Electronic Colloquium on Computational Complexity, Report No. 191 (2020)

Negations Provide Strongly Exponential Savings

Arkadev Chattopadhyay* Rajit Datta† Partha Mukhopadhyay‡

December 27, 2020

Abstract

We show that there is a family of monotone multilinear polynomials over n variables in VP, such that any monotone arithmetic circuit for it would be of size $2^{\Omega(n)}$. Before this result, strongly exponential size monotone lower bounds were known only for explicit polynomials in VNP [GS12, RY11, Sri19, CKR20]. The family of polynomials we prescribe are the spanning tree polynomials considered by Jerrum and Snir [JS82], but this time defined over constant-degree expander graphs.

1 Introduction

Proving lower bounds for the size of monotone arithmetic circuits computing explicit polynomials has attracted a lot of attention in algebraic complexity theory. In a seminal work, Valiant proved exponential lower bounds on the size of monotone arithmetic circuits computing the perfect matching polynomial for a class of planar graphs [Val80]. Shortly after that, Jerrum and Snir proved similar lower bounds for the permanent and the spanning tree polynomial for complete graphs [JS82]. These polynomials are n-variate and the lower bounds are of order $2^{\Omega(\sqrt{n})}$.

Notably, the matching polynomial considered in [Val80] and the spanning tree polynomial considered in [JS82] can be computed by algebraic branching programs of polynomial size. This showed that the presence of negations can exponentially cut down on the cost of computing monotone polynomials. The question we study here is whether negations can provide even strongly exponential savings.

Interestingly, monotone lower bounds for any polynomial which are strongly exponential in the number of variables were obtained much later. At present, there are several results which show strongly exponential monotone lower bounds for explicit polynomials in VNP [GS12, RY11, Sri19, CKR20]. The proof technique in [GS12] is based on the construction of Sidon Sets. In [RY11], Raz and Yehudayoff have used a sophisticated exponential sum estimate [BGK06] as one of their main tools. The technique used by Srinivasan [Sri19] is inspired by communication complexity and a separation of MVNP and MVP by Yehudayoff [Yeh19]. The proof in [CKR20] is very short and elegant. It is based on the explicit construction of a sufficiently good error correcting code [1].

All these results, therefore, still leave open the possibility that every monotone polynomial in VP can be computed in size $2^{o(n)}$ by monotone circuits. In this note, we rule out this possibility. Our argument is short. It is a reinterpretation of the argument of [JS82] in more modern terms combined with the use of expander graphs. The idea of using expander graphs is inspired from [Sri19]. Now, we explain our result in detail.

*TIFR, Mumbai. Partially supported by a MATRICS grant of the Science and Engineering Research Board, DST, India. arkadev.c@tifr.res.in

†CMI, Chennai. Partially supported by a TCS Fellowship. rajit@cmi.ac.in

‡CMI, Chennai. partham@cmi.ac.in

[1] Very recently, Hrubeš and Yehudayoff have given further example of VNP polynomial exhibiting strongly exponential size monotone lower bound [HY20].

ISSN 1433-8092

Let G be an undirected graph on n vertices and let $\widetilde{G}$ be the directed graph obtained from G which has edges (u, v) and (v, u) (in both directions) for every undirected edge (u, v) in G. Consider the directed spanning tree polynomial

$$\mathrm{ST}_n(\widetilde{G}) = \sum_{\tau \in T_n} x_{2,\tau(2)} x_{3,\tau(3)} \cdots x_{n,\tau(n)},$$

where $T_n = \{\tau : \{2, 3, \ldots, n\} \mapsto \{1, 2, \ldots, n\} \mid \forall i \; \exists k \; \tau^k(i) = 1 \, ; \forall i \; (i, \tau(i)) \in E(\widetilde{G})\}$. We note that the maps in T_n correspond to directed spanning trees rooted at 1 and every monomial κ of ST_n is of the form $x_{2,i_2} x_{3,i_3} \cdots x_{n,i_n}$. It is well-known that for every G, $\mathrm{ST}_n(\widetilde{G})$ can be computed even by an algebraic branching program of size $\mathsf{poly}(n)$ [W70] via a determinant computation [MV97]. Jerrum and Snir showed that if G is the complete graph, then any monotone circuit for $\mathrm{ST}_n(\widetilde{G})$ must be of size $2^{\Omega(n)}$ [JS82]. Note that, in this case the number of variables is n^2. In contrast, we show the following.

Theorem 1.1. *For a sufficiently large constant d, let G be a d regular expander graph on n vertices with $\lambda_2 \leq d^{1-\epsilon}$ for some $\epsilon > 0$. Then every monotone circuit for $\mathrm{ST}_n(\widetilde{G})$ must be of size at least $2^{\Omega(n)}$.*

2 Preliminaries

Notation.

Let $[n] = \{1, 2, \ldots, n\}$. Polynomials are always considered over $\mathbb{R}[X]$ where $\mathbb{R}$ is the set of reals. For a polynomial p, let $\mathsf{var}(p)$ denote the set of variables in p.

Set-multilinear Polynomials.

Let $X = \cup_{i=1}^{n} X_i$ be a set of variables where $X_i = \{x_{i,1}, x_{i,2}, \ldots, x_{i,m}\}$. A polynomial $p \in \mathbb{R}[X]$ is set-multilinear if each monomial in p respects the partition given by the set of variables $X_1, X_2, \ldots, X_n$. In other words, each monomial κ in p is of the form $x_{1,j_1} x_{2,j_2} \cdots x_{n,j_n}$.

Ordered Polynomial.

For a monomial of the form $\kappa = x_{i_1,j_1} x_{i_2,j_2} \cdots x_{i_n,j_n}$ we define the set $I(\kappa) = \{i_1, i_2, \ldots, i_n\}$. If a polynomial p has the same set $I(\kappa)$ for every monomial occurring it it with a non-zero coefficient, then we say that the polynomial is ordered and we write $I(p) = I(\kappa)$ for each κ. Clearly, the set-multilinear polynomials are ordered polynomials with $I(p) = \{1, 2, \ldots, n\}$.

Structure of Monotone Circuits.

The main structural result for monotone circuits that we use throughout, is the following theorem.

Theorem 2.1. *[Yeh19, Lemma 1] Let $n > 2$ and $p \in \mathbb{R}[X]$ be an ordered monotone polynomial with $I(p) = [n]$. Let C be a monotone circuit of size s that computes p. Then, we can write*

$$p = \sum_{t=1}^{s} a_t \cdot b_t$$

where a_t and b_t are monotone ordered polynomials with $\frac{n}{3} \leq |I(a_t)| \leq \frac{2n}{3}$ and $I(b_t) = I(a_t) \setminus [n]$. Moreover, $a_t b_t \leq p$ for each $1 \leq t \leq s$.

3 Strong Exponential Separation of VP and Monotone VP

In this section we prove Theorem 1.1. For a graph G, let $V(G), E(G)$ denote the set of vertices and edges of G respectively, and for any pair $S, T \subseteq V(G)$, let $E(S,T) \equiv \{(u,v) \in E(G) \,:\, u \in S\,, v \in T\}$.

Lemma 3.1 (Expander Mixing Lemma)**.** *[HLW06, Lemma 2.5] Let G be an undirected d regular graph such that λ_2 is the second largest eigenvalue of the adjacency matrix of G. Then, for every $S, T \subseteq V(G)$*

$$\Big||E(S,T)| - \frac{d}{n}|S||T|\Big| \leq \lambda_2\sqrt{|S||T|}.$$

We also need Matrix Tree Theorem which we state below.

Theorem 3.1. *[Matrix Tree Theorem][MM11, Theorem 13.1] Let G be an undirected graph on n vertices and let $0, \mu_1, \mu_2, \ldots, \mu_{n-1}$ be the eigenvalues of the Laplacian of G. Then the number of spanning trees in G is $\frac{1}{n}\mu_1 \cdot \mu_2 \cdots \mu_{n-1}$*

Proof of Theorem 1.1. Consider a family of d-regular expander graphs where d is a sufficiently large constant and the second largest eigenvalue is bounded by $d^{1-\epsilon}$ for a suitable $\epsilon > 0$. For example, the current proof works for $\epsilon = 0.25$ and such a family of graphs can be explicitly constructed [RVW00]. Let $G = G_n$ be the n^{th} graph in the family.
Suppose $\mathrm{ST}_n(\widetilde{G})$ has a monotone circuit of size S. Then applying Theorem 2.1 to the polynomial $\mathrm{ST}_n(\widetilde{G})$ we get

$$\mathrm{ST}_n(\widetilde{G}) = \sum_{s=1}^{S} a_s b_s. \tag{1}$$

For a fixed s, let $X_t = \{x_{t,j} | x_{t,j} \in \mathrm{var}(a_s) \cup \mathrm{var}(b_s)\}$. Since every monomial of $ST_n(\widetilde{G})$ has distinct first indices we conclude that $I(a_s) \cap I(b_s) = \emptyset$.
Now we upper bound $\sum_{t=2}^{n} |X_t|$. We note that if $i \in I(a_s)$ and $j \in I(b_s)$ then it cannot be the case that both $x_{i,j}$ and $x_{j,i}$ are in $\cup_{t=2}^{n} X_t$. Suppose $x_{i,j}, x_{j,i} \in \cup_{t=2}^{n} X_t$ then it must be the case that $x_{i,j} \in \mathrm{var}(a_s)$ and $x_{j,i} \in \mathrm{var}(b_s)$ (since $i \notin I(b_s)$ and $j \notin I(a_s)$). Then some monomial in $a_s b_s$ contains $x_{i,j}x_{j,i}$ which is a two cycle and cannot be part of the spanning tree polynomial.
This shows that in the set of undirected edges $E(I(a_s), I(b_s))$, at least one out of the two directed edge variables, corresponding to an undirected edge, must be absent in $\cup_{t=2}^{n} X_t$. Thus we may bound,

$$\sum_{t=2}^{n} |X_t| \leq dn - |E(I(a_s), I(b_s))|.$$

Since G is an expander, using Lemma 3.1 we conclude that

$$\Big||E(I(a_s), I(b_s))| - \frac{d}{n}|I(a_s)||I(b_s)|\Big| \leq \lambda_2\sqrt{|I(a_s)||I(b_s)|}.$$

On rearranging, we obtain

$$\Big|E(I(a_s), I(b_s))\Big| \geq \frac{d}{n}|I(a_s)||I(b_s)| - \lambda_2\sqrt{|I(a_s)||I(b_s)|}.$$

Since $|I(a_s)|, |I(b_s)| \geq \frac{n}{3}$ and $|I(a_s)| + |I(b_s)| = n$ we may simplify the right hand side as

$$\Big|E(I(a_s), I(b_s))\Big| \geq \frac{d}{n}\frac{n^2}{9} - \lambda_2\frac{n}{2} = n(\frac{d}{9} - \frac{\lambda_2}{2}).$$

Since $\lambda_2 \leq d^{1-\epsilon}$, we may relax the right hand side and write $|E(I(a_s), I(b_s))| \geq \frac{nd}{18}$ for sufficiently large d. Let $\alpha = \frac{1}{18}$. Now we bound the total numbers of monomials in $a_s b_s$ as

$$|\mathrm{mon}(a_s b_s)| \leq \prod_{t=2}^{n} |X_t| \leq \left(\frac{\sum_{t=2}^{n} |X_t|}{n-1} \right)^{n-1} \leq ((1-\alpha)\frac{nd}{n-1})^{n-1} \leq (1.01d(1-\alpha))^{n-1}$$

for sufficiently large n.
Then, the number of monomials in $\mathrm{ST}_n(\tilde{G})$:

$$|\mathrm{mon}(\mathrm{ST}_n(\widetilde{G}))| \leq S(1.01d(1-\alpha))^{n-1}. \tag{2}$$

Let $L(G)$ be the Laplacian of the graph G with eigenvalues $0 < \mu_1 \leq \mu_2 \leq \ldots \leq \mu_{n-1}$. Since G is an expander, we conclude that $\mu_1 \geq (d - \lambda_2)$. Then, Theorem 3.1 implies that

$$|\mathrm{mon}(\mathrm{ST}_n(\widetilde{G}))| = \frac{1}{n}\mu_1\mu_2\cdots\mu_{n-1} \geq \frac{1}{n}(d-\lambda_2)^{n-1} \geq \frac{1}{n}(d-d^{1-\epsilon})^{n-1}.$$

Remark 3.1. *Notice that each spanning tree rooted at the vertex* 1 *in* G *is in bijective correspondence with a rooted tree at the vertex* 1 *in* $\widetilde{G}$.

Putting the above bound together with the upper bound in Equation 2, we get that

$$\frac{1}{n}(d-d^{1-\epsilon})^{n-1} \leq |\mathrm{mon}(\mathrm{ST}_n(\widetilde{G}))| \leq S(1.01d(1-\alpha))^{n-1}.$$

This immediately implies that $S \geq \frac{1}{n}\left(\frac{d-d^{1-\epsilon}}{1.01d(1-\alpha)}\right)^{n-1} \geq \frac{1}{n}(\frac{99}{101(1-\alpha)})^{n-1} = 2^{\Omega(n)}$, for sufficiently large d. □

Acknowledgement

We thank Mrinal Kumar for his comments on this work.

References

[BGK06] J. Bourgain, A. A. Glibichuk, and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, Journal of London Mathematical Society **2** (2006), 380–398.

[CKR20] Bruno Pasqualotto Cavalar, Mrinal Kumar, and Benjamin Rossman, *Monotone circuit lower bounds from robust sunflowers*, LATIN 2020: Theoretical Informatics - 14th Latin American Symposium, São Paulo, Brazil, January 5-8, 2021, Proceedings (Yoshiharu Kohayakawa and Flávio Keidi Miyazawa, eds.), Lecture Notes in Computer Science, vol. 12118, Springer, 2020, pp. 311–322.

[GS12] S. B. Gashkov and I. S. Sergeev, *A method for deriving lower bounds for the complexity of monotone arithmetic circuits computing real polynomials*, Sbornik. Mathematics **203(10)** (2012).

[HLW06] Shlomo Hoory, Nathan Linial, and Avi Wigderson, *Expander graphs and their applications*, Bull. Amer. Math. Soc. **43** (2006), 439–561.

[HY20] Pavel Hrubeś and Amir Yehudayoff, *Shadows of Newton polytopes*, Electronic Colloquium of Computational Complexity **TR20-189** (2020).

[JS82] Mark Jerrum and Marc Snir, *Some exact complexity results for straight-line computations over semirings*, J. ACM **29** (1982), no. 3, 874–897.

[MM11] Christofer Moore and Stephan Mertens, *The nature of computation*, Oxford University Press, 2011.

[MV97] Meena Mahajan and V. Vinay, *Determinant: Combinatorics, algorithms, and complexity*, Chic. J. Theor. Comput. Sci. **1997** (1997).

[RVW00] Omer Reingold, Salil P. Vadhan, and Avi Wigderson, *Entropy waves, the zig-zag graph product, and new constant-degree expanders and extractors*, FOCS, 2000, pp. 3–13.

[RY11] Ran Raz and Amir Yehudayoff, *Multilinear formulas, maximal-partition discrepancy and mixed-sources extractors*, J. Comput. Syst. Sci. **77** (2011), no. 1, 167–190.

[Sri19] Srikanth Srinivasan, *Strongly exponential separation between monotone VP and monotone VNP*, Electron. Colloquium Comput. Complex. **26** (2019), 32.

[Val80] Leslie G. Valiant, *Negation can be exponentially powerful*, Theor. Comput. Sci. **12** (1980), 303–314, Preliminary version in STOC 1979.

[W70] Moon J W, *Counting labelled trees*, Canadian Mathematical Congress, Montreal (1970).

[Yeh19] Amir Yehudayoff, *Separating monotone VP and VNP*, Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, STOC 2019, Phoenix, AZ, USA, June 23-26, 2019 (Moses Charikar and Edith Cohen, eds.), ACM, 2019, pp. 425–429.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il