THEORY OF COMPUTING, Volume 7 (2011), pp. 185–188
www.theoryofcomputing.org

NOTE

Computing Polynomials with Few Multiplications

Shachar Lovett*

Received: June 19, 2011; published: September 16, 2011.

Abstract: It is a folklore result in arithmetic complexity that the number of multiplication gates required to compute a worst-case n-variate polynomial of degree d is at least

$$\Omega\left(\sqrt{\binom{n+d}{d}}\right),$$

even if addition gates are allowed to compute arbitrary linear combinations of their inputs. In this note we complement this by an almost matching upper bound, showing that for any n-variate polynomial of degree d over any field,

$$\sqrt{\binom{n+d}{d}} \cdot (nd)^{O(1)}$$

multiplication gates suffice.

ACM Classification: F.1.3

AMS Classification: 68Q25

Key words and phrases: arithmetic circuits, 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 natural model of

*Supported by NSF grant DMS-0835373.

DOI: 10.4086/toc.2011.v007a013

computation in these settings is an arithmetic circuit, where the inputs are variables $x_1,\dots,x_n$, gates correspond to the $+,\times$ operations and multiplication by field elements, and the output gate computes the required polynomial. The complexity measures associated with arithmetic circuits are their size and depth. We refer the reader to [3] for an extensive survey on arithmetic circuits.

In this note we focus on the minimal number of *multiplications* required to compute a polynomial, where additions of polynomials and multiplication by field elements are free. To this end, we consider a non-standard model of arithmetic circuits where addition gates can compute arbitrary linear combinations of their inputs (instead of just their sum). We assume both multiplication and addition gates have unbounded fan-in. For a polynomial f we define its *multiplicative complexity*, denoted $M(f)$, to be the minimal number of multiplication gates required to compute f in this non-standard model.

Consider polynomials of degree d in n variables over a field $\mathbb{F}$. (In this note, we write "degree-d polynomials" as a shorthand for "polynomials of total degree at most d.") The number of possible monomials of such a polynomial is $\binom{n+d}{d}$. It is a folklore result in arithmetic complexity (see, e. g., [1, Theorem 4.2]) that the number of *multiplications* required to compute some n-variate polynomial of degree d is at least the square root of this number.

Theorem 1.1 (Theorem 4.2 in [1])**.** *Let $\mathbb{F}$ be a field and n,d be two natural numbers. Then there exists an n-variate polynomial $f(x_1,\dots,x_n)$ of degree d for which $M(f)\geq\Omega\left(\sqrt{\binom{n+d}{d}}\right)$.*

Hrubeš and Yehudayoff [2] exhibit similar lower bounds even if one considers only polynomials with 0-1 coefficients.

Theorem 1.2 ([2])**.** *Let $\mathbb{F}$ be a field and n,d be two natural numbers. Then there exists an n-variate polynomial $f(x_1,\dots,x_n)$ of degree d with 0-1 coefficients for which $M(f)\geq\Omega\left(\sqrt{\binom{n+d}{d}}\right)$.*

The aim of this note is to complement these lower bounds by an almost matching upper bound.

Theorem 1.3. *Let $\mathbb{F}$ be a field and n,d be two natural numbers. Let $f(x_1,\dots,x_n)$ be any n-variate polynomial of degree d over $\mathbb{F}$. Then $M(f)\leq\sqrt{\binom{n+d}{d}}\cdot(nd)^{O(1)}$.*

To the best of our knowledge, the best previous upper bound on the number of multiplications was

$$M(f)\leq O\left(\frac{1}{n}\binom{n+d}{d}\right)$$

(see the discussion following Theorem 4.4 in [1]). We note that the circuit constructed in Theorem 1.3 has the following additional features, which can be immediately verified from the construction:

(1) It is a depth-4 circuit.

(2) If f has 0-1 coefficients, or if the field is of size at most $\text{poly}(n)$, then the bound holds also in the standard model of arithmetic circuits where addition gates compute the sum of their inputs (instead of linear combinations of their inputs).

(3) If f is a real polynomial with positive coefficients, then the circuit computing f is monotone (i. e., all coefficients in the addition gates are positive).

We now turn to the proof.

2 Proof of Theorem 1.3

We first fix some notation: let $\mathbb{N} := \{0,1,\dots\}$ and $[n] := \{1,\dots,n\}$. We identify monomials in $x_1,\dots,x_n$ with their exponent vectors $e \in \mathbb{N}^n$, where we use the shorthand $x^e := x_1^{e_1}\dots x_n^{e_n}$. We denote the set of all n-variate degree-d monomials by $\mathcal{M}(n,d) := \{e \in \mathbb{N}^n : \sum e_i \le d\}$. Note that $|\mathcal{M}(n,d)| = \binom{n+d}{d}$. The weight of a monomial is $|e| := \sum e_i$.

The main idea is to cover the set $\mathcal{M}(n,d)$ of monomials by few sums of pairs of sets. For sets $A, B \subseteq \mathbb{N}^n$ denote their sum by $A + B := \{a + b \mid a \in A, b \in B\}$.

Claim 2.1. *Let $\{(A_i,B_i)\}_{i\in[k]}$ be pairs of subsets of $\mathbb{N}^n$ such that $\mathcal{M}(n,d) \subseteq \bigcup_{i=1}^k (A_i + B_i)$. Then for any n-variate polynomial $f(x_1,\dots,x_n)$ of degree d we have $M(f) \le 2\sum_{i=1}^k(|A_i|+|B_i|)$.*

Proof. Let $f(x) = \sum_{e\in\mathcal{M}(n,d)} \lambda_e x^e$ be an n-variate polynomial of degree d. First compute all monomials x^e for $e \in A_1, B_1, \dots, A_k, B_k$. This can be done with $\sum_{i=1}^k(|A_i|+|B_i|)$ multiplications (recall that multiplication gates have unbounded fan-in). By assumption, for each monomial $e \in \mathcal{M}(n,d)$ there exists $i \in [k]$ such that $e \in A_i + B_i$. For $i \in [k], e' \in A_i, e'' \in B_i$ define $\delta_{i,e',e''} \in \{0,1\}$ as follows: enumerate the triples (i,e',e'') in some order; for a triple (i,e',e''), if the sum $e'+e''$ never occurred in a previous triple, set $\delta_{i,e',e''} = 1$, otherwise set $\delta_{i,e',e''} = 0$. We thus have

$$f(x) = \sum_{i=1}^k \sum_{e'\in A_i} x^{e'} \times \left(\sum_{e''\in B_i} \lambda_{e'+e''}\delta_{i,e',e''} \cdot x^{e''}\right).$$

This representation allows one to compute f using only $\sum_{i=1}^k |A_i|$ additional multiplications. $\square$

We thus need to construct small sets $\{(A_i,B_i)\}$ whose pairwise sums cover $\mathcal{M}(n,d)$. We will construct these sets from polynomials in $\sim n/2$ variables of degree $\sim d/2$.

For a subset $S \subseteq [n]$ of variables denote by $\mathcal{M}(S,d)$ the set of all monomials of degree at most d in the variables of S. Clearly $|\mathcal{M}(S,d)| = \binom{|S|+d}{d}$. In the following we identify $[n] := \mathbb{Z}_n$, i. e., we consider indices modulo n. For $i, j \in [n]$ define the interval $[i,j] := \{i, i+1, \dots, j\} \subseteq \mathbb{Z}_n$.

Claim 2.2. *Let n be odd and d be even. For $i = 1,\dots,n$, set $A_i := \mathcal{M}([i, i+(n-1)/2], d/2)$ and $B_i := \mathcal{M}([i-(n-1)/2, i], d/2)$. Then $\mathcal{M}(n,d) \subseteq \bigcup_{i=1}^n (A_i + B_i)$.*

Proof. Let $e \in \mathcal{M}(n,d)$. We need to show that $e \in A_i + B_i$ for some $i \in [n]$. Let $m := (n-1)/2$. For $i \in [n]$ define the partial sum $w_i := \sum_{\ell=1}^m e_{i+\ell}$ where indices are taken modulo n. Note that

$$w_i + w_{i+m} = |e| - e_i \le d - e_i\,. \tag{1}$$

We first claim that if $w_i, w_{i+m} \le d/2$ then $e \in A_i + B_i$. We then proceed to show such an index i indeed exists.

Assume first that $w_i, w_{i+m} \le d/2$. We will construct $e' \in A_i, e'' \in B_i$ such that $e = e' + e''$. By Equation (1), we can decompose $e_i = e'_i + e''_i$ such that $e'_i, e''_i \ge 0$, $w_i + e'_i \le d/2$ and $w_{i+m} + e''_i \le d/2$. For $j \ne i$ set $e'_j = e_j, e''_j = 0$ if $j \in [i, i+m] \setminus \{i\}$; and $e'_j = 0, e''_j = e_j$ if $j \in [i-m, i] \setminus \{i\}$.

To conclude the proof we need to show that there exists i for which $w_i, w_{i+m} \le d/2$. Assume this is not the case. Then there exists j for which $w_j > d/2$. But then $w_{j+m} < d/2$ by Equation (1). Therefore there must exist i such that $w_i \le d/2$ and $w_{i-1} \ge d/2$. This concludes the proof since $w_{i+m} = |e| - e_{i+m} - w_{i-1} \le d/2$ by Equation (1). $\square$

We now conclude with the proof of Theorem 1.3.

Proof of Theorem 1.3. Let $f(x)$ be an n-variate polynomial of degree d. Let $n' \geq n, d' \geq d$ be minimal such that n' is odd and d' is even. By Claim 2.2 we can find sets A_i, B_i, $i \in [n']$ such that

$$\mathcal{M}(n,d) \subseteq \mathcal{M}(n',d') \subseteq \sum_{i=1}^{n'} (A_i + B_i)\,,$$

and such that

$$|A_i|, |B_i| = \binom{(n'+1)/2 + d'/2}{d'/2} \leq O\left(\max\left(\frac{d}{n^{5/4}}, \frac{n^{1/2}}{d^{3/4}}\right)\right) \cdot \sqrt{\binom{n+d}{d}}\,.$$

Thus by Claim 2.2 we have $M(f) \leq O\left(\max\left(\frac{d}{n^{1/4}}, \frac{n^{3/2}}{d^{3/4}}\right)\right) \cdot \sqrt{\binom{n+d}{d}}$, justifying the claim. □

Acknowledgements I thank Avi Wigderson, Amir Shpilka, and Neeraj Kayal for helpful discussions. I thank the anonymous reviewers for a careful reading of this note and in particular for a simplification of Claim 2.2.

References

[1] XI CHEN, NEERAJ KAYAL, AND AVI WIGDERSON: Partial derivatives in arithmetic complexity (and beyond). *Found. Trends Theor. Comput. Sci.* To appear. 186

[2] PAVEL HRUBEŠ AND AMIR YEHUDAYOFF: Arithmetic complexity in ring extensions. *Theory of Computing*, 7(1):119–129, 2011. http://www.theoryofcomputing.org/articles/v007a008. [doi:10.4086/toc.2011.v007a008] 186

[3] AMIR SHPILKA AND AMIR YEHUDAYOFF: Arithmetic circuits: A survey of recent results and open questions. *Found. Trends Theor. Comput. Sci.*, 5:207–388, March 2010. [doi:10.1561/0400000039] 186

AUTHOR

Shachar Lovett
member, School of Mathematics
Institute for Advanced Study, Princeton, NJ
slovett@math.ias.edu
http://www.math.ias.edu/~slovett

ABOUT THE AUTHOR

SHACHAR LOVETT graduated from the Weizmann Institute of Science in 2010; his advisors were Omer Reingold and Ran Raz. He is interested in the theory of computing, combinatorics, and coding theory, and in particular in the interplay between structure, randomness, and pseudo-randomness.