HOMOGENEOUS FORMULAS AND SYMMETRIC POLYNOMIALS

Pavel Hrubeš and Amir Yehudayoff

Abstract. We investigate the arithmetic formula complexity of the elementary symmetric polynomials S_n^k. We show that every multilinear homogeneous formula computing S_n^k has size at least $k^{\Omega(\log k)}n$, and that product-depth d multilinear homogeneous formulas for S_n^k have size at least $2^{\Omega(k^{1/d})}n$. Since S_{2n}^n has a multilinear formula of size $O(n^2)$, we obtain a superpolynomial separation between multilinear and multilinear homogeneous formulas. We also show that S_n^k can be computed by homogeneous formulas of size $k^{O(\log k)}n$, answering a question of Nisan and Wigderson. Finally, we present a superpolynomial separation between monotone and non-monotone formulas in the noncommutative setting, answering a question of Nisan.

Keywords. Arithmetic circuits, homogeneous polynomials, symmetric polynomials.

Subject classification. 68W30

1. Introduction

We address two basic topics in arithmetic complexity: the power of homogeneity and computation of the symmetric polynomials. A basic structural result in arithmetic complexity (e.g., (Strassen 1973)) asserts that

($\star$) *if a homogeneous polynomial has a formula of size s, then it has a homogeneous formula of size at most $s^{O(\log s)}$.*

A natural question is whether the upper bound given by ($\star$) is tight, or whether formulas can be simulated by polynomial size homogeneous formulas. With our current techniques, this question is unfortunately out of reach. Most importantly, superpolynomial lower bounds on homogeneous formula complexity (for low degree polynomials) are not known. Still, we can investigate this question in restricted models of computation; we investigate the multilinear setting.

The elementary symmetric polynomials S_n^k (formally defined below) seem to be good candidates for a separation in ($\star$). Over an infinite field, they have non-homogeneous formulas of size $O(n^2)$, but the best known homogeneous formulas computing S_n^k are of a quasipolynomial size. Nisan & Wigderson (1996) made a stronger conjecture, that S_n^k require homogeneous formulas of size at least $n^{\Omega(\log k)}$. This, however, is not the case – we show that S_n^k have homogeneous formulas of size $k^{O(\log k)}n$, which is linear for a fixed k. In fact, the conjecture does not even hold for monotone formulas – S_n^k have monotone formulas of size $n^{1+o(1)}$, if k is fixed. The conjecture of Nisan & Wigderson was based on the assumption that in general, in order to simulate a formula of size s computing a polynomial of degree k, we need a homogeneous formula of size $s^{\Omega(\log k)}$. We have learned about a recent result of Raz, who gave a more efficient simulation, see (Raz 2009).

1.1. Results. Let us first give the usual definitions. An *arithmetic circuit* Φ over the field $\mathbb{F}$ is a directed acyclic graph as follows. Every node in Φ of in-degree 0 is labelled by either a variable or a field element in $\mathbb{F}$. Every other node in Φ has in-degree at least two and is labelled by either $\times$ or $+$. Nodes labelled by $\times$ are *product nodes*, and nodes labelled by $+$ are *sum nodes*. An arithmetic circuit is called a *formula*, if the out-degree of every node in it is one. A circuit Φ computes a polynomial $\widehat{\Phi}$ in the obvious manner.

A polynomial f is *homogeneous* if the total degrees of all the monomials that occur in f are the same. A polynomial f is *multilinear* if the degree of each variable in f is at most one. A circuit Φ is *homogeneous* if every node in Φ computes a homogeneous polynomial. A circuit Φ is *multilinear* if every node in it computes a multilinear polynomial. A circuit Φ over the real numbers is called *monotone* if every field element in Φ is a nonnegative real number.

We define the *size* of a formula as the number of leaves in it[1]. The *depth* of a formula is the length of the longest directed path in it. The *product-depth* of a formula Φ is the largest number of product nodes in a directed path in Φ.

The elementary symmetric polynomial S_n^k is the polynomial in variables $x_1, \dots, x_n$ defined as

$$\sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k};$$

it is a homogeneous multilinear polynomial of degree k.

We show the following lower bounds on the size of multilinear homogeneous formulas computing S_n^k.

[1]The total number of nodes in a tree where each internal node has in-degree at least two is at most twice the number of leaves.

Theorem 1. Let $n \geq 2k$ and d be nonzero natural numbers.

(*i*). Every homogeneous multilinear formula computing S_n^k has size at least $k^{\Omega(\log k)}n$.

(*ii*). Every homogeneous multilinear formula of product-depth d computing S_n^k has size at least $2^{\Omega(k^{1/d})}n$.

In the case of S_{2n}^n, the first lower bound is superpolynomial and the latter exponential. Since the symmetric polynomials have multilinear formulas of size $O(n^2)$ and product-depth one (see Section 3.1), the theorem shows that homogeneous multilinear formulas are superpolynomially weaker than multilinear formulas, and that constant depth homogeneous multilinear formulas are exponentially weaker than their nonhomogeneous counterparts. Since monotone formulas computing homogeneous multilinear polynomials are both homogeneous and multilinear, we have a superpolynomial separation between monotone and non-monotone formulas. This separation also holds in the noncommutative case, which answers a question raised by Nisan (1991). The lower bounds are based on counting the number of monomials that occur in a polynomial that is computed by a homogeneous multilinear formula. We obtain essentially the same bounds as Shamir & Snir (1979) get in the case of monotone formulas. In fact, lower bound (*i*) from Theorem 1 can also be proved using the bound in (Shamir & Snir 1979); see discussion at the end of Section 3.3. However, our techniques are different and simpler.

We also provide upper bounds on the formula complexity of S_n^k.

Theorem 2. Let n, k be nonzero natural numbers.

(*i*). S_n^k has a homogeneous formula of size $k^{O(\log k)}n$.

(*ii*). S_n^k has a depth four (product-depth two) homogenous formula of size $2^{O(k^{1/2})}n$.

(*iii*). S_n^k has a monotone formula of size

$$2n \cdot n^{\log\left(\frac{k-1}{\log(2n)}+1\right)} \cdot \left(\frac{\log(2n)}{k-1}+1\right)^{k-1} = n \cdot n^{O(\log(1+\frac{k}{\log n}))}.$$

For a fixed k, all of the upper bounds given by Theorem 2 are essentially linear in n (i.e., linear in the first two cases, and $n^{1+o(1)}$ in the last one).

2. Lower bounds

In this section we prove the lower bounds given by Theorem 1.

2.1. Technical estimates. We need the following technical estimate.

LEMMA 3. Let $n \geq 2k$ be nonzero natural numbers. Fix nonzero natural numbers $k_1, \ldots, k_p$ such that $k_1 + \cdots + k_p = k$. Then for every natural number $n_1, \ldots, n_p$ such that $n_1 + \cdots + n_p = n$,

$$\binom{n_1}{k_1} \cdots \binom{n_p}{k_p} \leq 3k^{1/2}(k_1 \cdots k_p)^{-1/2}\binom{n}{k}.$$

PROOF. 1) We shall first prove the lemma using the additional assumption that $k_i \geq 2$ for every $i = 1, \ldots, p$. We estimate the maximum of $\binom{n_1}{k_1} \cdots \binom{n_p}{k_p}$ with respect to $n_1, \ldots, n_p$ satisfying the given constraints.

First we show that we can assume $1.5k_i \leq n_i$ for every $i \in [p]$. Let $n_1, \ldots, n_p$ be the integers where the maximum is attained. Assume without loss of generality that $n_1/k_1 \geq n/k \geq 2$. For every $i \in \{2, \ldots, p\}$, the choice of $n_1, \ldots, n_p$ implies that $\binom{n_1-1}{k_1}\binom{n_i+1}{k_i} \leq \binom{n_1}{k_1}\binom{n_i}{k_i}$. Hence $(n_i+1)/(n_i+1-k_i) \leq n_1/(n_1-k_1)$, and so $n_i/k_i \geq n_1/k_1 - 1/k_i \geq 2 - 1/2$.

For $i = 1, \ldots, p$ and a real number z such that $z > k_i$, define $f_i(z) = \frac{z^z}{k_i^{k_i}(z-k_i)^{z-k_i}}$. Thus $\frac{\partial}{\partial z} f_i = f_i \cdot \ln(1/(1-k_i/z))$. Denote

$$F(z_1, \ldots, z_p) = f_1(z_1)f_2(z_2)\cdots f_p(z_p).$$

We shall determine the maximum of F on the set $S \subset \mathbb{R}^p$ defined by the constraints $z_1 + \cdots + z_p = n$ and $z_i \geq 1.5k_i$, $i = 1, \ldots, p$. Since S is compact and F continuous, F has a maximum on S. Let $(z_1, \ldots, z_p) \in S$ be the point at which F attains its maximum. Our goal is to show that $z_i/k_i = n/k$ for every $i \in \{1, \ldots, p\}$. Assume without loss of generality that $z_1/k_1 \leq z_i/k_i$ for every $i \in \{2, \ldots, p\}$. Assume towards a contradiction that there exists $i \in \{2, \ldots, p\}$ with $z_1/k_1 < z_i/k_i$, and consider $f_1(z_1 + x)f_i(z_i - x)$ as a function of x. Since

$$\frac{\partial}{\partial x} f_1(z_1 + x)f_i(z_i - x)\Big|_{x=0} = f_1(z_1)f_i(z_i)\ln\left(\frac{1 - k_i/z_i}{1 - k_1/z_1}\right) > 0,$$

there exists $\varepsilon > 0$ such that $(z_1 + \varepsilon, \ldots, z_i - \varepsilon, \ldots, z_p) \in S$ and $f_1(z_1 + \varepsilon)f_i(z_i - \varepsilon) > f(z_1)f(z_i)$; a contradiction to the choice of $z_1, \ldots, z_p$. Hence, since $z_1 +$

$\cdots + z_p = n$ and $k_1 + \cdots + k_p = k$, we have $z_i/k_i = n/k$ for every $i = 1, \ldots, p$. So the maximum value of F on S is

$$\prod_{i=1,\ldots,p} \frac{n^{k_i}}{k^{k_i}} \frac{n^{n-k_i}}{(n-k)^{z_i-k_i}} = \frac{n^n}{k^k(n-k)^{n-k}}$$

Stirling's approximation tells us that for every nonzero $N, K \in \mathbb{N}$ with $1.5K \leq N$,

$$(1/3)K^{-1/2} \frac{N^N}{K^K(N-K)^{N-K}} \leq \binom{N}{K} \leq K^{-1/2} \frac{N^N}{K^K(N-K)^{N-K}},$$

which implies

$$\begin{aligned} \binom{n_1}{k_1} \cdots \binom{n_p}{k_p} &\leq (k_1 \cdots k_p)^{-1/2} F(n_1, \ldots n_p) \\ &\leq (k_1 \cdots k_p)^{-1/2} \frac{n^n}{k^k(n-k)^{n-k}} \\ &\leq 3k^{1/2}(k_1 \cdots k_p)^{-1/2} \binom{n}{k}. \end{aligned}$$

2) Assume without loss of generality that $k_1, \ldots, k_\ell = 1$, and denote $k' = k_1 + \cdots + k_\ell$ and $n' = n_1 + \cdots + n_\ell$. Since $\binom{n_1}{k_1} \cdots \binom{n_\ell}{k_\ell} \leq \binom{n'}{k'}$ and $3(k - k')^{1/2}(k_{\ell+1} \ldots k_p)^{-1/2} \leq 3k^{1/2}(k_1, \ldots k_p)^{-1/2}$, part 1) shows that

$$\binom{n_1}{k_1} \cdots \binom{n_p}{k_p} \leq 3k^{1/2}(k_1 \cdots k_p)^{-1/2} \binom{n-n'}{k-k'} \binom{n'}{k'} \leq 3k^{1/2}(k_1 \cdots k_p)^{-1/2} \binom{n}{k}.$$

□

2.2. In-degree two. Let f be a homogeneous polynomial of degree k. We say that f is *balanced* if there exist p homogeneous polynomials $f_1, \ldots, f_p$ such that $f = f_1 f_2 \cdots f_p$ with

(i). $(1/3)^i k < \deg f_i \leq (2/3)^i k$, $i = 1, \ldots, p-1$, and

(ii). $\deg(f_p) = 1$.

For a balanced polynomial f, let $\mathrm{minv}(f)$ be the smallest number q such that f can be written as $f = f_1 f_2 \cdots f_p$ above, and f_p contains q variables.

The following lemma shows that a small homogeneous formula can be written as a short sum of balanced polynomials.

Lemma 4. Let Φ be a homogeneous formula with in-degree at most two of size s and $\deg(\widehat{\Phi}) = k > 0$. Then there exist balanced polynomials $f_1, \ldots, f_{s'}$ such that $s' \leq s$,

$$\widehat{\Phi} = f_1 + \cdots + f_{s'}$$

and $\sum_{i=1,\ldots,s'} \mathrm{minv}(f_i) \leq s$. If Φ is multilinear, so are $f_1, \ldots, f_{s'}$.

For a node w in a formula Φ, denote by Φ_w the sub-formula of Φ with output node w, and by $\Phi_{(w=\alpha)}$ the formula obtained by deleting the edges going into w and labeling w (which is now an input node) by the field element α. One can see that

$$\widehat{\Phi} = h \cdot \widehat{\Phi}_w + \widehat{\Phi}_{(w=0)} ,$$

for some polynomial h that depends on w.

Proof. Let us first note the following:

Claim 5. If Φ is a formula of degree $k \geq 2$, then there exists a node w in Φ such that $(1/3)k \leq \deg(w) < (2/3)k$, where $\deg(w) = \deg(\widehat{\Phi}_w)$.

Proof. There exists a node v in Φ such that $\deg(v) \geq (2/3)k$, but for every child w of v (i.e., the edge (w, v) occurs in Φ), $deg(w) < (2/3)k$. Hence v is a product node $v = w_1 \times w_2$. If $\deg(w_1) \geq \deg(w_2)$ then $w = w_1$ has the correct properties, otherwise set $w = w_2$. □

We prove the lemma by induction on s and k. If $k = 1$, $\widehat{\Phi}$ is a balanced polynomial and $\mathrm{minv}(\widehat{\Phi}) \leq s$, since Φ contains at most s variables. Assume that $k \geq 2$. Let w be a node in Φ of degree k' such that $(1/3)k \leq k' < (2/3)k$; the node w exists by Claim 5. Homogeneity implies that we can write

$$\widehat{\Phi} = h \cdot \widehat{\Phi}_w + \widehat{\Phi}_{(w=0)},$$

where h is a polynomial of degree $k - k'$. Let s_w denote the size of Φ_w and let $s_{(w=0)}$ denote the size of $\Phi_{(w=0)}$. Thus $s_w + s_{(w=0)} \leq s$. By the inductive assumption, $\widehat{\Phi}_w = h_1 + \cdots + h_{s'_w}$ and $\widehat{\Phi}_{w=0} = g_1 + \cdots + g_{s'_{(w=0)}}$, where $s'_w \leq s_w$, $s'_{w=0} \leq s_{w=0}$, $h_1, \ldots, h_{s'_w}$ are balanced polynomials such that $\sum_i \mathrm{minv}(h_i) \leq s_w$, and $g_1, \ldots, g_{s'_{(w=0)}}$ are balanced polynomials such that $\sum_j \mathrm{minv}(g_j) \leq s_{(w=0)}$. (It may happen that $\widehat{\Phi}_{(w=0)}$ is the zero polynomial.) Hence

$$\widehat{\Phi} = hh_1 + \cdots + hh_{s_w} + g_1 + \cdots + g_{s_{(w=0)}}. \tag{2.1}$$

Since $(1/3)k < \deg h \leq (2/3)k$ and $(1/3)k \leq k' < (2/3)k$, hh_i is a balanced polynomial of degree k. Hence (2.1) is an expression of $\widehat{\Phi}$ in terms of balanced polynomials. Moreover, $\mathrm{minv}(hh_i) = \mathrm{minv}(h_i)$, and hence $\sum_i \mathrm{minv}(hh_i) + \sum_j \mathrm{minv}(g_j) \leq s_w + s_{(w=0)} \leq s$.

In the case that Φ is multilinear, we can assume without loss of generality that Φ is in fact syntactically multilinear (see, for example, (Raz 2004)), that is, for every product node $v = v_1 \times v_2$ in Φ, the set of variables that occur in Φ_{v_1} and the set of variables that occur in Φ_{v_2} are disjoint. This implies that the polynomials $hh_1, \ldots, hh_{s'_w}$ are multilinear. The lemma follows by induction.

□

The following lemma bounds the number of monomials in a balanced polynomial.

LEMMA 6. Let f be a balanced multilinear polynomial of degree k with at most n variables, $2k \leq n$. Then the number of monomials that occur in f is at most

$$3k^{-c\log k+3/2}\binom{n}{k}\mathrm{minv}(f)/n,$$

where $c > 0$ is a universal constant.

PROOF. Assume that $f = f_1 \cdots f_p$, where f_i has degree k_i and n_i variables (so $n_p = \mathrm{minv}(f)$). Specifically, $k_1 + \cdots + k_p = k$. Multilinearity implies $n_1 + \cdots + n_p \leq n$ (without loss of generality we can assume that $n_1 + \cdots + n_p = n$). Since each f_i is also homogeneous and multilinear, it contains at most $\binom{n_i}{k_i}$ monomials. Thus, since $k_p = 1$, f contains at most $\binom{n_1}{k_1} \cdots \binom{n_{p-1}}{k_{p-1}} n_p$ monomials, which, by Lemma 3, is at most $3k^{1/2}(k_1 \cdots k_p)^{-1/2}\binom{n-n_p}{k-1}n_p$. For every $1 \leq i \leq \log k/(2\log 3)$, we have $k_i \geq k^{1/2}$, and so

$$3(k_1 \cdots k_p)^{-1/2} \leq 3 \prod_{1 \leq i \leq \log k/(2\log 3)} k_i^{-1/2} \leq 3k^{-c\log k}$$

with $c > 0$ a universal constant (when $k = 1$, the number of monomials is at most $n_p = \mathrm{minv}(f)$, and the lemma holds). Since $\binom{n-n_p}{k-1} \leq \binom{n-1}{k-1} = \binom{n}{k}\frac{k}{n}$, the number of monomials that occur in f is at most

$$3k^{-c\log k+1/2}\binom{n-n_p}{k-1}n_p \leq 3k^{-c\log k+3/2}\binom{n}{k}\frac{\mathrm{minv}(f)}{n}.$$

□

We can now bound the number of monomials in a polynomial by its multilinear homogeneous formula complexity.

PROPOSITION 7. Let Φ be a multilinear homogeneous formula with in-degree at most two. Assume that Φ has size s, degree $k > 0$ and at most n variables, $2k \leq n$. Then the number of monomials that occur in $\widehat{\Phi}$ is at most

$$3k^{-c\log k+3/2}\binom{n}{k}\frac{s}{n},$$

where c is a universal constant.

PROOF. By Lemma 4, there exist balanced multilinear polynomials $f_1, \ldots, f_{s'}$ such that $\widehat{\Phi} = f_1 + \cdots + f_{s'}$ and $\sum_{i=1,\ldots,s'} \mathrm{minv}(f_i) \leq s$. By Lemma 6, there exists a constant $c > 0$ such that for every $i = 1, \ldots, s'$, the number of monomials that occur in f_i is at most $3k^{-c\log k+3/2}\binom{n}{k}\mathrm{minv}(f)/n$. The proposition follows, since the number of monomials that occur in $\widehat{\Phi}$ is at most the sum of the number of monomials that occur in the f_i's. □

COROLLARY 8. The first part of Theorem 1 holds.

PROOF. The number of monomials in S_n^k is $\binom{n}{k}$. □

2.3. Bounded depth. A homogeneous polynomial f has a (p,ℓ)-*form* if there exist homogeneous polynomials $f_1, \ldots, f_p$ such that $f = f_1 f_2 \cdots f_p$ and every f_i has degree at least ℓ. Define $\mathrm{minv}(f)$ as the smallest q such that f can be written as $f_1 f_2 \cdots f_p$ above and $q = \min\{n_i : i \in \{1, \ldots, p\}\}$, where n_i is the number of variables that f_i is defined over. This definition depends on the choice of (p,ℓ), which will be determined from context.

The following lemma shows that a small constant depth multilinear formula can be written as a short sum of formed polynomials.

LEMMA 9. Let Φ be a multilinear homogeneous formula of size s and product-depth d computing a polynomial of degree k. Let $q > 1$ be a natural number such that $k(2q)^{-d} > 1$. Then there exist $(q, k(2q)^{-d})$-form polynomials $f_1, \ldots, f_{s'}$ such that

$$\widehat{\Phi} = f_1 + \cdots + f_{s'}$$

and $\sum_{i=1,\ldots,s'} \mathrm{minv}(f_i) \leq s$.

PROOF. First let us note the following:

CLAIM 10. Let $r > 1$ be a real number such that $kr^{-d} > 1$. Then there exists a product node w in Φ such that $\deg(w) \geq kr^{-d+1}$ and $\deg(v) < \deg(w)/r$ for every child v of w. Moreover, if $r = 2q$ with $q \in \mathbb{N}$, then $\widehat{\Phi}_w$ is in $(q, k(2q)^{-d})$-form.

PROOF. The proof is by induction on d. If $d = 1$ and $u = u_1 \times u_2 \cdots \times u_j$ is a product node in Φ, then $\deg(u) = k$ and $\deg(u_i) \leq 1 < k/r$. So we can set $w = u$. Assume that $d > 1$, and let $u = u_1 \times u_2 \cdots \times u_j$ be a product node in Φ with $\deg(u) = k$. If for every $i = 1, \ldots, j$, $\deg(u_i) < k/r$, then we can set $w = u$. Otherwise there exists u_i such that $\deg(u_i) \geq k/r$. In this case, Φ_{u_i} is of product-depth $d' < d$ and degree at least k/r. By the inductive assumption, there exists a product node w in Φ_{u_i} such that $\deg(w) \geq \deg(u_i) r^{-d'+1} \geq k r^{-d+1}$ with the desired property.

Let f be a polynomial of degree at least m. If $f = f_1 f_2 \cdots f_n$ with $\deg(f_i) < m/t$, $t \in \mathbb{N}$, for every $i = 1, \ldots, n$, then f is of $(\lfloor t/2 \rfloor, m/t)$-form; this is achieved by an appropriate grouping of $f_1, \ldots, f_n$. Hence if $r = 2q$, the node w defines a polynomial of $(q, k(2q)^{-d})$-form. $\square$

We proceed by induction. Let w be a node given by Claim 10. As in the proof of Lemma 4, we can write

$$\widehat{\Phi} = h \cdot \widehat{\Phi}_w + \widehat{\Phi}_{(w=0)}.$$

Let s_w denote the size of Φ_w and let $s_{(w=0)}$ denote the size of $\Phi_{(w=0)}$. The polynomial $\widehat{\Phi}_{(w=0)}$ is either zero or of degree k. In the latter case, by inductive assumption, it can be written as $\sum_{i=1,\ldots,s'_{(w=0)}} g_i$ with $s'_{(w=0)} \leq s_{(w=0)}$, where the g_i's are in $(q, k(2q)^{-d})$-form and $\sum_{i=1,\ldots,s'_{(w=0)}} \mathrm{minv}(g_i) \leq s_{(w=0)}$. The polynomial $\widehat{\Phi}_w$ is in $(q, k(2q)^{-d})$-form. Moreover, if it is written as $f_1 \cdots f_q$, then every f_i contains at most s_w variables. Since $q > 1$ and by multilinearity, the polynomial $f = (hf_1) f_2 \cdots f_q$ is a polynomial of $(q, k(2q)^{-d})$-form with $\mathrm{minv}(f) \leq s_w$. Altogether, $\widehat{\Phi}$ can be written as $f + \sum_{i=1,\ldots,s'_{(w=0)}} g_i$ where $\mathrm{minv}(f) + \sum_{i=1,\ldots,s'_{(w=0)}} \mathrm{minv}(g_i) \leq s_w + s_{(w=0)} \leq s$. $\square$

The following lemma bounds the number of monomials in a formed polynomial.

LEMMA 11. Let f be a homogeneous multilinear polynomial of (p, ℓ)-form of degree k with at most n variables, where $2k \leq n$ and $p, \ell \geq 2$. Then the number of monomials that occur in f is at most $3k^{3/2} \ell^{-(p-1)/2} \binom{n}{k} \mathrm{minv}(f)/n$.

PROOF. Assume that $f = f_1 \cdots f_p$, where f_i has degree k_i and n_i variables, assume without loss of generality that $n_p = \mathrm{minv}(f)$. Homogeneity implies $k_1 + \cdots + k_p = k$ and multilinearity implies $n_1 + \cdots + n_p \leq n$ (without loss of generality $n_1 + \cdots + n_p = n$). Since each f_i is also homogeneous and multilinear, it contains at most $\binom{n_i}{k_i}$ monomials. Thus, f contains at most $\binom{n_1}{k_1}\cdots\binom{n_{p-1}}{k_{p-1}}\binom{n_p}{k_p}$ monomials, which, by Lemma 3, is at most $3k^{1/2}(k_1\cdots k_{p-1})^{-1/2}\binom{n-n_p}{k-k_p}\binom{n_p}{k_p}$. We have

$$\binom{n-n_p}{k-k_p}\binom{n_p}{k_p} = \frac{k-k_p+1}{n-n_p+1}\binom{n-n_p+1}{k-k_p+1}\frac{n_p}{k_p}\binom{n_p-1}{k_p-1} \le \frac{(k-k_p+1)n_p}{(n-n_p+1)k_p}\binom{n}{k}.$$

The minimality of n_p implies $n_p \le n/p$. Hence

$$\frac{k-k_p+1}{(n-n_p+1)k_p} \le \frac{k}{(n-n_p)k_p} \le \frac{k}{n(1-1/p)k_p} \le \frac{k}{n},$$

where the last inequality follows from the assumption $p, k_p \ge 2$. Therefore $\binom{n-n_p}{k-k_p}\binom{n_p}{k_p} \le \frac{k}{n}\binom{n}{k}n_p$ and the lemma follows. $\square$

The following proposition bounds the number of monomials in a polynomial that has a small multilinear homogeneous formula of constant depth.

Proposition 12. Let Φ be a multilinear homogeneous formula of size s, degree k, product-depth d, and over at most n variables, where $n \ge 2k$ and $k^{1/d} \ge 8$. Then the number of monomials that occur in $\widehat{\Phi}$ is at most $6k^{3/2}2^{-k^{1/d}/8}\binom{n}{k}s/n$.

Proof. Let $q = \lfloor k^{1/d}/4 \rfloor \ge 2$ and let $\ell = k(2q)^{-d} \ge 2$. Combining Lemmas 11 and 9, the polynomial $\widehat{\Phi}$ contains at most $3k^{3/2}\ell^{-(q-1)/2}\binom{n}{k}s/n$. Since $\ell^{-(q-1)/2} \le 2 \cdot 2^{-k^{1/d}/8}$, the proposition follows. $\square$

Corollary 13. The second part of Theorem 1 holds.

Proof. The number of monomials in S_n^k is $\binom{n}{k}$ (when $k^{1/d} < 8$ the lower bound holds trivially). $\square$

3. Upper bounds and separations

In this section we show several upper bounds on the complexity of the symmetric polynomials. We consider four models of computation in the following subsections.

3.1. Multilinear nonhomogeneous depth three. We now show that S_n^k can be computed by multilinear formulas of depth three (and product-depth one) of size $O(n^2)$. These formulas are of course not homogeneous, and we obtain a separation between homogeneous multilinear and non-homogeneous multilinear formulas. The construction was first suggested by Ben-Or, see (Shpilka & Wigderson 2001), and we give it here for completeness.

For $t \in \mathbb{R}$, denote

$$f_t = (x_1 t + 1)(x_2 t + 1) \cdots (x_n t + 1) = \sum_{k=0}^{n} t^k S_n^k.$$

Evaluating at $t = 1, \ldots, n+1$,

$$\begin{bmatrix} f_1 \\ f_2 \\ \cdots \\ f_{n+1} \end{bmatrix} = A \begin{bmatrix} S_n^0 \\ S_n^1 \\ \cdots \\ S_n^n \end{bmatrix}$$

with

$$A = \begin{bmatrix} 1^0 & 1^1 & \cdots & 1^n \\ 2^0 & 2^1 & \cdots & 2^n \\ & & \cdots & \\ (n+1)^0 & (n+1)^1 & \cdots & (n+1)^n \end{bmatrix}.$$

Since the matrix A is invertible, we can express every S_n^k as a linear combination of $f_1, \ldots, f_{n+1}$. Since f_t has a formula of depth two and size roughly n computing it, we can compute the symmetric polynomials with a depth three formula of size roughly n^2. (The same argument holds whenever there are more than n nonzero elements in the underlying field.)

3.2. Homogeneous non-multilinear. We now give an upper bound on the homogeneous formula size of S_n^k. Let w be a weight function that assigns a positive natural number $w(x)$ to every variable x. The *w-degree* of a monomial $x_{i_1} x_{i_2} \cdots x_{i_k}$ is defined as $w(x_{i_1}) + w(x_{i_2}) + \cdots + w(x_{i_k})$. A constant has w-degree zero. We say that a polynomial f is *w-homogeneous* if all monomials in f have the same w-degree. A circuit Φ is *w-homogeneous* if every node in Φ computes a w-homogeneous polynomial.

Lemma 14. (i). Let Φ be a w-homogeneous formula in variables $x_1, \ldots, x_k$, and let $\phi_1, \ldots, \phi_k$ be homogeneous formulas of degrees $w(x_1), \ldots, w(x_k)$. Then the formula $\Phi(\phi_1, \phi_2, \ldots, \phi_k)$ is homogeneous of degree that is equal to the w-degree of Φ; the formula $\Phi(\phi_1, \phi_2, \ldots, \phi_k)$ is obtained by substituting the formula ϕ_i instead of x_i for every $i = 1, \ldots, k$.

(ii). Let f be a polynomial of degree k that has a w-homogeneous circuit of size s, then f has a w-homogeneous formula of size $(sk)^{O(\log k)}$.

PROOF. (i) is by a straightforward induction on the size of Φ.

The proof of (ii) follows by the construction in (Hyafil 1979) – this construction transforms a w-homogeneous circuit into a w-homogeneous formula with the appropriate size. Here is a rough sketch of the construction. Let Φ be the circuit computing f (assume without loss of generality that the in-degree of Φ is at most two). Let V be the set of nodes v in Φ such that the w-degree of v is at least $k/2$, and $v = v_1 \times v_2$ with the w-degrees of both v_1 and v_2 less than $k/2$. It can be shown that $f = \sum_{v \in V} h_v \widehat{\Phi}_{v_1} \widehat{\Phi}_{v_2}$ with h_v having a circuit of size at most roughly the size of Φ. If we denote by $L(s,k)$ the smallest formula for a polynomial of degree k that has a circuit of size s, we have that $L(s,k)$ is at most roughly $sL(s,k/2)$. Thus $L(s,k)$ is at most roughly $s^{\log k}$. □

THEOREM 15. S_n^k has a homogeneous formula of size $k^{O(\log k)} n$, and a depth four homogenous formula of size $2^{O(k^{1/2})} n$.

PROOF. We apply Newton's identities. Let P_n^k be the polynomial $\sum_{i=1,\ldots,n} x_i^k$. Let Z_k be a polynomial in the variables $y_1, \ldots, y_k$ defined inductively as $Z_0 = 1$, and for $k \geq 0$,

$$Z_{k+1} = \frac{1}{k+1}\big(y_1 \cdot Z_k - y_2 \cdot Z_{k-1} + y_3 \cdot Z_{k-2} - \cdots + (-1)^{k+1} y_{k+1} \cdot Z_0\big).$$

Newton's identities assert that

$$S_n^k = Z_k(P_n^1, \ldots, P_n^k).$$

Define the weight w as $w(y_i) = i$. Thus Z_k is a w-homogeneous polynomial of w-degree k and degree k (this follows by induction on k). The definition of Z_k shows that it has a w-homogeneous circuit of size $O(k^2)$. By Lemma 14, there exists a w-homogeneous formula of size $k^{O(\log k)}$ computing Z_k. Since the degree of P_n^i is i and it has a homogeneous formula of size kn, the polynomial $S_n^k = Z_k(P_n^1, \ldots, P_n^k)$ has a homogenous formula of size $k^{O(\log k)} n$.

Since Z_k is w-homogeneous of w-degree k, the only monomials that occur in it are of the form $y_{i_1} y_{i_2} \cdots y_{i_t}$ with $i_1 + i_2 + \cdots + i_t = k$. The number of $i_1 \geq i_2 \geq \cdots \geq i_t$ that sum up to k is known as the *partition function* of k. A classical result of Hardy and Ramanujan says that the partition function of k is at most $2^{O(k^{1/2})}$. Thus Z_k has $2^{O(k^{1/2})}$ monomials, and so it has a depth two formula of size $2^{O(k^{1/2})}$, which implies that S_n^k has a depth four homogeneous formula of the appropriate size. □

3.3. Monotone. Let $L(k,n)$ denote the size of a smallest monotone formula computing S_n^k. We present an elementary upper bound on $L(k,n)$. The main features of the estimate are the following:

(i). $L(k,n)$ is polynomial, if $k \leq \log n$. Moreover, $L(\log n, n) = O(n^3)$.

(ii). $L(k,n) = n^{O(\log(n))}$, if $k \geq \sqrt{n}$.

(iii). $L(k,n) = O(n \log^{k-1} n)$, for a constant k. More precisely, $L(k,n) \leq 3n \left(e\frac{\log n}{k-1}\right)^{k-1}$, if k is fixed and n sufficiently large.

Theorem 16. If $k \geq 2$ then

$$L(k,n) \;\leq\; 2n \cdot n^{\log\left(\frac{k-1}{\log(2n)}+1\right)} \cdot \left(\frac{\log(2n)}{k-1}+1\right)^{k-1}$$

Hence $L(k,n)$ can be written as $n^{O(\log(\frac{k}{\log n}))}$.

Proof. Let us assume that n is power of two. Otherwise choose n' which is a power of two such that $n < n' < 2n$. Recall that we define formula size as the number of leaves. Hence $L(1,n) = n$. Since

$$S_{2n}^k(x_1,\ldots,x_{2n}) = \sum_{i=0,\ldots,k} S_n^i(x_1,\ldots,x_n) S_n^{k-i}(x_{n+1},\ldots,x_{2n}),$$

we obtain $L(k,2n) \leq 2\sum_{i=1,\ldots,k} L(i,n)$. Hence in order to upper bound $L(k,n)$, it is sufficient to find a nonnegative function g s.t.

$$g(k,2n) \geq 2 \sum_{i=1,\ldots,k} g(i,n), \qquad g(1,n) \geq n, \tag{3.1}$$

for every $n,k \geq 1$.

Let us first show the following:

Claim 17. Let $\alpha > 0$ be a fixed parameter. Then $g(k,n) = \frac{n^{1+\alpha}}{(1-2^{-\alpha})^{k-1}}$ satisfies (3.1).

Proof. Consider $g(k,n) = n^{1+\alpha}\beta^{k-1}$. Then $g(1,n) \geq n$ if $n \geq 1$ and $\alpha \geq 0$. In order to satisfy (3.1), it suffices to have

$$\begin{aligned} (2n)^{1+\alpha}\beta^{k-1} &\geq 2n^{1+\alpha}\beta^{k-1} + 2n^{1+\alpha}\sum_{i=1,\ldots,k-1}\beta^{i-1}, \qquad \text{resp.} \\ \beta^{k-1} &\geq (2^\alpha-1)^{-1}\sum_{i=1,\ldots,k-1}\beta^{i-1}. \end{aligned}$$

This holds if $\beta = 1 + (2^\alpha - 1)^{-1} = (1-2^{-\alpha})^{-1}$. □

The claim shows that for every $\alpha > 0$, $L(k,n) \leq \frac{n^{1+\alpha}}{(1-2^{-\alpha})^{k-1}}$. Let $z := \frac{k-1}{\log n}$ and $\alpha := \log(1+z)$. Then

$$\begin{aligned} \frac{n^{1+\alpha}}{(1-2^{-\alpha})^{k-1}} &= \frac{n^{1+\alpha}}{(z/(1+z))^{k-1}} \\ &= n^{1+\log(1+z)}\left(1+z^{-1}\right)^{k-1}. \end{aligned}$$

This gives the statement of the theorem. □

Weakly equivalent polynomials and Boolean complexity. We say that two polynomials f and g are *weakly equivalent* if for every monomial α, the coefficient of α is nonzero in f iff its coefficient in g is nonzero. Results in Boolean complexity yield better upper bounds for a monotone polynomial weakly equivalent to S_n^k than the ones in Theorem 16. The k-threshold function Th_n^k is a Boolean function on n inputs such that $\mathrm{Th}_n^k(e_1,\ldots,e_n) = 1$ iff $e_1+\ldots+e_n \geq k$. It is a natural counterpart of the elementary symmetric polynomial S_n^k. As shown in (Friedman 1984; Khasin 1970), Th_n^k have monotone Boolean formulas of size $O(n\log n)$, if k is fixed. In fact, the construction gives a monotone arithmetic formula computing a monotone polynomial weakly equivalent to S_n^k. Our lower bounds apply to any polynomial weakly equivalent to S_n^k. This shows that using our techniques we cannot hope to prove better lower bounds than $\Omega(n\log n)$, if k is fixed.

In the converse direction, a monotone arithmetic formula computing S_n^k, or a weakly equivalent polynomial, can be interpreted as a monotone Boolean formula computing Th_n^k. (Interpret $+, \times$ as $\vee, \wedge$, and every $\alpha > 0$ as Boolean 1.) Since for $k \geq 2$ such a formula must be of size $\Omega(n\log n)$, see (Hansel 1964), we have $\Omega(n\log n)$ lower bound on the size of monotone formulas computing S_n^k, or a weakly equivalent polynomial.

Finally, observe that if S_n^k has a multilinear homogeneous formula Φ of size s, then there exists a monotone formula Φ' of size s computing a monotone polynomial weakly equivalent to S_n^k. (The formula Φ' is obtained by replacing every constant a in Φ by $|a|$.) Hence the lower bound $\Omega(n \log n)$ applies also to homogeneous multilinear formulas computing S_n^k, $k \geq 2$. This also shows how to deduce lower bound (i) in Theorem 1 from the monotone lower bound in (Shamir & Snir 1979).

3.4. Noncommutative. A *noncommutative* polynomial over a field $\mathbb{F}$ is a polynomial in which the variables do not multiplicatively commute, for example, x_1x_2 and x_2x_1 are two different polynomials. A *noncommutative* formula is a formula which we understand as computing a noncommutative polynomial. Exponential lower bounds on the size of noncommutative formulas computing determinant and permanent were given in Nisan (1991). In that paper, Nisan posed the problem of separating monotone and general noncommutative formulas. Let us define S_n^k as the noncommutative polynomial

$$\sum_{i_1<i_2<\cdots<i_k} x_{i_1}x_{i_2}\cdots x_{i_k}.$$

Results from previous sections imply:

PROPOSITION 18. S_{2n}^n has a noncommutative formula of size $O(n^2)$, but every monotone noncommutative formula for it has size at least $n^{O(\log n)}$.

PROOF. The lower bound from Section 2.2 and the upper bound from Section 3.1 apply also to noncommutative setting. The lower bound is immediate, since noncommutative computation is weaker. For the upper bound, notice that the variables in the construction in Section 3.1 are written in the correct order. □

4. Summary

Whereas Boolean complexity of threshold functions has been mapped quite accurately, the arithmetic complexity of symmetric polynomials is folded in subtle mist. Here we summarise the basic known results on the formula complexity of S_n^k.

	Lower bound	*Upper bound*
Depth three, infinite fields [3]	$\Omega(n^2)$, *if* $k \sim n$	$O(n^2)$
Homogeneous		$k^{O(\log k)}n$
Homogeneous multilinear	$k^{\Omega(\log k)}n$	$n^{O(\log(\frac{k}{\log n}))}$
Homogeneous depth three [4]	$\binom{n}{\lfloor k/2 \rfloor}2^{-k}$	
Homogeneous depth four		$2^{O(k^{1/2})}n$
Homog. mult. product-depth d	$2^{\Omega(k^{1/d})}n$	

Monotone bounds are the same as the multilinear homogeneous ones, and in both cases we can add the lower bound $\Omega(n \log n)$ taken from monotone Boolean complexity of threshold functions (see Section 3.3).

Note that the lower bound and the upper bound on multilinear homogeneous complexity are both polynomial, if $k = \log n$, both superpolynomial, if $k = n/2$, but if $k = \log^2 n$, the lower bound is polynomial, whereas the upper bound is $n^{O(\log \log n)}$. The 'match' between multilinear homogeneous lower bounds and homogeneous upper bounds is also slightly irritating. However, the bounds cannot be exactly the same, for in the multilinear homogeneous case, we need at least $\Omega(n \log n)$ if $k \geq 2$.

Let us end with the following two questions:

(i). Can S_n^k be computed by a monotone formula of size $\mathrm{poly(n)} \cdot k^{O(\log k)}$*?*

(ii). Does the central symmetric polynomial S_{2n}^n have polynomial size homogeneous formula?

References

J. Friedman (1984). Constructing $O(n \log n)$ size monotone formulae for the k–th elementary symmetric polynomial of n Boolean variables. In *Proceedings of the 25th FOCS*, 506–515.

G. Hansel (1964). Nombre minimal de contacts de fermeture nécessaire pour réaliser une function Booléenne symmétriques de n variables. *C. R. Acad. Sci. Paris* **258**, 6037–6040.

L. Hyafil (1979). On the parallel evaluation of multivariate polynomials. *SIAM J. Comput.* **8**(2), 120–123.

[3]See (Shpilka & Wigderson 2001).

[4]See (Nisan & Wigderson 1996).

L. S. Khasin (1970). Complexity bounds for the realization of monotone symmetrical functions by means of formulas in the basis +,*,-. *Sov. Phys. Dokl.* **14**, 1149–1151.

N. Nisan (1991). Lower bounds for non-commutative computation. In *Proceeding of the 23th STOC*, 410–418.

N. Nisan & A. Wigderson (1996). Lower bounds on arithmetic circuits via partial derivatives. *Computational Complexity* **6**, 217–234.

R. Raz (2004). Multi-linear formulas for Permanent and Determinant are of super-polynomial size. In *Proceeding of the 36th STOC*, 633–641.

R. Raz (2009). Tensor rank and lower bounds on arithmetic formulas. Manuscript.

E. Shamir & M. Snir (1979). On the depth complexity of formulas. *Journal Theory of Computing Systems* **13**(1), 301–322.

A. Shpilka & A. Wigderson (2001). Depth-3 arithmetic formulae over fields of characteristic zero. *Journal of Computational Complexity* **10**(1), 1–27.

V. Strassen (1973). Vermeidung von Divisionen. *J. of Reine Angew. Math.* **264**, 182–202.

Acknowledgements

Partially supported by NSF grant CCF 0832797.

Manuscript received 23 January 2010

Pavel Hrubeš
Department of Computer Science,
Princeton University, USA.
pahrubes@gmail.com

Amir Yehudayoff
Institute for Advanced Study,
Princeton, USA.
amir.yehudayoff@gmail.com