On approximate majority and probabilistic time

Emanuele Viola

Institute for advanced study

Work done during Ph.D. at Harvard University

June 2007

BPP vs. POLY-TIME HIERARCHY

- Probabilistic Polynomial Time (BPP):

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

- Belief: BPP = P [Babai Fortnow Impagliazzo Nisan Wigderson …]
  Still open: BPP $\subseteq$ NP ?

- Theorem[Sipser & Gacs, Lautemann; '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

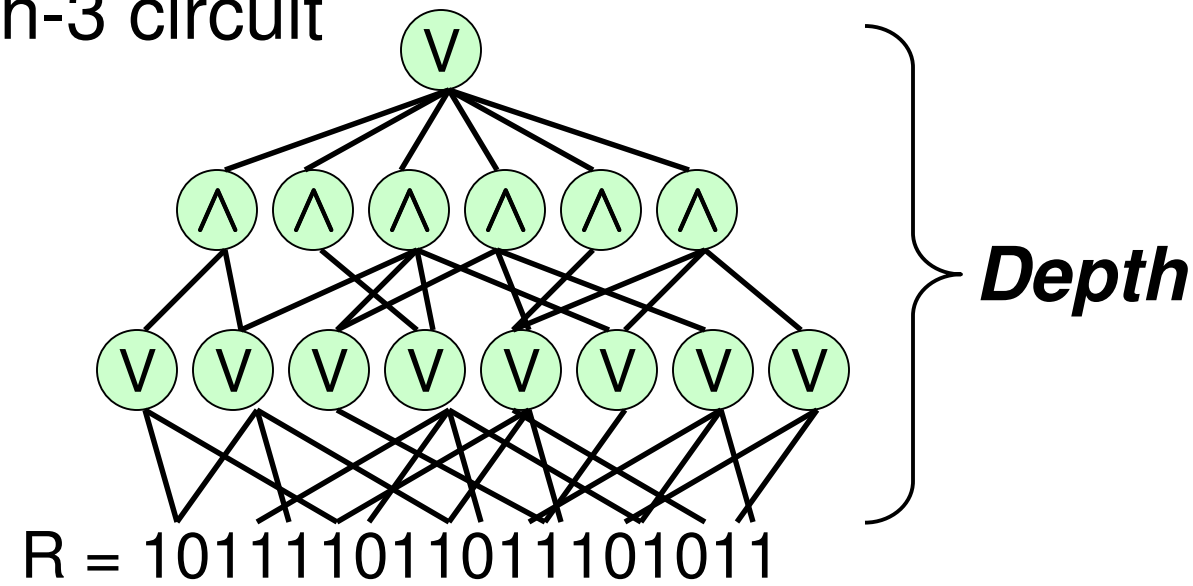
  To prove NTime ≠ BPTime cannot afford $Time(t^2)$

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



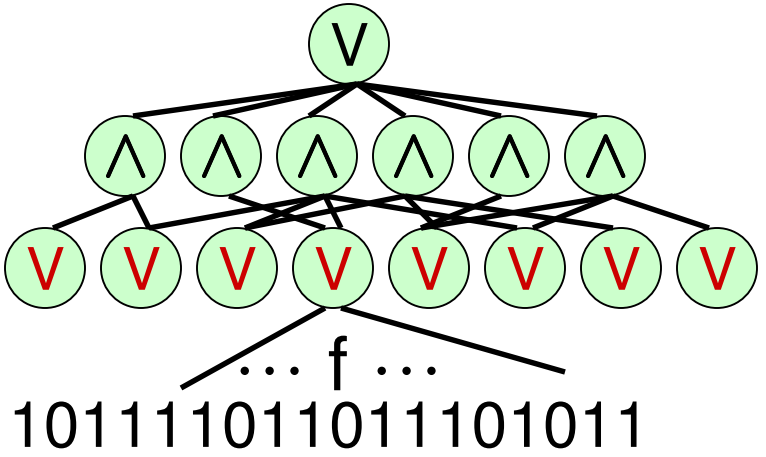
The connection [Furst Saxe Sipser]

$M(x;u) \in BPTime(t)$ ⇒ $R = 1101101110101011$, $|R| = 2^t$, $R_i = M(x;i)$

Compute M(x):

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

$BPTime(t) \subseteq \Sigma_2 Time(t') = \exists \forall Time(t')$ ⇒



Running time t' ⇒ **Bottom fan-in f = t' / t**

– run M at most t'/t times

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 $\cdot$ polylog t) ?

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

- Previous results & problems:

  [Sipser & Gacs, Lautemann] Appr-Maj $\in$ depth-3 size $N^{\log N}$

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

  [Ajtai] 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**[Diehl & van Melkebeek, 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	$\subseteq \Sigma_2\text{Time}(t^2)$
[A]	$\in$ size poly(N) depth 3 non-uniform	---
[A]	$\in$ size poly(N) depth O(1)	$\subseteq \Sigma_{O(1)}\text{Time}(t)$
[V]	~~$\in$~~ size $2^{N^{0.1}}$ depth 3 bottom fan-in $\varepsilon \cdot \log N$	~~$\subseteq$~~ $\Sigma_2\text{Time}(t^{1.99})$ w.r.t. oracle
[DvM,V]	$\in$ size poly(N) depth 3	$\subseteq \Sigma_3\text{Time}(t \cdot \log^5 t)$

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]:** $2^{N^{0.1}}$-size depth-3 circuits for N-bit Approximate Majority have bottom fan-in $\Omega(\log N)$

- Switching lemmas fail:

  Cannot use [Hastad] for Approximate-Majority

  [Segerlind Buss Impagliazzo] $\Rightarrow$ bottom fan-in $\geq (\log N)^{1/2}$

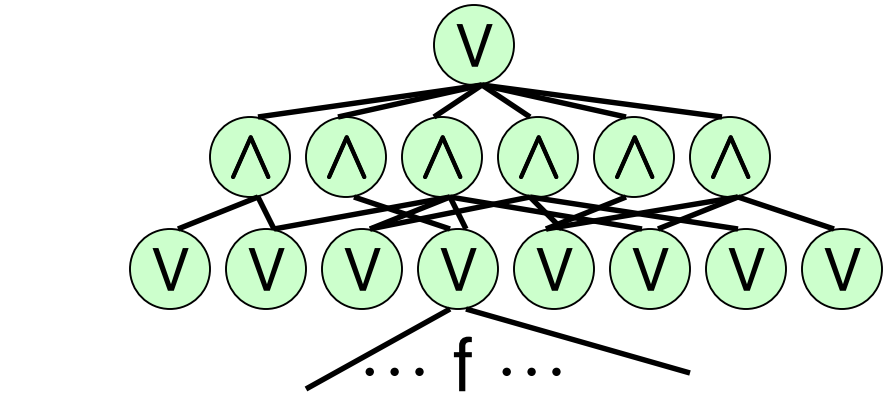
- [Razborov] improves [SBI], alternative proof of theorem

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

Our negative result

- **Theorem[V]:** $2^{N^{0.1}}$-size depth-3 circuits for N-bit Approximate Majority have bottom fan-in f = $\Omega(\log N)$

- Recall:

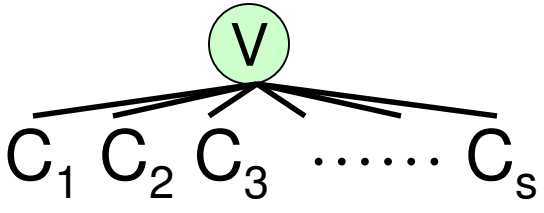


Tells $R \in$ YES := $\{ R : Pr_i [R_i = 1] \geq 2/3 \}$

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

Proof

- Circuit is OR of $s = 2^{N^{0.1}}$ CNF
  E.g. $C_i=(x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_4) \wedge (x_5 \vee x_3)$
  Bottom fan-in $\Rightarrow$ clause size



- 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 CNF $C = C_i$ s.t.

$$\Pr_{R \in YES}[C(R) = 1] \geq 1/s = 1/2^{N^{0.1}}$$
$$\forall R \in NO \Rightarrow C(R) = 0$$

- Claim: Impossible if C has clauses of size $\varepsilon \cdot \log N$

Either $Pr_{R \in YES}[C(R)=1] \leq 1/2^{N^{0.1}}$ 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 : $Pr_{R \in YES}[C(R) = 1] \leq 1 / 2^{N^{0.1}}$

  Case |S| tiny : Fix few variables and repeat

Either $\Pr_{R \in YES}[C(R)=1] \leq 1/2^{N^{0.1}}$ 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 $Pr_{R \in YES}[C(R)=1] \leq 1/2^{N^{0.1}}$ 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 $\Pr_{R \in YES}[C(R)=1] \leq 1/2^{N^{0.1}}$ 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

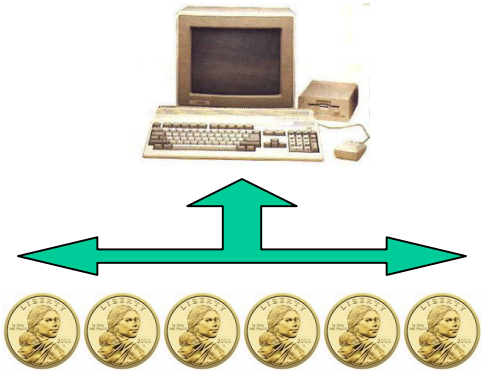
  Σ_3Time (t) $\not\subseteq$ BPTime ($t^{1+o(1)}$)

  on restricted models

Lower bounds on probabilistic models

- Space-bounded, probabilistic models
- [Ajtai, Beame Saks Sun Vee] $n \log^{0.5} n$ time lower bound
  - branching programs
- [Allender Koucký Ronneburger Roy Vinay, Diehl & van Melkebeek] $n^{1+\Omega(1)}$ time lower bounds
  one-way randomness

- Theor.[V]: Σ_3Time (n) $\not\subseteq$ BPTime($n^{1+o(1)}$)
  two-way randomness (sequential)
  - Proof uses our positive result
  - Our negative result is obstacle for Σ_2



Conclusion

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

	Appr-Maj on N bits	**BPTime(t)**
[V]	~~$\in$~~ size $2^{N^{0.1}}$ 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($n^{1+o(1)}$)
  two-way access to randomness

Thank you!