A Quadratic Size-Hierarchy Theorem for Small-Depth Multilinear Formulas

Suryajith Chillara

Joint work with

Nutan Limaye   Srikanth Srinivasan

WACT 2019, ICTS-TIFR, Bangalore.
28.03.2019

Fundamental Question

$$\textbf{More resources} \overset{?}{\Longrightarrow} \textbf{More computational power.}$$

Fundamental Question

$$\textbf{More resources} \stackrel{?}{\Longrightarrow} \textbf{More computational power.}$$

Answer: Yes in many cases.
Eg., *Time Hierarchy* and *Space Hierarchy* theorems in the classical complexity.

Classical Hierarchy Theorems over Turing Machines

Time Hierarchy Theorem

For every $t(n)$ and $\delta > 0$, there is a decision problem which can be solved in time $t(n)$ but not in the time $t(n)^{1-\delta}$, i.e., $\mathsf{DTIME}(t(n)^{1-\delta}) \subsetneq \mathsf{DTIME}(t(n))$.

Space Hierarchy Theorem

For every $s(n)$ and $\delta > 0$, there is a language L that is decidable in space $s(n)$ but not in space $s(n)^{1-\delta}$, i.e., $\mathsf{SPACE}(s(n)^{1-\delta}) \subsetneq \mathsf{SPACE}(s(n))$.

Generalized Meta Theorem for Any Resource

For every $f(n)$, there is a function that can be computed using $f(n)$ resources but cannot be computed using $\ll f(n)$ resources.

This gives us a strict computational hierarchy between $\ll f(n)$ resources and $f(n)$ resources.

Generalized Meta Theorem for Any Resource

For every $f(n)$, there is a function that can be computed using $f(n)$ resources but cannot be computed using $\ll f(n)$ resources.

This gives us a strict computational hierarchy between $\ll f(n)$ resources and $f(n)$ resources.

- **Our goal:** Similar theorems for *Arithmetic Formulas*.

Generalized Meta Theorem for Any Resource

For every $f(n)$, there is a function that can be computed using $f(n)$ resources but cannot be computed using $\ll f(n)$ resources.

This gives us a strict computational hierarchy between $\ll f(n)$ resources and $f(n)$ resources.

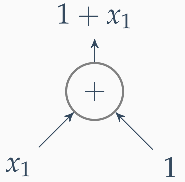
- **Our goal:** Similar theorems for *Arithmetic Formulas*.
- **Resource:** *Size* of the arithmetic formula, which corresponds to the maximum number of arithmetic operations.

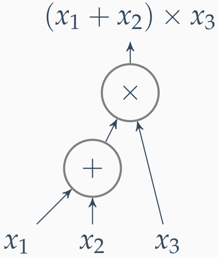
Computing polynomials syntactically

Definition

An Arithmetic Formula Φ over the field $\mathbb{F}$ and the set of variables $X = (x_1, x_2, \ldots, x_n)$ is a *directed tree* as follows:

- Leaf nodes are labelled either by a variable or a field element from $\mathbb{F}$ and the root node outputs the polynomial.
- Every other node is labelled by either $\times$ or $+$).
- The size of Φ is the number of nodes present in it.
- The depth of Φ is the length of the longest leaf to root path.





Size Hierarchy for Arithmetic Formulas

$$\textbf{More size} \stackrel{?}{\Longrightarrow} \textbf{More computational power.}$$

Size Hierarchy for Arithmetic Formulas

$$\textbf{More size} \overset{?}{\Longrightarrow} \textbf{More computational power.}$$

Fundamental Question Rephrased: Size Hierarchy

For any $\delta > 0$ and $s = n^c$, show that there is a polynomial P_n that it is computed by a formula of size $s(n)$ but not by formulas of size $s(n)^{1-\delta}$.

Size Hierarchy for Arithmetic Formulas

More size $\overset{?}{\Longrightarrow}$ More computational power.

Fundamental Question Rephrased: Size Hierarchy

For any $\delta > 0$ and $s = n^c$, show that there is a polynomial P_n that it is computed by a formula of size $s(n)$ but not by formulas of size $s(n)^{1-\delta}$.

- No techniques are available to prove size lower bounds any better than $\tilde{\Omega}(n^3)$ [Kayal et al., 2016, Balaji et al., 2016] for small depth circuits and $\Omega(n^2)$ [Kalorkoti, 1985] for general formulas.

Size Hierarchy for Arithmetic Formulas

More size $\stackrel{?}{\Longrightarrow}$ More computational power.

Fundamental Question Rephrased: Size Hierarchy

For any $\delta > 0$ and $s = n^c$, show that there is a polynomial P_n that it is computed by a formula of size $s(n)$ but not by formulas of size $s(n)^{1-\delta}$.

- No techniques are available to prove size lower bounds any better than $\tilde{\Omega}(n^3)$ [Kayal et al., 2016, Balaji et al., 2016] for small depth circuits and $\Omega(n^2)$ [Kalorkoti, 1985] for general formulas.
- Some techniques are available to prove lower bounds against formulas when every computation is restricted to be *multilinear*.

Multilinear polynomial

A polynomial $f \in \mathbb{F}[X]$ is called *multilinear* if the degree of f in each variable $x \in X$ is at most 1.

Multilinear polynomial

A polynomial $f \in \mathbb{F}[X]$ is called *multilinear* if the degree of f in each variable $x \in X$ is at most 1.

Multilinear Formula

An arithmetic formula is said to be multilinear if the polynomial computed at each gate is multilinear.

Multilinear polynomial

A polynomial $f \in \mathbb{F}[X]$ is called *multilinear* if the degree of f in each variable $x \in X$ is at most 1.

Multilinear Formula

An arithmetic formula is said to be multilinear if the polynomial computed at each gate is multilinear.

Syntactic Multilinearity

A product is said to be syntactically multilinear if the inputs are defined over disjoint sets of variables.

Multilinear polynomial

A polynomial $f \in \mathbb{F}[X]$ is called *multilinear* if the degree of f in each variable $x \in X$ is at most 1.

Multilinear Formula

An arithmetic formula is said to be multilinear if the polynomial computed at each gate is multilinear.

Syntactic Multilinearity

A product is said to be syntactically multilinear if the inputs are defined over disjoint sets of variables.

$$(x_1 + x_2)(x_1 + x_3) - (x_1 + x_4)(x_1 + x_2) = x_1x_3 + x_2x_3 - x_1x_4 - x_2x_4.$$

This is not a syntactically multilinear computation.

Size Hierarchy for Multilinear Formulas

Theorem ([Raz, 2004, Raz and Yehudayoff, 2008])

For any $s = n^c$ where c is a fixed constant, there is an explicit polynomial that can be computed by a multilinear arithmetic formula of size $s(n)$ but not by any multilinear arithmetic formulas of size $s(n)^\alpha$ where $\alpha \leq 1/30$.

Size Hierarchy for Multilinear Formulas

Theorem ([Raz, 2004, Raz and Yehudayoff, 2008])

For any $s = n^c$ where c is a fixed constant, there is an explicit polynomial that can be computed by a multilinear arithmetic formula of size $s(n)$ but not by any multilinear arithmetic formulas of size $s(n)^\alpha$ where $\alpha \leq 1/30$.

Theorem (This work)

For any $\delta \in (0, 1/2)$ and $s(n) = n^c$ for some fixed constant c, there is an explicit polynomial that can be computed by a multilinear arithmetic formula of size $s(n)$ and depth-3 but not by any multilinear formulas of size $s^{0.5-\delta}$ and depth $O(\log s / \log \log s)$.

Related Work

Our result is incomparable to the works [Raz, 2004] and [Raz and Yehudayoff, 2008].

Related Work

Our result is incomparable to the works [Raz, 2004] and [Raz and Yehudayoff, 2008].

[Raz, 2004, Raz and Yehudayoff, 2008]	This Work
There is no restriction on the depth of multilinear formulas.	👎 We can prove a size lower bound only when the depth is $O(\log s / \log\log s)$.
The separation they show is s vs s^{α} where $\alpha < 1/30$, even at small-depths.	👍 At small-depths, we show a better separation of s vs $s^{1/2-\delta}$.
The hard polynomial has a formula of size s and depth $\Omega(\sqrt{\log s})$.	👍 The hard polynomial has a formula of size s and depth 3.

Tools & Techniques

Theme of the proofs

- We can define a suitable complexity measure $\mu : \mathbb{F}[X] \mapsto \mathbb{N}$ such that the following holds:
  - If f is computed by a *small*-depth multilinear formula then $\mu(f)$ is *small*.
  - For the hard polynomial P, $\mu(P)$ is *large*.

Tool 1: Partial Derivative Matrix & Complexity Measure

Following Raz [Raz, 2004], we too use the rank arguments.

- Let $\rho : X \mapsto Y \sqcup Z$ be a partitioning function such that $|Y| = |Z|$.

Tool 1: Partial Derivative Matrix & Complexity Measure

Following Raz [Raz, 2004], we too use the rank arguments.

- Let $\rho : X \mapsto Y \sqcup Z$ be a partitioning function such that $|Y| = |Z|$.

$$f = \sum_{i=1}^{2^n} c_i \cdot m_i \quad \mapsto \quad f|_\rho = \sum_{i=1}^{2^n} c_i \cdot m_{i,Y} \cdot m_{i,Z}$$

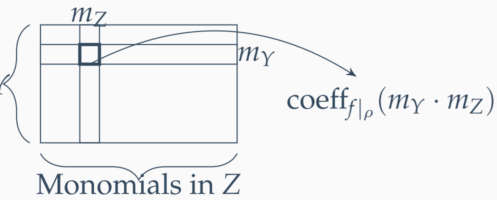
Tool 1: Partial Derivative Matrix & Complexity Measure

Following Raz [Raz, 2004], we too use the rank arguments.

- Let $\rho : X \mapsto Y \sqcup Z$ be a partitioning function such that $|Y| = |Z|$.

$$f = \sum_{i=1}^{2^n} c_i \cdot m_i \quad \mapsto \quad f|_\rho = \sum_{i=1}^{2^n} c_i \cdot m_{i,Y} \cdot m_{i,Z}$$

$M_{(Y,Z)}(f|_\rho)$: Monomials in Y



Complexity of f under ρ is $\text{rank}(M_{(Y,Z)}(f|_\rho))$.

Fact: $\text{rank}(M_{(Y,Z)}(f|_\rho)) \leq 2^{\frac{|Y|+|Z|}{2}}$.

Example

Consider the polynomial $f(x_1, x_2) = (x_1 + x_2)$ and the partition map of $\{x_1, x_2\}$ such that

$$x_1 \mapsto y; \quad x_2 \mapsto z.$$

It follows that $f|_\rho = (y + z)$ and thus,

$$M_{(\{y\},\{z\})}(f|_\rho) = \begin{array}{c} \\ 1 \\ y \end{array} \begin{array}{c} \begin{matrix} 1 & z \end{matrix} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{array},$$

$$\text{rank}(M_{(\{y\},\{z\})}(f|_\rho)) = 2.$$

Example

Consider the polynomial $f(x_1, x_2, x_3, x_4) = (x_1 + x_2)(x_3 + x_4)$ and the partition map of $\{x_1, x_2, x_3, x_4\}$ such that

$$x_1 \mapsto y_1; \quad x_2 \mapsto z_1; \quad x_3 \mapsto y_2 \quad ; x_4 \mapsto z_2.$$

It follows that $f|_\rho = (y_1 + z_1)(y_2 + z_2) = y_1y_2 + y_1z_2 + z_1y_2 + z_1z_2$ and thus,

$$M_{(\{y_1,y_2\},\{z_1,z_2\})}(f|_\rho) = \begin{array}{c} \\ 1 \\ y_1 \\ y_2 \\ y_1y_2 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & z_1 & z_2 & z_1z_2 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \end{array},$$

$$\mathrm{rank}(M_{(\{y_1,y_2\},\{z_1,z_2\})}(f|_\rho)) = 4.$$

Example

Consider the polynomial $f(x_1, x_2, x_3, x_4) = (x_1 + x_2)(x_3 + x_4)$ and the partition map of $\{x_1, x_2, x_3, x_4\}$ such that

$$x_1 \mapsto y_1; \quad x_2 \mapsto y_2; \quad x_3 \mapsto z_1 \quad ; x_4 \mapsto z_2.$$

It follows that $f|_\rho = (y_1 + y_2)(z_1 + z_2) = y_1z_1 + y_1z_2 + y_2z_1 + y_2z_2$ and thus,

$$M_{(\{y_1,y_2\},\{z_1,z_2\})}(f|_\rho) = \begin{array}{c} \\ 1 \\ y_1 \\ y_2 \\ y_1y_2 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & z_1 & z_2 & z_1z_2 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \end{array},$$

$$\operatorname{rank}(M_{(\{y_1,y_2\},\{z_1,z_2\})}(f|_\rho)) = 1.$$

Observation

- Given a partition ρ of the variables, we can construct an easy polynomial that has full rank w.r.t ρ.

Observation

- Given a partition ρ of the variables, we can construct an easy polynomial that has full rank w.r.t ρ.

- Let the variable mapping under ρ be the following.

$$
\begin{array}{ccccccc}
x_{i_1} \mapsto y_1; & x_{i_2} \mapsto y_2; & \dots & ; & x_{i_m} \mapsto y_m; \\
x_{j_1} \mapsto z_1; & x_{j_2} \mapsto z_2; & \dots & ; & x_{j_m} \mapsto z_m.
\end{array}
$$

Observation

- Given a partition ρ of the variables, we can construct an easy polynomial that has full rank w.r.t ρ.

- Let the variable mapping under ρ be the following.

$$x_{i_1} \mapsto y_1; \quad x_{i_2} \mapsto y_2; \quad \ldots \quad ; \quad x_{i_m} \mapsto y_m;$$
$$x_{j_1} \mapsto z_1; \quad x_{j_2} \mapsto z_2; \quad \ldots \quad ; \quad x_{j_m} \mapsto z_m.$$

- Under ρ, it is easy to see that the polynomial defined as follows will have full rank.

$$\Gamma_\rho(X) = (x_{i_1} + x_{j_1})(x_{i_2} + x_{j_2}) \cdots (x_{i_m} + x_{j_m})$$
$$\Gamma_\rho(\rho(X)) = (y_1 + z_1)(y_2 + z_2) \cdots (y_m + z_m)$$

Observation

- Given a partition ρ of the variables, we can construct an easy polynomial that has full rank w.r.t ρ.

- Let the variable mapping under ρ be the following.

$$\begin{array}{cccc} x_{i_1} \mapsto y_1; & x_{i_2} \mapsto y_2; & \dots \quad ; & x_{i_m} \mapsto y_m; \\ x_{j_1} \mapsto z_1; & x_{j_2} \mapsto z_2; & \dots \quad ; & x_{j_m} \mapsto z_m. \end{array}$$

- Under ρ, it is easy to see that the polynomial defined as follows will have full rank.

$$\Gamma_\rho(X) = (x_{i_1} + x_{j_1})(x_{i_2} + x_{j_2}) \cdots (x_{i_m} + x_{j_m})$$
$$\Gamma_\rho(\rho(X)) = (y_1 + z_1)(y_2 + z_2) \cdots (y_m + z_m)$$

- Γ_ρ has a very small formula.

Observation

- Instead, consider a set of partitions $S = \{\rho_1, \rho_2, \cdots, \rho_m\}$.

Observation

- Instead, consider a set of partitions $S = \{\rho_1, \rho_2, \cdots, \rho_m\}$.
- A polynomial P_S which can be defined as follows has full rank.

$$P_S(X) = \sum_{\rho \in S} \mathbf{1}_\rho \cdot \Gamma_\rho(X).$$

Observation

- Instead, consider a set of partitions $S = \{\rho_1, \rho_2, \cdots, \rho_m\}$.
- A polynomial P_S which can be defined as follows has full rank.

$$P_S(X) = \sum_{\rho \in S} \mathbf{1}_\rho \cdot \Gamma_\rho(X).$$

- Road map:

Observation

- Instead, consider a set of partitions $S = \{\rho_1, \rho_2, \cdots, \rho_m\}$.
- A polynomial P_S which can be defined as follows has full rank.

$$P_S(X) = \sum_{\rho \in S} \mathbf{1}_\rho \cdot \Gamma_\rho(X).$$

- Road map:
    1. Construct a suitable set of partitions S such that $|S|$ is not too large.

Observation

- Instead, consider a set of partitions $S = \{\rho_1, \rho_2, \cdots, \rho_m\}$.
- A polynomial P_S which can be defined as follows has full rank.

$$P_S(X) = \sum_{\rho \in S} \mathbf{1}_\rho \cdot \Gamma_\rho(X).$$

- Road map:
  1. Construct a suitable set of partitions S such that $|S|$ is not too large.
  2. Show that a multilinear formula of small size and depth is not of full rank w.r.t at least one of the partitions.

Observation

- Instead, consider a set of partitions $S = \{\rho_1, \rho_2, \cdots, \rho_m\}$.
- A polynomial P_S which can be defined as follows has full rank.

$$P_S(X) = \sum_{\rho \in S} \mathbf{1}_\rho \cdot \Gamma_\rho(X).$$

- Road map:
  1. Construct a suitable set of partitions S such that $|S|$ is not too large.
  2. Show that a multilinear formula of small size and depth is not of full rank w.r.t at least one of the partitions.
  3. Construct a polynomial from S as defined above.

Example

- Consider fixed sets Y, Z such that $|Y| = |Z|$.

Example

- Consider fixed sets Y, Z such that $|Y| = |Z|$.
- For $i \in [2]$, let $Y = Y_1 \sqcup Y_2$ and $Z = Z_1 \sqcup Z_2$.

Example

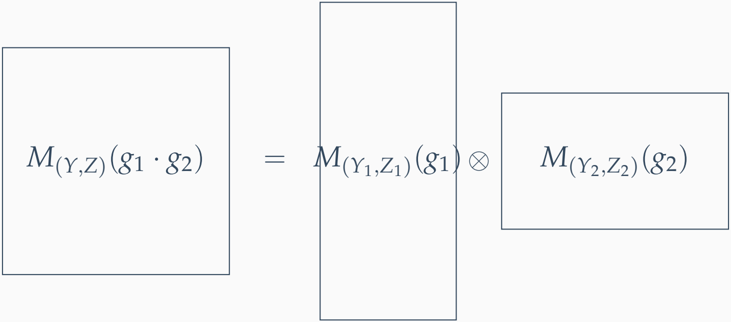
- Consider fixed sets Y, Z such that $|Y| = |Z|$.
- For $i \in [2]$, let $Y = Y_1 \sqcup Y_2$ and $Z = Z_1 \sqcup Z_2$.
- For $i \in [2]$, let $g_i \in \mathbb{F}[Y_i \cup Z_i]$ and $|Y_i| \neq |Z_i|$.

Example

- Consider fixed sets Y, Z such that $|Y| = |Z|$.
- For $i \in [2]$, let $Y = Y_1 \sqcup Y_2$ and $Z = Z_1 \sqcup Z_2$.
- For $i \in [2]$, let $g_i \in \mathbb{F}[Y_i \cup Z_i]$ and $|Y_i| \neq |Z_i|$.

Example

- Consider fixed sets Y, Z such that $|Y| = |Z|$.
- For $i \in [2]$, let $Y = Y_1 \sqcup Y_2$ and $Z = Z_1 \sqcup Z_2$.
- For $i \in [2]$, let $g_i \in \mathbb{F}[Y_i \cup Z_i]$ and $|Y_i| \neq |Z_i|$.



$$
\begin{aligned}
\operatorname{rank}(M_{(Y,Z)}(g_1 \cdot g_2)) &= \operatorname{rank}(M_{(Y_1,Z_1)}(g_1)) \cdot \operatorname{rank}(M_{(Y_2,Z_2)}(g_2)) \\
&\leq 2^{\frac{|Y_1|+|Z_1|-1}{2}} \cdot 2^{\frac{|Y_2|+|Z_2|-1}{2}} = 2^{\frac{|Y|+|Z|}{2}-1}.
\end{aligned}
$$

Observation

- Consider a product of t polynomials, $f = f_1 f_2 \cdots f_t$ where f_i's are defined over the disjoint sets $X_1, X_2, \cdots, X_t$.

Observation

- Consider a product of t polynomials, $f = f_1 f_2 \cdots f_t$ where f_i's are defined over the disjoint sets $X_1, X_2, \cdots, X_t$.

- Consider a partition map $\rho : X \mapsto Y \sqcup Z$ and let

$$Y_i = \rho(\text{vars}(f_i)) \cap Y; \quad Z_i = \rho(\text{vars}(f_i)) \cap Z.$$

Observation

- Consider a product of t polynomials, $f = f_1 f_2 \cdots f_t$ where f_i's are defined over the disjoint sets $X_1, X_2, \cdots, X_t$.

- Consider a partition map $\rho : X \mapsto Y \sqcup Z$ and let

$$Y_i = \rho(\text{vars}(f_i)) \cap Y; \quad Z_i = \rho(\text{vars}(f_i)) \cap Z.$$

- If ρ is such that there there ℓ factors f_i such that $|Y_i| \neq |Z_i|$, we get that

$$\text{rank}(M_{(Y,Z)}(f|_\rho)) \leq 2^{\frac{|Y|+|Z|}{2} - \frac{\ell}{2}}.$$

Tool 2: Product decomposition of Multilinear Formulas

Lemma (Product Decomposition, [Shpilka and Yehudayoff, 2010])

Any multilinear formula of size s_0 and product depth Δ, over n variables can be decomposed into a sum of $s = s_0 n$ many products each of which has a lot of factors.

$$f = \sum_{i=1}^{s} f_i = \sum_{i=1}^{s} f_{i,1} \cdot f_{i,2} \cdot \ldots \cdot f_{i,t} \text{ where } t \geq n^{1/2\Delta}.$$

and

- *for all $i \in [s]$ and $j \in [t]$, $\left|\mathrm{vars}(f_{i,j})\right| > 1$,*
- *for all $i \in [s]$, $f_{i,1}, f_{i,2}, \cdots, f_{i,t}$ are defined over disjoint sets of variables.*

Subadditivity of rank

Let $g, g_1, g_2, \cdots, g_r$ be polynomials over $\mathbb{F}[Y \cup Z]$ such that

$$g = \sum_{i \in [r]} g_i$$

then

$$\operatorname{rank}(M_{(Y,Z)}(g)) \leq \sum_{i \in [r]} \operatorname{rank}(M_{(Y,Z)}(g_i)).$$

Subadditivity of rank

Let $g, g_1, g_2, \cdots, g_r$ be polynomials over $\mathbb{F}[Y \cup Z]$ such that

$$g = \sum_{i \in [r]} g_i$$

then

$$\mathrm{rank}(M_{(Y,Z)}(g)) \leq \sum_{i \in [r]} \mathrm{rank}(M_{(Y,Z)}(g_i)).$$

- We know that $f = \sum_{i=1}^{s} f_i$ where $f_i = f_{i1} f_{i2} \cdots f_{it}$.

Subadditivity of rank

Let $g, g_1, g_2, \cdots, g_r$ be polynomials over $\mathbb{F}[Y \cup Z]$ such that

$$g = \sum_{i \in [r]} g_i$$

then

$$\text{rank}(M_{(Y,Z)}(g)) \leq \sum_{i \in [r]} \text{rank}(M_{(Y,Z)}(g_i)).$$

- We know that $f = \sum_{i=1}^{s} f_i$ where $f_i = f_{i1} f_{i2} \cdots f_{it}$.
- Let $\rho : X \to Y \cup Z$ is such that for each i, there are at least ℓ of the factors f_{ij} with $|Y_{ij}| \neq |Z_{ij}|$, then

Subadditivity of rank

Let $g, g_1, g_2, \cdots, g_r$ be polynomials over $\mathbb{F}[Y \cup Z]$ such that

$$g = \sum_{i \in [r]} g_i$$

then

$$\operatorname{rank}(M_{(Y,Z)}(g)) \leq \sum_{i \in [r]} \operatorname{rank}(M_{(Y,Z)}(g_i)).$$

- We know that $f = \sum_{i=1}^{s} f_i$ where $f_i = f_{i1} f_{i2} \cdots f_{it}$.
- Let $\rho : X \to Y \cup Z$ is such that for each i, there are at least ℓ of the factors f_{ij} with $|Y_{ij}| \neq |Z_{ij}|$, then

Subadditivity of rank

Let $g, g_1, g_2, \cdots, g_r$ be polynomials over $\mathbb{F}[Y \cup Z]$ such that

$$g = \sum_{i \in [r]} g_i$$

then

$$\operatorname{rank}(M_{(Y,Z)}(g)) \leq \sum_{i \in [r]} \operatorname{rank}(M_{(Y,Z)}(g_i)).$$

- We know that $f = \sum_{i=1}^{s} f_i$ where $f_i = f_{i1} f_{i2} \cdots f_{it}$.
- Let $\rho : X \to Y \cup Z$ is such that for each i, there are at least ℓ of the factors f_{ij} with $|Y_{ij}| \neq |Z_{ij}|$, then

$$\operatorname{rank}(M_{(Y,Z)}(f|_\rho)) \leq \sum_{i \in [s]} \operatorname{rank}(M_{(Y,Z)}(f_i|_\rho)) \leq s \cdot 2^{\frac{|Y|+|Z|}{2} - \frac{\ell}{2}}.$$

Subadditivity of rank

Let $g, g_1, g_2, \cdots, g_r$ be polynomials over $\mathbb{F}[Y \cup Z]$ such that

$$g = \sum_{i \in [r]} g_i$$

then

$$\text{rank}(M_{(Y,Z)}(g)) \leq \sum_{i \in [r]} \text{rank}(M_{(Y,Z)}(g_i)).$$

- We know that $f = \sum_{i=1}^{s} f_i$ where $f_i = f_{i1} f_{i2} \cdots f_{it}$.
- Let $\rho : X \to Y \cup Z$ is such that for each i, there are at least ℓ of the factors f_{ij} with $\left|Y_{ij}\right| \neq \left|Z_{ij}\right|$, then

$$\text{rank}(M_{(Y,Z)}(f|_\rho)) \leq \sum_{i \in [s]} \text{rank}(M_{(Y,Z)}(f_i|_\rho)) \leq s \cdot 2^{\frac{|Y|+|Z|}{2} - \frac{\ell}{2}}.$$

We want $s \cdot 2^{\frac{|Y|+|Z|}{2} - \frac{\ell}{2}}$ to be strictly less than $2^{\frac{|Y|+|Z|}{2}}$ and thus we want $\ell > 2 \log s$.

Rephrasing the problem

For a partition ρ:

- For each i, we want at least ℓ many j's to be such that $|Y_{ij}| \neq |Z_{ij}|$.

Rephrasing the problem

For a partition ρ:

- For each i, we want at least ℓ many j's to be such that $|Y_{ij}| \neq |Z_{ij}|$.
- It is sufficient to prove that for each i, there exists a set A of ℓ many j's such that $|Y_{ij}| - |X_{ij}|/2 \equiv 1 \mod 2$ for each of them. Let the bad event against this event be denoted by E_i.

Rephrasing the problem

For a partition ρ:

- For each i, we want at least ℓ many j's to be such that $|Y_{ij}| \neq |Z_{ij}|$.
- It is sufficient to prove that for each i, there exists a set A of ℓ many j's such that $|Y_{ij}| - |X_{ij}|/2 \equiv 1 \mod 2$ for each of them. Let the bad event against this event be denoted by E_i.

Rephrasing the problem

For a partition ρ:

- For each i, we want at least ℓ many j's to be such that $\left|Y_{ij}\right| \neq \left|Z_{ij}\right|$.

- It is sufficient to prove that for each i, there exists a set A of ℓ many j's such that $\left|Y_{ij}\right| - \left|X_{ij}\right|/2 \equiv 1 \mod 2$ for each of them. Let the bad event against this event be denoted by E_i.

For a set of partitions $S = \{\rho_1, \rho_2, \cdots, \rho_m\}$:

- E_i is also defined by a system of linear equations.
- It is sufficient to show that, for each i,

$$\mathbb{P}_{\rho \in S}\left[E_i\right] < 1/s.$$

Rephrasing the problem

- Construct a set of partitions $S = \{\rho_1, \rho_2, \cdots, \rho_m\}$.

Rephrasing the problem

- Construct a set of partitions $S = \{\rho_1, \rho_2, \cdots, \rho_m\}$.
- Show that the polynomial computed by a multilinear formula of size s and *small* depth has less than full rank for at least one of the partitions in S.

Rephrasing the problem

- Construct a set of partitions $S = \{\rho_1, \rho_2, \cdots, \rho_m\}$.
- Show that the polynomial computed by a multilinear formula of size s and *small* depth has less than full rank for at least one of the partitions in S.
- Construct a full rank polynomial for the set S.

$$P_S(X) = \sum_{\rho \in S} \mathbf{1}_\rho \cdot \Gamma_\rho(X).$$

Rephrasing the problem

- Construct a set of partitions $S = \{\rho_1, \rho_2, \cdots, \rho_m\}$.
- Show that the polynomial computed by a multilinear formula of size s and *small* depth has less than full rank for at least one of the partitions in S.
- Construct a full rank polynomial for the set S.

$$P_S(X) = \sum_{\rho \in S} \mathbf{1}_\rho \cdot \Gamma_\rho(X).$$

- Polynomial P_S has a small formula of size $O(|S|\, n)$

Rephrasing the problem

- Construct a set of partitions $S = \{\rho_1, \rho_2, \cdots, \rho_m\}$.
- Show that the polynomial computed by a multilinear formula of size s and *small* depth has less than full rank for at least one of the partitions in S.
- Construct a full rank polynomial for the set S.

$$P_S(X) = \sum_{\rho \in S} \mathbf{1}_\rho \cdot \Gamma_\rho(X).$$

- Polynomial P_S has a small formula of size $O(|S|\, n)$

Rephrasing the problem

- Construct a set of partitions $S = \{\rho_1, \rho_2, \cdots, \rho_m\}$.
- Show that the polynomial computed by a multilinear formula of size s and *small* depth has less than full rank for at least one of the partitions in S.
- Construct a full rank polynomial for the set S.

$$P_S(X) = \sum_{\rho \in S} \mathbf{1}_\rho \cdot \Gamma_\rho(X).$$

- Polynomial P_S has a small formula of size $O(|S|\, n)$

Probabilistic Method	Our derandomization using subspace evading sets
$m = O(ns)$	$m = O(ns^2)$

Thank you![*][†]

[*] Figure of the coefficient matrix were sourced from Ramprasad Saptharishi's survey, under CC BY-NC-SA licence.

[†] The theme of these slides is based on mtheme by matze https://github.com/matze/mtheme, under CC BY-SA licence.