Exponential Lower-bounds via Exponential Sums

Somnath Bhattacharjee
(Chennai Mathematical Institute)

Joint work with Markus Bläser (Saarland University), Pranjal Dutta (NUS), Saswata Mukherjee (NUS)

(ICALP 2024)

Outline

NP Problems: Is Brute Force Optimal?

NP Problems: Is Brute Force Optimal?

Given a word x, check for

$$\bigvee_{e \in \{0,1\}^n} M(x, e) = 1$$

NP Problems: Is Brute Force Optimal?

Given a word x, check for

$$\bigvee_{e \in \{0,1\}^n} M(x, e) = 1$$

M runs in m time

NP Problems: Is Brute Force Optimal?

Given a word x, check for

$$\bigvee_{e \in \{0,1\}^n} M(x, e) = 1$$

M runs in m time

- Running time upper bound : $2^n m$ (Brute force!)

NP Problems: Is Brute Force Optimal?

Given a word x, check for

$$\bigvee_{e \in \{0,1\}^n} M(x, e) = 1$$

M runs in m time

- Running time upper bound : $2^n m$ (Brute force!)
- Improve to $2^{o(n)} poly(m)$ possible?

NP Problems: Is Brute Force Optimal?

Given a word x, check for

$$\bigvee_{e \in \{0,1\}^n} M(x, e) = 1$$

M runs in m time

- Running time upper bound : $2^n m$ (Brute force!)
- Improve to $2^{o(n)} poly(m)$ possible?
- **ETH** says NO! (informally)

Is Brute Force Optimal?

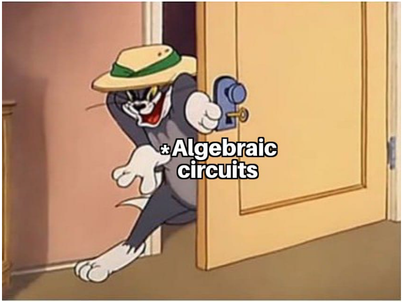
- Can we ask the same question in *algebraic setting*?

Is Brute Force Optimal?

- Can we ask the same question in *algebraic setting*?
- What is even the *Computational Model* in that setting?

Is Brute Force Optimal?

- Can we ask the same question in *algebraic setting*?
- What is even the *Computational Model* in that setting?
- Hence Algebraic Circuit enters the picture



Algebraic Circuits (Constant-free)

- Arithmetic Circuits are directed acyclic graphs.

Algebraic Circuits (Constant-free)

- Arithmetic Circuits are directed acyclic graphs.
- Each internal node: $+$ or $\times$ gate.

Algebraic Circuits (Constant-free)

- Arithmetic Circuits are directed acyclic graphs.
- Each internal node: $+$ or $\times$ gate.
- Each leaf: $\{1, 0, -1\}$ or variables $\mathbf{X}$

Algebraic Circuits (Constant-free)

- Arithmetic Circuits are directed acyclic graphs.
- Each internal node: $+$ or $\times$ gate.
- Each leaf: $\{1, 0, -1\}$ or variables $\mathbf{X}$
- Computes a polynomial in $\mathbb{Z}[\mathbf{X}]$

Algebraic Circuits (Constant-free)

- Arithmetic Circuits are directed acyclic graphs.
- Each internal node: $+$ or $\times$ gate.
- Each leaf: $\{1, 0, -1\}$ or variables $\mathbf{X}$
- Computes a polynomial in $\mathbb{Z}[\mathbf{X}]$
- Complexity Measure: $\#$ Edges in the circuit

Tau-Complexity

Given a polynomial $P(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$

Tau-Complexity

Given a polynomial $P(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$

$\tau(P(\mathbf{X}))$: Size of smallest circuit that computes $P(\mathbf{X})$

Tau-Complexity

Given a polynomial $P(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$

$\tau(P(\mathbf{X}))$: Size of smallest circuit that computes $P(\mathbf{X})$

Examples

1. $\tau(2^{2^k}) = \Theta(k), \qquad \tau(x^n) = \Theta(\log n)$

Tau-Complexity

Given a polynomial $P(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$

$\tau(P(\mathbf{X}))$: Size of smallest circuit that computes $P(\mathbf{X})$

Examples

1. $\tau(2^{2^k}) = \Theta(k)$, $\quad \tau(x^n) = \Theta(\log n)$
2. $\tau(n!) = ?$, $\quad \tau(\prod_{i=1}^{n} (x+i)) = ?$

Tau-Complexity

Given a polynomial $P(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$

$\tau(P(\mathbf{X}))$: Size of smallest circuit that computes $P(\mathbf{X})$

Examples

1. $\tau(2^{2^k}) = \Theta(k)$, $\tau(x^n) = \Theta(\log n)$
2. $\tau(n!) =?$, $\tau(\prod_{i=1}^{n}(x+i)) =?$

We believe these are $\geq \Omega(n)$

Tau-Complexity

Blum-Shub-Smale Tau-Conjecture:

Tau-Complexity

Blum-Shub-Smale Tau-Conjecture: For $P(x) \in \mathbb{Z}[x]$

Tau-Complexity

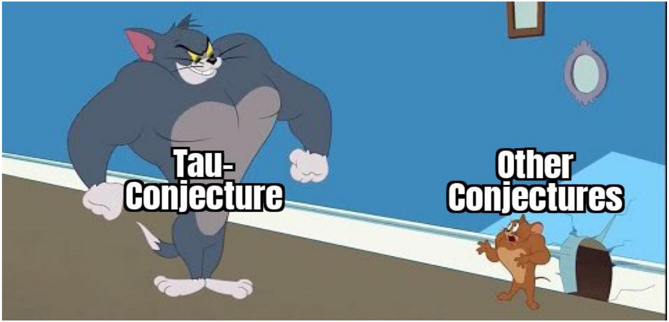
Blum-Shub-Smale Tau-Conjecture: For $P(x) \in \mathbb{Z}[x]$

$$\tau(P(x)) \geq [\# \text{ integer roots of } P(x)]^c$$

Tau-Complexity

Blum-Shub-Smale Tau-Conjecture: For $P(x) \in \mathbb{Z}[x]$

$$\tau(P(x)) \geq [\#\text{ integer roots of } P(x)]^c$$



Exponential sum (VNP_0)

$$P_{n,m}(\mathbf{X}) = \sum_{\mathbf{y} \in \{0,1\}^n} g(\mathbf{X}, \mathbf{y})$$

Exponential sum (VNP_0)

$$P_{n,m}(\mathbf{X}) = \sum_{\mathbf{y}\in\{0,1\}^n} g(\mathbf{X}, \mathbf{y})$$

Circuit size of g is m, $g[\mathbf{X}, \mathbf{Y}] \in \mathbb{Z}[\mathbf{X}, \mathbf{Y}]$.

Exponential sum (VNP_0)

$$P_{n,m}(\mathbf{X}) = \sum_{\mathbf{y}\in\{0,1\}^n} g(\mathbf{X}, \mathbf{y})$$

Circuit size of g is m, $g[\mathbf{X}, \mathbf{Y}] \in \mathbb{Z}[\mathbf{X}, \mathbf{Y}]$.

- Note $\tau(P_{n,m}) \leq 2^n m$

Exponential sum (VNP_0)

$$P_{n,m}(\mathbf{X}) = \sum_{\mathbf{y} \in \{0,1\}^n} g(\mathbf{X}, \mathbf{y})$$

Circuit size of g is m, $g[\mathbf{X}, \mathbf{Y}] \in \mathbb{Z}[\mathbf{X}, \mathbf{Y}]$.

- Note $\tau(P_{n,m}) \leq 2^n m$
- $\tau(P_{m,n}) = 2^{o(n)} poly(m)$ possible?

Exponential sum (VNP_0)

$$P_{n,m}(\mathbf{X}) = \sum_{\mathbf{y} \in \{0,1\}^n} g(\mathbf{X}, \mathbf{y})$$

Circuit size of g is m, $g[\mathbf{X}, \mathbf{Y}] \in \mathbb{Z}[\mathbf{X}, \mathbf{Y}]$.

- Note $\tau(P_{n,m}) \leq 2^n m$
- $\tau(P_{m,n}) = 2^{o(n)} poly(m)$ possible?
- Does τ-conjecture imply some lower bound?

Exponential sum (VNP_0)

$$P_{n,m}(\mathbf{X}) = \sum_{\mathbf{y}\in\{0,1\}^n} g(\mathbf{X},\mathbf{y})$$

Circuit size of g is m, $g[\mathbf{X},\mathbf{Y}] \in \mathbb{Z}[\mathbf{X},\mathbf{Y}]$.

- Note $\tau(P_{n,m}) \leq 2^n m$
- $\tau(P_{m,n}) = 2^{o(n)} poly(m)$ possible?
- Does τ-conjecture imply some lower bound?
- [Bürgisser'07] showed super-polynomial lowerbound on $P_{m,n}$ assuming τ-conjecture

Main result

Conditional Optimal Lower Bound

Assuming τ-conjecture $\exists$ a polynomial family $P_{n,m}(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$ of exponential sum which requires $2^{\Omega(n)} poly(m)$ size circuit.

Bürgisser's Proof analysis

Assume every $P_{n,m}(\mathbf{X})$ has $poly(m)$ circuit

Bürgisser's Proof analysis

Assume every $P_{n,m}(\mathbf{X})$ has $poly(m)$ circuit

$$\Downarrow$$

Lots of Bad things happen

Bürgisser's Proof analysis

Assume every $P_{n,m}(\mathbf{X})$ has $poly(m)$ circuit

$$\Downarrow$$

Lots of Bad things happen

$$\Downarrow$$

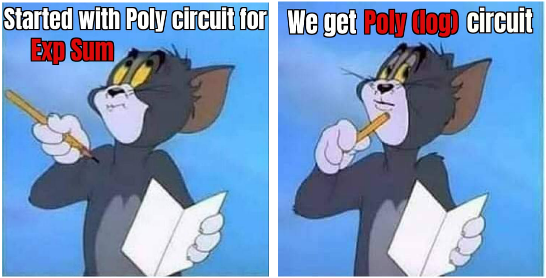
$$\prod_{i=1}^{n}(x+i)$$ has easy coefficients

$$\Downarrow$$

It has poly($\log n$) size circuit

Bürgisser's Proof analysis: Observations

Bürgisser's Proof analysis: Observations



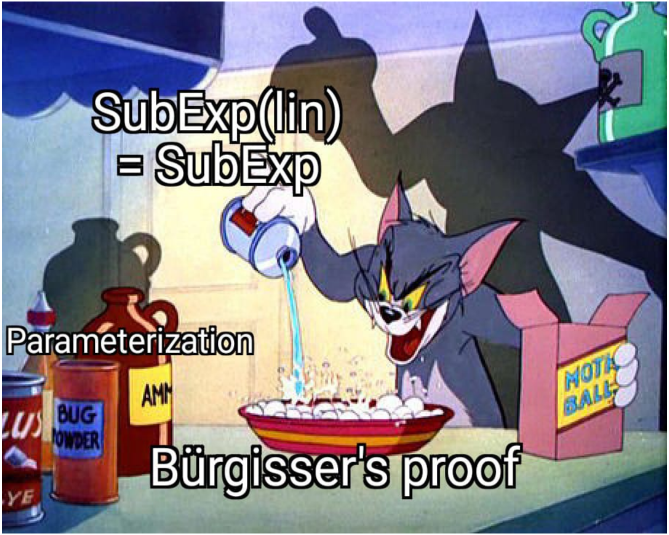
Bürgisser's Proof analysis: Observations

Bürgisser's Proof analysis: Observations

Bürgisser's Proof analysis: Observations

Bürgisser's Proof analysis: Observations

But we can improve it!



What's the Magic

$$\prod_{i=1}^{n} (x+i) = \sum_{k=0}^{n} S_{n,k}(1,\ldots,n)x^k$$

What's the Magic

$$\prod_{i=1}^{n}(x+i)=\sum_{k=0}^{n}S_{n,k}(1,\ldots,n)x^k$$

where

$$S_{n,k}(X_1,\ldots,X_n)=\sum_{S\subseteq[n],|S|=k}\prod_{i\in S}X_i$$

What's the Magic

$1, 2, \ldots, n, \quad x^k$

What's the Magic

$$1 \times \ldots \times k, \quad 2 \times \ldots \times (k+1), \quad \ldots$$

$$1, 2, \ldots, n, \quad x^k$$

What's the Magic

$$S_{n,k} := 1 \times \cdots \times k + 2 \times \cdots \times (k+1) + \ldots$$

$$1 \times \ldots \times k, \quad 2 \times \ldots \times (k+1), \quad \ldots$$

$$1, 2, \ldots, n, \quad x^k$$

What's the Magic

$$S_{n,n}x^n + S_{n,n-1}x^{n-1} + \cdots + S_{n,0}$$

$$S_{n,k} := 1 \times \cdots \times k + 2 \times \cdots \times (k+1) + \ldots$$

$$1 \times \ldots \times k, \quad 2 \times \ldots \times (k+1), \quad \ldots$$

$$1, 2, \ldots, n, \quad x^k$$

What's the Magic

$$S_{n,n}x^n + S_{n,n-1}x^{n-1} + \cdots + S_{n,0}$$

3 level

$$S_{n,k} := 1\times \cdots \times k + 2\times \cdots \times (k+1) + \ldots$$

2 level

$$1\times \ldots \times k, \quad 2\times \ldots \times (k+1), \quad \ldots$$

1 level

$$1, 2, \ldots, n, \quad x^k$$

0 level

Linear Counting Hierarchy

Linear Counting Hierarchy

Linear Counting Hierarchy

Given a complexity class K,

Linear Counting Hierarchy

Linear Counting Hierarchy

Given a complexity class K,
we define $\mathbf{C}_{lin}.K$ by

Linear Counting Hierarchy

Linear Counting Hierarchy

Given a complexity class K,
we define $\mathbf{C}_{lin}.K$ by
$A \in \mathbf{C}_{lin}.K$ if there is some $B \in K$

Linear Counting Hierarchy

Linear Counting Hierarchy

Given a complexity class K,
we define $\mathbf{C}_{lin}.K$ by
$A \in \mathbf{C}_{lin}.K$ if there is some $B \in K$
and a linear function $\ell : \mathbb{N} \to \mathbb{N}$, $\ell(n) = O(n)$

Linear Counting Hierarchy

Linear Counting Hierarchy

Given a complexity class K,
we define $\mathbf{C}_{lin}.K$ by
$A \in \mathbf{C}_{lin}.K$ if there is some $B \in K$
and a linear function $\ell : \mathbb{N} \to \mathbb{N}$, $\ell(n) = O(n)$
and some polynomial time computable function $f : \{0,1\}^* \to \mathbb{N}$

Linear Counting Hierarchy

Linear Counting Hierarchy

Given a complexity class K,
we define $\mathbf{C}_{lin}.K$ by
$A \in \mathbf{C}_{lin}.K$ if there is some $B \in K$
and a linear function $\ell : \mathbb{N} \to \mathbb{N}$, $\ell(n) = O(n)$
and some polynomial time computable function $f : \{0,1\}^* \to \mathbb{N}$
such that,

$$x \in A \iff |\{y \in \{0,1\}^{\ell(|x|)} : \langle x, y \rangle \in B\}| > f(x).$$

Linear Counting Hierarchy

Linear Counting Hierarchy

Given a complexity class K,

Linear Counting Hierarchy

Linear Counting Hierarchy

Given a complexity class K,
We define $\text{C-lin}_0 K := K$ and for all $k \in \mathbb{N}$,
$\text{C-lin}_{k+1} K := \mathbf{C}_{\text{lin}}.\text{C-lin}_k K$.

Linear Counting Hierarchy

Linear Counting Hierarchy

Given a complexity class K,
We define $\text{C-lin}_0 K := K$ and for all $k \in \mathbb{N}$,
$\text{C-lin}_{k+1} K := \mathbf{C}_{\text{lin}}.\text{C-lin}_k K$.
The *linear counting hierarchy* is $\text{CH}_{\text{lin}} K := \bigcup_{k \geq 0} \text{C-lin}_k K$

Linear Counting Hierarchy ($\mathsf{CH}_{\mathrm{lin}}$)

Characterization of $\mathsf{CH}_{\mathrm{lin}}$

$(k+1)^{\mathsf{th}}$ level of $\mathsf{CH}_{\mathrm{lin}}$ is Exponential sum of k^{th} level

Linear Counting Hierarchy ($\mathrm{CH}_{\mathrm{lin}}$)

Characterization of $\mathrm{CH}_{\mathrm{lin}}$

$(k+1)^{\text{th}}$ level of $\mathrm{CH}_{\mathrm{lin}}$ is Exponential sum of k^{th} level

Hence Exponential sum is EASY $\implies$ $\mathrm{CH}_{\mathrm{lin}}$ collapses

$$\implies \prod_{i=1}^{n}(x+i) \text{ is EASY}$$

Permanent

Given a variable matrix

$$\mathbf{X} := \begin{bmatrix} X_{11} & X_{12} & \dots & X_{1n} \\ X_{21} & X_{22} & \dots & X_{2n} \\ \vdots & & \ddots & \vdots \\ X_{n1} & X_{s2} & \dots & X_{nn} \end{bmatrix}_{n\times n}$$

Permanent

Given a variable matrix

$$\mathbf{X} := \begin{bmatrix} X_{11} & X_{12} & \dots & X_{1n} \\ X_{21} & X_{22} & \dots & X_{2n} \\ \vdots & & \ddots & \vdots \\ X_{n1} & X_{s2} & \dots & X_{nn} \end{bmatrix}_{n \times n}$$

$$Per_n(\mathbf{X}) := \sum_{\sigma \in S_n} X_{1,\sigma_1} X_{2,\sigma_2} \dots X_{n,\sigma_n}$$

Completeness of Permanent

Ryser formula: Per_n can be written as Exponential sum (n, n^2)

Completeness of Permanent

Ryser formula: Per_n can be written as Exponential sum (n, n^2)

[Valiant 79]: Any Exponential sum (n, m) can be written as Per of $m^4 \times m^4$ matrix with entries $1, 0, -1, \mathbf{X}$

Completeness of Permanent

Ryser formula: Per_n can be written as Exponential sum (n, n^2)

[Valiant 79]: Any Exponential sum (n, m) can be written as Per of $m^4 \times m^4$ matrix with entries $1, 0, -1, \mathbf{X}$

- Super Polynomial lower bound on Exponential sum $\iff$ Super Polynomial lower bound on Per

Completeness of Permanent

Ryser formula: Per_n can be written as Exponential sum (n, n^2)

[Valiant 79]: Any Exponential sum (n, m) can be written as Per of $m^4 \times m^4$ matrix with entries $1, 0, -1, \mathbf{X}$

- Super Polynomial lower bound on Exponential sum $\iff$ Super Polynomial lower bound on Per
- NOT true for Exponential lower bounds

Completeness of Permanent

Ryser formula: Per_n can be written as Exponential sum (n, n^2)

[Valiant 79]: Any Exponential sum (n, m) can be written as Per of $m^4 \times m^4$ matrix with entries $1, 0, -1, \mathbf{X}$

- Super Polynomial lower bound on Exponential sum $\iff$ Super Polynomial lower bound on Per
- NOT true for Exponential lower bounds
- We gave $2^{n^{1/8}}$ lower bound for Per_n

Completeness of Permanent

Ryser formula: Per_n can be written as Exponential sum (n, n^2)

[Valiant 79]: Any Exponential sum (n, m) can be written as Per of $m^4 \times m^4$ matrix with entries $1, 0, -1, \mathbf{X}$

- Super Polynomial lower bound on Exponential sum $\iff$ Super Polynomial lower bound on Per
- NOT true for Exponential lower bounds
- We gave $2^{n^{1/8}}$ lower bound for Per_n (Conditionally)

Other Results

1. We achieved optimal lower bound from tau conjecture for Parameterized Algebraic classes defined in [Bläser and Engles 18] (which are analogous to $\#W[t]$ classes)

Other Results

1. We achieved optimal lower bound from tau conjecture for Parameterized Algebraic classes defined in [Bläser and Engles 18] (which are analogous to $\#W[t]$ classes)

2. We achieved completeness result for parameterized valiant classes.

Open Problems

1. Can we established conditional truly exponential (ie, $2^{\Omega(n)}poly(n)$) lower bound for Per_n? (Unconditional will be better :))

2. Can we get Lower Bounds for NP from tau-conjecture? (We don't know even super-polynomial bound)