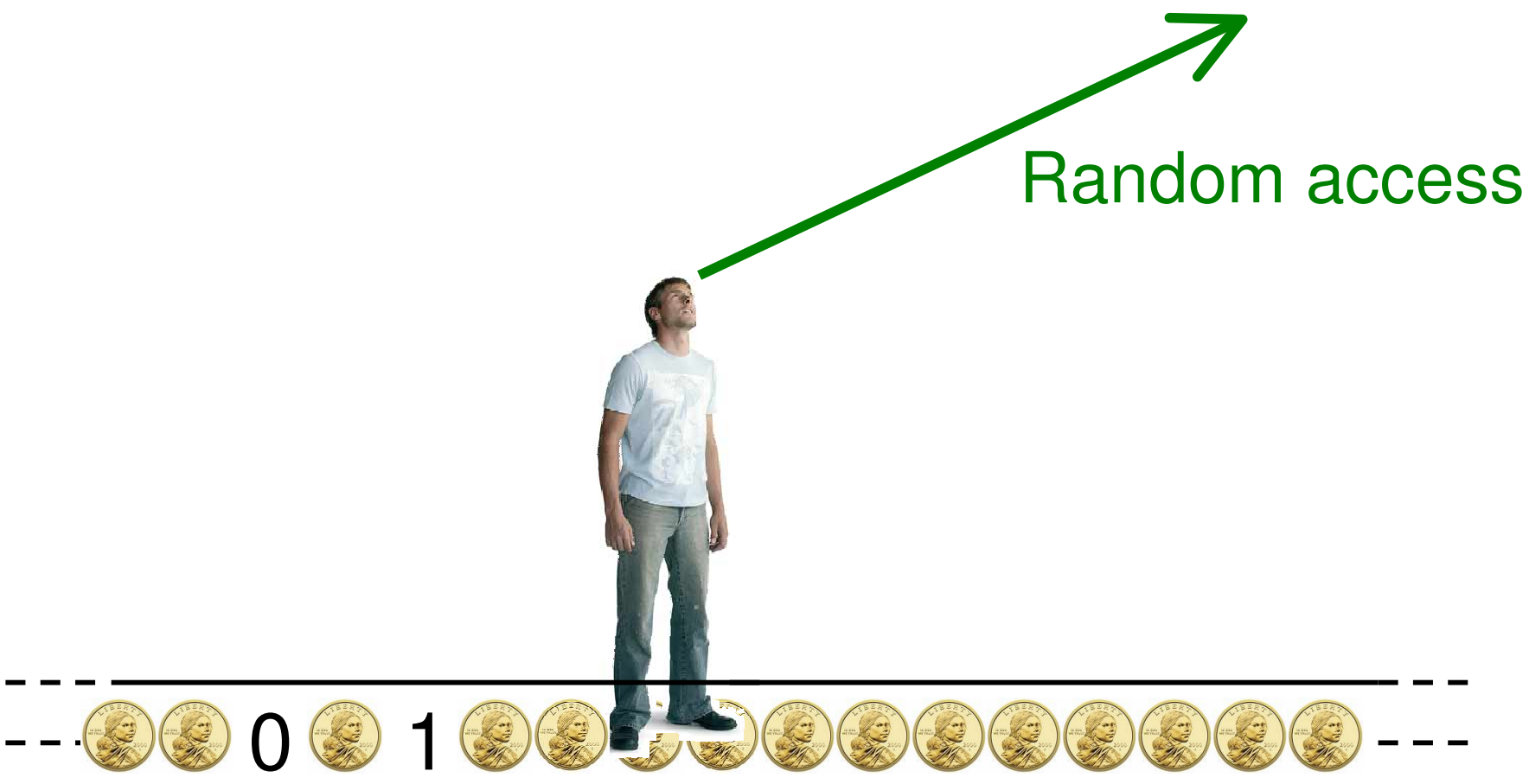
  $\subseteq$ NTime($n^{0.9}$) (collapse by assumption)

  Contradicts NTime hierarchy Q.E.D.

The model $BPTime_1$

Input

$$(x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_4) \wedge (x_5 \vee x_3) \wedge (x_1 \vee x_6 \vee \neg x_3)$$



Sequential access work tape with coins

Our BPTime Lower Bound for Σ_3

- Theorem [V] : $\Sigma_3 \text{Time}(n) \not\subseteq \text{BPTime}_1(n^{1+o(1)})$
- Proof by contradiction (Inspired by [DvM]):

  Suppose $\Sigma_3 \text{Time}(n) \subseteq \text{BPTime}_1(n^{1+o(1)})$

  $\subseteq \text{BP}^{n^{0.9}}\text{Time}_1(n^{1+o(1)})$ (derandomize [INW])

  $\subseteq \Sigma_3 \text{Time}(n^{.99})$ ([**V**] + [MS])

  Contradicts Σ_3 Time hierarchy Q.E.D.

- Note: Quadratic slow-down $\Rightarrow$ won't work for Σ_2

Seen so far

- Theorem[SG,L]: BPTime(t) $\subseteq \Sigma_2$Time(t^2)
  - Related to Approximate Majority

	Appr-Maj on N bits	**BPTime(t)**
[**V**]	~~$\in$~~ size $2^{N^{\varepsilon}}$ depth 3 bottom fan-in $\varepsilon \cdot \log N$	~~$\subseteq$~~ Σ_2Time ($t^{1.99}$) w.r.t. oracle
[DvM,**V**]	$\in$ size poly(N) depth 3 uniform	$\subseteq \Sigma_3$Time ($t \cdot \log^5 t$)

- Theorem [V] : Σ_3Time (n) ~~$\subseteq$~~ BPTime_1 ($n^{1+o(1)}$)