Monotone separations for constant degree polynomials

Pavel Hrubeš* Amir Yehudayoff*

Abstract

We prove a separation between monotone and general arithmetic formulas for polynomials of constant degree. We give an example of a polynomial C in n variables and degree k which is computable by a homogeneous arithmetic formula of size $O(k^2n^2)$, but every monotone formula computing C requires size $(n/k^c)^{\Omega(\log k)}$, with $c \in (0,1)$. Since the upper bound is achieved by a homogeneous arithmetic formula, we also obtain a separation between monotone and homogeneous formulas, for polynomials of constant degree.

1 Introduction

Facing the unyielding challenge of proving lower bounds on arithmetic circuit or formula size, researchers have focused on several restricted models of computation. The first and most notable of such restrictions is the case of monotone computation. For example, lower bounds on monotone circuit size were proved in [2], and on monotone formula size in [4]. An exponential separation between monotone and general arithmetic circuits was given in [6]; this implies an exponential separation between monotone and general formulas as well.

An interesting class of polynomials is that of polynomials of constant degree. Proving nontrivial lower bounds for constant degree polynomials is, apparently, a harder task than for general polynomials. For example, super-linear lower bounds for the size of general arithmetic circuits are known for super-constant degree polynomials, whereas no super-linear lower bound is known for constant degree polynomials. See [3] for a longer discussion of constant degree polynomials.

---

*School of Mathematics, Institute for Advanced Study, Princeton NJ. Emails: `pahrubes@centrum.cz` and `amir.yehudayoff@gmail.com`. Partially supported by NSF grant CCF 0832797.

Nevertheless, Shamir and Snir [4] proved a lower bound of $n^{\Omega(\log k)}$ on the monotone formula size of a polynomial of degree k – multiplication of k $n \times n$ matrices. It is not known whether this polynomial can be computed by a small arithmetic formula, and hence this result does not imply a separation. We note that Valiant's separation [6] involves a high (linear in the number of variables) degree polynomial, which is a 'variant' of the permanent.

The purpose of this note is to fill this gap, and to give a separation between monotone and general arithmetic formulas for constant degree polynomials. Our lower bound employs techniques presented in [1]. We note that the proofs of [1] are based on counting monomials, whereas here we need to use subtler properties of monotone formulas. Our upper bound uses an interpolation argument, in the spirit of Ben-Or (cf. [5]).

2 Counting polynomials

We are interested in *arithmetic formulas* with fan-in at most two over the field of real numbers (see, e.g., [1] for a formal definition). We define formula *size* as the number of leaves in the formula. A *monotone polynomial* is a polynomial with only non-negative coefficients. A *monotone formula* is a formula with only non-negative constants. A *homogeneous formula* is a formula in which every node computes a homogeneous polynomial (i.e., a polynomial whose monomials have the same degree.)

If $I = \langle i_1, \dots i_k \rangle$ is a k-tuple of natural numbers, let x_I denote the monomial $x_{i_1} \cdot x_{i_2} \cdot \dots x_{i_k}$. Let $n, k, \ell \in \mathbb{N}$ and let $S \subseteq [n]$, where $[n] = \{0, 1, \dots, n\}$. Denote by $\mathcal{I}(S, k, \ell)$ the set of k-tuples $\langle i_1, i_2, \dots, i_k \rangle \in S^k$ such that $i_1 + i_2 + \dots + i_k = \ell$. Let $C_{n,k,\ell}$ be a polynomial in variables $x_0, \dots, x_n$ defined as

$$C_{n,k,\ell} = \sum_{I \in \mathcal{I}([n],k,\ell)} x_I \, . \tag{2.1}$$

We call $C_{n,k,\ell}$ a *counting* polynomial. It is a homogeneous polynomial of degree k in $n+1$ variables.

The following theorem implies a superpolynomial separation between monotone and general formulas. In particular, it gives a separation for constant degree (constant k).

Theorem 1. *Let $C = C_{n,k,n}$. Then*

(i). every monotone formula for C has size at least $(n/k^c)^{\Omega(\log k)}$, where $0 < c < 1$ is a universal constant, and

(ii). there exists a formula of size $O(k^2 n^2)$ for C; this formula is homogeneous.

2.1 Lower bound

We use some terminology from [1]. 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*). $\deg(f_p) = 1$.

The following lemma shows that a small monotone formula can be written as a short sum of balanced polynomials. It is a straightforward adaptation of the lemma from [1] to the case of monotone formulas.

Lemma 2. *Let Φ be a monotone formula of size s computing a homogeneous polynomial f of degree $k > 0$. Then there exist balanced monotone polynomials $f_1, \ldots, f_{s'}$ of degree k such that $s' \leq s$ and $f = f_1 + \cdots + f_{s'}$.*

The following proposition and Lemma 2 imply part (i) of Theorem 1.

Proposition 3. *Let $n, k \in \mathbb{N}$ and let $C = C_{n,k,n}$. If $C = f_1 + \cdots + f_s$ with $f_1, \ldots, f_s$ balanced monotone polynomials of degree k, then $s \geq (n/k^c)^{\Omega(\log k)}$, where $0 < c < 1$ is a universal constant.*

Before proving the proposition we recall the following estimate from [1].

Lemma 4. *Let $n \geq 2k$ and $k_1, \ldots, k_p$ be non-zero natural numbers such that $k_1 + \cdots + k_p = k$. Then for every natural numbers $n_1, \ldots, n_p$ 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 of Proposition 3. Since C is homogeneous of degree k and $f_1, \ldots, f_s$ are monotone, $f_1, \ldots, f_s$ are homogeneous polynomials of degree k. Fix $t \in \{1, \ldots, s\}$ and denote f_t by f. Since f is a balanced polynomial, we can write $f = g_1 g_2 \cdots g_p$.

Claim 5. *There exist natural numbers $n_1, n_2, \ldots, n_p, k_1, k_2, \ldots, k_p$ such that $n_1 + \cdots + n_p = n$ and $k_1 + \cdots + k_p = k$ and for every $j = 1, \ldots p$, all the monomials that occur in g_j are of the form x_I with $I \in \mathcal{I}([n_j], k_j, n_j)$.*

Proof. Define k_j to be the degree of g_j. Since f is homogeneous of degree k, $k_1+\cdots+k_p = k$ and each g_j is homogeneous. Hence if a monomial x_I occurs in g_j then $|I| = k_j$. Let us fix n_j as some natural number such that there exists a monomial x_I which occurs in g_j and $\sum_{i\in I} i = n_j$. Monotonicity implies that for every monomial x_L occurring in g_j, $\sum_{i\in L} i = n_j$. For assume otherwise, and let x_M be a monomial that occurs in $g_1 \cdots g_{j-1}g_{j+1}, \ldots g_p$. Then both the monomials $x_I x_M, x_L x_M$ occur in C, which is impossible since $\sum_{i\in I\cup M} i \neq \sum_{i\in L\cup M} i$. For a similar reason, $n_1 + \cdots + n_p = n$. Finally, since $\sum_{i\in L} i = n_j$ implies that, as a set, $L \subseteq [n_j]$, we have $L \in \mathcal{I}([n_j], k_j, n_j)$ for every x_L occurring in g_j. $\square$

Claim 5 shows that for every $j = 1, \ldots, p$, the number of monomials that occur in g_j is at most $|\mathcal{I}([n_j], k_j, n_j)|$. The size of $\mathcal{I}([n_j], k_j, n_j)$ is

$$\binom{n_j + k_j - 1}{k_j - 1}.$$

If $k_j = 1$, g_j contains exactly one monomial. Setting q to be the maximal j such that $k_j \geq 2$, Lemma 4 shows that the number of monomials in f is at most

$$\begin{aligned}\binom{n_1 + k_1 - 1}{k_1 - 1} \cdots \binom{n_q + k_q - 1}{k_q - 1} &\leq 3k^{1/2} \prod_{i=1,\ldots,q} (k_i - 1)^{-1/2} \binom{n + k - q}{k - q} \\ &= 3k^{1/2} \prod_{i=1,\ldots,q} (k_i - 1)^{-1/2} \prod_{i=1,\ldots,q-1} \frac{k - i}{n + k - i} \cdot \binom{n + k - 1}{k - 1}.\end{aligned}$$

For every $1 \leq i \leq \log k/(2\log 3) - 1$, we have $k_i \geq 3k^{1/2}$, and so $k_i - 1 \geq k^{1/2}$. Hence

$$k^{1/2} \prod_{i=1,\ldots,q} (k_i - 1)^{-1/2} \leq k^{-c_1 \log k + 1}$$

with a constants $c_1 > 0$. Since $q \leq k$, we have

$$\prod_{i=1,\ldots,q-1} \frac{k - i}{n + k - i} \leq \left(\frac{k}{n}\right)^{q-1}$$

Since f is balanced, q is at least $c_2 \log k - 2$ with $c_2 > 0$ a universal constant. Hence the number of monomials in $f = f_t$ is at most

$$3k^{-c_1 \log k + 1} \left(\frac{k}{n}\right)^{c_2 \log k - 3} \binom{n + k - 1}{k - 1} \leq \left(\frac{k^c}{n}\right)^{-\Omega(\log k)} \binom{n + k - 1}{k - 1},$$

with an adequate constant $c \in (0, 1)$. Since this holds for every t and since the number of monomials in C is $\binom{n+k-1}{k-1}$, we have that s is at least $(n/k^c)^{\Omega(\log k)}$. $\square$

2.2 Upper bound

We now construct polynomial size formulas for $C_{n,k,\ell}$.

Proof of part (ii) of Theorem 1. Fix $n, k \in \mathbb{N}$. Let Z be the polynomial

$$Z(t) = (x_0 t^0 + x_1 t^1 + \cdots + x_n t^n)^k ,$$

where t is an auxiliary variable. Observe that

$$Z(t) = \sum_{0 \le \ell \le nk} t^\ell C_{n,k,\ell}.$$

Evaluating at $t = 0, \ldots, nk$,

$$\begin{bmatrix} Z(0) \\ Z(1) \\ \cdots \\ Z(nk) \end{bmatrix} = A \begin{bmatrix} C_{n,k,0} \\ C_{n,k,1} \\ \cdots \\ C_{n,k,nk} \end{bmatrix}$$

with

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

Since the matrix A is invertible, we can express every $C_{n,k,\ell}$ as a linear combination of $Z(0), \ldots, Z(nk)$. For a particular number a, $Z(a)$ has a homogeneous formula of size roughly kn computing it, hence we can compute $C_{n,k,\ell}$ by a homogeneous formula of size roughly $k^2 n^2$. □

References

[1] P. Hrubeš and A. Yehudayoff. Homogeneous formulas and symmetric polynomials. arXiv: 0907.2621v1.

[2] M. Jerrum and M. Snir. Some exact complexity results for straight-line computations over semirings. Journal of the ACM 29 (3), pp. 874–897, 1982.

[3] R. Raz. Elusive functions and lower bounds for arithmetic circuits. Proceeding of the 40th STOC, pp. 711–720, 2008.

[4] E. Shamir and M. Snir. On the depth complexity of formulas. Journal Theory of Computing Systems 13 (1), pp. 301–322, 1979.

[5] A. Shpilka and A. Wigderson. Depth-3 arithmetic formulae over fields of characteristic zero. Journal of Computational Complexity 10 (1), pp. 1–27, 2001.

[6] L. G. Valiant. Negation can be exponentially powerful. Theoretical Computer Science 12, pp. 303–314, 1980.