Logic and Semantics seminar, University of Cambridge
10 May 2019

Hardness magnification near state-of-the-art lower bounds

Ján Pich

Department of Computer Science
University of Oxford

based on a joint paper with
Igor C. Oliveira and Rahul Santhanam
+ early fragments from a joint work with
L.Chen, S.Hirahara, I.C.Oliveira, N.Rajgopal and R.Santhanam

Hardness magnification

In short:

a strategy for deriving strong circuit lower bounds from lower bounds for weaker models

e.g.

$$n^{1.1}\text{-size formula lower bounds on a variant of MCSP}$$
$$\Rightarrow$$
$$\mathsf{NP} \not\subseteq \mathsf{NC}^1$$

◦ proposed by Oliveira-Santhanam (2018)

◦ seems to avoid the natural proofs barrier of Razborov and Rudich

Core issue: Minimum Circuit Size Problem (MCSP)

Definition:

$$\mathrm{MCSP}(\mathrm{tt}(f), s) = 1 \quad \Leftrightarrow \quad f \in \mathrm{Circuit}[s]$$

- $\mathrm{tt}(f)$: truth-table of a Boolean function $f : \{0,1\}^n \mapsto \{0,1\}$
- s: size parameter
- $\mathrm{Circuit}[s]$: circuits of size s

◦ **fundamental** problem with a history preceeding NP-completeness
◦ **many natural variants**: succinct, average-case, gap version, . . .
◦ **meta-computational character** explored in many structural results:
e.g. natural proofs barrier, hardness amplification, learning algorithms

Initial Magnification Theorem

Oliveira-Santhanam (2018): $(s = 2^{\sqrt{n}}, t = 9s\log s, N = 2^n)$

$$\text{succinct-MCSP}[s,t] \in \mathsf{NC}^1 \quad \Rightarrow \quad (1, 2/3)\text{-MCSP}[s] \in \text{Formula}[N^{1.1}]$$

Initial Magnification Theorem

Oliveira-Santhanam (2018): $(s = 2^{\sqrt{n}}, t = 9s \log s, N = 2^n)$

$$\text{succinct-MCSP}[s, t] \in \mathsf{NC}^1 \quad \Rightarrow \quad (1, 2/3)\text{-MCSP}[s] \in \text{Formula}[N^{1.1}]$$

$$\uparrow$$

input: $y_1, f(y_1), \ldots, y_t, f(y_t)$

$y_i \in \{0,1\}^n, f(y_i) \in \{0,1\}$

output: $1 \Leftrightarrow \exists$ s-size circuit C s.t.

$$\bigwedge_{i \leq t} C(y_i) = f(y_i)$$

Initial Magnification Theorem

Oliveira-Santhanam (2018): $(s = 2^{\sqrt{n}}, t = 9s \log s, N = 2^n)$

$$\text{succinct-MCSP}[s, t] \in \mathsf{NC}^1 \quad \Rightarrow \quad {\color{red}(1, 2/3)\text{-MCSP}[s]} \in \text{Formula}[N^{1.1}]$$

$\uparrow$ $\uparrow$

input: $y_1, f(y_1), \ldots, y_t, f(y_t)$
$y_i \in \{0,1\}^n, f(y_i) \in \{0,1\}$
output: $1 \Leftrightarrow \exists$ s-size circuit C s.t.
$\bigwedge_{i \leq t} C(y_i) = f(y_i)$

YES inputs: $\text{tt}(f)$ s.t. $f \in \text{Circuit}[s]$
NO inputs: $\text{tt}(f)$ s.t. $\forall |C| \leq s$,
$\Pr[C(y) = f(y)] < 2/3$

Initial Magnification Theorem

Oliveira-Santhanam (2018): $(s = 2^{\sqrt{n}}, t = 9s \log s, N = 2^n)$

$$\text{succinct-MCSP}[s, t] \in \mathsf{NC}^1 \quad \Rightarrow \quad (1, 2/3)\text{-MCSP}[s] \in \text{Formula}[N^{1.1}]$$

WHY INTERESTING?

previous "magnification" results (including a trivial padding) ask for

- ○ a lower bound on an artificial problem which is hard to analyze, or for
- ○ a lower bound on a strong computational model for which we have no lower bound at all

Initial Magnification Theorem

Oliveira-Santhanam (2018): $(s = 2^{\sqrt{n}}, t = 9s \log s, N = 2^n)$

$$\text{succinct-MCSP}[s, t] \in \mathsf{NC}^1 \quad \Rightarrow \quad (1, 2/3)\text{-MCSP}[s] \in \text{Formula}[N^{1.1}]$$

WHY INTERESTING?

previous "magnification" results (including a trivial padding) ask for

- a lower bound on an artificial problem which is hard to analyze, or for
- a lower bound on a strong computational model for which we have no lower bound at all

On the other hand,

Hirahara-Santhanam (2017):

$$\text{MCSP}[2^{\sqrt{n}}] \notin \text{Formula}[N^{1.99}]$$

where

$$\text{MCSP}(\text{tt}(f)) = 1 \quad \Leftrightarrow \quad f \in \text{Circuit}[2^{\sqrt{n}}]$$

Initial Magnification Theorem

Oliveira-Santhanam (2018): $(s = 2^{\sqrt{n}}, t = 9s \log s, N = 2^n)$

$$\text{succinct-MCSP}[s, t] \in \mathsf{NC}^1 \quad \Rightarrow \quad (1, 2/3)\text{-MCSP}[s] \in \mathsf{Formula}[N^{1.1}]$$

WHY INTERESTING?

previous "magnification" results (including a trivial padding) ask for

- ○ a lower bound on an artificial problem which is hard to analyze, or for
- ○ a lower bound on a strong computational model for which we have no lower bound at all

On the other hand,

Hirahara-Santhanam (2017):

$$\text{MCSP}[2^{\sqrt{n}}] \notin \mathsf{Formula}[N^{1.99}]$$

Additionally, sidesteps the natural proofs barrier: methods seem to work only for specific problems like MCSP, not clear how to naturalize them.

History

Earlier "magnification" results: e.g.

Srinivasan (2003): seems hard to analyze his problem/model
(approximating clique vs randomized algorithms)

Allender-Koucký (2010), **Lipton-Williams (2013)**:
ask for lower bounds on too strong computational models
for which no lower bounds are known

History

Earlier "magnification" results: e.g.

Srinivasan (2003): seems hard to analyze his problem/model
(approximating clique vs randomized algorithms)

Allender-Koucký (2010), **Lipton-Williams (2013)**:
ask for lower bounds on too strong computational models
for which no lower bounds are known

Proof complexity magnification

History

Earlier "magnification" results: e.g.

Srinivasan (2003): seems hard to analyze his problem/model
(approximating clique vs randomized algorithms)

Allender-Koucký (2010), **Lipton-Williams (2013)**:
ask for lower bounds on too strong computational models
for which no lower bounds are known

Proof complexity magnification

$$\text{polynomial-size proofs of } \underset{\text{"succinct-MCSP"}}{\underset{\uparrow}{\mathrm{lb}(f, n^k)}} \;\Rightarrow\; \text{linear-size proofs of } \underset{\text{"MCSP"}}{\underset{\uparrow}{\mathrm{tt}(f, n^k)}}$$

(both $\mathrm{lb}(f, n^k)$ and $\mathrm{tt}(f, n^k)$ encode $f \notin \mathrm{Circuit}[n^k]$)

History

Earlier "magnification" results: e.g.
Srinivasan (2003): seems hard to analyze his problem/model
(approximating clique vs randomized algorithms)
Allender-Koucký (2010), **Lipton-Williams (2013)**:
ask for lower bounds on too strong computational models
for which no lower bounds are known

Proof complexity magnification

Müller-P. (2017):

$\mathrm{tt}(f, n^k)$ hard for constant-depth Frege $\Rightarrow$ $\mathrm{lb}(f, n^k)$ hard for Frege

History

Earlier "magnification" results: e.g.

Srinivasan (2003): seems hard to analyze his problem/model
(approximating clique vs randomized algorithms)

Allender-Koucký (2010), **Lipton-Williams (2013)**:
ask for lower bounds on too strong computational models
for which no lower bounds are known

Proof complexity magnification

Müller-P. (2017):

$\mathrm{tt}(f, n^k)$ hard for constant-depth Frege $\Rightarrow$ $\mathrm{lb}(f, n^k)$ hard for Frege

History

Earlier "magnification" results: e.g.

Srinivasan (2003): seems hard to analyze his problem/model
(approximating clique vs randomized algorithms)

Allender-Koucký (2010), **Lipton-Williams (2013)**:
ask for lower bounds on too strong computational models
for which no lower bounds are known

Proof complexity magnification

Müller-P. (2017):

$\mathrm{tt}(f, n^k)$ hard for constant-depth Frege $\Rightarrow$ $\mathrm{lb}(f, n^k)$ hard for Frege

$\nwarrow$ $\nearrow$ $\uparrow$

known lower bounds central open problem

but proof complexity LBs tend to be harder to obtain than circuit LBs

New results: magnification for $\mathsf{MCSP}[2^{\sqrt{n}}]$

Problem with Oliveira-Santhanam (2018):

$(1, 2/3)$-MCSP still hard to analyze, i.e. Hirahara-Santhanam LB fails

New results: magnification for $\mathsf{MCSP}[2^{\sqrt{n}}]$

Problem with Oliveira-Santhanam (2018):

$(1, 2/3)$-MCSP still hard to analyze, i.e. Hirahara-Santhanam LB fails

---

"**Solutions**":

1. Hardness amplification (error-correcting codes)
2. Anticheckers (and approximate counting)
3. Compression [McKay-Murray-Williams 2019]

New results: magnification for $\mathsf{MCSP}[2^{\sqrt{n}}]$

Problem with Oliveira-Santhanam (2018):

$(1, 2/3)$-MCSP still hard to analyze, i.e. Hirahara-Santhanam LB fails

---

"**Solutions**":

1. Hardness amplification (error-correcting codes)
2. Anticheckers (and approximate counting)
3. Compression [McKay-Murray-Williams 2019]

A gap emerges: 1.-3. slightly increase the required lower bound

e.g.

$$\mathsf{NQP} \in \mathsf{NC}^1 \quad \Rightarrow \quad \mathsf{MCSP}[2^{\sqrt{n}}] \in \mathsf{Formula}[N^{3.1}]$$

(similar gap for TC^0, branching programs,. . .)
i.e. we end up above any known lower bound

New results: magnification for MCSP$[2^{\sqrt{n}}]$

Problem with Oliveira-Santhanam (2018):

$(1, 2/3)$-MCSP still hard to analyze, i.e. Hirahara-Santhanam LB fails

---

"**Solutions**":

1. Hardness amplification (error-correcting codes)
2. Anticheckers (and approximate counting)
3. Compression [McKay-Murray-Williams 2019]

A gap emerges: 1.-3. slightly increase the required lower bound

e.g.

$$\mathsf{NQP} \in \mathsf{NC}^1 \quad \Rightarrow \quad \mathsf{MCSP}[2^{\sqrt{n}}] \in \mathsf{Formula}[N^{3.1}]$$

(similar gap for TC^0, branching programs,...)

i.e. we end up above any known lower bound

Exceptions: e.g. $\mathsf{NQP} \in \mathsf{NC}^1 \quad \Rightarrow \quad \mathsf{MCSP}[2^{\sqrt{n}}] \in \mathsf{Formula}\text{-}\oplus[N^{1.1}]$

Tal (2016): $\mathsf{IP} \notin \mathsf{Formula}\text{-}\oplus[N^{1.9}]$

New results: non-naturalizability

Hardness magnification for (1,2/3)-MCSP is provably non-naturalizable:

$$(1,2/3)\text{-MCSP}[n^{O(1)}, 2^{\sqrt{n}}] \ \notin \text{Circuit}[N^{1.1}]$$

$$\Rightarrow$$

$$\neg\exists \ \text{P/poly-natural property against P/poly}$$

A way to avoid natural proofs is to show that there are no natural proofs

New results: non-naturalizability

Hardness magnification for (1,2/3)-MCSP is provably non-naturalizable:

$$(1,2/3)\text{-MCSP}[n^{O(1)},2^{\sqrt{n}}] \not\in \text{Circuit}[N^{1.1}]$$

$$\Rightarrow$$

$$\neg\exists \text{ P/poly-natural property against P/poly}$$

A way to avoid natural proofs is to show that there are no natural proofs

Crucial observation:

$$(1,2/3)\text{-MCSP}[n^{O(1)},2^{\sqrt{n}}] \not\in \text{Circuit}[N^{1.1}]$$

$$\Rightarrow$$

$$\neg\exists \text{ subexponential-size circuits learning P/poly}$$

New results: non-naturalizability

Hardness magnification for (1,2/3)-MCSP is provably non-naturalizable:

$$(1, 2/3)\text{-MCSP}[n^{O(1)}, 2^{\sqrt{n}}] \;\notin \text{Circuit}[N^{1.1}]$$

$$\Rightarrow$$

$$\neg\exists \text{ P/poly-natural property against P/poly}$$

A way to avoid natural proofs is to show that there are no natural proofs

Crucial observation:

$$(1, 2/3)\text{-MCSP}[n^{O(1)}, 2^{\sqrt{n}}] \;\notin \text{Circuit}[N^{1.1}]$$

$$\Leftrightarrow$$

$$\neg\exists \text{ subexponential-size circuits learning P/poly}$$

($\Leftrightarrow$ $\exists$ pseudorandom function families [Oliveira-Santhanam 2016])

New results: non-naturalizability

Hardness magnification for (1,2/3)-MCSP is provably non-naturalizable:

$$(1,2/3)\text{-MCSP}[n^{O(1)}, 2^{\sqrt{n}}] \;\notin \text{Circuit}[N^{1.1}]$$
$$\Rightarrow$$
$$\neg\exists \text{ P/poly-natural property against P/poly}$$

A way to avoid natural proofs is to show that there are no natural proofs

Crucial observation:

$$(1,2/3)\text{-MCSP}[n^{O(1)}, 2^{\sqrt{n}}] \;\notin \text{Circuit}[N^{1.1}]$$
$$\Leftrightarrow$$

$\neg\exists$ subexponential-size circuits learning P/poly

($\Leftrightarrow$ $\exists$ pseudorandom function families [Oliveira-Santhanam 2016])

$\Leftrightarrow$ (Carmosino-Impagliazzo-Kabanets-Kolokolova 2016) $\Leftrightarrow$

$\neg\exists$ P/poly-natural property against P/poly

New results: non-naturalizability

Hardness magnification for (1,2/3)-MCSP is provably non-naturalizable:

$$(1,2/3)\text{-MCSP}[n^{O(1)}, 2^{\sqrt{n}}] \ \not\in \text{Circuit}[N^{1.1}]$$

$$\Rightarrow$$

$$\neg\exists \text{ P/poly-natural property against P/poly}$$

A way to avoid natural proofs is to show that there are no natural proofs

Crucial observation:

$$(1,2/3)\text{-MCSP}[n^{O(1)}, 2^{\sqrt{n}}] \ \not\in \text{Circuit}[N^{1.1}]$$

$$\Leftrightarrow$$

$\neg\exists$ subexponential-size circuits learning P/poly

($\Leftrightarrow$ $\exists$ pseudorandom function families [Oliveira-Santhanam 2016])

$\Leftrightarrow$ (Carmosino-Impagliazzo-Kabanets-Kolokolova 2016) $\Leftrightarrow$

$\neg\exists$ P/poly-natural property against P/poly

Open: our non-naturalizability proof does not work for MCSP$[2^{\sqrt{n}}]$

Hardness magnification via error-correcting codes

Recall the **initial magnification** theorem (Oliveira-Santhanam '18):

$$\text{succinct-MCSP}[s,t] \in \mathsf{NC}^1 \quad \Rightarrow \quad (1,2/3)\text{-MCSP}[s] \in \text{Formula}[N^{1.1}]$$

$(s = 2^{\sqrt{n}}, t = 9s \log s, N = 2^n)$

Hardness magnification via error-correcting codes

Recall the **initial magnification** theorem (Oliveira-Santhanam '18):

$$\text{succinct-MCSP}[s,t] \in \mathsf{NC}^1 \quad \Rightarrow \quad (1,2/3)\text{-MCSP}[s] \in \text{Formula}[N^{1.1}]$$

$(s = 2^{\sqrt{n}}, t = 9s\log s, N = 2^n)$

Proof: Define an algorithm F': given $\mathrm{tt}(f)$

- pick random $y_1, f(y_1), \ldots, y_t, f(y_t)$
- use $F_1 \in \mathsf{NC}^1$ to decide if $\exists$ s-size circuit C s.t. $\bigwedge_{i\leq t} C(y_i) = f(y_i)$

Then,

$(1,\frac{2}{3})$-MCSP[s](f)=1 $\Rightarrow F'(f) = 1$

$(1,\frac{2}{3})$-MCSP[s](f)=0 $\Rightarrow \forall |C| \leq s$, $\Pr_{\overline{y}}[\bigwedge C(y_i) = f(y_i)] \leq (\frac{2}{3})^t \leq e^{-3s\log s}$

$\Rightarrow \Pr[\exists |C| \leq s, \bigwedge C(y_i) = f(y_i)] < \frac{1}{2} \Rightarrow \Pr[F'(f) = 1] < 1/2$

Derandomization:

F repeats F' N-times and accepts if all rounds accept

i.e. $\Pr[\exists f$ s.t. (1,2/3)-MCSP$[s](f) = 0 \wedge F(f) = 1] < 1$

resulting formula size: $N poly(s)$ ☐

Hardness magnification via error-correcting codes

Recall the **initial magnification** theorem (Oliveira-Santhanam '18):

$$\text{succinct-MCSP}[s,t] \in \mathsf{NC}^1 \quad \Rightarrow \quad (1,2/3)\text{-MCSP}[s] \in \text{Formula}[N^{1.1}]$$

$(s = 2^{\sqrt{n}}, t = 9s\log s, N = 2^n)$

Extending it to MCSP[s]:

use hardness amplification $H : \{0,1\}^N \mapsto \{0,1\}^{O(N)}$ s.t.

$f \in \text{Circuit}[s] \Rightarrow H(f) \in \text{Circuit}[s]$

$f \notin \text{Circuit}[s] \Rightarrow H(f)$ hard to 2/3-approximate by s-size circuits

Hardness magnification via error-correcting codes

Recall the **initial magnification** theorem (Oliveira-Santhanam '18):

$$\text{succinct-MCSP}[s,t] \in \mathsf{NC}^1 \quad \Rightarrow \quad (1,2/3)\text{-MCSP}[s] \in \text{Formula}[N^{1.1}]$$

$(s = 2^{\sqrt{n}}, t = 9s\log s, N = 2^n)$

Extending it to MCSP[s]:

use hardness amplification $H : \{0,1\}^N \mapsto \{0,1\}^{O(N)}$ s.t.

$f \in \text{Circuit}[s] \Rightarrow H(f) \in \text{Circuit}[s]$

$f \notin \text{Circuit}[s] \Rightarrow H(f)$ hard to 2/3-approximate by s-size circuits

---

Problem: error-correcting codes (ECCs) do not preserve circuit complexity

Solution: they do if QP=TIME$[n^{O(\log^2 n)}]\subseteq$ P/poly

Hardness magnification via error-correcting codes

Recall the **initial magnification** theorem (Oliveira-Santhanam '18):

$$\text{succinct-MCSP}[s,t] \in \mathsf{NC}^1 \quad \Rightarrow \quad (1,2/3)\text{-MCSP}[s] \in \text{Formula}[N^{1.1}]$$

$(s = 2^{\sqrt{n}}, t = 9s \log s, N = 2^n)$

Extending it to MCSP[s]:

use hardness amplification $H : \{0,1\}^N \mapsto \{0,1\}^{O(N)}$ s.t.

$f \in \text{Circuit}[s] \Rightarrow H(f) \in \text{Circuit}[s]$

$f \notin \text{Circuit}[s] \Rightarrow H(f)$ hard to $2/3$-approximate by s-size circuits

---

Problem: error-correcting codes (ECCs) do not preserve circuit complexity

Solution: they do if QP=TIME$[n^{O(\log^2 n)}]\subseteq$ P/poly

Theorem: $\mathsf{NQP} \subseteq \mathsf{NC}^1 \Rightarrow \text{MCSP}[2^{n^{1/3}}, 2^{n^{2/3}}] \in \text{Formula-}\oplus[N^{1.1}]$

Hardness magnification via error-correcting codes

Recall the **initial magnification** theorem (Oliveira-Santhanam '18):

$$\text{succinct-MCSP}[s,t] \in \mathsf{NC}^1 \quad \Rightarrow \quad (1,2/3)\text{-MCSP}[s] \in \text{Formula}[N^{1.1}]$$

$(s = 2^{\sqrt{n}}, t = 9s\log s, N = 2^n)$

Extending it to MCSP[s]:

use hardness amplification $H : \{0,1\}^N \mapsto \{0,1\}^{O(N)}$ s.t.

$f \in \text{Circuit}[s] \Rightarrow H(f) \in \text{Circuit}[s]$

$f \notin \text{Circuit}[s] \Rightarrow H(f)$ hard to 2/3-approximate by s-size circuits

---

Problem: error-correcting codes (ECCs) do not preserve circuit complexity

Solution: they do if QP=TIME$[n^{O(\log^2 n)}]\subseteq$ P/poly

Theorem: $\mathsf{NQP} \subseteq \mathsf{NC}^1 \Rightarrow \text{MCSP}[2^{n^{1/3}}, 2^{n^{2/3}}] \in \text{Formula-}\oplus[N^{1.1}]$

- Formula-$\oplus$: formula with XOR-gates at the bottom (implements ECCs)
- $\text{MCSP}[s_1,s_2]$: YES instances $\in \text{Circuit}[s_1]$, NO instances $\notin \text{Circuit}[s_2]$

Hardness magnification via error-correcting codes

Recall the **initial magnification** theorem (Oliveira-Santhanam '18):

$$\text{succinct-MCSP}[s,t] \in \mathsf{NC}^1 \quad \Rightarrow \quad (1,2/3)\text{-MCSP}[s] \in \text{Formula}[N^{1.1}]$$

$(s = 2^{\sqrt{n}}, t = 9s\log s, N = 2^n)$

Extending it to MCSP[s]:

use hardness amplification $H : \{0,1\}^N \mapsto \{0,1\}^{O(N)}$ s.t.

$f \in \text{Circuit}[s] \Rightarrow H(f) \in \text{Circuit}[s]$

$f \notin \text{Circuit}[s] \Rightarrow H(f)$ hard to 2/3-approximate by s-size circuits

---

Problem: error-correcting codes (ECCs) do not preserve circuit complexity

Solution: they do if QP=TIME$[n^{O(\log^2 n)}]\subseteq$ P/poly

Theorem: $\mathsf{NQP} \subseteq \mathsf{NC}^1 \Rightarrow \text{MCSP}[2^{n^{1/3}}, 2^{n^{2/3}}] \in \text{Formula-}\oplus[N^{1.1}]$

- Formula-$\oplus$: formula with XOR-gates at the bottom (implements ECCs)
- MCSP$[s_1, s_2]$: YES instances $\in$ Circuit$[s_1]$, NO instances $\notin$ Circuit$[s_2]$

Hirahara-Santhanam '17: $\text{MCSP}[2^{n^{1/3}}, 2^{n^{2/3}}] \notin \text{Formula}[N^{1.9}]$

Hardness magnification via anticheckers

Lipton-Young: $f \notin \mathsf{Circuit}[n^{O(1)}] \Rightarrow \exists A \subseteq \{0,1\}^n$ of size $n^{O(1)}$ s.t. no $n^{O(1)}$-size circuit computes f on the set of anticheckers A

Hardness magnification via anticheckers

Lipton-Young: $f \notin \text{Circuit}[n^{O(1)}] \Rightarrow \exists A \subseteq \{0,1\}^n$ of size $n^{O(1)}$ s.t.
no $n^{O(1)}$-size circuit computes f on the set of anticheckers A

Clear: $\text{NP} \subseteq \text{P/poly} \Rightarrow poly(n)$-size circuits finding A given $\text{tt}(f)$

Hardness magnification via anticheckers

Lipton-Young: $f \notin \text{Circuit}[n^{O(1)}] \Rightarrow \exists A \subseteq \{0,1\}^n$ of size $n^{O(1)}$ s.t.
no $n^{O(1)}$-size circuit computes f on the set of anticheckers A

Clear: $\text{NP} \subseteq \text{P/poly} \Rightarrow \mathit{poly}(n)$-size circuits finding A given $\text{tt}(f)$
We show: $\text{NP} \subseteq \text{P/poly} \Rightarrow n^{1.1}$-size circuits finding A given $\text{tt}(f)$
- employs approximate counting with linear hash functions

Hardness magnification via anticheckers

Lipton-Young: $f \notin \mathsf{Circuit}[n^{O(1)}] \Rightarrow \exists A \subseteq \{0,1\}^n$ of size $n^{O(1)}$ s.t. no $n^{O(1)}$-size circuit computes f on the set of anticheckers A

Clear: $\mathsf{NP} \subseteq \mathsf{P/poly} \Rightarrow poly(n)$-size circuits finding A given $\mathsf{tt}(f)$

We show: $\mathsf{NP} \subseteq \mathsf{P/poly} \Rightarrow n^{1.1}$-size circuits finding A given $\mathsf{tt}(f)$

- employs approximate counting with linear hash functions

Theorem: $\mathsf{NP} \subseteq \mathsf{P/poly} \Rightarrow \mathsf{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}] \in \mathsf{Circuit}[N^{1.1}]$

Hardness magnification via anticheckers

Lipton-Young: $f \notin \text{Circuit}[n^{O(1)}] \Rightarrow \exists A \subseteq \{0,1\}^n$ of size $n^{O(1)}$ s.t. no $n^{O(1)}$-size circuit computes f on the set of anticheckers A

Clear: $\text{NP} \subseteq \text{P/poly} \Rightarrow$ $poly(n)$-size circuits finding A given $\text{tt}(f)$

We show: $\text{NP} \subseteq \text{P/poly} \Rightarrow$ $n^{1.1}$-size circuits finding A given $\text{tt}(f)$

- employs approximate counting with linear hash functions

Theorem: $\text{NP} \subseteq \text{P/poly} \Rightarrow \text{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}] \in \text{Circuit}[N^{1.1}]$

"$\text{NP} \subseteq \text{NC}^1 \Rightarrow \text{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}] \in \text{Formula}[N^{1.1}]$"

would give us $\text{NP} \not\subseteq \text{NC}^1$

Hardness magnification via anticheckers

Lipton-Young: $f \notin \mathsf{Circuit}[n^{O(1)}] \Rightarrow \exists A \subseteq \{0,1\}^n$ of size $n^{O(1)}$ s.t. no $n^{O(1)}$-size circuit computes f on the set of anticheckers A

Clear: $\mathsf{NP} \subseteq \mathsf{P}/\mathsf{poly} \Rightarrow \mathit{poly}(n)$-size circuits finding A given $\mathrm{tt}(f)$

We show: $\mathsf{NP} \subseteq \mathsf{P}/\mathsf{poly} \Rightarrow n^{1.1}$-size circuits finding A given $\mathrm{tt}(f)$

- employs approximate counting with linear hash functions

Theorem: $\mathsf{NP} \subseteq \mathsf{P}/\mathsf{poly} \Rightarrow \mathsf{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}] \in \mathsf{Circuit}[N^{1.1}]$

"$\mathsf{NP} \subseteq \mathsf{NC}^1 \Rightarrow \mathsf{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}] \in \mathsf{Formula}[N^{1.1}]$"

would give us $\mathsf{NP} \not\subseteq \mathsf{NC}^1$

Theorem: $\mathsf{NP} \subseteq \mathsf{NC}^1 \Rightarrow \mathsf{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}] \in \mathsf{Formula\text{-}like}[N^{1.1}]$

Hardness magnification via anticheckers

Lipton-Young: $f \notin \mathrm{Circuit}[n^{O(1)}] \Rightarrow \exists A \subseteq \{0,1\}^n$ of size $n^{O(1)}$ s.t. no $n^{O(1)}$-size circuit computes f on the set of anticheckers A

Clear: $\mathrm{NP} \subseteq \mathrm{P/poly} \Rightarrow$ $poly(n)$-size circuits finding A given $\mathrm{tt}(f)$

We show: $\mathrm{NP} \subseteq \mathrm{P/poly} \Rightarrow$ $n^{1.1}$-size circuits finding A given $\mathrm{tt}(f)$

- employs approximate counting with linear hash functions

Theorem: $\mathrm{NP} \subseteq \mathrm{P/poly} \Rightarrow \mathrm{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}] \in \mathrm{Circuit}[N^{1.1}]$

"$\mathrm{NP} \subseteq \mathrm{NC}^1 \Rightarrow \mathrm{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}] \in \mathrm{Formula}[N^{1.1}]$"
would give us $\mathrm{NP} \not\subseteq \mathrm{NC}^1$

Theorem: $\mathrm{NP} \subseteq \mathrm{NC}^1 \Rightarrow \mathrm{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}] \in \text{Formula-like}[N^{1.1}]$

Formula-like: formula with a few gates with fanout > 1
and a fixed structure

Hardness magnification via anticheckers

Lipton-Young: $f \notin \text{Circuit}[n^{O(1)}] \Rightarrow \exists A \subseteq \{0,1\}^n$ of size $n^{O(1)}$ s.t. no $n^{O(1)}$-size circuit computes f on the set of anticheckers A

Clear: $\text{NP} \subseteq \text{P/poly} \Rightarrow \mathit{poly}(n)$-size circuits finding A given $\text{tt}(f)$

We show: $\text{NP} \subseteq \text{P/poly} \Rightarrow n^{1.1}$-size circuits finding A given $\text{tt}(f)$

- employs approximate counting with linear hash functions

Theorem: $\text{NP} \subseteq \text{P/poly} \Rightarrow \text{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}] \in \text{Circuit}[N^{1.1}]$

"$\text{NP} \subseteq \text{NC}^1 \Rightarrow \text{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}] \in \text{Formula}[N^{1.1}]$"

would give us $\text{NP} \not\subseteq \text{NC}^1$

Theorem: $\text{NP} \subseteq \text{NC}^1 \Rightarrow \text{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}] \in \text{Formula-like}[N^{1.1}]$

Formula-like: formula with a few gates with fanout > 1
and a fixed structure

Known: $\text{PARITY} \notin \text{Formula-like}[N^{1.9}]$

Final mystery

We reached the following situation:

- $\circ$ $\mathsf{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}] \notin \mathsf{Formula\text{-}like}[N^{1.1}] \Rightarrow \mathsf{NP} \not\subseteq \mathsf{NC}^1$
- $\circ$ $\mathsf{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}] \notin \mathsf{Formula}[N^{1.9}]$
- $\circ$ $\mathsf{PARITY} \notin \mathsf{Formula\text{-}like}[N^{1.9}]$

Final mystery

We reached the following situation:

- ∘ $\mathrm{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}] \notin \text{Formula-like}[N^{1.1}] \Rightarrow \mathrm{NP} \not\subseteq \mathrm{NC}^1$
- ∘ $\mathrm{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}] \notin \text{Formula}[N^{1.9}]$
- ∘ $\mathrm{PARITY} \notin \text{Formula-like}[N^{1.9}]$

---

but $\mathrm{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}]$ is much harder than PARITY.

Final mystery

We reached the following situation:

- $\circ$ $\mathrm{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}] \notin \text{Formula-like}[N^{1.1}] \Rightarrow \mathrm{NP} \not\subseteq \mathrm{NC}^1$
- $\circ$ $\mathrm{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}] \notin \text{Formula}[N^{1.9}]$
- $\circ$ $\mathrm{PARITY} \notin \text{Formula-like}[N^{1.9}]$

---

but $\mathrm{MCSP}[2^{\sqrt{n}}/2n, 2^{\sqrt{n}}]$ is much harder than PARITY.

Thank You for Your Attention