Lower Bounds for some Algebraic Models of Computation

Prerona Chatterjee

March 27, 2024

• design a computational model that captures the constraints

- design a computational model that captures the constraints
- study the amount of resource required by the model to complete the task.

- design a computational model that captures the constraints
- study the amount of resource required by the model to complete the task.

Traditional Time Complexity: Given a boolean function f on n inputs, how many steps are required by a Turing machine to compute the f (in terms of n)?

- design a computational model that captures the constraints
- study the amount of resource required by the model to complete the task.

Traditional Time Complexity: Given a boolean function f on n inputs, how many steps are required by a Turing machine to compute the f (in terms of n)?

Communication Complexity: Given a boolean function f, assuming Alice and Bob are computationally unbounded but have partial inputs $\mathbf{x}, \mathbf{y} \in \{0, 1\}^n$ respectively, how many bits need to be communicated for them to know $f(\mathbf{x}, \mathbf{y})$ (in terms of n)?

- design a computational model that captures the constraints
- study the amount of resource required by the model to complete the task.

Traditional Time Complexity: Given a boolean function f on n inputs, how many steps are required by a Turing machine to compute the f (in terms of n)?

Communication Complexity: Given a boolean function f, assuming Alice and Bob are computationally unbounded but have partial inputs $\mathbf{x}, \mathbf{y} \in \{0, 1\}^n$ respectively, how many bits need to be communicated for them to know $f(\mathbf{x}, \mathbf{y})$ (in terms of n)?

Boolean Circuit Complexity: Given a boolean function f on n inputs, how many \land , \lor , \neg gates are needed for a boolean circuit to compute f (in terms of n)?

Q: Given $f(\mathbf{x}) \in \mathbb{F}[x_1, \ldots, x_n]$ of degree *d*, how many $+, \times, -$ gates are needed to compute *f*?

Q: Given $f(\mathbf{x}) \in \mathbb{F}[x_1, \ldots, x_n]$ of degree d, how many $+, \times, -$ gates are needed to compute f?



Q: Given $f(\mathbf{x}) \in \mathbb{F}[x_1, \ldots, x_n]$ of degree *d*, how many $+, \times, -$ gates are needed to compute *f*?







• Label on each edge: An affine linear form in $\{x_1, x_2, \dots, x_n\}$



- Label on each edge: An affine linear form in $\{x_1, x_2, \ldots, x_n\}$
- Polynomial computed by the path p = wt(p): Product of the edge labels on p



- Label on each edge: An affine linear form in $\{x_1, x_2, \ldots, x_n\}$
- Polynomial computed by the path p = wt(p): Product of the edge labels on p
- Polynomial computed by the ABP: $f_{\mathcal{A}}(\mathbf{x}) = \sum_{p} \operatorname{wt}(p)$

VP: Polynomials computable by circuits of size poly(n, d).



VF: Polynomials computable by formulas of size poly(n, d).

VP: Polynomials computable by circuits of size poly(n, d).



VF: Polynomials computable by formulas of size poly(n, d).

VBP: Polynomials computable by ABPs of size poly(n, d).

VP: Polynomials computable by circuits of size poly(n, d).



VF: Polynomials computable by formulas of size poly(n, d).

VBP: Polynomials computable by ABPs of size poly(n, d).

VP: Polynomials computable by circuits of size poly(n, d).

VNP: Explicit Polynomials



VF: Polynomials computable by formulas of size poly(n, d).

VBP: Polynomials computable by ABPs of size poly(n, d).

VP: Polynomials computable by circuits of size poly(n, d).

VNP: Explicit Polynomials



Central Question: Find explicit polynomials that cannot be computed by efficient circuits.

VF: Polynomials computable by formulas of size poly(n, d).

VBP: Polynomials computable by ABPs of size poly(n, d).

VP: Polynomials computable by circuits of size poly(n, d).

VNP: Explicit Polynomials

Are the inclusions tight?



Central Question: Find explicit polynomials that cannot be computed by efficient circuits.

[Baur-Strassen]: Any algebraic circuit computing $\sum_{i=1}^{n} x_i^d$ requires $\Omega(n \log d)$ wires.

[Baur-Strassen]: Any algebraic circuit computing $\sum_{i=1}^{n} x_i^d$ requires $\Omega(n \log d)$ wires.

General ABPs

[C-Kumar-She-Volk]: Any ABP computing $\sum_{i=1}^{n} x_i^d$ requires $\Omega(nd)$ vertices.

[Baur-Strassen]: Any algebraic circuit computing $\sum_{i=1}^{n} x_i^d$ requires $\Omega(n \log d)$ wires.

General ABPs

[C-Kumar-She-Volk]: Any ABP computing $\sum_{i=1}^{n} x_i^d$ requires $\Omega(nd)$ vertices.

General Formulas

[Kalorkoti]: Any formula computing the n^2 -variate $Det_n(\mathbf{x})$ requires $\Omega(n^3)$ wires.

[Baur-Strassen]: Any algebraic circuit computing $\sum_{i=1}^{n} x_i^d$ requires $\Omega(n \log d)$ wires.

General ABPs

[C-Kumar-She-Volk]: Any ABP computing $\sum_{i=1}^{n} x_i^d$ requires $\Omega(nd)$ vertices.

General Formulas

[Kalorkoti]: Any formula computing the n^2 -variate $Det_n(\mathbf{x})$ requires $\Omega(n^3)$ wires.

[Shpilka-Yehudayoff] (using Kalorkoti's method): There is an *n*-variate multilinear polynomial such that any formula computing it requires $\Omega(n^2/\log n)$ wires.

[Baur-Strassen]: Any algebraic circuit computing $\sum_{i=1}^{n} x_i^d$ requires $\Omega(n \log d)$ wires.

General ABPs

[C-Kumar-She-Volk]: Any ABP computing $\sum_{i=1}^{n} x_i^d$ requires $\Omega(nd)$ vertices.

General Formulas

[Kalorkoti]: Any formula computing the n^2 -variate $Det_n(\mathbf{x})$ requires $\Omega(n^3)$ wires.

[Shpilka-Yehudayoff] (using Kalorkoti's method): There is an *n*-variate multilinear polynomial such that any formula computing it requires $\Omega(n^2/\log n)$ wires.

[C-Kumar-She-Volk]: Any formula computing $\text{ESYM}_{n,0.1n}(\mathbf{x})$ requires $\Omega(n^2)$ vertices, where

$$\mathrm{ESYM}_{n,d}(\mathbf{x}) = \sum_{i_1 < \cdots < i_d \in [n]} x_{i_1} \cdots x_{i_d}.$$

Show that if a structured *n*-variate, degree-*d* polynomial is computable by a general model of size *s*, then they can also be computed by a structured model of size func(s, n, d) for some function func.

Show that if a structured *n*-variate, degree-*d* polynomial is computable by a general model of size *s*, then they can also be computed by a structured model of size func(s, n, d) for some function func.

Study Structured Models

Prove strong lower bounds against structured models computing f.

Show that if a structured *n*-variate, degree-*d* polynomial is computable by a general model of size *s*, then they can also be computed by a structured model of size func(s, n, d) for some function func.

[Agrawal-Vinay, Koiran, Tavenas]

Size *s* circuits computing *n*-variate degree *d* polynomials can be converted into depth-4 circuits of size $s^{O(\sqrt{d})}$.

Study Structured Models

Prove strong lower bounds against structured models computing f.

Show that if a structured *n*-variate, degree-*d* polynomial is computable by a general model of size *s*, then they can also be computed by a structured model of size func(s, n, d) for some function func.

[Agrawal-Vinay, Koiran, Tavenas]

Size *s* circuits computing *n*-variate degree *d* polynomials can be converted into depth-4 circuits of size $s^{O(\sqrt{d})}$.

[Gupta-Kamath-Kayal-Saptharishi]

Size *s* circuits computing *n*-variate degree *d* polynomials can be converted into depth-3 circuits of size $s^{O(\sqrt{d})}$.

Study Structured Models

Prove strong lower bounds against structured models computing f.

Show that if a structured *n*-variate, degree-*d* polynomial is computable by a general model of size *s*, then they can also be computed by a structured model of size func(s, n, d) for some function func.

[Agrawal-Vinay, Koiran, Tavenas]

Size *s* circuits computing *n*-variate degree *d* polynomials can be converted into depth-4 circuits of size $s^{O(\sqrt{d})}$.

[Gupta-Kamath-Kayal-Saptharishi]

Size *s* circuits computing *n*-variate degree *d* polynomials can be converted into depth-3 circuits of size $s^{O(\sqrt{d})}$.

Study Structured Models Prove strong lower bounds against structured models

computing f.

A lot of work that culminated in

[Limaye-Srinivasan-Tavenas] Any depth-3 or depth-4 circuit computing $IMM_{n,\log n}(\mathbf{x})$ must have size $n^{\Omega(\sqrt{d})}$. **[C-Kumar-She-Volk]**: Any ABP computing $\sum_{i=1}^{n} x_i^d$ requires $\Omega(nd)$ vertices.

[C-Kumar-She-Volk]: Any ABP computing $\sum_{i=1}^{n} x_i^d$ requires $\Omega(nd)$ vertices.

[Bhargav-Dwivedi-Saxena]: Super polynomial lower bound against total-width of $\sum \text{osmABP}$ for a polynomial of degree $d = O\left(\frac{\log n}{\log \log n}\right) \implies$ super-polynomial lower bound against ABPs.

[C-Kumar-She-Volk]: Any ABP computing $\sum_{i=1}^{n} x_i^d$ requires $\Omega(nd)$ vertices.

[Bhargav-Dwivedi-Saxena]: Super polynomial lower bound against total-width of $\sum \text{osmABP}$ for a polynomial of degree $d = O\left(\frac{\log n}{\log \log n}\right) \implies$ super-polynomial lower bound against ABPs.

[C-Kush-Saraf-Shpilka]: For $\omega(\log n) = d \leq n$, there is a polynomial $G_{n,d}(\mathbf{x})$ which is set-multilinear w.r.t $\mathbf{x} = {\mathbf{x}_1, \dots, \mathbf{x}_d}$, where $|\mathbf{x}_i| \leq n$ for every $i \in [d]$, such that:

- $G_{n,d}$ is computable by a set-multilinear ABP of size poly(n),
- any $\sum \text{osmABP}$ computing $G_{n,d}$ must have super-polynomial total-width.

The variable set is divided into buckets.

$$\mathbf{x} = \mathbf{x}_1 \cup \cdots \cup \mathbf{x}_d$$
 where $\mathbf{x}_i = \{x_{i,1}, \dots, x_{i,n_i}\}$.

The variable set is divided into buckets.

$$\mathbf{x} = \mathbf{x}_1 \cup \cdots \cup \mathbf{x}_d$$
 where $\mathbf{x}_i = \{x_{i,1}, \dots, x_{i,n_i}\}$.

f is set-multilinear with respect to $\{\mathbf{x}_1, \ldots, \mathbf{x}_d\}$ if

every monomial in f has exactly one variable from \mathbf{x}_i for each $i \in [d]$.

The variable set is divided into buckets.

$$\mathbf{x} = \mathbf{x}_1 \cup \cdots \cup \mathbf{x}_d$$
 where $\mathbf{x}_i = \{x_{i,1}, \dots, x_{i,n_i}\}$.

f is set-multilinear with respect to $\{x_1, \ldots, x_d\}$ if

every monomial in f has exactly one variable from \mathbf{x}_i for each $i \in [d]$.

An ABP is set-multilinear with respect to $\{\mathbf{x}_1, \dots, \mathbf{x}_d\}$ if every path in it

computes a set-multilinear monomial with respect to $\{\mathbf{x}_1, \ldots, \mathbf{x}_d\}$.

For $\sigma \in S_d$, an ABP is σ -ordered set-multilinear with respect to $\{\mathbf{x}_1, \dots, \mathbf{x}_d\}$ if

- there are *d* layers in the ABP
- every edge in layer *i* is labelled by a homogeneous linear form in $\mathbf{x}_{\sigma(i)}$

For $\sigma \in S_d$, an ABP is σ -ordered set-multilinear with respect to $\{\mathbf{x}_1, \ldots, \mathbf{x}_d\}$ if

- there are *d* layers in the ABP
- every edge in layer *i* is labelled by a homogeneous linear form in $\mathbf{x}_{\sigma(i)}$

 \sum osmABP: Sum of ordered set-multilinear ABPs, each with a possibly different ordering.

For $\sigma \in S_d$, an ABP is σ -ordered set-multilinear with respect to $\{\mathbf{x}_1, \dots, \mathbf{x}_d\}$ if

- there are *d* layers in the ABP
- every edge in layer *i* is labelled by a homogeneous linear form in $\mathbf{x}_{\sigma(i)}$

 \sum osmABP: Sum of ordered set-multilinear ABPs, each with a possibly different ordering.

[Bhargav-Dwivedi-Saxena]: Super polynomial lower bound against total-width of $\sum \text{osmABP}$ for a polynomial of degree $d = O\left(\frac{\log n}{\log \log n}\right) \implies$ super-polynomial lower bound against ABPs.

For $\sigma \in S_d$, an ABP is σ -ordered set-multilinear with respect to $\{\mathbf{x}_1, \ldots, \mathbf{x}_d\}$ if

- there are *d* layers in the ABP
- every edge in layer *i* is labelled by a homogeneous linear form in $\mathbf{x}_{\sigma(i)}$

 \sum osmABP: Sum of ordered set-multilinear ABPs, each with a possibly different ordering.

[Bhargav-Dwivedi-Saxena]: Super polynomial lower bound against total-width of \sum osmABP for a polynomial of degree $d = O\left(\frac{\log n}{\log \log n}\right) \implies$ super-polynomial lower bound against ABPs.

[C-Kush-Saraf-Shpilka]: Super polynomial lower bound against total-width of $\sum \text{osmABP}$ for a polynomial of degree $d = \omega(\log n)$ that is computable by polynomial-sized ABPs.

Non-Commutativity

$$f(x, y) = (x + y) \times (x + y) = x^{2} + xy + yx + y^{2} \neq x^{2} + 2xy + y^{2}$$

$$f(x, y) = (x + y) \times (x + y) = x^{2} + xy + yx + y^{2} \neq x^{2} + 2xy + y^{2}$$

$$f(x, y) = (x + y) \times (x + y) = x^{2} + xy + yx + y^{2} \neq x^{2} + 2xy + y^{2}$$

Can we do better in this setting?

$$f(x, y) = (x + y) \times (x + y) = x^{2} + xy + yx + y^{2} \neq x^{2} + 2xy + y^{2}$$

Can we do better in this setting? For general circuits, continues to be $\Omega(n \log d)$.

$$f(x,y) = (x + y) \times (x + y) = x^{2} + xy + yx + y^{2} \neq x^{2} + 2xy + y^{2}$$

Can we do better in this setting? For general circuits, continues to be $\Omega(n \log d)$.

[C-Hrubeš]: Any homogeneous non-commutative circuit computing

$$\operatorname{OSym}_{n,d}(\mathbf{x}) = \sum_{1 \le i_1 < \dots < i_d \le n} x_{i_1} \cdots x_{i_d}$$

has size $\Omega(nd)$ for $d \leq \frac{n}{2}$.

$$f(x,y) = (x + y) \times (x + y) = x^{2} + xy + yx + y^{2} \neq x^{2} + 2xy + y^{2}$$

Can we do better in this setting? For general circuits, continues to be $\Omega(n \log d)$.

[C-Hrubeš]: Any homogeneous non-commutative circuit computing

$$\operatorname{OSym}_{n,d}(\mathbf{x}) = \sum_{1 \le i_1 < \cdots < i_d \le n} x_{i_1} \cdots x_{i_d}$$

has size $\Omega(nd)$ for $d \leq \frac{n}{2}$. The lower bound is tight for homogeneous non-commutative circuits.

$$f(x,y) = (x + y) \times (x + y) = x^{2} + xy + yx + y^{2} \neq x^{2} + 2xy + y^{2}$$

Can we do better in this setting? For general circuits, continues to be $\Omega(n \log d)$.

[C-Hrubeš]: Any homogeneous non-commutative circuit computing

$$\operatorname{OSym}_{n,d}(\mathbf{x}) = \sum_{1 \le i_1 < \cdots < i_d \le n} x_{i_1} \cdots x_{i_d}$$

has size $\Omega(nd)$ for $d \leq \frac{n}{2}$. The lower bound is tight for homogeneous non-commutative circuits.

[Nisan]: Any ABP computing $\operatorname{Pal}_n(x_0, x_1) = \sum_{w \in \{0,1\}^{n/2}} \mathbf{x}_w \cdot \mathbf{x}_{w^R}$ has size $2^{\Omega(n)}$.

(bucket index) ordered set-multilinear \equiv homogeneous non-commutative (position index)

(bucket index) ordered set-multilinear \equiv homogeneous non-commutative (position index)

Abecedarian Polynomials: Let $f \in \mathbb{F} \langle \mathbf{x} \rangle$ and $\{X_1, \ldots, X_m\}$ be a partition of \mathbf{x} into buckets.

(bucket index) ordered set-multilinear \equiv homogeneous non-commutative (position index)

Abecedarian Polynomials: Let $f \in \mathbb{F} \langle \mathbf{x} \rangle$ and $\{X_1, \ldots, X_m\}$ be a partition of \mathbf{x} into buckets. f is abecedarian with respect to $\{X_1, \ldots, X_m\}$ if every monomial in f has the form $X_1^* X_2^* \cdots X_m^*$.

(bucket index) ordered set-multilinear \equiv homogeneous non-commutative (position index)

Abecedarian Polynomials: Let $f \in \mathbb{F} \langle \mathbf{x} \rangle$ and $\{X_1, \ldots, X_m\}$ be a partition of \mathbf{x} into buckets. f is abecedarian with respect to $\{X_1, \ldots, X_m\}$ if every monomial in f has the form $X_1^* X_2^* \cdots X_m^*$.

[Cha]: For $\mathbf{x} = \bigcup_{i \in [n]} \{X_i\}$ with $X_i = \{x_{i,j}\}_{j \in [n]}$,

(bucket index) ordered set-multilinear \equiv homogeneous non-commutative (position index)

Abecedarian Polynomials: Let $f \in \mathbb{F} \langle \mathbf{x} \rangle$ and $\{X_1, \ldots, X_m\}$ be a partition of \mathbf{x} into buckets. f is abecedarian with respect to $\{X_1, \ldots, X_m\}$ if every monomial in f has the form $X_1^* X_2^* \cdots X_m^*$.

[Cha]: For $\mathbf{x} = \bigcup_{i \in [n]} \{X_i\}$ with $X_i = \{x_{i,j}\}_{j \in [n]}$, there exists a (log *n*)-degree abecedarian polynomial $f \in \mathbb{F} \langle \mathbf{x} \rangle$

(bucket index) ordered set-multilinear \equiv homogeneous non-commutative (position index)

Abecedarian Polynomials: Let $f \in \mathbb{F} \langle \mathbf{x} \rangle$ and $\{X_1, \ldots, X_m\}$ be a partition of \mathbf{x} into buckets. f is abecedarian with respect to $\{X_1, \ldots, X_m\}$ if every monomial in f has the form $X_1^* X_2^* \cdots X_m^*$.

[Cha]: For $\mathbf{x} = \bigcup_{i \in [n]} \{X_i\}$ with $X_i = \{x_{i,j}\}_{j \in [n]}$, there exists a $(\log n)$ -degree abecedarian polynomial $f \in \mathbb{F} \langle \mathbf{x} \rangle$ such that any abecedarian formula computing it has size $n^{\Omega(\log \log n)}$.

(bucket index) ordered set-multilinear \equiv homogeneous non-commutative (position index)

Abecedarian Polynomials: Let $f \in \mathbb{F} \langle \mathbf{x} \rangle$ and $\{X_1, \ldots, X_m\}$ be a partition of \mathbf{x} into buckets. f is abecedarian with respect to $\{X_1, \ldots, X_m\}$ if every monomial in f has the form $X_1^* X_2^* \cdots X_m^*$.

[Cha]: For $\mathbf{x} = \bigcup_{i \in [n]} \{X_i\}$ with $X_i = \{x_{i,j}\}_{j \in [n]}$, there exists a $(\log n)$ -degree abecedarian polynomial $f \in \mathbb{F} \langle \mathbf{x} \rangle$ such that any abecedarian formula computing it has size $n^{\Omega(\log \log n)}$. If an *n*-variate polynomial is abecedarian with respect to $\{X_1, \ldots, X_m\}$ for $m = \log n$,

(bucket index) ordered set-multilinear \equiv homogeneous non-commutative (position index)

Abecedarian Polynomials: Let $f \in \mathbb{F} \langle \mathbf{x} \rangle$ and $\{X_1, \ldots, X_m\}$ be a partition of \mathbf{x} into buckets. f is abecedarian with respect to $\{X_1, \ldots, X_m\}$ if every monomial in f has the form $X_1^* X_2^* \cdots X_m^*$.

[Cha]: For $\mathbf{x} = \bigcup_{i \in [n]} \{X_i\}$ with $X_i = \{x_{i,j}\}_{j \in [n]}$, there exists a $(\log n)$ -degree abecedarian polynomial $f \in \mathbb{F} \langle \mathbf{x} \rangle$ such that any abecedarian formula computing it has size $n^{\Omega(\log \log n)}$.

If an *n*-variate polynomial is abecedarian with respect to $\{X_1, \ldots, X_m\}$ for $m = \log n$, then any formula computing f can be made abecedarian with only poly(n) blow-up in size.

• Better lower bounds against homogeneous formulas?

- Better lower bounds against homogeneous formulas?
- Better lower bounds against set-multilinear ABPs?

- Better lower bounds against homogeneous formulas?
- Better lower bounds against set-multilinear ABPs?
- Bootstrapping statement, similar to [CILM], which is sensitive to both degree and number of variables?

- Better lower bounds against homogeneous formulas?
- Better lower bounds against set-multilinear ABPs?
- Bootstrapping statement, similar to [CILM], which is sensitive to both degree and number of variables?
- Separating formulas and ABPs in the non-commutative setting?

- Better lower bounds against homogeneous formulas?
- Better lower bounds against set-multilinear ABPs?
- Bootstrapping statement, similar to [CILM], which is sensitive to both degree and number of variables?
- Separating formulas and ABPs in the non-commutative setting?

Questions?