Homogeneous ABP complexity of Elementary Symmetric Polynomials

Nutan Limaye, Kunal Mittal, and Mukesh Pareek

IIT Bombay, India.

Abstract

In this note we show that the homogeneous ABP complexity of the Elementary Symmetric Polynomial on n variables and degree d is $\Theta(nd)$.

1 Introduction

Algebraic Branching Program (ABP) over a field $\mathbb{F}$ on variables $x_1, x_2, \ldots, x_n$ is a directed acyclic graph (DAG) which has a designated source node s (with in-degree 0), a designated sink node t (with out-degree 0) and in which every edge is labelled with an affine linear form from $\mathbb{F}[x_1, \ldots, x_n]$.

Let π be a path in the ABP. The weight of the path π, denoted as $w(\pi)$, is a polynomial obtained by taking the product of all the linear forms labelling the edges along π. The polynomial computed at a particular vertex v in the ABP, denoted as $[v]$, is the sum of the weights of all the paths from s to v. In particular, the polynomial computed by the ABP is $[t]$. The size of the ABP is the number of vertices in the underlying DAG.

An ABP is said to be homogeneous if the polynomial computed at every node of the ABP is homogeneous.

Definition 1. *Let $X = \{x_1, \ldots, x_n\}$. We say that the homogeneous ABP complexity of a polynomial $p(X) \in \mathbb{F}[X]$, which we denote by $\alpha_{\mathbb{F}}(p)$, is the size of the smallest homogeneous ABP computing that polynomial. We drop the subscript $\mathbb{F}$ if the underlying field is clear from the context.*

In [Kum17] it was shown that $\alpha_{\mathbb{F}}(P_{n,d})$ is $\Omega(nd)$, where $P_{n,d} = \sum_{i=1}^{n} x_i^d$ and $\mathbb{F}$ is any algebraically closed field of characteric zero or relatively prime to d. In fact they showed that $\alpha_{\mathbb{F}}(P_{n,d})$ is at least $\lceil n/2 \rceil (d-1) + 2$. Over algebraically closed fields one can show that[1] there is a homogeneous ABP computing $P_{n,d}$ of size $\lceil n/2 \rceil (d-1) + 2$. This shows that the bound proved in [Kum17] is tight.

Here we analyse the homogeneous ABP complexity of the Elementary Symmetric polynomials. The Elementary Symmetric polynomial on n variables of degree d is defined as follows: $\mathsf{Sym}_n^d(X) = \sum_{S \subseteq [n], |S|=d} \prod_{i \in S} x_i$. We show the following about $\mathsf{Sym}_n^d(X)$.

Theorem 2. *Let $\mathbb{F}$ be any algebraically closed field. The homogeneous ABP complexity of $\mathsf{Sym}_n^d(X)$ over the field $\mathbb{F}$ is $\Theta(nd)$.*

In what follows, we first introduce some background and notations. The proof of the lower bound is our main contribution, which is presented in Section 3. The upper bound of $O(nd)$ on $\alpha(\mathsf{Sym}_n^d(X))$ is folklore and we present it for the sake of completeness.

[1] Consider $\lceil n/2 \rceil$ disjoint paths from source s to t. The i^{th} path computes $x_{2i}^d + x_{2i+1}^d$. Since $\mathbb{F}$ is algebraically closed, we can factor $x_{2i}^d + x_{2i+1}^d$ into d linear terms and keep these as the ABP edge weights.

2 Preliminaries

Let $X = \{x_1, \ldots, x_n\}$. Let $\mathbb{F}$ be any algebraically closed field. As mentioned earlier, $\mathsf{Sym}_n^d(X)$ is the Elementary Symmetric polynomial on n variables of degree d. For $S \subseteq X$ and $|S| \leq n-d$, we use $\mathsf{Sym}_{-|S|}^d(X \setminus S)$ to denote the Elementary Symmetric polynomial on $|X \setminus S|$ many variables of degree d. If S is a singleton set, say $S = \{i\}$, then we use $\mathsf{Sym}_{-i}^d(X)$ to denote $\mathsf{Sym}_{-|\{i\}|}^d(X \setminus \{i\})$. For a point $\tilde{a} \in \mathbb{F}^n$, we use $\mathsf{Sym}_n^d(\tilde{a})$ (or $\mathsf{Sym}_{-i}^d(\tilde{a})$) to denote the polynomial $\mathsf{Sym}_n^d(X)$ (or $\mathsf{Sym}_{-i}^d(X)$) evaluated at $\tilde{a}$. We use $[n]$ to denote the set $\{1, 2, \ldots, n\}$.

2.1 Structural results about homogeneous ABPs

Here we present some preliminaries about homogeneous ABPs. The results mentioned here are from [Kum17]. Let A be a homogeneous ABP. Let π be a path from s to v. We say that *the index* of the path, $w'(\pi)$, is k if there are k edges along the path with non-constant weights. Let *the formal degree* of a vertex v be the maximum index along any s to v path.

Lemma 3 ([Kum17])**.** *Let A be a homogeneous ABP with $\mathfrak{s}$ vertices. It can be converted to an ABP B with at most $\mathfrak{s}$ vertices such that for all vertices, the formal degree equals the degree of the polynomial computed at that vertex.*

Lemma 4 ([Kum17])**.** *Let A be a homogeneous ABP with $\mathfrak{s}$ vertices, computing an n-variate polynomial $p(X) \in \mathbb{F}[X]$ of degree d. For any $i \in [d-1]$, let $S_i = \{u_1, \ldots, u_m\}$ denote the set of vertices in A with formal degree equal to i, where $m \leq \mathfrak{s}$. Then*

$$p(X) = (\sum_{j=1}^{m} [u_j] h_j) + R$$

for some polynomials $h_1, \ldots, h_m \in \mathbb{F}[X]$ and $R \in \mathbb{F}[X]$ such that the degree of R is at most $d-1$.

2.2 Ideals, Varieties and Projective spaces

For a set of n-variate polynomials $S = \{p_1, p_2, \ldots, p_k\}$ in $\mathbb{F}[X]$, let $\mathbb{V}(S)$ be the affine variety of S in $\mathbb{F}^n$, i.e., the set of common zeroes of S.

$$\mathbb{V}(S) = \{a \in \mathbb{F}^n \mid p(a) = 0 \ \forall p \in S\}.$$

For a variety $\mathbb{V} \in \mathbb{F}^n$, the ideal generated by the variety, $\mathbb{I}(\mathbb{V})$, is defined as

$$\mathbb{I}(\mathbb{V}) = \{q \in \mathbb{F}[X] \mid q(a) = 0 \ \forall a \in \mathbb{V}\}$$

Consider the equivalence relation $\sim$ on $\mathbb{F}^{n+1}$ given by $(a_0, \ldots, a_n) \sim (a'_0, \ldots, a'_n)$ if there is a constant $\lambda \in \mathbb{F}$ such that $(a_0, \ldots, a_n) = \lambda(a'_0, \ldots, a'_n)$. Then the n dimensional projective space over $\mathbb{F}$ is defined as

$$\mathbb{P}^n(\mathbb{F}) = (\mathbb{F}^{n+1} - \{\mathbf{0}\}) / \sim$$

where $\mathbf{0}$ denotes the all zero point in $\mathbb{F}^{n+1}$.

Let $\mathbb{V} \subset \mathbb{F}^n$ be an affine variety. The coordinate ring $\mathbb{F}[\mathbb{V}]$ is defined as the set of all polynomial maps from $\mathbb{V}$ to $\mathbb{F}$. In particular, $\mathbb{F}[\mathbb{V}] \cong \mathbb{F}[X] / \mathbb{I}(\mathbb{V})$. For a polynomial p, we denote by $[p]$ its coset in $\mathbb{F}[X] / \mathbb{I}(\mathbb{V})$.

A set of elements $f_1, \ldots, f_r \in \mathbb{F}[\mathbb{V}]$ is said to be algebraically independent if there is no non-zero polynomial p such that $p(f_1, \ldots, f_r) = 0$ in $\mathbb{F}[\mathbb{V}]$.

An important property of a variety $\mathbb{V}$ is its dimension. Informally, the dimension is the minimum number of hyperplanes in general position whose intersection with the variety is a finite and non-zero set of points. We state some results without proof. The details of these can be found in a wonderful exposition by Cox, Little and O'Shea [CLO07].

Lemma 5. *Let S be a set of polynomials in $\mathbb{F}[x_1, \ldots, x_n]$, where $\mathbb{F}$ is algebraically closed and $|S| \leq n$. Let $\mathbb{V} = \mathbb{V}(S)$ be non-empty. Then $dim(\mathbb{V}) \geq n - |S|$.*

Lemma 6. *Let $\mathbb{F}$ be an algebraically closed field and $\mathbb{V}_1 \subseteq \mathbb{V}_2 \subseteq \mathbb{F}^n$ be two affine varieties. Then $dim(\mathbb{V}_1) \leq dim(\mathbb{V}_2)$.*

Theorem 7. *Let $\mathbb{F}$ be algebraically closed and $\mathbb{V} \subset \mathbb{P}^n(\mathbb{F})$ be a projective variety with $dim(\mathbb{V}) > 0$. If f is any non-constant homogeneous polynomial, then*

$$dim(\mathbb{V}) \geq dim(\mathbb{V} \cap \mathbb{V}(f)) \geq dim(\mathbb{V}) - 1$$

In particular we will be interested in intersection of $\mathbb{V}$ with the plane $\mathbb{V}(x_0)$.

Lemma 8. *Let $V = \mathbb{V}(f_1, \ldots, f_s) \subset \mathbb{P}^n(\mathbb{F})$ be a projective variety. Let $U = \left\{a \in \mathbb{F}^{n+1} \mid a_0 \neq 0\right\}$. Then $V \cap U$ can be identified with the affine variety $W = \mathbb{V}(g_1, \ldots, g_s)$ where $g_i = f_i(1, x_1, \ldots, x_n)$ for $1 \leq i \leq s$.*

In particular, Lemma 6 gives us that $dim(W) \leq dim(V)$.

Theorem 9. *Let $V \subset \mathbb{F}^n$ be an affine variety. Then the dimension of V is equal to the maximum number of elements of $\mathbb{F}[V]$ that are algebraically independent.*

Moreover, if $dim(V) = d$, then there are coordinates $x_{i_1}, \ldots, x_{i_d}$ such that $[x_{i_1}], \ldots, [x_{i_d}]$ are algebraically independent with respect to $\mathbb{F}[V]$.

3 Lower bound on the ABP complexity of $\mathsf{Sym}_n^d(X)$

In this section we prove the following theorem.

Theorem 10. *Let B be a homogeneous ABP of formal degree at most d over $\mathbb{C}$, computing $\mathsf{Sym}_n^d(X)$. Then number of vertices in B is at least $(d-1) \cdot (n-d+1)/2 + 2$.*

We follow the proof outline of [Kum17] closely to prove a lower bound on the ABP complexity of $\mathsf{Sym}_n^d(X)$. We prove the following technical lemma about $\mathsf{Sym}_n^d(X)$. A very similar Lemma was proved by [Kum17] for $P_n^d(X)$. Once this lemma is proved, the rest of the proof of the Theorem is exactly like in [Kum17]. In order to prove the following lemma, we will need an upper bound on the dimension of the variety of the first derivatives of $\mathsf{Sym}_n^d(X)$. This bound is proved using Lemma 12 and Lemma 13. These two lemmas are the new contributions of this note.

Lemma 11. *Suppose $\mathsf{Sym}_n^d(X)$ can be expressed in the following form*

$$\mathsf{Sym}_n^d(X) = P + \sum_{i=1}^{k} Q_i R_i,$$

where polynomial P has degree at most $d-1$, and $S = \{Q_1, \ldots, Q_k, R_1, \ldots, R_k\}$ is such that $\mathbb{V}(S)$ is non-empty. Then $k \geq (n-d+1)/2$.

Assuming this lemma, the proof of the theorem follows easily.

Proof of Theorem 10. Let B be a homogeneous ABP of formal degree at most d over algebraically closed field $\mathbb{F}$, computing $\mathsf{Sym}_n^d(X)$. We will show that for any $i \in [d-1]$, the number of vertices in B with formal degree i is at least $\lfloor (n-d+1)/2 \rfloor$. This will give us the theorem.

Fix an $i_0 \in [d-1]$. Using Lemma 4, we know that $\mathsf{Sym}_n^d(X)$ can be expressed as follows:

$$\mathsf{Sym}_n^d(X) = (\sum_{j=1}^{m} [u_j] h_j) + R,$$

where $\{u_1, \ldots, u_m\}$ denotes the set of vertices in B with formal degree equal to i_0, and $h_1, \ldots, h_m, R \in \mathbb{F}[X]$ are some polynomials such that the degree of R is at most $d-1$. For $j \in [m]$, let $D_{1,j}$ denote the degree of u_j and $D_{2,j}$ denote the degree of h_j. Now for each $j \in [m]$, we will write u_j as $P_j + p_j$ and each h_j as $Q_j + q_j$, where P_j and Q_j are degree $D_{1,j}$ and degree $D_{2,j}$ homogeneous components of u_j and h_j, respectively. Now we can rewrite $\mathsf{Sym}_n^d(X)$ as follows.

$$\mathsf{Sym}_n^d(X) = (\sum_{j=1}^{m} P_j Q_j) + R'$$

where R' still has degree at most $d-1$. Moreover, $\mathbf{0}$ is the variety of $\{P_1, \ldots, P_m, Q_1, \ldots, Q_m\}$. Now, using Lemma 11, we get that $m \geq (n-d+1)/2$.

As this lower bound holds for each $i \in [d-1]$ and as there is one node in layer 0 (i.e. s) and one in layer d, we get the lower bound mentioned in Theorem 10. □

Proof of Lemma 11. Suppose $k < (n-d+1)/2$. Then consider $\mathbb{V}(S)$ which has $2k$ polynomials, each over n variables. By Lemma 5, $dim(\mathbb{V}(S)) \geq n - 2k > d-1$.
Differentiating with respect to some x_j, we have that

$$\mathsf{Sym}_{-j}^{d-1} - \frac{\partial P}{\partial x_j} = \frac{\partial \mathsf{Sym}_n^d}{\partial x_j} - \frac{\partial P}{\partial x_j} = \sum_{i=1}^{k} \left(Q_i \frac{\partial R_i}{\partial x_j} + \frac{\partial Q_i}{\partial x_j} R_i \right)$$

Since all Q_i and R_i vanish on $\mathbb{V}(S)$, the right hand side does too. Thus

$$\mathbb{V}(S) \subseteq \mathbb{V}\left(\left\{ \mathsf{Sym}_{-j}^{d-1} - \frac{\partial P}{\partial x_j} \text{ for } j \in [n] \right\} \right) = V_1 \text{ (say)}$$

By Lemma 6, $dim(V_1) \geq dim(\mathbb{V}(S)) > d-1$. On the other hand as P is of degree at most $d-1$, its derivatives are of degree at most $d-2$. Hence by Lemma 12 (stated and proved below) we have that $dim(V_1) \leq d-1$, giving us a contradiction. □

Lemma 12. *Let $d > 0$ be a parameter, $g_1, \ldots, g_n \in \mathbb{F}[X]$ be of degree less than $d-1$, and $S = \left\{ \mathsf{Sym}_{-i}^{d-1}(X) - g_i \text{ for } i \in [n] \right\}$. Then $dim(\mathbb{V}(S)) \leq d-1$.*

Proof. Let $V = \mathbb{V}(S)$, and the set S' be the *homogenized version* of S, given by

$$S' = \left\{ \mathsf{Sym}_{-i}^{d-1} - g_i \cdot x_0^{d-1-deg(g_i)} \text{ for } i \in [n] \right\}$$

We think of $\mathbb{V}(S')$ as a projective variety in $\mathbb{P}^n(\mathbb{F})$. By Theorem 7 and Lemma 8, we have that

$$dim(V) \leq dim(\mathbb{V}(S')) \leq dim(\mathbb{V}(S') \cap \mathbb{V}(x_0)) + 1$$

From Lemma 13 (stated and proved below), we have that $dim(\mathbb{V}(S') \cap \mathbb{V}(x_0)) \leq d-2$ giving the desired result.

□

Lemma 13. *Let* $S = \left\{\mathsf{Sym}_{-i}^{d-1}(X) \text{ for } i \in [n]\right\}$ *and* $V = \mathbb{V}(S)$. *Then* $dim(V) \leq d-2$.

Proof. Suppose that $dim(V) > d-2$. Then by Theorem 9, we have that some $[x_{i_1}], \ldots, [x_{i_{d-1}}]$ are algebraically independent over $\mathbb{F}[V]$. By symmetry we can assume these to be $[x_1], \ldots, [x_{d-1}]$. We shall show this is not possible. Consider the following polynomial on $d-1$ variables:

$$p(y_1, \ldots, y_{d-1}) = \Big(\prod_{1 \leq i \leq d-1} y_i\Big)\Big(\prod_{1 \leq i < j \leq d-1} (y_i - y_j)\Big)$$

We know $p([x_1], \ldots, [x_{d-1}]) = [p(x_1, \ldots, x_{d-1})] \neq [0]$ in $\mathbb{F}[V]$. Hence there is a point $\tilde{\mathbf{a}} = (a_1, \ldots, a_n) \in V$ such that $p(a_1, \ldots, a_{d-1}) \neq 0$. For that point we have:
As $p(a_1, \ldots, a_{d-1}) \neq 0$:

$$a_i \neq 0 \text{ for all } i \in [d-1] \tag{1}$$
$$a_i \neq a_j \text{ for all } i, j \in [d-1] \text{ such that } i \neq j \tag{2}$$

As $\tilde{\mathbf{a}} \in V$

$$\mathsf{Sym}_{-i}^{d-1}(\tilde{\mathbf{a}}) = 0 \text{ for all } i \in \{1, \ldots, n\} \tag{3}$$

Assuming (1), (2), (3) we will prove the following claim.

Claim 14. *For any* $0 \leq j \leq d-2$ *and any* $j < i \leq d-1$, *if we evaluate the Elementary Symmetric polynomial on* $n-j-1$ *variables of degree* $d-j-2$, *at* $\tilde{\mathbf{a}}$ *at* $[n] \setminus ([j] \cup \{i\})$ *indices, then it evaluates to* 0.

Before we prove the claim, we will first show that the claim proves Lemma 13. The claim when applied for $j = d-2$, implies that the Elementary Symmetric polynomial on $n-d-3$ variables of degree 0 evaluates to 0. But we know that the degree zero Elementary symmetric polynomial (on any number of variables) by definition is a constant 1 polynomial. This gives us a contradiction. This proving that our initial assumption that $dim(V) > d-2$ is wrong. □

Proof of Claim 14. For ease of notation, we will denote the polynomial $\mathsf{Sym}_{-|([j]\cup\{i\})|}^{d-j-2}(X \setminus ([j] \cup \{i\}))$ by $\mathsf{Sym}_{-[j],-i}^{d-j-2}(X)$ and its value at point $\tilde{\mathbf{a}}$ by $\mathsf{Sym}_{-[j],-i}^{d-j-2}(\tilde{\mathbf{a}})$.
We will prove the claim by induction on j. For the base case, let $j = 0$. Using (3) we get n equations; one for each $i \in [n]$. If we add these n equations, we get that $(n-d+1) \cdot \mathsf{Sym}_{n}^{d-1}(\tilde{\mathbf{a}}) = 0$. This gives us

$$\mathsf{Sym}_{n}^{d-1}(\tilde{\mathbf{a}}) = 0. \tag{4}$$

As $\mathsf{Sym}_{n}^{d-1}(X) - \mathsf{Sym}_{-i}^{d-1}(X) = x_i \cdot \mathsf{Sym}_{-i}^{d-2}(X)$, using (4) and (3), we get that $a_i \cdot \mathsf{Sym}_{-i}^{d-2}(\tilde{\mathbf{a}}) = 0$. Using (1), we obtain

$$\text{For } 0 < i \leq d-1,\ \mathsf{Sym}_{-i}^{d-2}(\tilde{\mathbf{a}}) = 0. \tag{5}$$

This proves the base case.

Now let us consider the inductive case. We get the following using the induction hypothesis.

$$\text{For } j < i \leq d-1,\ \mathsf{Sym}_{-[j],-i}^{d-j-2}(\tilde{\mathbf{a}}) = 0 \tag{6}$$

From the definition of Elementary Symmetric polynomials and by simple arithmetic, we also know the following. For all i such that $j+1 < i \leq d-1$,

$$\begin{aligned} &\mathsf{Sym}^{d-j-2}_{-[j],-i}(X) - \mathsf{Sym}^{d-j-2}_{-[j],-(j+1)}(X) \\ &= (x_{j+1} - x_i) \cdot \mathsf{Sym}^{d-j-3}_{-[j+1],-i}(X) \end{aligned} \tag{7}$$

Now, using (6) we can say that, the right hand side of (7) evaluated at $\tilde{\mathbf{a}}$ must be zero. However from (2) we also know that $a_{j+1} - a_i \neq 0$ for any $j+1 < i \leq d-1$. Hence we get $\mathsf{Sym}^{d-j-3}_{-[j+1],-i}(\tilde{\mathbf{a}}) = 0$, which proves the inductive statement. This finishes the proof of Claim 14. □

3.1 Upper Bound on Homogeneous ABPs

In this section we sketch the construction of a homogeneous ABP computing $\mathsf{Sym}^d_n(X)$. In particular, we prove the following statement.

Lemma 15. *There is an ABP of size* $(n-d+1)(d-1)+2$ *for* $\mathsf{Sym}^d_n(X)$.

Construction of an ABP for $\mathsf{Sym}^d_n(X)$ We construct an ABP with d layers each with n nodes. Between each consecutive layers ℓ and $\ell+1$, where $1 \leq \ell \leq d-1$, there is an edge from node i in layer ℓ to a node j in $(\ell+1)^{\text{th}}$ layer if $i < j$. The weight of this edge is x_j. In the first layer, only the first node is required (and is labelled as s). In the last layer, we can merge all the n nodes into t and adding edge weights appropriately.

The correctness of the construction follows from the fact that any term in $\mathsf{Sym}^d_n(X)$ is uniquely of the form $x_{i_1} \cdot x_{i_2} \ldots x_{i_d}$ where $i_1 < i_2 < \cdots < i_d$. Observe that in any layer j $(1 < j < d+1)$ the nodes $1, 2, \ldots, j-2$ and $n-d+j, \ldots, n$ are redundant. Hence, the total number of nodes in the ABP is $(n-d+1)(d-1)+2$.

Ackowledgements We would like to thank Prasad Chaugule and Srikanth Srinivasan for discussions. The discussions with Srikanth also led to an easy proof of Lemma 12.

References

[CLO07] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3/e (Undergraduate Texts in Mathematics)*. Springer-Verlag, Berlin, Heidelberg, 2007.

[Kum17] Mrinal Kumar. A quadratic lower bound for homogeneous algebraic branching programs. *Electronic Colloquium on Computational Complexity (ECCC)*, 24:28, 2017.