

On Probabilistic Time versus Alternating Time

Emanuele Viola
Harvard University

March 2006

BPP vs. POLY-TIME HIERARCHY

- Probabilistic Polynomial Time (BPP):
for every x , $\Pr [M(x) \text{ errs }] \leq 1/3$
- Strong belief: $BPP = P$ [NW,BFNW,IW,...]
Still open: $BPP \subseteq NP$?
- **Theorem** [SG,L; '83]: $BPP \subseteq \Sigma_2 P$
- Recall
$$\begin{array}{l} NP = \Sigma_1 P \quad \rightarrow \quad \exists y M(x,y) \\ \Sigma_2 P \quad \quad \rightarrow \quad \exists y \forall z M(x,y,z) \end{array}$$

The Problem we Study

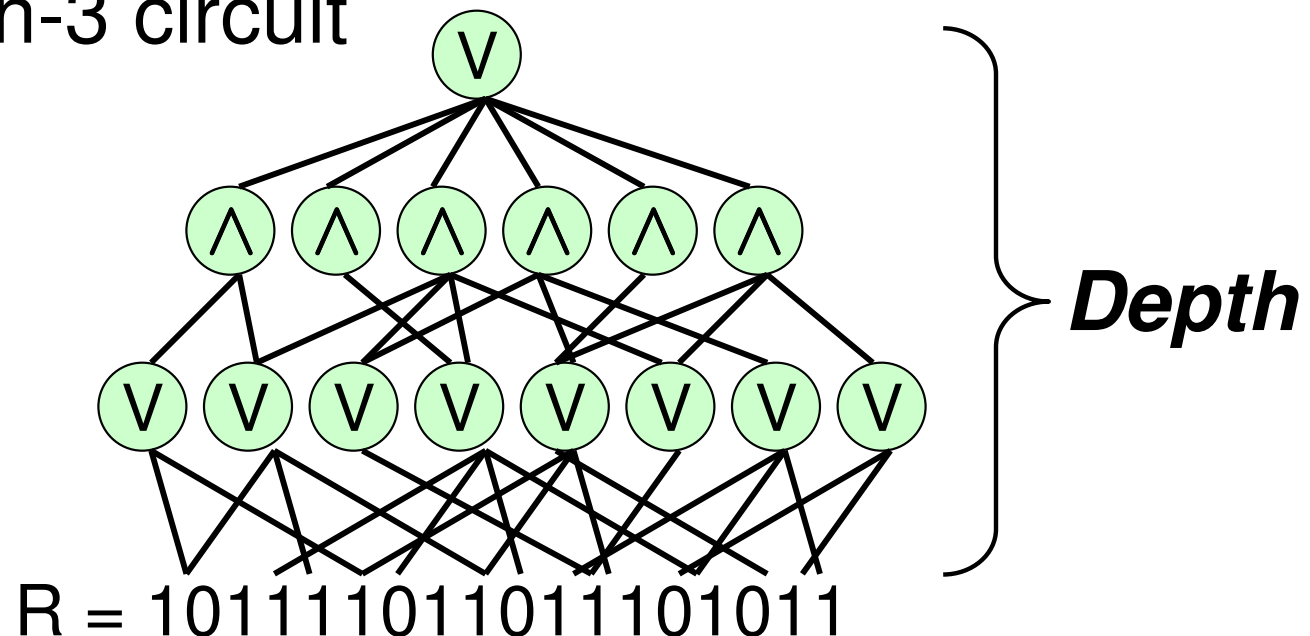
- More precisely [SG,L] give
$$\text{BPTime}(t) \subseteq \Sigma_2\text{Time}(t^2)$$
- Question[This Talk]:
Is **quadratic slow-down** necessary?
- Motivation: Lower bounds
Know $\text{NTime} \neq \text{Time}$ on some models [P+,F+,...]
Technique: *speed-up* computation with quantifiers
To prove $\text{NTime} \neq \text{BPTime}$ cannot afford $\text{Time}(t^2)$ [DvM]

Approximate Majority

- Input: $R = 101111011011101011$
- Task: Tell $\Pr_i [R_i = 1] \geq 2/3$ from $\Pr_i [R_i = 1] \leq 1/3$

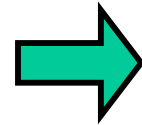
Do not care if $\Pr_i [R_i = 1] \sim 1/2$ (approximate)

- Model: Depth-3 circuit



The connection [FSS]

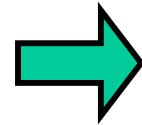
$M(x;u) \in \text{BPTime}(t)$



$R = 11011011101011$
 $|R| = 2^t \quad \curvearrowright \quad R_i = M(x;i)$

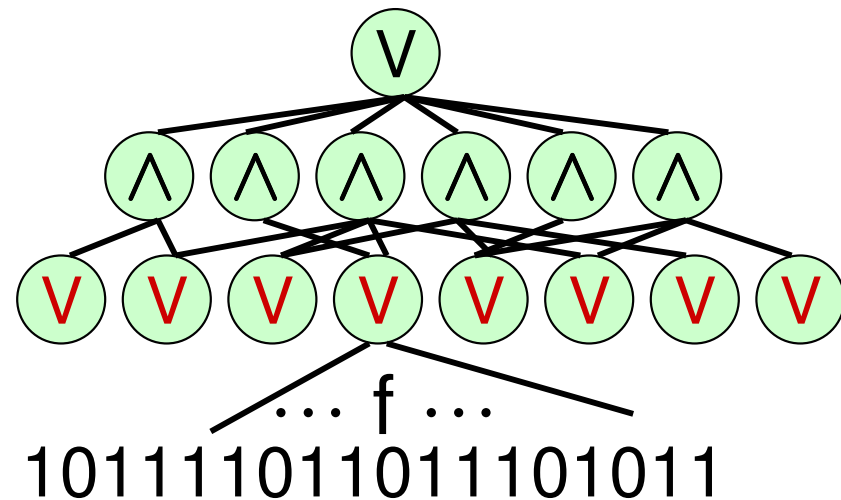
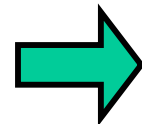
Compute $M(x)$:

Tell $\Pr_u[M(x) = 1] \geq 2/3$
from $\Pr_u[M(x) = 1] \leq 1/3$



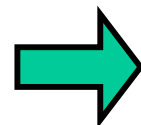
Compute Appr-Maj

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



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:

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

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:** $\text{BPTIME}(t) \subseteq \Sigma_3 \text{Time}(t \cdot \text{polylog } t)$?

Related: $\text{Appr-Maj} \in \text{depth-3 poly-size}$?

– arbitrary bottom fan-in

- Previous results & **problems:**

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

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

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

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]:**

$\text{BPTime}(t) \subseteq \Sigma_3\text{Time}(t \cdot \log^5 t)$

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 $\text{poly}(N)$ depth 3 non-uniform	-----
[A]	\in size $\text{poly}(N)$ depth $O(1)$	$\subseteq \Sigma_{O(1)} \text{Time}(t)$
[V]	\in size 2^{N^ϵ} depth 3 bottom fan-in $\epsilon \cdot \log N$	$\subseteq \Sigma_2 \text{Time}(t^{1.99})$ w.r.t. oracle
[DvM, V]	\in size $\text{poly}(N)$ depth 3	$\subseteq \Sigma_3 \text{Time}(t \cdot \log^5 t)$

Rest of this talk

- Proof of bottom fan-in lower bound

- Other result

$$\Sigma_3 \text{Time}(t) \not\subseteq \text{BPTime}(t^{1+o(1)})$$

on restricted models

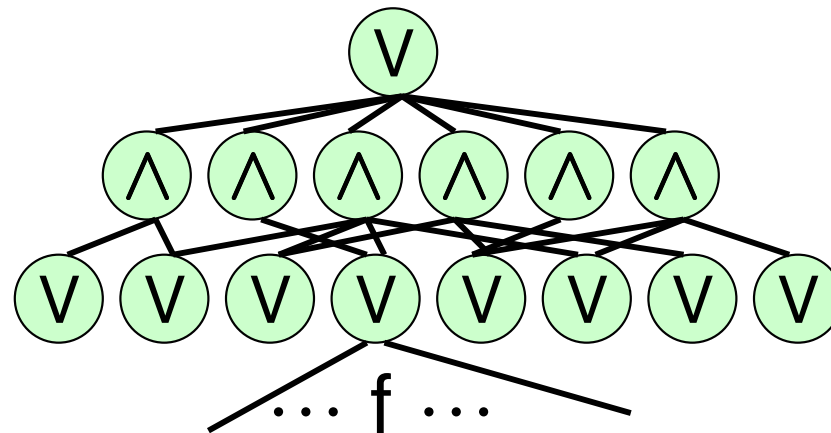
Our Negative Result

- **Theorem[V]:** 2^{N^ϵ} -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 $\geq (\log N)^{1/2}$
- Note: No known $2^{\Omega(N)}$ size lower bound for depth-3 circuits w/ bottom fan-in $\omega(1)$

Our Negative Result

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

- Recall:



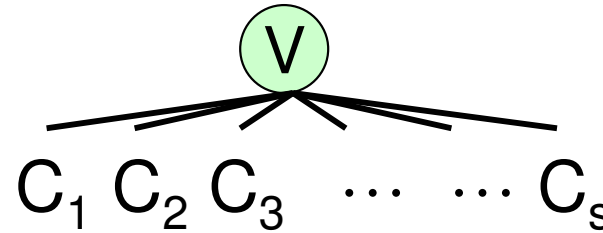
$R = 101111011011101011 \quad |R| = N$

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

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

Proof

- Circuit is OR of s depth-2 circuits



- By definition of OR :

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

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

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

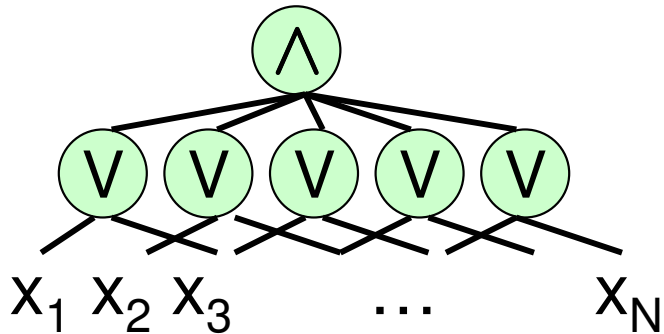
$$\Pr_{R \in \text{YES}} [C(x) = 1] \geq 1/s$$

$$\forall R \in \text{NO} \Rightarrow C(R) = 0$$

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

- Note: Claim \Rightarrow Theorem

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

Proof Outline

- **Definition:** $S \subseteq \{x_1, x_2, \dots, x_N\}$ 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 : $\Pr_{R \in \text{YES}} [C(x) = 1] \leq 1 / 2^{N^\epsilon}$

Case $|S|$ tiny : Fix few variables and repeat

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

Case $|S|$ BIG

- $|S| \geq N^\delta \Rightarrow$ have $N^\delta / (\epsilon \cdot \log N)$ **disjoint** clauses Γ_i
 - Can find Γ_i greedily
- $\Pr_{R \in \text{YES}} [C(R) = 1] \leq \Pr [\forall i, \Gamma_i(R) = 1]$
 - $= \prod_i \Pr[\Gamma_i(R) = 1]$ (independence)
 - $\leq \prod_i (1 - 1/3^{\epsilon \log N}) = \prod_i (1 - 1/N^{O(\epsilon)})$
 - $= (1 - 1/N^{O(\epsilon)})^{|S|} \leq e^{-N^{\Omega(1)}} \quad \checkmark$

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

Case $|S|$ tiny

- $|S| < N^\delta \Rightarrow$ Fix variables in S
 - Maximize $\Pr_{R \in \text{YES}} [C(x)=1]$
- Note: S **covering** \Rightarrow clauses shrink

Example

$$(x_1 \vee x_2 \vee x_3) \wedge (\neg x_3) \wedge (x_5 \vee \neg x_4) \quad \begin{array}{l} x_3 \leftarrow 0 \\ x_4 \leftarrow 1 \end{array} \Rightarrow (x_1 \vee x_2) \wedge (x_5)$$

- Repeat
 - Consider smallest covering S' , etc.

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

Finish up

- Recall: Repeat \Rightarrow shrink clauses
So repeat at most $\epsilon \cdot \log N$ times
- When you stop:
 - Either smallest covering size $\geq N^\delta$ ✓
 - Or $C = 1$
 - Fixed $\leq (\epsilon \cdot \log N) N^\delta \ll N$ vars.
 - Set rest to 0 $\Rightarrow R \in \text{NO} : C(R) = 1$ ✓

Q.E.D.

Rest of this talk

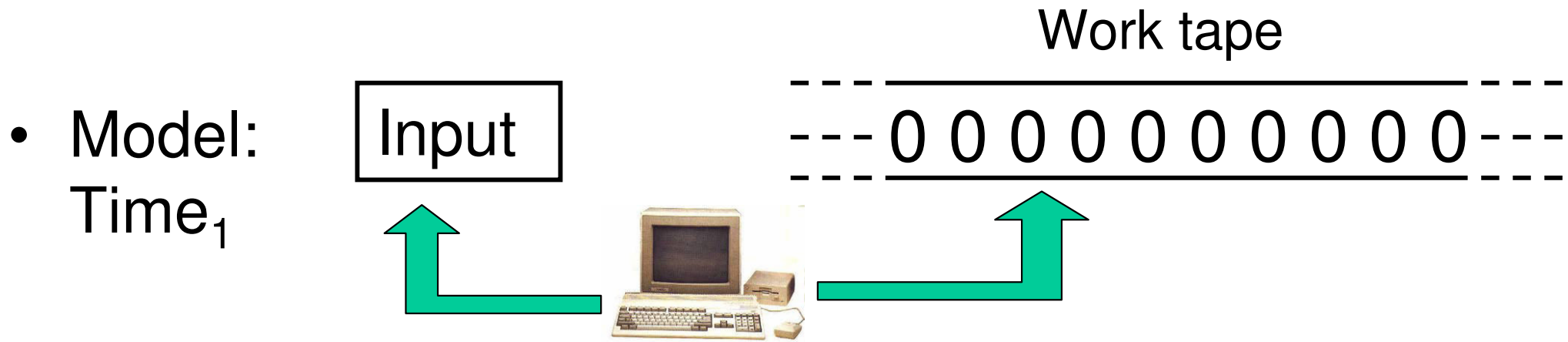
- Proof of bottom fan-in lower bound

- Other result

$\Sigma_3 \text{Time}(t) \not\subseteq \text{BPTime}(t^{1+o(1)})$

on restricted models

Time Lower Bound for SAT



• **Theorem** [MS,vMR]: $\text{NTime}(n) \not\subseteq \text{Time}_1(n^{1.22})$

• Proof (by contradiction):

$$\text{NTime}(n) \subseteq \text{Time}_1(n^{1.22})$$

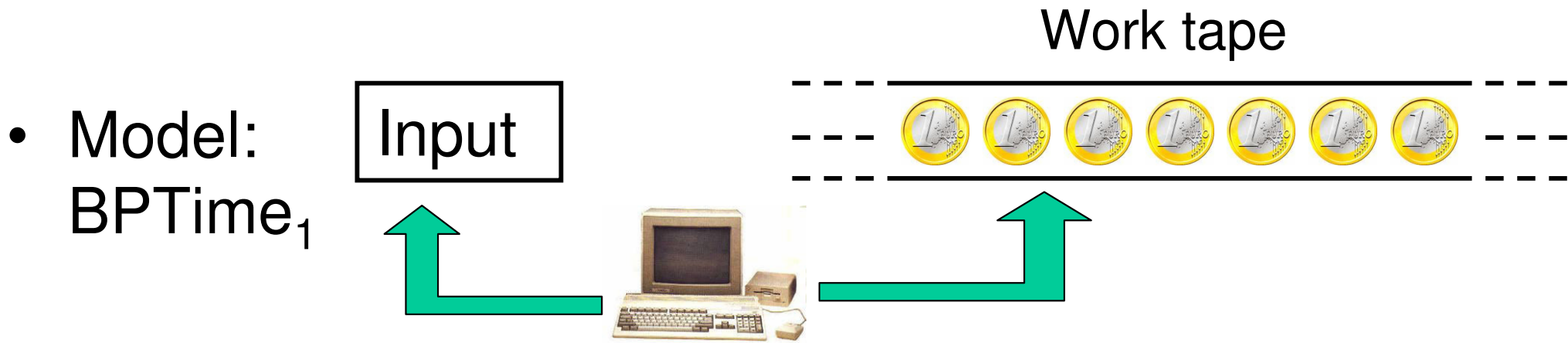
$$\subseteq \Sigma_{O(1)} \text{Time}(n \cdot 1) \quad (\text{speed-up with quantifiers})$$

$$\subseteq \text{NTime}(n \cdot 9) \quad (\text{collapse by assumption})$$

Contradiction with NTime hierarchy

Q.E.D.

Our BPTIME Lower Bound for Σ_3



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

$$\begin{aligned} \Sigma_3 \text{Time}(n) &\subseteq \text{BPTIME}_1(n^{1+o(1)}) \\ &\subseteq \text{BP}^{n^\epsilon} \text{Time}_1(n^{1+o(1)}) \quad (\text{derandomize [INW]}) \\ &\subseteq \Sigma_3 \text{Time}(n \cdot 9) \quad (\text{collapse [DvM, V]}) \quad \text{Q.E.D.} \end{aligned}$$
- Note: Quadratic slow-down in $\Sigma_2 \Rightarrow$ idea won't work for Σ_2

Conclusion

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

	Appr-Maj on N bits	BPTime(t)
[V]	\in size 2^{N^ϵ} depth 3 bottom fan-in $\epsilon \cdot \log N$	\subseteq $\Sigma_2\text{Time}(t^{1.99})$ w.r.t. oracle
[DvM, V]	\in size $\text{poly}(N)$ depth 3 uniform	$\subseteq \Sigma_3\text{Time}(t \cdot \log^5 t)$

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