Computing polynomials with few multiplications

Shachar Lovett *
June 19, 2011

Abstract

A folklore result in arithmetic complexity shows that the number of multiplications required to compute some \( n \)-variate polynomial of degree \( d \) is \( \sqrt{\binom{n+d}{n}} \). We complement this by an almost matching upper bound, showing that any \( n \)-variate polynomial of degree \( d \) over any field can be computed with only \( \sqrt{\binom{n+d}{n}} \cdot (nd)^{O(1)} \) multiplications.

1 Introduction

Arithmetic complexity is a branch of theoretical computer science which studies the minimal number of operations (additions and multiplications) required to compute polynomials. A basic question is the following: what is the minimal number of operations required to compute any \( n \)-variate polynomial of degree \( d \)? A folklore result (see, e.g., [1, Theorem 4.2]) shows that the number of multiplications required to compute any polynomial is at least the square root of the total number of monomials. That is, there exist \( n \)-variate polynomials of degree \( d \) which require \( \sqrt{\binom{n+d}{n}} \) multiplications. The aim of this note is to complement this lower bound by an almost matching upper bound.

Theorem 1. Any \( n \)-variate polynomial of degree \( d \) over any field can be computed by at most \( \sqrt{\binom{n+d}{n}} \cdot (nd)^{O(1)} \) multiplications.

The best previous upper bound on the number of multiplications was \( O\left(\left(\frac{1}{n}\right)^{n} \binom{n+d}{n}\right) \).

2 General framework

We first fix notations: let \( \mathbb{N} := \{0, 1, \ldots\} \) and \( [n] := \{1, \ldots, n\} \). We identify monomials in \( x_1, \ldots, x_n \) with their degree vector \( e \in \mathbb{N}^n \), where we shorthand \( x^e := x_1^{e_1} \cdots x_n^{e_n} \). We denote the set of all \( n \)-variate degree \( d \) monomials by \( \mathcal{M}(n, d) := \{ e \in \mathbb{N}^n : \sum e_i \leq d \} \), where \( |\mathcal{M}(n, d)| = \binom{n+d}{n} \). The weight of a monomial is \( |e| := \sum e_i \).

*The Institute for Advanced Study. slovett@math.ias.edu. Supported by NSF grant DMS-0835373.
The main idea is to cover the set of monomials by a few sums of pairs of sets. For sets $A, B \subseteq \mathbb{N}^n$ denote their sum by $A + B := \{a + b | a \in A, b \in B\}$. A set $A$ is monotone if $e \in A$ implies $e' \in A$ for all $e' \leq e$ (that is, $e'_i \leq e_i$ for all $i \in [n]$).

**Claim 2.** Let $\{(A_i, B_i)\}_{i \in [k]}$ be pairs of monotone sets such that $\mathcal{M}(n, d) \subseteq \bigcup_{i=1}^{k} (A_i + B_i)$. Then any $n$-variate polynomial of degree $d$ can be computed by an arithmetic circuit with $\sum_{i=1}^{k} O(|A_i| + |B_i|)$ multiplications.

**Proof.** Compute first all monomials $x^e$ for $e \in A_1, B_1, \ldots, A_k, B_k$. This can be done with $\sum(|A_i|+|B_i|)$ multiplications since the sets are monotone. By assumption, for each monomial $e \in \mathcal{M}(n,d)$ there exists $i \in [k]$ such that $e \in A_i + B_i$. Thus for any set of coefficients $\{\lambda_e : e \in \mathcal{M}(n,d)\}$ we can find coefficients $\{\lambda_{i,e',e''} : i \in [k], e' \in A_i, e'' \in B_i\}$ such that

$$\sum_{e \in \mathcal{M}(n,d)} \lambda_e x^e = \sum_{i=1}^{k} \sum_{e' \in A_i} x^{e'} \left( \sum_{e'' \in B_i} \lambda_{i,e',e''} x^{e''} \right).$$

This requires additional $\sum |A_i|$ multiplications. \qed

An easy way to show the existence of pairs $\{(A_i, B_i)\}_{i \in [k]}$ is to exhibit a distribution over pairs $(A, B)$ such that each monomial belongs to $A + B$ with a noticeable probability.

**Claim 3.** Assume there is a distribution over pairs $(A, B)$ of monotone sets of bounded size $|A|, |B| \leq N$, such that for any monomial $e \in \mathcal{M}(n,d)$,

$$\Pr_{A,B}[e \in A + B] \geq \varepsilon.$$

Then any $n$-variate polynomial of degree $d$ can be computed with $O(N \cdot (n+d)/\varepsilon)$ multiplications.

**Proof.** Sample $(A_1, B_1), \ldots, (A_k, B_k)$ independently. For each $e \in \mathcal{M}(n,d)$, the probability that $e \notin A_i + B_i$ for all $i \in [k]$ is at most $(1-\varepsilon)^k$. Thus for $k = O(\varepsilon^{-1} \log |\mathcal{M}(n,d)|) \leq O((n+d)/\varepsilon)$ we have by the union bound that $\mathcal{M}(n,d) \subseteq \bigcup_{i=1}^{k} (A_i + B_i)$ almost surely. \qed

## 3 Constructing a distribution

We construct in this section a distribution over pairs of monotone sets $(A, B)$ such that

1. For each monomial $e \in \mathcal{M}(n,d)$, $\Pr_{A,B}[e \in A + B] \geq 1/n$.

2. $|A|, |B| \leq \sqrt{(n/d) \cdot (nd)^{O(1)}}$.

We can assume w.l.o.g that $n$ is odd and $d$ is even, at the price of increasing the number of monomials at most by a factor of $O(nd)$. For a set of variables $S \subseteq [n]$ we denote by $\mathcal{M}(S,d)$ the set of degree $d$ polynomials with variables restricted to $S$. We construct the
distribution over pairs $A,B$ as follows: let $S,T \subset [n]$ be chosen uniformly conditioned on $|S| = |T| = (n + 1)/2$ and $|S \cap T| = 1$. Set $A := \mathcal{M}(S, d/2)$ and $B := \mathcal{M}(T, d/2)$.

First note that $|A|, |B| = \left( \frac{(n+d+1)/2}{d/2} \right) \leq \sqrt{n + d + 1} \leq (n + d)^{1/2} \cdot \sqrt{n/d}$ as claimed. To conclude we need to show that any monomial belongs to $A + B$ with noticeable probability.

**Lemma 4.** Let $e \in \mathcal{M}(n, d)$. Then $\Pr_{A,B}[e \in A + B] \geq 1/n$.

**Proof.** Fix a monomial $e \in \mathcal{M}(n, d)$. Let $\{\ell\} = S \cap T, S' := S \setminus \{\ell\}, T' := T \setminus \{\ell\}$ and define the sums $s := \sum_{i \in S} e_i$ and $t := \sum_{i \in T'} e_i$. Consider the event

$$E := [s \leq d/2 \mbox{ and } t \leq d/2].$$

We first claim that if $E$ holds then $e \in A + B$. Define $a \in A, b \in B$ as follows: $a_i = e_i$ for $i \in S'; b_i = e_i$ for $i \in T'$; and set $a_\ell + b_\ell = e_\ell$ where $a_\ell + s \leq d/2$ and $b_\ell + t \leq d/2$.

We analyze $\Pr[E]$ by considering an equivalent event. The distribution of $S,T$ can be sampled as follows: first choose a random permutation on $[n]$, then choose a uniform index $\ell \in [n]$ and set $S = \{\pi(\ell), \pi(\ell+1), \ldots, \pi(\ell+(n-1)/2)\}$ and $T = \{\pi(\ell-(n-1)/2), \ldots, \pi(\ell)\}$, where sums are evaluated modulo $n$. Thus, we have

$$\Pr[E] = \Pr_{\pi,\ell} \left[ \sum_{i=\ell+1}^{\ell+(n-1)/2} e_{\pi(i)} \leq d/2 \mbox{ and } \sum_{i=\ell-(n-1)/2}^{\ell-1} e_{\pi(i)} \leq d/2 \right].$$

We will lower bound $\Pr[E/\pi]$ for any permutation $\pi$, which implies a lower bound on $\Pr[E]$. Fix a permutation $\pi$ and set $f_i := e_{\pi(i)}$. Define the sums $w_j := \sum_{i=j+1}^{j+(n-1)/2} f_i$ for $j \in [n]$, i.e. all possible consecutive sequences of $(n-1)/2$ elements. We will show there exists $j^* = j^*(\pi)$ for which $w_{j^*} \leq d/2$ and $w_{j^*+(n-1)/2} \leq d/2$. This implies that if we choose $\ell = j^*$ then the event $E$ indeed holds, which implies

$$\Pr[\ell \in E/\pi] \geq \Pr[\ell = j^*(\pi)] \geq 1/n.$$

Thus to conclude we just need to establish the existence of such $j^*$. If $w_j \leq d/2$ for all $j \in [n]$ then any $j^*$ will do. Otherwise, there must exist $j'$ for which $w_{j'} > d/2$. There also must exist $j''$ for which $w_{j''} \leq d/2$, since $\frac{1}{n} \sum_{j \in [n]} w_j = \frac{1}{n} |e| (n-1)/2 \leq d/2$. Thus there must exist two consecutive sums with this property, i.e. $k$ for which $w_k > d/2$ and $w_{k+1} \leq d/2$. Setting $j^* = k - 1$ concludes the proof, since $w_{j^*} = w_{k+1} \leq d/2$ and $w_{j^*+(n-1)/2} = |e| - w_k \leq d/2$. 

**Acknowledgements** I thank Avi Wigderson, Amir Shpilka and Neeraj Kayal for helpful discussions.

**References**