Tighter Circuit Lower Bounds for MA/1 With Efficient PCPs

Based on a Joint Work of Joshua Cook and Dana Moshkovitz
Main Result

∃ a > 1 and g(n) = o(1) such that ∀ k < a

\[ \text{MATIME}[n^{k+g(n)}]/1 \not\subset \text{SIZE}[O(n^k)] \]

- Super linear circuit lower bound.
- MA is similar to NP.
- Tighter parameters than previous results.
Explaining Our Result
Circuit Definition

Circuits have NOT, AND, OR gates, fan in at most 2.

SIZE[f(n)] are languages computable by families of circuits with f(n) gates.

Non uniform, circuits may be hard to find.
Uniform vs Non-Uniform

Uniform
• Fast Algorithm
• Constant Description
• No Preprocessing
• Static Program

Non-Uniform
• Fast Algorithm
• New Description For Every Input Size
• Precomputed
• Contains Unary Halting: HALT*
Circuit bounds

SPACE[T]: Programs That Use T bits of RAM

By Search:
For $2^n/n > T_1 > T_0$, $\text{SPACE}[T_1] \not\subseteq \text{SIZE}[T_0]$

$\text{HALT}^* \in \text{SIZE}[O(1)]$

$\text{HALT}^* \notin R$
Hope And Dream

Fear And Dread

TIME[n^6] SIZE[n^6]
TIME[n^5] SIZE[n^5]
TIME[n^4] SIZE[n^4]
TIME[n^3] SIZE[n^3]
TIME[n^2] SIZE[n^2]
TIME[n] SIZE[n]

SPACE[n^5] SIZE[n^5]
SPACE[n^4] SIZE[n^4]
SPACE[n^3] SIZE[n^3]
SPACE[n^2] SIZE[n^2]
SPACE[n] SIZE[n]
TIME[2^n]
Towards Our Dreams

TIME circuit lower bounds hard?
Try NTIME!
Still too hard?
Try MATIME!
What is MATIME[T]?

MA, ‘Merlin Arthur’.
All Powerful Merlin Sends Proof.
Arthur Verifies in Time T with Randomness.
Previous MA Lower Bounds
Santhanam, for some constant c, for all k:
\[ \text{MATIME}[n^{ck}]/1 \not\subseteq \text{SIZE}[O(n^k)]. \]

For some L
\[ \text{MATIME}[n^{ck}]/1 \]
\[ \text{SIZE}[n^k] \]

Might Still Have
\[ \text{SIZE}[n] \]
\[ \text{MATIME}[n^4]/1 \]
Removing c!

We remove the factor of c, well, *almost*.

\[ \text{MATIME}[n^{k+g(n)}]/1 \subsetneq \text{SIZE}[O(n^k)]. \]

- Has a subconstant, \( g(n) = o(1) \).
- Only works for some \( k > 1 \), not all \( k \).
What is “/1” in MATIME[T]/1?

A bit of trusted advice per input length.

A bit of non-uniformity.

Precomputing, Single Bit Result.
How to get Circuit Lower Bounds
Interactive Proofs (IPs)?

Untrusted Merlin
Randomized Arthur.

Many Questions and Answers.

$\text{IVTIME}[T]$: Arthur time $T$. 
How powerful is IP?

Shamir 92 proved IP = PSPACE!

\[
\text{SPACE}[n] \subseteq \text{IVTIME}[n^4]
\]

\[
\text{IVTIME}[n] \subseteq \text{SPACE}[n]
\]

Prover’s for IP also small space!

Circuit bounds for SPACE apply to IP!
Main Idea

Use a Circuit as Merlin in IP.

Merlin Gives a Circuit
Arthur Uses it to run IP
Santhanam’s Proof

If $\text{PSPACE} \subseteq \text{P/poly}$

Problem in $\text{SPACE}[n^k]$

Hard for $\text{SIZE}[o(n^k)]$

Guess Circuit for Prover

PSPACE $\not\subseteq \text{P/poly}$

$\text{SPACE}[n] \not\subseteq \text{SIZE}[n^k]$

Pad $\text{SPACE}[n]$ till prover has $\text{SIZE}[n^k]$
PSPACE \not\subseteq \mathsf{P/poly} Comments
Bit of Advice Needed for Pad Length.
Already Efficient, Case Unchanged by Us.
PSPACE \subseteq P/poly Analysis

\[
PSPACE \subseteq P/poly \quad \rightarrow \quad SPACE[n] \subseteq SIZE[n^a]
\]

\[
L \in SPACE[n^k] \quad \rightarrow \quad L \text{ IP Verifier Time } n^{4k}
\]

\[
SPACE[n] \subseteq SIZE[n^a] \quad \rightarrow \quad L \text{ Prover Space } n^{4k}
\]

\[
L \text{ IP Verifier Time } n^{4k} \quad \rightarrow \quad n^{4k} \text{ Prover Queries}
\]

\[
L \text{ MA Verifier Time} \quad \rightarrow n^{4k} + n^{4k} n^{a4k} = n^{(a+1)4k}
\]
Areas for improvement?

\[ \text{SPACE}[n^k] \subseteq \text{MATIME}[n^{(a+1)4k}] \]

- a? Overhead From Circuit for SPACE.
  - Add Case Where \( \text{SPACE}[n] \subseteq \text{SIZE}[n^{1+o(1)}] \)

- +1? Too many Queries.
  - Use Low Query PCP.

- 4? IP Verifier is Slow.
  - Use Very Efficient PCP.
PCP: Non Adaptive Proof Faster Verification
IP vs PCP (or IP vs MIP)

- PCP Prover Strategy Non-Adaptive
  - Prover Can’t Use Past Questions
  - New Prover Per Query
- PCP Can Use Fewer Queries
- PCP Is Faster
- Circuit Has No Memory, is PCP, not IP!
Example: Graph Three Coloring

Assign Each Vertex a Color: Red, Green, or Blue.

Make Adjacent Vertices Different Colors.
Bad
Green touching

Bad
Uses 5 Colors

Good
3 Colors,
No touching
Grötzsch graph

IP

PCP

ERROR!
Main Take Away
Fast Protocols Give Lower Bounds

Circuit Lower Bounds From Fast Verification / Algorithms
• Santhanam 2007 (Prior Work)
  – Circuit lower bound for MA/1
  – Through Efficient Interactive Proofs PSPACE
• Williams 2010
  – ACC Lower Bounds For NEXP
  – Through Fast SAT algorithms for ACC
• Murray Williams 2018
  – ACC Bounds for NQP
  – Through Interactive Proofs AND SAT algorithms
Second Result, Main Lemma

For L computable in time T and space S,

There is a PCP with

- Verifier time $\sim n + \log(T)$,
- $\text{polylog}(n + \log(T))$ Queries
- and Prover space $\sim n + S$, 
PCP Performance

For time T, space S algorithm

Old: Either verifier time $\sim n + \log(T)^2$
     Queries $\sim \log(T)$

New: Verifier time $\sim n+\log(T)$, Prover
     space $\sim n+S$, $\log(n+\log(T))$ Queries.
Citations