Simple general magnification

Moritz Müller

joint with Albert Atserias

Circuit lower bounds

Conjecture $\quad \mathsf{NP} \not\subseteq \mathsf{SIZE}[n^{O(1)}]$

Open $\quad \mathsf{NP} \subseteq \mathsf{FML}[n^c]$ for some $c \in \mathbb{N}$

Best explicit lower bounds

circuits:	$5n - o(1)$	(Iwama, Morizumi 2002)
formulas:	$n^{3-o(1)}$	(Håstad 1998)

Arora, Barak: "*complexity theory's Waterloo*"

Why difficult?

Is it hard to recognize hard functions?

Let $\sigma : \mathbb{N} \to \mathbb{N}$.

MCSP[σ]
Input: $x \in \{0,1\}^n, n = 2^m$
Problem: is x computable by a circuit of size $\leqslant \sigma(m)$?

i.e., $x = \mathrm{tt}(C)$ for some C with m inputs and size $\leqslant \sigma(m)$
i.e, $x_i = C(i\text{-th } m\text{-bit string})$

Is it hard to recognize hard functions?

Let $\sigma : \mathbb{N} \to \mathbb{N}$.

MCSP[σ]
Input: $x \in \{0,1\}^n, n = 2^m$
Problem: is x computable by a circuit of size $\leqslant \sigma(m)$?

i.e., $x = \mathrm{tt}(C)$ for some C with m inputs and size $\leqslant \sigma(m)$
i.e, $x_i = C(i\text{-th } m\text{-bit string})$

Buhrmann-Hitchcock 2008

$n^{o(1)}$-sparse problems are not NP-hard unless PH $\subseteq \Sigma_2^{\mathrm{P}}$.

- $Q \subseteq \{0,1\}^*$ $q(n)$-sparse if $|Q \cap \{0,1\}^n| \leqslant 2^{q(n)}$.
- MCSP[$2^{o(m)}$] is $n^{o(1)}$-sparse.

Is it hard to recognize hard functions?

Let $\sigma : \mathbb{N} \to \mathbb{N}$.

MCSP[σ]
Input: $x \in \{0,1\}^n, n = 2^m$
Problem: is x computable by a circuit of size $\leqslant \sigma(m)$?

i.e., $x = \mathrm{tt}(C)$ for some C with m inputs and size $\leqslant \sigma(m)$
i.e, $x_i = C(i\text{-th } m\text{-bit string})$

Hirahara-Santhanam 2017 $\mathrm{MCSP}[2^{\sqrt{m}}] \notin \mathrm{FML}[n^{2-\delta}]$ for all $\delta > 0$.

Magnification

Let $\sigma : \mathbb{N} \to \mathbb{N}$, $\epsilon : \mathbb{N} \to [0,1]$.

ϵ-MCSP$[\sigma]$
Input: $x \in \{0,1\}^n, n = 2^m$
YES: x computable by a circuit of size $\leqslant \sigma(m)$.
NO: for every C with m inputs and size $\leqslant \sigma(m)$:

$$d_H(x, \mathsf{tt}(C)) = |\{i \in [n] \mid x_i \neq \mathsf{tt}(C)_i\}| \geqslant \epsilon(n) \cdot n$$

Hirahara-Santhanam 2017 MCSP$[2^{\sqrt{m}}] \notin$ FML$[n^{2-\delta}]$ for all $\delta > 0$.

Magnification

Let $\sigma : \mathbb{N} \to \mathbb{N}$, $\epsilon : \mathbb{N} \to [0,1]$.

ϵ-MCSP[σ]
Input: $x \in \{0,1\}^n, n = 2^m$
YES: x computable by a circuit of size $\leqslant \sigma(m)$.
NO: for every C with m inputs and size $\leqslant \sigma(m)$:

$$d_H(x, \mathsf{tt}(C)) = |\{i \in [n] \mid x_i \neq \mathsf{tt}(C)_i\}| \geqslant \epsilon(n) \cdot n$$

Hirahara-Santhanam 2017 MCSP[$2^{\sqrt{m}}$] $\notin$ FML[$n^{2-\delta}$] for all $\delta > 0$.

Oliveira-Santhanam 2018

Let $1/\epsilon(n) \leqslant n^{o(1)}$ and $\delta > 0$. Then NP $\not\subseteq$ FML[$n^{O(1)}$], if

ϵ-MCSP[$2^{\sqrt{m}}$] $\notin$ FML[$n^{1+\delta}$]

Magnification almost known lower bound $\Rightarrow$ breakthrough lower bound

General magnification

Chen, Jin, Williams 2020

NP $\not\subseteq$ FML$[n^c]$ for all $c \in \mathbb{N}$ if exists $n^{o(1)}$-sparse $Q \in$ NP:

$Q \notin$ FML$[n^{3+o(1)}]$.

General magnification

Chen, Jin, Williams 2020

NP $\not\subseteq$ FML$[n^c]$ for all $c \in \mathbb{N}$ if exists $n^{o(1)}$-sparse $Q \in$ NP:

$$Q \notin \text{FML}[n^{3+o(1)}].$$

Theorem Let $\epsilon \in (0, 1]$.

NP $\not\subseteq$ FML$[n^c]$ for all $c \in \mathbb{N}$ if exists $n^{o(1)}$-sparse $Q \in$ NP:

$$n^{-\epsilon}\text{-}Q \notin \text{FML}[n^{1+2\epsilon+o(1)}]$$

Input: $x \in \{0,1\}^n$
YES: $x \in Q$
NO: $d_H(x, y) \geqslant n^{-\epsilon} \cdot n$ for all $y \in Q$

- $n^{-1}\text{-}Q = Q$

Distinguishers

- (n, m, δ)-code $C \in \mathbb{F}_2^{n \times m}$ such that for all $x, y \in \mathbb{F}_2^n$:

$$d_H(x, y) > 0 \implies d_H(xC, yC) \geqslant \delta \cdot m$$

- Reed-Solomon $*$ Hadamard gives $(n, m, 1/4)$-code for $m \leqslant n^4$

Distinguishers

- (n, m, δ)-code $C \in \mathbb{F}_2^{n \times m}$ such that for all $x, y \in \mathbb{F}_2^n$:

$$d_H(x, y) > 0 \implies d_H(xC, yC) \geqslant \delta \cdot m$$

- Reed-Solomon $*$ Hadamard gives $(n, m, 1/4)$-code for $m \leqslant n^4$

- (n, m, δ, ϵ)-distinguisher $D \in \mathbb{F}_2^{n \times m}$ such that for all $x, y \in \mathbb{F}_2^n$:

$$d_H(x, y) \geqslant \epsilon \cdot n \implies d_H(xD, yD) \geqslant \delta \cdot m$$

Want small weight (of columns)

Distinguishers

- (n, m, δ)-code $C \in \mathbb{F}_2^{n \times m}$ such that for all $x, y \in \mathbb{F}_2^n$:

  $$d_H(x, y) > 0 \implies d_H(xC, yC) \geqslant \delta \cdot m$$

- Reed-Solomon $*$ Hadamard gives $(n, m, 1/4)$-code for $m \leqslant n^4$

- (n, m, δ, ϵ)-distinguisher $D \in \mathbb{F}_2^{n \times m}$ such that for all $x, y \in \mathbb{F}_2^n$:

  $$d_H(x, y) \geqslant \epsilon \cdot n \implies d_H(xD, yD) \geqslant \delta \cdot m$$

Want small weight (of columns)

Theorem $0 < w < n$ and $\delta \leqslant 1/4 \cdot (1 - \frac{1}{\epsilon w})$.

There exists a (n, m, δ, ϵ)-distinguisher D with $m \leqslant n^7$ and weight $\leqslant w$.
Computable in time $n^{O(1)}$.

Example $\left(n, \leqslant n^7, 1/8, n^{-\epsilon}\right)$-distinguisher of weight $\leqslant 2n^{\epsilon}$.

Distinguisher construction

Assume n is a power of 2, $w < n$.

Input: $x = x(1) \cdots x(n)$ of weight $\geqslant \epsilon \cdot n$
1: sample $i_1, \ldots, i_w \in [n]$ pairwise independently
2: $y := x(i_1) \cdots x(i_w)$
3: output a random bit of yC

- C is an $(w, w', 1/4)$-code, $w' \leqslant w^4$
- W:= weight of y

$$\Pr[W = 0] \leqslant \frac{\mathrm{Var}[W]}{\mathbb{E}[W]^2} \leqslant \frac{1}{\mathbb{E}[W]} \leqslant \frac{1}{\epsilon w}$$

- output 1 with probability $\geqslant 1/4 \cdot (1 - \frac{1}{\epsilon w})$

Distinguisher construction

Assume n is a power of 2, $w < n$.

Input: $x = x(1) \cdots x(n)$ of weight $\geqslant \epsilon \cdot n$

1: sample $i_1, \ldots, i_w \in [n]$ pairwise independently

2: $y := x(i_1) \cdots x(i_w)$

3: sample $k \in [w']$ and output $(yC)_k$

Distinguisher construction

Assume n is a power of 2, $w < n$.

Input: $x = x(1) \cdots x(n)$ of weight $\geqslant \epsilon \cdot n$

1: sample $i_1, \ldots, i_w \in [n]$ pairwise independently

2: $y := x(i_1) \cdots x(i_w)$

3: sample $k \in [w']$ and output $(yC)_k$

Joffe 1974 There is $X \in \mathbb{F}_n^{w \times n^2}$ such for all $i \neq k \in [w]$:

if j uniform in $[n^2]$, then $\big(X(i,j), X(k,j)\big)$ uniform in $\mathbb{F}_n^2$

Distinguisher construction

Assume n is a power of 2, $w < n$.

Input: $x = x(1) \cdots x(n)$ of weight $\geqslant \epsilon \cdot n$

1: sample $j \in [n^2]$

2: $y := x(X(1, j)) \cdots x(X(w, j))$

3: sample $k \in [w']$ and output $(yC)_k$

Joffe 1974 There is $X \in \mathbb{F}_n^{w \times n^2}$ such for all $i \neq k \in [w]$:

if j uniform in $[n^2]$, then $\big(X(i, j), X(k, j)\big)$ uniform in $\mathbb{F}_n^2$

Distinguisher construction

Assume n is a power of 2, $w < n$.

Input: $x = x(1) \cdots x(n)$ of weight $\geqslant \epsilon \cdot n$
1: sample $j \in [n^2]$
2: $y := x(X(1,j)) \cdots x(X(w,j))$
3: sample $k \in [w']$ and output $(yC)_k$

Joffe 1974 There is $X \in \mathbb{F}_n^{w \times n^2}$ such for all $i \neq k \in [w]$:

if j uniform in $[n^2]$, then $\big(X(i,j), X(k,j)\big)$ uniform in $\mathbb{F}_n^2$

- $(yC)_k = \sum_{i \in [w]} x(X(i,j)) \cdot C(i,k) = \sum_{p \in [n]} x(p) \cdot \underbrace{\sum_{\substack{i \in [w] \\ X(i,j)=p}} C(i,k)}_{(p,(j,k)) \text{ entry of } D} = (xD)_{(j,k)}$

Then $D \in \mathbb{F}_2^{n \times n^2 w'}$ has weight $\leqslant w$.

Proof of main result $Q \in \mathsf{NP}$ $n^{o(1)}$-sparse, $\epsilon, \delta \in (0, 1]$.

Assume $\mathsf{NP} \subseteq \mathsf{FML}[n^c]$

Want formula for $n^{-\epsilon}$-Q of size $n^{1+2\epsilon+\delta}$

Proof of main result $Q \in \mathsf{NP}$ $n^{o(1)}$-sparse, $\epsilon, \delta \in (0, 1]$.

Assume $\mathsf{NP} \subseteq \mathsf{FML}[n^c]$
Want formula for $n^{-\epsilon}$-Q of size $n^{1+2\epsilon+\delta}$

Algorithm

1: given $x \in \{0,1\}^n$ compute fingerprint:

$$n, u_1 \cdots u_r, (xD)_{u_1} \cdots (xD)_{u_r}$$

$r := n^{small}$,
$u_i \in [m]$ random
distinguisher D

Proof of main result $Q \in \mathsf{NP}$ $n^{o(1)}$-sparse, $\epsilon, \delta \in (0, 1]$.

Assume $\mathsf{NP} \subseteq \mathsf{FML}[n^c]$
Want formula for $n^{-\epsilon}$-Q of size $n^{1+2\epsilon+\delta}$

Algorithm

1: given $x \in \{0,1\}^n$ compute fingerprint:

$$n, u_1 \cdots u_r, (xD)_{u_1} \cdots (xD)_{u_r}$$

$r := n^{small}$,
$u_i \in [m]$ random
distinguisher D

2: accept if computed fingerprint is fingerprint of some YES

- accepts x in YES with probability 1
- accepts x in NO with probability $\leqslant 2^{n^{o(1)}} \cdot (7/8)^r < 1/2$

Proof of main result $Q \in \mathsf{NP}$ $n^{o(1)}$-sparse, $\epsilon, \delta \in (0, 1]$.

Assume $\mathsf{NP} \subseteq \mathsf{FML}[n^c]$
Want formula for $n^{-\epsilon}$-Q of size $n^{1+2\epsilon+\delta}$

Algorithm

1: given $x \in \{0,1\}^n$ compute fingerprint:

$$n, u_1 \cdots u_r, (xD)_{u_1} \cdots (xD)_{u_r}$$

$r := n^{small}$,
$u_i \in [m]$ random
distinguisher D

2: accept if computed fingerprint is fingerprint of some YES

- accepts x in YES with probability 1
- accepts x in NO with probability $\leqslant 2^{n^{o(1)}} \cdot (7/8)^r < 1/2$

Implementation

1: each bit is XOR of $\leqslant 2n^\epsilon$ input bits: formulas of size $O(n^{2\epsilon})$

2: Assumption gives formula of size $O(r \log m)^c < n^\delta$

Proof of main result $Q \in \mathsf{NP}$ $n^{o(1)}$-sparse, $\epsilon, \delta \in (0,1]$.

Assume $\mathsf{NP} \subseteq \mathsf{FML}[n^c]$

Want formula for $n^{-\epsilon}$-Q of size $n^{1+2\epsilon+\delta}$

Algorithm

1: given $x \in \{0,1\}^n$ compute fingerprint:

$$n, u_1 \cdots u_r, (xD)_{u_1} \cdots (xD)_{u_r}$$

$r := n^{small}$,
$u_i \in [m]$ random
distinguisher D

2: accept if computed fingerprint is fingerprint of some YES

- accepts x in YES with probability 1
- accepts x in NO with probability $\leqslant 2^{n^{o(1)}} \cdot (7/8)^r < 1/2$

Implementation

1: each bit is XOR of $\leqslant 2n^\epsilon$ input bits: formulas of size $O(n^{2\epsilon})$

2: Assumption gives formula of size $O(r \log m)^c < n^\delta$

Derandomization AND of n independent copies gives probability $< 2^{-n}$

General magnification

Let $\epsilon \in (0, 1]$.

Theorem

NP $\not\subseteq$ FML$[n^c]$ for all $c \in \mathbb{N}$ if exists $n^{o(1)}$-sparse $Q \in$ NP:

$$n^{-\epsilon}\text{-}Q \quad \notin \quad \text{FML}[n^{1+2\epsilon+o(1)}]$$

General magnification

Let $\epsilon \in (0, 1]$.

Theorem

NP $\not\subseteq$ FML$[n^c]$ for all $c \in \mathbb{N}$ if exists $n^{o(1)}$-sparse $Q \in$ NP:

$n^{-\epsilon}$-$Q \notin$ PFML$[n^{2\epsilon+o(1)}]$

there is no random formula F of size $\leqslant n^{2\epsilon+o(1)}$

- F accepts every YES with probability 1
- F rejects every NO with probability $\geqslant 3/4$.

General magnification

Let $\epsilon \in (0, 1]$.

Theorem

NP $\not\subseteq$ FML$[n^c]$ for all $c \in \mathbb{N}$ if exists $n^{o(1)}$-sparse $Q \in$ NP:

$n^{-\epsilon}$-$Q \notin$ PFML$[n^{2\epsilon+o(1)}]$

there is no random formula F of size $\leqslant n^{2\epsilon+o(1)}$

- F accepts every YES with probability 1
- F rejects every NO with probability $\geqslant 3/4$.

Sharp lower bound

$n^{-\epsilon}$-MCSP$[2^{\sqrt{m}}] \notin$ PFML$[n^{2\epsilon-\delta}]$ for all $\delta > 0$.

Localization barrier

Let $\epsilon \in (0, 1]$.

Localization Lemma

For every $n^{o(1)}$-sparse Q there exists K such that for sufficiently large n

$n^{-\epsilon}$-Q is decided by a probabilistic formula of size $n^{2\epsilon+o(1)}$

with K-oracle gates of fan-in $n^{o(1)}$.

Localization barrier

Let $\epsilon \in (0, 1]$.

Localization Lemma

For every $n^{o(1)}$-sparse Q there exists K such that for sufficiently large n

$n^{-\epsilon}$-Q is decided by a probabilistic formula of size $n^{2\epsilon+o(1)}$

with K-oracle gates of fan-in $n^{o(1)}$.

Theorem

$\mathsf{P} \neq \mathsf{NP}^{\oplus\mathsf{P}}$ if $\quad n^{-\epsilon}$-$\mathsf{MCSP}[2^{o(m)}] \notin \mathsf{P}$-uniform-$\mathsf{SIZE}[n^{1+\epsilon+o(1)}]$.

Santhanam, Williams 2014

Let $c \in \mathbb{N}$. Then $\mathsf{P} \not\subseteq \mathsf{P}$-uniform-$\mathsf{SIZE}[n^c]$.