Slightly Improved Lower Bounds for Homogeneous Formulas of Bounded Depth and Bounded Individual Degree

Suryajith Chillara

Indian Institute of Technology, Bombay.
suryajith@cse.iitb.ac.in

Abstract

Kayal, Saha and Tavenas (Theory of Computing, 2018), showed that any bounded-depth homogeneous formula of bounded individual degree (bounded by $r$) that computes an explicit polynomial over $n$ variables must have size $\exp\left(\Omega\left(\frac{1}{r} \left(\frac{n}{4}\right)^{1/\Delta}\right)\right)$ for all depths $\Delta \leq \BigO{\frac{\log n}{\log r + \log \log n}}$. In this article we show an improved lower bound of $\exp\left(\Omega\left(\frac{n}{r} \left(\frac{nr}{2}\right)^{1/\Delta}\right)\right)$ for all depths $\Delta \leq \BigO{\frac{\log n}{\log r}}$, for the same explicit polynomial. In comparison to Kayal, Saha and Tavenas (Theory of Computing, 2018) (1) our results give superpolynomial lower bounds in a wider regime of depth $\Delta$, and (2) for all $\Delta \in \left[\omega(1), o\left(\frac{\log n}{\log r}\right)\right]$ our lower bound is asymptotically better.

This improvement is a result of a new and finer product decomposition of general homogeneous formulas of bounded-depth. This is motivated by an improved product decomposition for bounded-depth multilinear formulas shown by Chillara, Limaye and Srinivasan (SIAM Journal of Computing, 2019).

Keywords:
Algebraic Complexity Theory, Lower Bounds, Bounded Depth

1. Introduction

One of the major focal points in the area of algebraic complexity theory is to show that certain polynomials are hard to compute syntactically. Here, the hardness of computation is quantified by the number of arithmetic
operations that are needed to compute the target polynomial. Instead of the standard Turing Machine model, we consider Arithmetic Circuits and Arithmetic Formulas as models of computation. We refer the readers to the standard resources [1, 2] for more information on arithmetic formulas and arithmetic circuits. Without loss of generality, in this paper we assume that our formulas are layered with alternate layers of + - nodes and ×-nodes, with a single output node labeled by + (sometimes suitably denoted symbolically as \( \Sigma \Pi \Sigma \cdots \Sigma \Pi \cdots \Pi \Sigma \)). Product-depth refers to the maximum number of ×-nodes encountered on any leaf-to-output path. Thus product-depth is related to depth by a factor of at most 2.

Valiant conjectured that Permanent does not have polynomial sized arithmetic circuits [3]. Thus the holy grail is to prove superpolynomial size lower bounds against arithmetic circuits and formulas. However, the best known circuit size lower bound is \( \Omega(n \log n) \), for a Power Symmetric polynomial, due to Baur and Strassen [4, 5], and, the best known formula size lower bound is \( \Omega(n^2) \), due to Kalorkoti [6]. Due to the slow progress towards proving general circuit/formula lower bounds, it is natural to study some restricted classes of arithmetic circuits and formulas.

Since most of the polynomials of interest like Determinant, Permanent, etc. are multilinear polynomials, it is natural to consider the restriction where every intermediate computation is in fact multilinear. Due to the phenomenal work in the last two decades [7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17], the complexity of multilinear formulas and circuits is better understood than that of general formulas and circuits.

Motivation for this work. Hrubeš and Yehudayoff [12] showed that any homogeneous multilinear formula that computes an Elementary Symmetric polynomial\(^1\) (of “large enough” degree) must be of quasipolynomial size. Further they showed that any homogeneous multilinear formula of bounded depth that computes an Elementary Symmetric polynomial (of “large enough” degree) must be of exponential size. They prove this by first exhibiting a structural property of homogeneous multilinear formulas (of bounded depth resp.) – they show that any polynomial that is computed by a homogeneous multilinear formula can be expressed as a sum of a very few summands each

\(^1\)The Elementary Symmetric polynomial of degree \( d \) on \( n \) variables, denoted by \( \text{ESym}_n^d(x_1, x_2, \ldots, x_n) \), is defined as \( \sum_{S \subseteq [n]} \prod_{i \in S} x_i \).
of which is a product of a large number of factors. We shall henceforth refer to such an expression as *Product Decomposition*. They then use the structure obtained from product decomposition to prove that, if the size of such formulas is strictly less than quasipolynomial (exponential resp.) then the polynomial computed is “sparse”. They show that Elementary Symmetric polynomial (of “large enough” degree) is not “sparse” and thus infer that it can not be computed by such formulas.

Kayal, Saha and Tavenas [18] have shown that even homogeneous Multi-

$r$-ic Arithmetic Formulas (cf. Definition 2.2) can be expressed as a *small* sum of *large* products. Using this, they prove lower bounds against homogeneous multi-$r$-ic formulas using a suitable notion of *sparsity* which is the number of $r$-extremal monomials computed, as the complexity measure. In particular, they showed that for an explicit polynomial $P_{n,r}$ (cf. Definition 2.5) over $n$ variables and degree $nr/2$, any homogeneous multi-$r$-ic formula of depth $\Delta \leq O\left(\frac{\log n}{\log r + \log \log n}\right)$ computing it must have size $\exp\left(\Omega\left(\frac{1}{r} \left(\frac{n}{4}\right)^{1/\Delta}\right)\right)$.

In this article, we first prove a refined product decomposition (cf. Lemma 3.2) for general homogeneous formulas of bounded depth – we show that homogeneous formulas of bounded depth can be expressed as a *small* sum of *larger* products. This is analogous to the product decomposition in [15] for bounded depth multilinear formulas. This structure can be further transformed into a *required* product decomposition (to prove lower bounds) for homogeneous multi-$r$-ic formulas (cf. Lemma 4.1). That is, in comparison to [18] we show that each summand in the *required* product decomposition has more factors. As a result of this, we get quantitatively better lower bounds than [18] for homogeneous multi-$r$-ic formulas at bounded depths.

**Theorem 1.1.** Let $\Delta, n$ and $r$ be integers such that $n$ is even, $\Delta \leq O(\log n/\log r)$ and $r^{(\Delta-1)/\Delta} = o(\Delta(n/2)^{1/\Delta})$. Then any homogeneous multi-$r$-ic formula of product-depth $\Delta$ computing $P_{n,r}$ must have size $2^{\Omega\left(\frac{\Delta}{r} \left(\frac{n}{4}\right)^{1/\Delta}\right)}$.

Our lower bound is superpolynomial for all depths which are $o\left(\frac{\log n}{\log r}\right)$ compared to [18] that gives a superpolynomial lower bound for all depths that are $o\left(\frac{\log n}{\log r + \log \log n}\right)$. It is important to remark that this lower bound is exponentially far from the current known upper bounds [19]. The following corollary easily follows from **Theorem 1.1**.
Corollary 1.2. Let $\Delta, n$ and $r$ be integers such that $n$ is even, $\Delta \leq O(\log n / \log r)$ and $r^{(\Delta-1)/\Delta} = o(\Delta n/2 \Delta)$. Then any homogeneous multi-$r$-ic circuit of product-depth $\Delta$ computing $P_{n,r}$ must be of size $2^{\Omega\left(\frac{1}{r} \left(\frac{n}{2}\right)^{1/\Delta}\right)}$.

2. Preliminaries

Notation:

- For a polynomial $f$, $\deg(f)$ denotes its total degree.
- For a monomial $m$, $\deg_{x_i}(m)$ denotes the degree of the variable $x_i$ in $m$.
- For a polynomial $f$, $\deg_x(f)$ denotes the maximum over $\deg_{x_i}(m)$ over all the monomials $m$ that appear in $f$. That is, $\deg_x(f) = \max_{m \in \text{monomials}(f)} \{\deg_{x_i}(m)\}$.
- For a monomial $m$, $\text{Supp}(m)$ denotes the set of variables $\{x_i \mid \deg_{x_i}(m) \geq 1\}$.
- For a polynomial $f$, $\text{Supp}(f)$ denotes the set $\bigcup_{m \in \text{monomials}(f)} \text{Supp}(m)$.

Arithmetic Formulas:

Definition 2.1. An arithmetic formula $\Phi$ is said to be homogeneous if the following is satisfied for all nodes $u$ in $\Phi$.

- If $u \in \Phi$ is a sum gate, i.e., $u = u_1 + u_2 + \cdots + u_t$ then $\deg(f_u) = \deg(f_{u_i})$ for all $i \in [t]$.
- If $u \in \Phi$ is a product gate, i.e., $u = u_1 u_2 \cdots u_t$ then $\deg(f_u) = \sum_{i \in [t]} \deg(f_{u_i})$.
- If $u \in \Phi$ is a leaf, then $\deg(f_u)$ is equal to 1 or 0 depending upon whether the label is a variable or a constant respectively.

Definition 2.2 (multi-$r$-ic formulas). Let $r = (r_1, r_2, \ldots, r_n)$.

1. A polynomial $f(x_1, x_2, \ldots, x_n)$ is said to be multi-$r$-ic if for all $i \in [n]$, if $\deg_{x_i}(f) \leq r_i$. If $r_1 = r_2 = \cdots = r_n = r$, we simply refer to it as a multi-$r$-ic polynomial.
2. A product $g_1 g_2 \cdots g_k$ is said to be syntactically multi-$r$-ic if for all $i \in [n]$, the variable $x_i$ appears in the support of at most $r_i$ many of the polynomials in $\{g_1, g_2, \cdots, g_k\}$.

3. An arithmetic formula $\Phi$ is said to be a syntactically multi-$r$-ic formula if the computation at every product gate in $\Phi$ is syntactically multi-$r$-ic.

In this paper, we are only concerned about the homogeneous syntactically multi-$r$-ic formulas of bounded depth.

**Definition 2.3 (Extremal monomials).** Let $r = (r_1, r_2, \cdots, r_n)$. A monomial $m(x)$ is said to be $r$-extremal if the degree of a variable $x_i$ (for all $i$) in $m(x)$ is either 0 or $r_i$. If $r_1 = r_2 = \cdots = r_n = r$, we simply call it $r$-extremal.

Kayal, Saha and Tavenas [18] have generalized the complexity measure introduced by Hrubeš and Yehudayoff [12] for multilinear polynomials.

**Definition 2.4 (Complexity Measure: $r$-extremal monomials).** The complexity measure that we consider for a polynomial $f(x)$ with respect to a parameter $r \geq 1$ is the total number of $r$-extremal monomials in $f$.

**Definition 2.5 (Hard polynomial).** Let $n, r$ be integers such that $n$ is even and $r \geq 1$. The polynomial $P_{n,r}(x)$ over the variables $x = \{x_1, x_2, \cdots, x_n\}$ is defined as $P_{n,r}(x) = \sum_{S \subset [n]} \prod_{i \in S} x_i^{r_i}$.

It is easy to see that the polynomial $P_{n,r}$ can be expressed in terms of Elementary Symmetric polynomial of degree $n/2$ over $n$ variables, i.e. $\text{ESym}_{n/2}^{n/2}(x_1^r, x_2^r, \cdots, x_n^r)$.

We need the following proposition to help us obtain the “required” product decomposition (cf. Lemma 4.1) to help us obtain better lower bounds.

**Proposition 2.6.** Let $t$ and $r$ be integers such that $r < t$. Let $T$ be a syntactically multi-$r$-ic product of $t$ polynomials $\{g_1, g_2, \cdots, g_t\}$ over $n$ variables $\{x_1, x_2, \cdots, x_n\}$ such that $|\text{Supp}(g_i)| \geq 1$ for all $i \in [t]$. Then $T$ can also be expressed as a syntactically multi-$r$-ic product of at least $t' = \lfloor (t-r)/2 \rfloor$ many polynomials $\{h_1, h_2, \cdots, h_{t'}\}$ over the same set of variables, such that $|\text{Supp}(h_i)| \geq 2$ for all $i \in [t']$.  

---

2In spirit, the measure of Hrubeš and Yehudayoff [12] is similar to the complexity measure introduced by Jerrum and Snir [20] for monotone formulas.
Proof. If $|\text{Supp}(g_i)| \geq 2$ for all $i \in [t]$, then we already have $T$ in the required form. Else, split the factors $\{g_i \mid i \in [g]\}$ into two bags $B_1, B_2, \ldots, B_N$ such that for all $i \in [n]$, $B_i = \{g_i \mid |\text{Supp}(g_i)| = 1; \text{Supp}(g_i) = \{x_i\}\}$ and $B_0 = \{g_i \mid |\text{Supp}(g_i)| = 2\}$. By suitable renaming, let $S_1, S_2, \ldots, S_n$ be the enumeration of these bags in the non decreasing order of their cardinalities. Note that for all $i$, each element of the bag $S_i$ is an univariate polynomial. Algorithm 1 describes the process of pairing two univariate polynomials to obtain polynomials of support 2. By invoking Algorithm 1 with $i = 1$, we finally get the set $S_n$, a set of univariate polynomials that couldn’t be paired.

**Algorithm 1**: Pair($i$)

1. if $i=n$ then
2. return $S_n$;
3. else
4. Pair each element of $S_i$, sequentially, with the first $|S_i|$-many elements of $S_{i+1}$;
5. Update $S_{i+1}$ by removing all its elements that are already paired;
6. return Pair($i+1$);
7. end

Cardinality of $S_n$ is at most $r$ and thus using the aforementioned procedure, we have paired up at least $\sum_{i=1}^{n} |S_i| - r$ many polynomials to generate at least $\left(\frac{\sum_{i=1}^{n} |S_i| - r}{2}\right)$ many new polynomials of support 2. Recall that $|B_0| + \sum_{i=1}^{n} |S_i| = t$. Post the procedure, the total number of polynomials that have support at least 2 is at least

$$|B_0| + \left[\frac{\sum_{i=1}^{n} |S_i| - r}{2}\right] \geq \left[\frac{|B_0| + \sum_{i=1}^{n} |S_i| - r}{2}\right] \geq \left[\frac{t - r}{2}\right].$$

3. New Product Decomposition for Homogeneous Formulas of Bounded Depth

Before we derive a new product decomposition for homogeneous formulas of bounded depth, we need the following definition.

**Definition 3.1.** A homogeneous polynomial $f$ is said to be a $(t, L)$-product if there exist $t$ homogeneous polynomials $\{f_1, \cdots, f_t\}$ such that

1. $f = f_1f_2 \cdots f_t$,  

\[ 3 \]
Lemma 3.2. Let $\Delta$ be an integer such that $\Delta = O(\log d)$. Let $f$ be a polynomial of total degree $d$ over $n$ variables that is computed by a homogeneous formula of size $s$ and product-depth $\Delta$. Then $f$ can also be expressed as a sum of at most $s$-many $(t, 1)$-products where $t \geq \Delta (d^{1/\Delta} - 1)$.

Proof. We shall prove by induction on $\Delta$ that $f$ can be expressed as a sum of at most $s$-many $(v, 1)$-products where $v \geq \Delta (d^{1/\Delta} - 1)$.

Base Case: $\Delta = 1$. Let the polynomial $f$ be computed by a homogeneous depth three $((\Sigma \Pi) \Sigma)$ formula $\Phi$ of size $s$ and degree $d$. Here $f = \sum_{i=1}^{s_0} T_i$ and $T_i = \prod_{j=1}^{d} f_{i,j}$. It is important to note that each summand $T_i$ has exactly $d$ factors and each $f_{i,j}$ is a homogeneous linear polynomial with $|\text{Supp}(f_{i,j})| \geq 1$. Since $f = \sum_{i=1}^{s_0} T_i$, $f$ can now be expressed as a sum of at most $s_0 \leq s$ many $(d, 1)$-products and trivially $d > (d - 1)$.

Induction Step. Let $f$ be computed by a $((\Sigma \Pi) \Sigma)$ formula $\Phi$ of size $s$. Let $\Phi_1, \ldots, \Phi_{s_0}$ (for some $s_0 \leq s$) be the sub-formulas feeding into the output node in $\Phi$, computing the polynomials $f_1, f_2, \ldots, f_{s_0}$ respectively. That is, $f = f_1 + \cdots + f_{s_0}$. Since $\Phi$ is homogeneous, $\deg(f) = \deg(f_i)$ for all $i \in [s_0]$. Let $f_i = \prod_{j=1}^{k_i} f_{i,j}$ for all $i \in [s_0]$. Note that each sub-formula $\Phi_{i,j}$ computing $f_{i,j}$ is a $((\Sigma \Pi)^{\Delta-1} \Sigma)$ formula of size at most $s$.

Consider an arbitrary polynomial $f_i$ from $\{f_1, f_2, \ldots, f_{s_0}\}$. Recall that $f_i = \prod_{j=1}^{k_i} f_{i,j}$ for some parameter $k_i$. Since the product of $f_{i,j}$’s is homogeneous, by an averaging argument we get that there exists a factor, say $f_{i,j'}$, in $f_i$ such that $\deg(f_{i,j'})$ is at least $d/k_i$. By suitable renaming, we can assume that $f_{i,1}$ to be that factor.

By applying the induction hypothesis on $f_{i,1}$, we get that $f_{i,1}$ can be expressed as a sum of at most $s' = \text{size}(\Phi_{i,1})$ many $(v', 1)$-products where $v' \geq (\Delta - 1) ((d/k_i)^{1/(\Delta - 1)} - 1)$. Multiplying each of these summands in the expression obtained for $f_{i,1}$ through inductive hypothesis, with the rest of the factors in $f_i$, we get that there are $v = v' + k_i - 1$ many factors in each of the summands in $f_i$. We now have at most $\text{size}(\Phi_{i,1}) \leq \text{size}(\Phi_i)$ many summands.

$$v = v' + k_i - 1 \geq \min_{k_i \in [d]} \left\{ (\Delta - 1) ((d/k_i)^{1/(\Delta - 1)} - 1) + k_i - 1 \right\} \geq \Delta (d^{1/\Delta} - 1).$$
The last inequality follows from the fact that the term before the inequality attains a minima at $k_i = d^{1/\Delta}$. Thus, we can express every $f_i$ as a sum of at most $\text{size}(\Phi_i)$ many $(v,1)$-products. Recall that $\text{size}(\Phi) = 1 + \sum_{i=1}^{n_0} \text{size}(\Phi_i) = s$ and $f = \sum_{i=1}^{n_0} f_i$. Using this, we get that $f$ can be expressed as a sum of at most $s$ many $(v,1)$-products with $v \geq \Delta \left( d^{1/\Delta} - 1 \right)$. This completes the proof.

\[ \square \]

4. Lower Bound for Homogeneous Multi-$r$-ic Formulas of Bounded-Depth

Using Lemma 3.2, we shall first show that homogeneous multi-$r$-ic formulas of bounded-depth can be expressed as a sum of a few summands each of which is in $(v,2)$-form where $v$ is large enough.

**Lemma 4.1.** Let $r, d$ and $\Delta$ be integers such that $r = o(\Delta(d^{1/\Delta} - 1))$. Let $f$ be a polynomial of total degree $d$ and individual degree $r$ over $n$ variables, and is computed by a homogeneous multi-$r$-ic formula of size $s$ and product-depth $\Delta$. Then $f$ can also be expressed as a sum of at most $s$-many $(t,2)$-products where $t \geq \left\lfloor \frac{(\Delta(d^{1/\Delta} - 1) - r)}{2} \right\rfloor$.

**Proof.** From Lemma 3.2, we get that $f$ can be expressed as a sum of at most $s$-many $(v,1)$-products where $v \geq \Delta \left( d^{1/\Delta} - 1 \right)$. Using Proposition 2.6, we can transform each of these summands, which is a $(v,1)$-product, into a $(t,2)$-product where $t \geq \left\lfloor \frac{v - r}{2} \right\rfloor$. Thus, we can express $f$ as a sum of at most $s$-many $(t,2)$-products where $t \geq \left\lfloor \frac{(\Delta(d^{1/\Delta} - 1) - r)}{2} \right\rfloor$. \[ \square \]

To prove the lower bound we need the following definition and two lemmas that were proved in [18] using elegant combinatorial arguments.

**Definition 4.2.** A homogeneous polynomial $f$ is said to be in $(v, L)$-form if there exist $v$ homogeneous polynomials $\{f_1, \cdots, f_v\}$ such that

1. $f = f_1 f_2 \cdots f_v$,
2. $|\text{Supp}(f_i) \setminus (\cup_{j < i} \text{Supp}(f_j))| \geq L$ for all $i \in [v]$,
3. $\deg(f) = \deg(f_1) + \deg(f_2) + \cdots + \deg(f_v)$.

\[ \diamond \]
Lemma 4.3 (Lemma 5.5, [18]). Let $v, r \geq 1$ be integers. If a polynomial $T$ is a $(t, 2)$-product then $T$ has a $\left(\left\lfloor t/2r \right\rfloor, 2\right)$-form.

Lemma 4.4 (Bound on the extremal monomials, Lemma 4.6, [18]). Let $T$ be a $n$-variate polynomial in $(v, L)$-form. Then the number of $r$-extremal monomials in $T$ is at most $2^n v/2$.

With this background, we can now prove an improved lower bound.

Proof of Theorem 1.1. Let $\Phi$ be a homogeneous multi-$r$-ic formula of product-depth $\Delta$ of size $s$ computing $P_{n,r}$. Recall that $P_{n,r} = \sum_{S \subseteq \{n\}} \prod_{i \in S} x_i^r$ and $\deg(P_{n,r}) = nr/2$. From Lemma 4.1 and Lemma 4.3, we get that the computation of $\Phi$ can be expressed as a sum of at most $s$ many terms each of which is in $(v, 2)$-form where $v \geq \left[(\Delta ((nr/2)^{1/\Delta} - 1) - r)/4r\right]$. By invoking the Lemma 4.4, we get that the number of $r$-extremal monomials is at most $s \cdot 2^n v/2$.

It is easy to see that there are $\binom{n}{n/2}$ monomials in $P_{n,r}$ and each of these monomials is a $r$-extremal monomial.

Since $\Phi$ computes $P_{n,r}$, the number of $r$-extremal monomials of $\Phi$ must be the same as the number of $r$-extremal monomials in $P_{n,r}$. Thus by using the fact that $\binom{n}{n/2}$ is at most $2^n/\sqrt{n}$ (from Stirling’s approximation) we get the following.

$$s \cdot 2^n \geq \binom{n}{n/2} \implies s \geq 2^n v/2 \cdot 2^n \sqrt{2n} \geq \exp \left( \Omega \left( \frac{\Delta}{r} \cdot \left( \frac{nr}{2} \right)^{1/\Delta} \right) \right).$$

The floor in the expression for $v$ can be subsumed into the $\Omega$ in the last inequality. This lower bound is superpolynomial when $\Delta \leq o \left( \frac{\log n}{\log r} \right)$. \hfill \qed

Proof of Corollary 1.2. Any circuit of product-depth $\Delta$ has depth at most $2\Delta + 1$. By replicating nodes, any homogeneous multi-$r$-ic circuit of size $s$ can be converted into a homogeneous multi-$r$-ic formula of product-depth $\Delta$ and size $s^{2\Delta + 1}$. From Theorem 1.1, we get that any homogeneous multi-$r$-ic formula of product-depth $\Delta$ computing $P_{n,r}$ must be of size at least $2^{\Omega \left( \frac{nr}{2}^{1/\Delta} \right)}$. Thus, $s^{2\Delta + 1} \geq 2^{\Omega \left( \frac{nr}{2}^{1/\Delta} \right)}$ and $s \geq 2^{\Omega \left( \frac{1}{r} \left( \frac{nr}{2} \right)^{1/\Delta} \right)}$. This lower bound is strictly superpolynomial when $\Delta \leq o \left( \frac{\log n}{\log r + \log \log n} \right)$. \hfill \qed
References


URL http://doi.acm.org/10.1145/322326.322341