

Computing the Elementary Symmetric Polynomials in Positive Characteristics

Ian Orzel*

Department of Computer Science
University of Copenhagen
Copenhagen, Denmark

February 9, 2026

Abstract

We first extend the results of Chatterjee, Kumar, Shi, Volk (Computational Complexity 2022) by showing that the degree d elementary symmetric polynomials in n variables have formula lower bounds of $\Omega(d(n-d))$ over fields of positive characteristic. Then, we show that the results of the universality of linear projections of elementary symmetric polynomials from Shpilka (Journal of Computer and System Sciences 2002) and of border fan-in two $\Sigma\Pi\Sigma$ circuits from Kumar (ACM Trans. Comput. Theory 2020) over zero characteristic fields do not extend to fields of positive characteristic. In particular, we show that

1. There are polynomials that cannot be represented as linear projections of the elementary symmetric polynomials (in fact, we show linear lower bounds over the size of the sum of such linear projections) and
2. There are polynomials that cannot be computed by border depth-3 circuits of top fan-in k , called $\Sigma^{[k]}\Pi\Sigma$, for $k = o(n)$.

To prove the first result, we consider a geometric property of the elementary symmetric polynomials, namely, the set of all points in which the polynomial and all of its first-order partial derivatives vanish. It was previously shown that the dimension of this space was exactly $d-2$ for fields of zero characteristic. We extend this to fields of positive characteristic by showing that this dimension must be between $d-2$ and $d-1$. In fact, we provide some criterion where it is $d-2$ and others where it is $d-1$.

Then, to consider the border top fan-in of linear projections of the elementary symmetric polynomials and border depth-3 circuits (sometimes called border affine Chow rank), we show that it is sufficient to consider the border top fan-in of the sum of such linear projections of the elementary symmetric polynomials. This is done by an explicit construction of a 'metapolynomial,' meaning that this result also applies in the border setting.

1 Introduction

Given n independent variables x_1, \dots, x_n and a degree $d \leq n$, we define the *elementary symmetric polynomial* of degree d (over an arbitrary field \mathbb{F} of characteristic denoted by $\text{char}(\mathbb{F})$) to be the sum

*Email: iano@di.ku.dk. This work was funded by the European Research Council (ERC) under grant agreement no. 101125652 (ALBA).

of all degree d multilinear monomials, i.e.,

$$e_d^n = \sum_{S \in \binom{[n]}{d}} \prod_{i \in S} x_i.$$

This polynomial naturally appears in many situations; for instance, they show up when considering the product of affine polynomials.

$$\prod_{i=1}^n (x + a_i) = \sum_{k=0}^n x^{n-k} e_k^n(a_1, \dots, a_n). \quad (1)$$

We say that these polynomials are symmetric because they are invariant under permutations of the variables, and we say that they are elementary because they are the basic building blocks of symmetric polynomials; namely, the set of symmetric polynomials can be expressed as $\mathbb{F}[e_0^n, \dots, e_n^n]$. We include more fundamental properties in the appendix, Section A.

Motivation In this paper, we will study the computation of elementary symmetric polynomials through the lens of algebraic complexity theory. We commonly define computation through *algebraic circuits*, which we model using acyclic directed graphs, where certain nodes represent the operations of addition or multiplication and other nodes represent inputs, which are given as independent variables and field constants. We can then restrict this to so-called *algebraic formulas*, which require that the underlying graph be a tree (each node has at most one outgoing edge). We can further restrict the depth of a tree and force layers to alternate in operations, creating, for example, *depth-three $\Sigma\Pi\Sigma$ formulas*, where we force the root node to be an addition node. We may further restrict this model to $\Sigma^{[k]}\Pi\Sigma$ *formulas*, where the root node may only have at most k children.

Elementary symmetric polynomials Elementary symmetric polynomials are very common polynomials that appear naturally in various algebraic complexity problems. These polynomials are relatively easy to compute (they can be computed by $\Sigma\Pi\Sigma$ formulas of size $O(n^2)$), so there is hope they are simple enough that a deep understanding of them is achievable. One recent motivation of them was explored in [LST24] and [FLST24], where the computation of the elementary symmetric polynomials naturally appears from studying constant-depth arithmetic formulas. For example, when considering $\Sigma\Pi\Sigma$ formulas, we could study how to convert these formulas to be homogeneous, where each node computes a homogeneous polynomial. To do this, one idea is to apply (1) to each product gate and then compute each resulting elementary symmetric polynomial using homogeneous circuits (for instance, we could use the upper bound of [SW01] for homogeneous computation of e_d^n by $\Sigma\Pi\Sigma\Pi$ formulas of size $n2^{O(\sqrt{d})}$, but this only works for characteristic zero fields). This idea can be extended to work for deeper constant-depth circuits.

Fields of positive characteristic Specifically, in this paper, we will study such computations over fields of positive characteristic. Recall that the characteristic of a field is the smallest k such that adding one to itself k times gives zero, where we say that characteristic is zero if no such k exists. For a positive prime $p > 1$, the easiest example of a field of characteristic p is the integers modulo p , or $\mathbb{F}_p = \{0, \dots, p-1\}$. Fields of characteristic zero are generally seen as more “natural,” as examples include the real and complex numbers. Specifically, if results require division by natural numbers, they often fail in certain characteristics. For this reason, many results in algebraic complexity theory only work in fields of characteristic zero. This paper is focused on extending some of these results to fields of arbitrary characteristic, but it is also natural to ask why we should study this case.

One simple reasoning follows from the underlying algebraic complexity theory program, whose major goal is to show that VP is not equal to VNP (also known as Valiant’s hypothesis). From [Bü00], we see that it is sufficient to show that VP equals VNP in a field of any characteristic to collapse the polynomial hierarchy. In fact, classical complexity problems are usually posed over alphabets described by $\{0, 1\}$, which can be viewed as a field of characteristic two. It is thus not only interesting to study positive characteristics, but fundamentally, our strategy to approach this problem *should* be independent of the underlying field.

Interestingly, the issue of positive characteristic also shows up in the field of proof complexity, whose focus is on developing lower bounds for the size of “proofs” of logical statements in various proof systems. Specifically, one major proof systems studied is known as the $AC^0[p]$ -Frege proof systems, which are bounded-depth proof systems with MOD_p gates, where a major open problem is to find superpolynomial lower bounds for this system. The theory of proof complexity was brought into the world of algebraic complexity through the introduction of the Ideal Proof System (IPS), which defines its proofs using algebraic circuits. In the influential work [GP18], it was shown that superpolynomial lower bounds for IPS over fields of characteristic $p \neq 0$ give superpolynomial $AC^0[p]$ -Frege lower bounds. They further showed that superpolynomial circuit lower bounds lead to superpolynomial IPS lower bounds, so finding such lower bounds over fields of nonzero characteristic can lead to solving this open problem in proof complexity.

Another field containing interesting applications comes from polynomial identity testing (PIT). We typically define the problem of PIT by, given a polynomial belonging to some class of polynomials in a predefined representation, can you write a *deterministic* algorithm to determine if it is identically the zero polynomial. One major line of research in algebraic complexity is finding polynomial-time PIT algorithms for interesting subclasses of polynomials. In the search of such algorithms, the relationship between lower bounds and PIT algorithms has been uncovered, revealing that lower bounds often lead to PIT algorithms. For instance, in [KI04], it was shown that exponential lower bounds for the permanent would lead to polynomial-time PIT algorithms for polynomial-sized circuits. Unfortunately, if the lower bounds discovered only apply for fields of characteristic zero, then so will the PIT algorithms. If we would like our PIT algorithms to work over any field, we also need our lower bound strategies to work in these cases.

Recently, there has been a theme of extending lower bound results from fields of characteristic zero to fields of positive characteristic. This trend can be seen in papers such as [And20], [DIK⁺24], [For24], [BLRS25], and [BKR⁺25].

Border complexity For some of our results, we will focus on studying the approximate complexity of computing polynomials, known as *border complexity*. To define border complexity, we introduce a new variable ϵ and extend our underlying field \mathbb{F} to the field of fractions $\mathbb{F}(\epsilon)$. Then, instead of requiring our computational model to compute a polynomial f exactly, it must compute some $\epsilon^N f(x) + \epsilon^{N+1} Q(x, \epsilon)$ for some $N \in \mathbb{N}$ and $Q \in \mathbb{F}[x, \epsilon]$. The idea of border complexity is well-studied through the geometric complexity theory program, which hopes to use techniques from algebraic geometry and representation theory to give border complexity lower bounds. Perhaps the most fundamentally interesting reason to study border complexity is that most of our lower bound techniques also work in the world of border complexity, meaning that our techniques do not separate the cases of exact and approximate computation. In spite of this, we know that the border setting can add a lot of power; for example, it was shown in [Kum20] that, in fields of characteristic zero, all polynomials can be approximated by the sum of two (very large) products of affine forms, whereas exact computation can require $\Omega(n)$ lower bounds. Thus, a deeper understanding of the power difference between exact and approximate computation is fundamental to the study of algebraic complexity.

1.1 Results

We have considered computation of the elementary symmetric polynomials using formulas over fields of positive characteristic. By the Ben-Or construction, we know that there is a $\Sigma\Pi\Sigma$ circuit computing e_d^n of size $O(n^2)$ over infinite fields (independent of characteristic). In this paper, we extend the results of [CKSV22] and show that their results on fields of zero characteristic extend to fields of positive characteristic, namely that this upper bound is tight for formulas for certain elementary symmetric polynomials.

Theorem 1.1. *For an arbitrary field, any algebraic formula computing e_d^n has size $\Omega(d(n-d))$.*

In the second part of the paper, we show that the results of [Shp02] and [Kum20] do not extend to fields of positive characteristic. First, we show that the symmetric model is not universal over such fields. In fact, we show something stronger; we show that there are some polynomials that cannot be represented by k -linear combinations of projections of the symmetric model, even if we extend to the border setting.

Theorem 1.2. *If $\text{char}(\mathbb{F}) \neq 0$, then, for every $n \in \mathbb{N}$, there is a homogeneous polynomial $f \in \mathbb{F}[x_1, \dots, x_n]$ of degree d such that, for every linear $L_1^{(1)}, \dots, L_{m_1}^{(1)}, L_1^{(2)}, \dots, L_{m_k}^{(k)} \in \mathbb{F}[x_1, \dots, x_n]$ and constants $c_1, \dots, c_k \in \mathbb{F}$,*

$$f \neq \sum_{i=1}^k c_i e_d^{m_i}(L_1^{(i)}, \dots, L_{m_i}^{(i)}), \quad (2)$$

for $k = o(n)$. Further, this applies in the border setting.

As we have previously mentioned, the symmetric model is intimately related to the models studied in [Kum20], namely the $\overline{\Sigma^{[k]}\Pi\Sigma}$ model. Through this, as an immediate corollary of Theorem 1.2, we show that the results of [Kum20] also do not extend to fields of positive characteristic. In fact, we prove, under such bounds, $\Omega(n)$ lower bounds for the border affine Chow rank of certain polynomials.

Theorem 1.3. *If $\text{char}(\mathbb{F}) \neq 0$, then there exists a polynomial in at most n variables that is not in $\overline{\Sigma^{[k]}\Pi\Sigma}$ for $k = o(n)$.*

1.2 Proof techniques

Proof of Theorem 1.1 We will first focus on proving Theorem 1.1 in Section 2. This proof will largely rely on the proof for the case of characteristic zero from [CKSV22] but with a modification to the step that relies on the field characteristic. Namely, the proof revolves around studying what we will call the set of order-two zeros of a polynomial.

Algebraic complexity theory focuses on using the algebraic properties of polynomials to split them into classes based on how “hard” they are to compute. One such property that has been utilized (see [Gat87], [Kum19], [CKSV22], [KV22], [ABV17]) is what we will call the *order-2 zero space*. Given a polynomial $f \in \mathbb{F}[x_1, \dots, x_n]$, we define its order-2 zero space, denoted $V_2(f)$, to be the points where it vanishes along with its first-order partial derivatives, i.e.,

$$V_2(f) = V\left(f, \frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n}\right) = \left\{a \in \mathbb{F}^n \mid f(a) = \frac{\partial f}{\partial x_1}(a) = \dots = \frac{\partial f}{\partial x_n}(a) = 0\right\}, \quad (3)$$

where $V(f_1, \dots, f_\ell)$ denotes the affine variety defining the zero set of some polynomials f_1, \dots, f_ℓ .

Remark 1.4. *This idea of the order-2 zero space is utilized in [Kum19] and [CKSV22] without a name. Then, in [KV22], it is introduced as the “singular locus” of a polynomial, denoted $\text{sing}(f)$, which is a well-known object in algebraic geometry, in a nod to the notation of [Gat87]. For this paper, we have decided to change this notation, as this definition of singular locus does not precisely align with the algebraic geometric definition. Although it is true that, when f is square-free, this definition exactly characterizes the singular locus ($V_2(f) = \text{sing}(f)$), this is not true in general. This follows from the fact that the singular locus of a polynomial is a property of its corresponding hypersurface, a purely geometric object, while the order-2 zero space is a property of the polynomial, itself. Specifically, if we consider the power polynomial $p_d^n = x_1^d + \dots + x_n^d$, it is well-known that $\text{sing}(p_d^n) = \{0\}$ (see Example 10.21 of [Gat21]), but, if we consider $\text{char}(\mathbb{F}) = q \neq 0$, we trivially observe that $V_2(p_d^n) = V(p_d^n)$. We find that letting this definition differ from its natural geometric definition is confusing, so we have, therefore, decided to change it.*

In many of these recent results, this geometric object appears due to an important lemma that relates its dimension to the size of a product decomposition of the polynomial.

Lemma 1.5 (See Lemma 1.7 of [Kum19] and Lemma 3.4 of [CKSV22]). *Suppose \mathbb{F} is algebraically closed. Let $f \in \mathbb{F}[x_1, \dots, x_n]$ be homogeneous of degree d . If there are constant-free polynomials $f_1, g_1, \dots, f_k, g_k \in \mathbb{F}[x_1, \dots, x_n]$ and a polynomial $h \in \mathbb{F}[x_1, \dots, x_n]$ such that $\deg(h) < d$ and*

$$f = \sum_{i=1}^k f_i g_i + h,$$

then $\dim V_2(f) \geq n - 2k$.

Proof. The proof follows from the following inequality,

$$\dim V_2(f) \geq \dim V_2(f - h) = \dim V_2\left(\sum_{i=1}^k f_i g_i\right) \geq \dim V(f_1, g_1, \dots, f_k, g_k) \geq n - 2k,$$

where the first inequality comes from Lemma 5.8 of [CKSV22] and the last inequality is a basic fact from algebraic geometry. \square

Note 1.6. *Notice that the hypothesis of algebraic closure is necessary for the previous lemma. For example, consider $f = (x_1^2 + \dots + x_n^2)^2$. We notice that $V_2(f) = V(f) = \{0\}$ over \mathbb{R} , but we get a lower bound of $\dim V_2(f) \geq n - 2$ over \mathbb{C} .*

The key observation for the proof in [CKSV22] was that small formulas computed polynomials with “many” order-2 zeros. Then, they prove an upper bound of the dimension of the set of order-2 zeros of the elementary symmetric polynomials and utilize this to show an $\Omega(d(n - d))$ lower bounds on formulas that compute them over fields of zero characteristic (with n being the number of variables and d being the degree). For certain selections of n and d , this bound is tight, as the Ben-Or construction shows an $O(n^2)$ upper bound on the size of $\Sigma\Pi\Sigma$ formulas computing e_d^n . This was known to be tight for $\Sigma\Pi\Sigma$ formulas over fields of characteristic zero from [Shp02].

Tight bound on the order-2 space of the elementary symmetric polynomials It was shown in [MZ17], [LMP19], and [CKSV22] that $\dim V_2(e_d^n) = d - 2$ over fields of characteristic zero, where dimension is, of course, defined in terms of affine varieties. No such equivalent statement was known (to the author’s knowledge) for fields of positive characteristic. In this paper, we show that the dimension is slightly different over such fields; specifically, it can vary between being $d - 2$ or $d - 1$.

Lemma 1.7. For $\text{char}(\mathbb{F}) = p$, we have that $d - 2 \leq \dim V_2(e_d^n) \leq d - 1$. If we have that

- $p \neq 0$,
- $n - d + 1 \equiv 0 \pmod{p^{\lceil \log_p d \rceil}}$, and
- $n \geq 2d - 1$,

then $\dim V_2(e_d^n) = d - 1$. On the other hand, if we have that

- $p = 0$,
- $n - d + 1 \equiv 0 \pmod{p}$, or
- $n < 2d - 1$,

then $\dim V_2(e_d^n) = d - 2$.

Then, for the rest of the proof in [CKSV22] to work, we need only that $\dim V_2(e_d^n) \leq d - 1$, so this lemma suffices for proving the main result.

Interestingly, Lemma 1.7 allows us to also extend the lower bound techniques in [Shp02] used to show that e_d^n require $\Sigma\Pi\Sigma$ formulas of size $\Omega(d(n - d))$ to fields of positive characteristics¹. In [Shp02], they show that, over fields of characteristic zero, for every vector space $V \subseteq \mathbb{F}^n$ such that e_d^n vanishes on V , we have that $\dim(V) < \frac{n+d}{2}$. For fields of positive characteristic, observe that if we combine Proposition 6 from [GGIL22] with Lemma 1.7, we conclude that we have the upper bound of $\dim(V) \leq \frac{n+d-1}{2}$.

Proof of Theorem 1.3 We will now turn our attention to the proof of Theorem 1.2 (and hence Theorem 1.3 by extension), which we prove in Section 3. Consider $\text{char}(\mathbb{F}) = p \neq 0$. From a basic application of (1), we will show that Theorem 1.2 easily implies Theorem 1.3. We then show that a polynomial that can be written in the form given by (2) can be rewritten as

$$f = \sum_{i=1}^{\ell} g_i h_i + \sum_{i=1}^r L_i^d,$$

where g_i, h_i are homogeneous, L_i are linear, d is the degree of f , and $\ell = O(p)$. Then, our goal will be to carefully select a value of f that cannot be written in this form.

We will now give a brief explanation to why it makes sense that such an f exists. Suppose that we select an f that is set-multilinear, meaning that we can split the variables into d groups where each monomial consists of exactly one variable from each group. Then, we can take the set-multilinear part of the right-hand side of the equation, which means, namely, that we can ignore the $\sum_{i=1}^r L_i^d$ part of the expression due to the fact that $(a + b)^p = a^p + b^p$ (assuming that $d \geq p$). Then, we can split each g_i, h_i based on subsets of the set-multilinear groups each monomial falls in, so we can write it as some form of

$$f = \sum_{i=1}^{\ell \cdot 2^d} g'_i h'_i.$$

¹Our results, of course, immediately imply this lower bound, but it is still of interest that we can also extend the results of their main technical lemma

²Using the fact that we can represent a polynomial as a “strength” decomposition of size $\text{codim}(V)$

Then, we clearly have a product decomposition, so we can use Lemma 1.5 to conclude that $\dim V_2(f) \geq n - \ell \cdot 2^{d+1}$. Then, if we select d as a constant, we conclude that $\ell \geq \Omega(n - \dim V_2(f))$. We should observe that this argument only works in the non-border case, and it would require a careful argument to show that it works in the border setting.

While this explanation can provide some intuition behind the claim, the proof does not follow this argument. Instead, we analyze the coefficients of f and construct a polynomial that “witnesses” the condition. Specifically, it is used to show that, if a certain set of multilinear monomials have nonzero coefficients in f , then there must be another multilinear monomial that is nonzero. This approach is preferable to the one described above, as it is then obvious why this applies in the border setting. Recall that a property is called “closed,” meaning it being satisfied in the non-border setting implies that it is satisfied in the border setting, if there is a metapolynomial, meaning a polynomial whose variables are seen as the coefficients of an input polynomial, that evaluates to zero if and only if the input polynomial satisfies the property. It is thus often advantageous to explicitly give such a metapolynomial when showing that a property is closed.

Note 1.8. *In the proofs of some of the theorems, we will sometimes require our field to be algebraically closed. Because the main results from this paper are lower bounds, these results also apply to fields that are not algebraically closed fields, as every field can be extended into one that is algebraically closed.*

1.3 Prior Work

The earliest-known motivation for studying the complexity of the elementary symmetric polynomials came from boolean circuit complexity, where circuits compute boolean functions using a graph labeled with and-gates, or-gates, and not-gates. When considering boolean formulas of constant depth, it was shown in [FSS84] that the majority function had super-polynomial lower bounds, where the majority function is given by $\bigvee_{I \in \binom{[n]}{n/2}} \bigwedge_{i \in I} x_i$. Clearly, $e_{n/2}^n$ looks like an algebraic analogue of the majority function, so it was believed to be a good candidate for a polynomial that would have constant-depth formulas with super-polynomial lower bounds. Unfortunately, due to a construction of Ben-Or (see Theorem 3.1 of [Shp02]), e_d^n was shown to have $\Sigma\Pi\Sigma$ formulas of size $O(n^2)$ (but the problem of super-polynomial $\Sigma\Pi\Sigma$ lower bounds has since been solved, see [LST24]). In [SW01] and [Shp02], it was shown that this upper bound is tight for $\Sigma\Pi\Sigma$ formulas of certain elementary symmetric polynomials over fields of characteristic zero. This was further extended in [CKSV22] to be tight over general algebraic formulas, also over fields of characteristic zero. In the more restrictive model of homogeneous multilinear formulas, where each node computes a homogeneous, multilinear polynomial, [HY11] found super-polynomial lower bounds for certain elementary symmetric polynomials (the result of which is independent of field characteristic).

In [Shp02], the elementary symmetric polynomials were used to define an algebraic computational model, which was called the *symmetric model*. It was defined by taking a series of linear polynomials $L_1, \dots, L_m \in \mathbb{F}[x_1, \dots, x_n]$ and a degree $d \leq m$ and defining the computation by $e_d^m(L_1, \dots, L_m)$. [Shp02] then showed that the symmetric model is universal over fields of characteristic zero, meaning that it can compute any (homogeneous) polynomial. This was done using Fischer’s identity (see [Fis94] and [Shp02]), which tells us that we can write any degree d homogeneous polynomial $f \in \mathbb{F}[x_1, \dots, x_n]$ as $f = L_1^d + \dots + L_m^d$, for some linear polynomials $L_1, \dots, L_m \in \mathbb{F}[x_1, \dots, x_n]$, and it was then shown that polynomials written in this form can be expressed in the symmetric model. We observe that this only works over fields of characteristic zero, as there are many polynomials in positive characteristic that cannot be written in this way, as, for example, $(x + y)^p = x^p + y^p$ when $\text{char}(\mathbb{F}) = p$.

Then, in [Kum20], the results around the symmetric model were used to study the border “affine Chow rank”³ of a polynomial. We say that the *affine Chow rank* of a polynomial $f \in \mathbb{F}[x_1, \dots, x_n]$ is the smallest k such that f can be computed by a $\Sigma^{[k]}\Pi\Sigma$ circuit. We mention that there are polynomials with affine Chow rank that is $\Omega(n)$ over any field (see Lemma 3.2 of [CGJ⁺18]). Recall that, given a complexity measure, we define its border complexity by extending the underlying field to $\mathbb{F}(\epsilon)$, for some new variable ϵ , and, instead of requiring our model to compute $f(x)$, we need only to compute $\epsilon^N f + \epsilon^{N+1} F(x, \epsilon)$ for some $N \geq 0$ and $F \in \mathbb{F}[x, \epsilon]$ (where we may sometimes write that $\epsilon^N \cdot f + \epsilon^{N+1} \cdot F(x, \epsilon) \simeq f$). Through the results of the symmetric model, [Kum20] showed that, over fields of characteristic zero, every homogeneous polynomial has border affine Chow rank of at most two.

2 Order-2 zero space of the elementary symmetric polynomials

In this section, we will focus on extending the results on the formula complexity of the elementary symmetric polynomials from [CKSV22]; we will prove Theorem 1.1 and Lemma 1.7. Specifically, we will show that these results extend when we consider fields of positive characteristic, which we do by analyzing the order-2 zero set of the elementary symmetric polynomials, as this is the only part of the proof that uses the characteristic of the field. Upon careful inspection of [CKSV22], we can state the main result we rely on in the following lemma. For the sake of completeness, we prove this lemma in the appendix in Section B.

Lemma 2.1 ([CKSV22]). *Suppose $f \in \mathbb{F}[x_1, \dots, x_n]$ is a polynomial of degree $d \geq 3$ that can be computed by a formula Φ of size s . Then,*

$$s \geq \frac{d}{6}(n - \dim V_2(f))$$

Then, in [CKSV22], the proof is completed through the following claim.

Claim 2.2 ([MZ17], Lemma 12 of [LMP19], Lemma 5.2 of [CKSV22]). *Let $\text{char}(\mathbb{F}) = 0$. If $d \geq 2$ and $d \leq n$, then $\dim V_2(e_d^n) = d - 2$.*

In particular, we have that $V_2(e_d^n) = \bigcup_{I \in \binom{[n]}{d-2}} \{a \in \mathbb{F}^n \mid \forall i \in I, a_i = 0\}$.

One should notice that a formula complexity lower bound of $\Omega(d(n-d))$ on e_d^n when $\text{char}(\mathbb{F}) = 0$ immediately follows from this. We will spend the rest of this section studying this result over fields of positive characteristic.

One may first ask whether the result from Claim 2.2 can be extended to fields of positive characteristic. From the following example, we can see that this is not the case.

Example 2.3. *Consider the field $\mathbb{F}_2 = \{0, 1\}$ (or even its algebraic closure $\overline{\mathbb{F}_2}$). We consider the set $V_2(e_2^5)$, and we will show that $\{(\alpha, \alpha, \alpha, \alpha, \alpha) \mid \alpha \in \overline{\mathbb{F}_2}\} \subseteq V_2(e_2^5)$, implying that $\dim V_2(e_2^5) \geq 1$. To see this, consider an arbitrary $\alpha \in \overline{\mathbb{F}_2}$, and notice that*

$$e_2^5(\alpha, \alpha, \alpha, \alpha, \alpha) = \binom{5}{2} \alpha^2 = 10\alpha^2 = 0, \quad \frac{\partial e_2^5}{\partial x_i}(\alpha, \alpha, \alpha, \alpha, \alpha) = e_1^4(\alpha, \alpha, \alpha, \alpha) = 4\alpha = 0.$$

³This name was selected based on [Dut25]

Clearly, we cannot hope to get an upper bound of $d-2$ for arbitrary choices of field characteristic, number of variables, and degree. But, if we instead turn our attention to an upper bound of $d-1$, this is possible. Luckily, for the sake of asymptotic bounds, the difference between $d-1$ and $d-2$ is not important.

Before getting to the proof of this result, we believe that it is useful to provide some motivation for where the proof stems from. Specifically, we consider the case of $V_2(e_2^n)$ for some $n \geq 2$. Observe that we can write each $\frac{\partial e_2^n}{\partial x_i}(a) = \sum_{j \neq i} a_j$. Then, for $i \neq j$, $\sum_{k \neq i} a_k - \sum_{k \neq j} a_k = a_i - a_j$. We thus conclude that, if $a \in V_2(e_2^n)$, then $a_1 = \dots = a_n$. As we repeat this strategy for increasing values of d , we observe that $a \in V_2(e_d^n)$ if and only if the indices of a can be partitioned into $d-1$ sets, where all indices in the same set correspond to the same value. We will now formalize this approach.

Lemma 2.4. *Over any field, if $1 \leq d \leq n$, then $\dim V_2(e_d^n) \leq d-1$.*

Proof. We will show that all points in $V_2(e_d^n)$ have at most $d-1$ distinct values in their coordinates. To define this rigorously, we first define vector spaces corresponding to each partition of $[n]$. Recall that, given a set S , we say that $\pi \subseteq 2^{[n]}$ is a partition of S of size k if $|\pi| = k$, $\emptyset \notin \pi$, $\bigcup_{U \in \pi} U = S$, and, for every $U, U' \in \pi$ such that $U \neq U'$, we have that $U \cap U' = \emptyset$. We say that the set of all such π is $\mathcal{P}_k(S)$. Given a partition $\pi \in \mathcal{P}_k([n])$, we define the vector space P_π formed by π to be the set of all points such that, for every pair of indices that are in the same set in the partition, they also always have the same value in the space. Rigorously, we say that

$$P_\pi = \{a \in \mathbb{F}^n \mid \forall S \in \pi, \forall i, j \in S, a_i = a_j\}. \quad (4)$$

Then, we can define the set of all points that can be split into k groups with the same value by

$$S_k = \bigcup_{\pi \in \mathcal{P}_k([n])} P_\pi.$$

We will then show that $V_2(e_d^n) \subseteq S_{d-1}$. From this, the claim immediately follows, as $\dim S_k = k$.

To prove this result, we will inductively prove the following claim.

Claim 2.5. *For $d \geq 0$ and $m > d$, let $\alpha_0, \dots, \alpha_d \in \mathbb{F}$ be such that $\alpha_d = 1$. Then, we have that*

$$\left\{ a \in \mathbb{F}^m \mid \forall i \in [m], \sum_{k=0}^d \alpha_k e_k^{m-1}(x_j \mid j \neq i) = 0 \right\} \subseteq S_d.$$

We can apply the above claim for $d-1$ and set $\alpha_{d-1} = 1$ and $\alpha_{d-2} = \dots = \alpha_0 = 0$ to prove the lemma. We will now focus on proving the claim, which we will do by induction on d . Notice that the case of $d=0$ is obvious, as $\alpha_0 = 1$, so the set is empty. Now, consider the claim for d , using the inductive hypotheses for $d-1$. Let $a = (a_1, \dots, a_m)$ be such that, for every $i \in [m]$, $\sum_{k=0}^d \alpha_k e_k^{m-1}(a_j \mid j \neq i) = 0$. Observe that

$$\begin{aligned} 0 &= \sum_{i=0}^d \alpha_i e_i^{m-1}(a_1, \dots, a_{m-1}) - \sum_{i=0}^d \alpha_i e_i^{m-1}(a_2, \dots, a_m) = \sum_{i=0}^d \alpha_i (e_i^{m-1}(a_1, \dots, a_{m-1}) - e_i^{m-1}(a_2, \dots, a_m)) \\ &= \sum_{i=1}^d \alpha_i (a_1 e_{i-1}^{m-2}(a_2, \dots, a_{m-1}) - a_m e_{i-1}^{m-2}(a_2, \dots, a_{m-1})) = (a_1 - a_m) \sum_{i=1}^d \alpha_i e_{i-1}^{m-2}(a_2, \dots, a_{m-1}). \end{aligned}$$

Hence, we have that either $a_1 = a_m$ or $\sum_{i=1}^d \alpha_i e_{i-1}^{m-2}(a_2, \dots, a_{m-1}) = 0$. Observe that we can easily extend this argument to any pair of indices.

Now, let $I = \{k \in [m-1] \mid a_k = a_m\}$. Without loss of generality, assume that $[m-1] \setminus I = [\ell]$. Observe that if $\ell < d$, then the claim trivially follows, so we assume that $\ell \geq d$. Consider some $k \in [\ell]$, and, using the fact that $a_i = a_m$ for each $i \in I$ and $a_k \neq a_m$, observe that

$$\begin{aligned} 0 &= \sum_{i=0}^{d-1} \alpha_{i+1} e_i^{m-2}(a_j \mid j \in [m-1] \setminus \{k\}) = \sum_{i=0}^{d-1} \alpha_{i+1} \sum_{j=0}^i \binom{|I|}{i-j} a_m^{i-j} e_j^{\ell-1}(a_p \mid p \in [\ell] \setminus \{k\}) \\ &= \sum_{j=0}^{d-1} \left(\sum_{i=j}^{d-1} \alpha_{i+1} \binom{|I|}{i-j} a_m^{i-j} \right) e_j^{\ell-1}(a_p \mid p \in [\ell] \setminus \{k\}) = \sum_{j=0}^{d-1} \alpha'_j e_j^{\ell-1}(x_p \mid p \in [\ell] \setminus \{k\}), \end{aligned}$$

where $\alpha'_i \in \mathbb{F}$. Observe that $\alpha'_{d-1} = \alpha_d \cdot \binom{|I|}{0} = 1$. We then can use the inductive hypothesis to conclude that $(a_1, \dots, a_\ell) \in S_{d-1}$. Because $a_{\ell+1} = \dots = a_m$, we conclude that $a \in S_d$. \square

With the above proof, we have now extended the results of [CKSV22] to fields of positive characteristic. But, it is still independently interesting to get an understanding of how tight this bound is. We have shown a specific example where this lower bound is tight, but it would be nice to generalize this example for different number of variables and field characteristics. We do this in the following proposition.

Proposition 2.6. *Let $\text{char}(\mathbb{F}) = p \neq 0$ and $n, d \geq 1$. If $n - d + 1 \equiv 0 \pmod{p^{\lceil \log_p d \rceil}}$ and $n \geq 2d - 1$, then $\dim V_2(e_d^n) \geq d - 1$.*

Proof. Consider arbitrary $\beta_1, \dots, \beta_{d-1} \in \mathbb{F}$. We will consider the point $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{F}^n$ defined by

$$\alpha_i = \begin{cases} \beta_i & i \leq d-2 \\ \beta_{d-1} & \text{otherwise.} \end{cases}$$

First, observe that

$$e_d^n(\alpha) = \sum_{i=2}^{\min(d, n-d+2)} \binom{n-d+2}{i} e_{d-i}^{d-2}(\beta_1, \dots, \beta_{d-2}) \beta_{d-1}^i.$$

Then, for $k \in [d-2]$, we have that

$$\begin{aligned} \frac{\partial e_d^n}{\partial x_k}(\alpha) &= e_{d-1}^{n-1}(\alpha_1, \dots, \alpha_{k-1}, \alpha_{k+1}, \dots, \alpha_n) \\ &= \sum_{i=2}^{\min(d-1, n-d+2)} \binom{n-d+2}{i} e_{d-1-i}^{d-3}(\beta_1, \dots, \beta_{k-1}, \beta_{k+1}, \dots, \beta_{d-2}) \beta_{d-1}^i. \end{aligned}$$

Further, for $k \in [d-1, n]$, we have that

$$\begin{aligned} \frac{\partial e_d^n}{\partial x_k}(\alpha) &= e_{d-1}^{n-1}(\alpha_1, \dots, \alpha_{k-1}, \alpha_{k+1}, \dots, \alpha_n) \\ &= \sum_{i=1}^{\min(d-1, n-d+1)} \binom{n-d+1}{i} e_{d-1-i}^{d-2}(\beta_1, \dots, \beta_{d-2}) \beta_{d-1}^i. \end{aligned}$$

It is thus sufficient to show that $\binom{n-d+2}{i} \equiv 0 \pmod{p}$ for every $i \in [2, \min(d, n-d+2)]$ and $\binom{n-d+1}{i} \equiv 0 \pmod{p}$ for every $i \in [1, \min(d-1, n-d+1)]$. We will do this using Lucas's Theorem.

Theorem 2.7 (Lucas's Theorem, see [Luc78], [Mes14]). *Let $p \in \mathbb{N}$ be a prime and $a, b \in \mathbb{N}$ be numbers. We then write a and b by their unique base- p expansion, namely, $a = \sum_{i=0}^k a_i \cdot p^i$ and $b = \sum_{i=0}^k b_i \cdot p^i$. Then, we have that*

$$\binom{a}{b} \equiv \prod_{i=0}^{\ell} \binom{a_i}{b_i} \pmod{p},$$

where we say $\binom{a_i}{b_i} = 0$ if $a_i < b_i$.

We will now explain how to apply Lucas's Theorem. Let $N \in \mathbb{N}$ and $a_0, \dots, a_N \in \mathbb{N}$ be such that $n - d + 1 = \sum_{k=0}^N a_k \cdot p^k$. Notice, because $n - d + 1 \equiv 0 \pmod{p^{\lceil \log_p d \rceil}}$, we have that $a_k = 0$ for every $k \in [0, \lceil \log_p d \rceil]$. Now, consider some $i \in [2, d - 1]$, and we will write it as its base p expansion $i = \sum_{k=0}^N b_k \cdot p^k$. By applying Lucas's Theorem, notice that

$$\binom{n - d + 2}{i} = \left(\prod_{k=1}^N \binom{a_k}{b_k} \right) \cdot \binom{1}{b_0} = \left(\prod_{k=\lceil \log_p d \rceil + 1}^N \binom{a_k}{b_k} \right) \left(\prod_{k=1}^{\lceil \log_p d \rceil} \binom{a_k}{b_k} \right) \cdot \binom{1}{b_0}.$$

Because $i \in [2, d - 1]$, either there is a $j \in [2, \lceil \log_p d \rceil]$ such that $b_j > 0$ or $b_0 > 1$. Hence, $\binom{n - d + 2}{i} = 0$.

Then, for the other case, consider $i \in [1, d - 1]$, and, similarly to previous, we write $i = \sum_{k=0}^N b_k \cdot p^k$. Then, by Lucas's Theorem, we have that

$$\binom{n - d + 1}{i} = \left(\prod_{k=0}^N \binom{a_k}{b_k} \right) = \left(\prod_{k=\lceil \log_p d \rceil + 1}^N \binom{a_k}{b_k} \right) \left(\prod_{k=0}^{\lceil \log_p d \rceil} \binom{0}{b_k} \right).$$

Then, because $i < d$, we conclude that there is a $j \in [0, \lceil \log_p d \rceil]$ such that $b_j > 0$, so $\binom{n - d + 1}{i} = 0$. \square

With this in mind, we turn our attention to the following question: can we characterize when the space has dimension $d - 1$ versus when it has dimension $d - 2$. We will not be able to do this, but we will make some progress towards this. First, we would like to adapt the proof for characteristic zero fields to arbitrary fields (with some conditions). Unfortunately, the issue with the original proof is that it relies on $n - d + 1$ not being zero, but it uses an inductive argument that may not preserve the difference between n and d . But it turns out, if we combine this original proof with the result of Lemma 2.4, we can show that $d - 2$ is sometimes tight.

Claim 2.8. *Let $\text{char}(\mathbb{F}) = p$ and $2 \leq d \leq n$. If $p = 0$ or $n - d + 1 \not\equiv 0 \pmod{p}$, then $\dim V_2(e_d^n) = d - 2$.*

Proof. Consider an arbitrary vector space V_I , for some $I \subseteq [n]$, which is defined by points where all coordinates in I are zero, i.e.,

$$V_I = \{a \in \mathbb{F}^n \mid \forall i \in I, a_i = 0\}.$$

Without loss of generality, we will assume that $I = [n - k + 1, n]$. Then, we will show that $V_2(e_d^n) \cap V_I \subseteq V_2(f_d)$, where $f_d = e_{d-1}^{n-k}(x_1, \dots, x_{n-k}) \in \mathbb{F}[x_1, \dots, x_n]$. Then, by Lemma 2.4, we know that $\dim V_2(f_d) = \dim V_2(e_{d-1}^{n-k}) \leq d - 2$. Thus, by taking the union over all V_I , we get the bound we are interested in.

Now, let $a \in V_2(e_d^n)$ be such that $a_1, \dots, a_{n-k} \neq 0$ and $a_{n-k+1} = \dots = a_n = 0$. We can apply (7) and (8) to say

$$0 = \sum_{i=1}^n \frac{\partial e_d^n}{\partial x_i}(a) = n \cdot e_{d-1}^n(a) - \sum_{i=1}^n a_i \frac{\partial e_{d-1}^n}{\partial x_i}(a) = (n - d + 1)e_{d-1}^n(a).$$

Hence, we conclude that $e_{d-1}^n(a) = 0$. We further notice that, by (7), for every $i \in [n]$,

$$e_{d-1}^n(a) = a_i \frac{\partial e_{d-1}^n}{\partial x_i}(a).$$

Thus, we observe that $f_d(a) = e_{d-1}^n(a) = 0$ and, for $i \leq n - k$, we have that $\frac{\partial f_d}{\partial x_i}(a) = \frac{\partial e_{d-1}^n}{\partial x_i}(a) = 0$. Hence, we conclude, by definition, that $(a_1, \dots, a_{n-k}) \in V_2(e_{d-1}^{n-k})$. \square

Interestingly, we can also get a full understanding when the degree is large in comparison to the number of variables.

Claim 2.9. *If $n < 2d - 1$, then we have that $\dim V_2(e_d^n) = d - 2$.*

Proof. Recall that $\mathcal{P}_k([n])$ denotes the set of all partitions of $[n]$ into k groups. We thus know that $V_2(e_d^n) \subseteq \bigcup_{\pi \in \mathcal{P}_{d-1}([n])} P_\pi$ from the proof of Lemma 2.4 (see (4)). Let $V \subseteq V_2(e_d^n)$ be an irreducible component (as $V_2(e_d^n)$ is a variety), and let π be such that $V \subseteq P_\pi$, which we know exists as P_π is a vector space, meaning it is irreducible. Further notice that $\dim P_\pi = d - 1$, so, to show that $\dim V \leq d - 2$, it suffices to show that $V \subsetneq P_\pi$.

Let $\pi = \{S_1, \dots, S_k\}$ and $L_i = |S_i|$ for every $i \in [k]$. Without loss of generality, we assume that $i \in S_i$. Observe that $P_\pi \cong \mathbb{F}^k$ via the isomorphism $\varphi : P_\pi \rightarrow \mathbb{F}^k$ defined by $\varphi(x_1, \dots, x_n) = (x_1, \dots, x_k)$. After applying the morphism to $V_2(e_d^n)$, we see that, in this space, it is defined by the equations

$$e_d^n(P_\pi) = \sum_{\substack{(j_1, \dots, j_k) \in [L_1] \times \dots \times [L_k] \\ j_1 + \dots + j_k = d}} \binom{L_1}{j_1} \dots \binom{L_k}{j_k} x_1^{j_1} \dots x_k^{j_k},$$

and, for $i \in [k]$,

$$\frac{\partial e_d^n}{\partial x_i}(P_\pi) = \sum_{\substack{(j_1, \dots, j_k) \in [L_1] \times \dots \times [L_i-1] \times \dots \times [L_k] \\ j_1 + \dots + j_k = d-1}} \binom{L_1}{j_1} \dots \binom{L_i-1}{j_i} \dots \binom{L_k}{j_k} x_1^{j_1} \dots x_k^{j_k}.$$

To separate V and P_π , it suffices to show that one of these polynomials is not identically zero. Our strategy will be to find $\ell_1, \dots, \ell_c \in [k]$ such that $L_{\ell_1} + \dots + L_{\ell_c} \in \{d - 1, d\}$. Without loss of generality, we say that $\ell_i = i$ for every $i \in [c]$. Notice that, if we can find such sets, then the coefficient of $x_1^{L_1} \dots x_c^{L_c}$ in at least one of these polynomials is one.

It now suffices to show that such a selection exists. We will describe a simple algorithmic selection procedure. The idea is to greedily grab the biggest set iteratively that does not cause the sum of the set sizes we have taken to be larger than d . We then must only argue that this procedure will always end with the sum being $d - 1$ or d . To see this, notice that, because d is close to n , there should be a lot of sets of size one. Hence, from this strategy, the proof follows from the following claim.

Claim 2.10. *Let N be the number of sets of size exactly one. Then, for each S_i , we have that $N \geq L_i - 2$.*

Proof. By assumption, we know that $n \leq 2d - 2$. Further, because all of the other sets are of size at least two, we conclude that $N + 2(d - 1 - N) + L_i \leq n$. Thus, it follows that $2d - 2 \geq 2d - N + L_i - 4$. Hence, we have that $N \geq L_i - 2$. \square

Thus, we can guarantee that there is enough 1's to get to $d - 1$. \square

Observe that this does not characterize when the answer is $d - 1$ versus $d - 2$. Specifically, we do not know what happens when $p \neq 0$, $n \geq 2d - 1$, and $n - d + 1 \equiv 0 \pmod{p}$, but $n - d + 1 \not\equiv 0 \pmod{p^{\lceil \log_p d \rceil}}$. Based on the behavior in smaller cases, we propose the following characterization.

Conjecture 2.11. *Given $1 \leq d \leq n$ and $\text{char}(\mathbb{F}) = p$, we have that $\dim V_2(e_d^n) = d - 1$ if and only if*

- $p \neq 0$,
- $n \geq 2d - 1$, and
- $n - d + 1 \equiv 0 \pmod{p^{\lceil \log_p d \rceil}}$.

Otherwise, $\dim V_2(e_d^n) = d - 2$.

3 The Symmetric Model

In this section, we will study a computational model defined from the elementary symmetric polynomials. Specifically, we will define Sym to represent the set of homogeneous polynomials of some degree, say d , that can be written as $e_d^m(L_1, \dots, L_m)$ for some linear (homogeneous) polynomials L_1, \dots, L_m . We will then say that $\Sigma^{[k]}\text{Sym}$ are all polynomials that can be written as a linear combination of k elements of Sym . We will use $\overline{\text{Sym}}$ and $\overline{\Sigma^{[k]}\text{Sym}}$ to denote the border versions of these classes. Later in the section, we will prove Theorem 3.9, meaning the fact that some polynomials cannot be computed by $\overline{\Sigma^{[k]}\text{Sym}}$ implies that they cannot be computed by $\overline{\Sigma^{[k]}\Pi\Sigma}$ circuits.

This model of computation was introduced and studied in [Shp02], where it was shown that, in fields of characteristic zero, every polynomial can be computed by Sym . This result used the fact that, under such conditions, every polynomial has finite Waring rank (the smallest k such that a polynomial can be written as $L_1^d + \dots + L_k^d$, for linear L_i). This was proved in Lemma 2.4 of [Shp02], but we provide here a slight variation of this lemma, which is slightly stronger and uses a slightly different method.

Lemma 3.1. *Assume that \mathbb{F} is algebraically closed (or simply that $z^d + 1$ is fully reducible in \mathbb{F}). If $f \in \mathbb{F}[x_1, \dots, x_n]$ is a degree d homogeneous polynomial that is in Sym and $q \in \mathbb{F}[x_1, \dots, x_n]$ is linear, then $f + q^d$ is in Sym . This is also true in the border setting.*

Proof. Let $\omega_1, \dots, \omega_d \in \mathbb{F}$ be all of the solutions to $z^d + 1 = 0$ (counted with multiplicities). Then, we know that $e_d^d(-\omega_1, \dots, -\omega_d) = 1$ and $e_k^d(-\omega_1, \dots, -\omega_d) = 0$ for every $k \in [d - 1]$, as

$$z^d + 1 = \prod_{i=1}^d (z - \omega_i) = \sum_{k=0}^d z^{d-k} e_k^d(-\omega_1, \dots, -\omega_d).$$

Now, let $L_1, \dots, L_m \in \mathbb{F}[x_1, \dots, x_n]$ be linear such that $e_d^m(L_1, \dots, L_m) = f$. Then, observe that, using (6),

$$e_d^{m+d}(L_1, \dots, L_m, -\omega_1 q, \dots, -\omega_d q) = \sum_{i=0}^d e_i^m(L_1, \dots, L_m) e_{d-i}^d(-\omega_1 q, \dots, -\omega_d q) = f + q^d.$$

We finally note that this also works in the border setting if we let L_1, \dots, L_m be border polynomials approximating f . \square

Unfortunately, the Waring rank model is known to be not universal in positive characteristic. If $\text{char}(\mathbb{F}) = p \neq 0$, then we observe that, for every $d \geq p$, monomials in L^d , where $L \in \mathbb{F}[x_1, \dots, x_n]$ is linear, must be divisible by some x_i^p . For example, we cannot represent multilinear polynomials using this model. In this section, we will build on this fact to show that $\overline{\text{Sym}}$ and $\overline{\Sigma^{[k]}\text{Sym}}$ are not universal. Specifically, we will show that polynomials in these classes can be expressed as the sum of a small number of reducible polynomials and an arbitrary number of powers of linear forms. Then, if we consider the computation of a multilinear polynomial, we can ignore these linear powers and only consider the reducible polynomials.

We will spend this section proving Theorem 1.2. Then, Theorem 1.3 will follow from Theorem 3.9. To begin with, we will restrict our attention to fields of characteristic two, as this will make the proofs simpler. We will then extend them to higher field characteristics.

3.1 The case of characteristic two

For this section, we assume that $\text{char}(\mathbb{F}) = 2$. Before we can show that there is a polynomial that cannot be computed by Sym , we must identify one such polynomial. We observe that the polynomial x_1x_2 has infinite Waring rank over fields of characteristic two, so one may hope that this polynomial (or a similar one) could be a good candidate. Unfortunately, our first discovery is that all polynomials of degree two can be computed in Sym .

Claim 3.2. *For every degree two homogeneous polynomial $f \in \mathbb{F}[x_1, \dots, x_n]$, there are linear $L_1, \dots, L_m \in \mathbb{F}[x_1, \dots, x_n]$ such that $e_2^m(L_1, \dots, L_m) = f$ and $e_1^m(L_1, \dots, L_m) = 0$.*

Proof. Without loss of generality, we assume that $f = \sum_{i=1}^n x_i y_i$ (we can then make any polynomial through a change of variables). Let $\omega \in \mathbb{F}$ be the 3rd order primitive root of unity. Then, observe

$$e_2^3(\omega x + \omega^2 y, \omega^2 x + \omega y, x + y) = xy, \quad e_1^3(\omega x + \omega^2 y, \omega^2 x + \omega y, x + y) = 0.$$

Hence, $e_2^{3n}(\omega x_1 + \omega^2 y_1, \omega^2 x_1 + \omega y_1, x_1 + y_1, \dots, \omega x_n + \omega^2 y_n, \omega^2 x_n + \omega y_n, x_n + y_n) = \sum_{i=1}^n x_i y_i$ and $e_1^{3n}(\omega x_1 + \omega^2 y_1, \omega^2 x_1 + \omega y_1, x_1 + y_1, \dots, \omega x_n + \omega^2 y_n, \omega^2 x_n + \omega y_n, x_n + y_n) = 0$. \square

We thusly turn our attention to polynomials of degree three. Our key observation is that, by Lemma 3.1, we can compute linear powers “for free.” We then further observe that it is very easy to compute reducible polynomials. Finally, with a trivial application of Newton’s identities, we observe that this condition is not only sufficient but also necessary.

Claim 3.3. *For every degree three homogeneous polynomial $f \in \mathbb{F}[x_1, \dots, x_n]$, f is in Sym if and only if there is a reducible homogeneous degree three polynomial $g \in \mathbb{F}[x_1, \dots, x_n]$ and linear $q_1, \dots, q_k \in \mathbb{F}[x_1, \dots, x_n]$ such that*

$$f = g + q_1^3 + \dots + q_k^3.$$

Proof. First, suppose that f is in Sym . Let $L_1, \dots, L_m \in \mathbb{F}[x_1, \dots, x_n]$ be linear such that $e_3^m(L_1, \dots, L_m) = f$. Then, by the Newton identities (9) and the fact that $p_2^m = (e_1^m)^2$, we observe that

$$\begin{aligned} f &= e_2^m(L_1, \dots, L_m)p_1^m(L_1, \dots, L_m) + e_1^m(L_1, \dots, L_m)p_2^m(L_1, \dots, L_m) + p_3^m(L_1, \dots, L_m) \\ &= e_2^m(L_1, \dots, L_m)e_1^m(L_1, \dots, L_m) + (e_1^m(L_1, \dots, L_m))^3 + L_1^3 + \dots + L_m^3. \end{aligned}$$

For the other direction, let g be a reducible homogeneous degree three polynomial and q_1, \dots, q_k be linear. Let g_1 be homogeneous degree two and g_2 be linear such that $g = g_1g_2$. By Claim 3.2, let

$L_1, \dots, L_m \in \mathbb{F}[x_1, \dots, x_n]$ be linear such that $g_1 = e_2^m(L_1, \dots, L_m)$ and $0 = e_1^m(L_1, \dots, L_m)$. Then, observe that

$$\begin{aligned} e_3^m(L_1, \dots, L_m, g_2) &= e_2^m(L_1, \dots, L_m, g_2)e_1^m(L_1, \dots, L_m, g_2) + [e_1^m(L_1, \dots, L_m, g_2)]^3 \\ &\quad + L_1^3 + \dots + L_m^3 + g_2^3 \\ &= g_1g_2 + (e_1^m(L_1, \dots, L_m, g_2))^3 + L_1^3 + \dots + L_m^3 + g_2^3. \end{aligned}$$

Then, the proof is completed by Lemma 3.1. \square

As a simple corollary to this claim, we can characterize the elements of $\Sigma^{[k]}\text{Sym}$.

Corollary 3.4. *For every degree three homogeneous polynomial $f \in \mathbb{F}[x_1, \dots, x_n]$, f is in $\Sigma^{[k]}\text{Sym}$ if and only if there are reducible homogeneous degree three polynomials $g_1, \dots, g_k \in \mathbb{F}[x_1, \dots, x_n]$ and linear $q_1, \dots, q_\ell \in \mathbb{F}[x_1, \dots, x_n]$ such that*

$$f = g_1 + \dots + g_k + q_1^3 + \dots + q_\ell^3.$$

Utilizing this characterization, we will now focus on constructing a polynomial that cannot be computed under this model of computation. We will focus our attention on multilinear polynomials, as, as we have previously described, they cannot be computed by cubes of linear forms in characteristic two. In fact, cubes of linear forms cannot contain any multilinear monomials, so we can ignore this part of the representation. Hence, it will suffice to find a polynomial that cannot be written as the multilinear part of a reducible polynomial. Specifically, we will focus on the polynomial $x_1y_1z_1 + x_2y_2z_2$.

The argument will follow by showing that, if the multilinear part of a reducible polynomial has nonzero coefficients of $x_1y_1z_1$ and $x_2y_2z_2$, there must be another multilinear monomial with a nonzero coefficient. We will do this by constructing a 'metapolynomial' in the coefficients of a linear and quadratic polynomial that relates the coefficients of the multilinear monomials in their product. Then, the fact that this also works in the border case will follow from the polynomial identity.

Claim 3.5. *The polynomial $f = x_1y_1z_1 + x_2y_2z_2 \in \mathbb{F}[x_1, \dots, x_6]$ is not in Sym . This is also true in the border setting.*

Proof. For simplicity, we will write $f = x_1x_2x_3 + x_4x_5x_6$. Suppose that f is in Sym . Let g be a reducible homogeneous degree three polynomial and q_1, \dots, q_k be linear such that $f = g + q_1^3 + \dots + q_k^3$. First, we observe that all monomials in $q_1^3 + \dots + q_k^3$ are not multilinear. Thus, the coefficients of the multilinear monomials in f are given by g .

We will denote the coefficient of an arbitrary multilinear monomial $(x_i x_j x_k)$ of g (and hence f) by c_{ijk} . Because g is reducible, we will split it into a linear part, denoted g_1 , and a quadratic part, denoted g_2 , given by

$$g_1 = \sum_{i=1}^6 a_i x_i, \quad g_2 = \sum_{i=1}^6 \sum_{j=i}^6 b_{ij} x_i x_j,$$

where $g = g_1g_2$. Notice that the multilinear coefficients are given by $c_{ijk} = a_i b_{jk} + a_j b_{ik} + a_k b_{ij}$.

Our goal will be to use the fact that $c_{123} \neq 0$ and $c_{456} \neq 0$ (meaning that $c_{123}c_{456} \neq 0$) to show that some other $c_{ijk} \neq 0$, a contradiction. We will consider these c_{ijk} values as polynomials in the coefficients of g_1 and g_2 .

Notice that there must be a coefficient (in terms of the a 's and b 's) within $c_{123}c_{456}$ that is non-zero, say $a_1 b_{23} a_4 b_{56}$, for example. This monomial also has a nonzero coefficient in $c_{234}c_{156}$ (which corresponds to a different variable partition). In fact, if we consider all possible partitioning of

the variables, this is the only other partition that has this coefficient nonzero. Our strategy will then be to take combinations of these pairs formed from partitions, which will form a 'metapolynomial' in the coefficient of f that vanishes, meaning that the result will also work in the border setting.

We will state this more formally to show that this indeed happens. Let $\mathcal{P}_3[6]$ represent all of the ways to partition $[6]$ into two sets of size three.⁴ Then, we will show that

$$\sum_{\mathcal{I} \in \mathcal{P}_3[6]} \prod_{\{i,j,k\} \in \mathcal{I}} c_{ijk} \equiv 0 \pmod{2}. \quad (5)$$

Observe that this equality proves the claim, as $c_{123} = c_{456} = 1$, implying that there is another partition $\{i, j, k\}, \{i', j', k'\}$ such that $c_{ijk}c_{i'j'k'} \neq 0$, which is a contradiction. We further observe that this argument works in the border setting.

We now prove the equality. Consider (5) as a polynomial in the indeterminants given by a_i and b_{jk} . Observe that the monomials in this equation can be written in the form $a_i b_{jk} a_{i'} b_{j'k'}$, where $\{i, j, k, i', j', k'\} = [6]$. But this monomial can only be generated by two partitions, $\{\{i, j, k\}, \{i', j', k'\}\}$ and $\{\{i', j, k\}, \{i, j', k'\}\}$, where the corresponding coefficient is one. This lets us conclude that

$$\sum_{\mathcal{I} \in \mathcal{P}_3[6]} \prod_{\{i,j,k\} \in \mathcal{I}} c_{ijk} = 2 \sum_{\{i,i'\} \subseteq [6]} \sum_{\{\{j,k\}, \{j',k'\}\} \in \mathcal{P}_2([6] \setminus \{i,i'\})} a_i a_{i'} b_{jk} b_{j'k'}. \quad \square$$

With a bit of carefulness, we can extend this argument to $\Sigma^{[k]} \text{Sym}$. We will use a similar polynomial for our counterexample, but we will add more monomials of the form $x_i y_i z_i$. We will then use the same identity as the previous case, but we will instead take a sum over partitions of the 3ℓ variables into groups of three. We can now consider this as a polynomial in the coefficients of the decompositions of the reducible polynomials. Now, each monomial can be split up into ℓ parts based on the reducible polynomial the variable comes from. Then, we can permute the corresponding linear parts, as we did in the previous part, for those that came from the same equation, and we conclude that the number of partitions that generate this monomial is given by the product of factorials of the corresponding size of the groups. Thus, if ℓ is big enough, one of these sizes must be at least two, and we conclude that the whole equation is zero.

Claim 3.6. *The polynomial $f = \sum_{i=1}^{\ell} x_i y_i z_i$ is not in $\Sigma^{[k]} \text{Sym}$ for $k \leq \ell - 1$. This is also true in the border setting.*

Proof. For simplicity of proof, we will write $f = \sum_{i=1}^{\ell} x_{3i-2} x_{3i-1} x_{3i} \in \mathbb{F}[x_1, \dots, x_n]$ (with $n = 3\ell$). Let $k \leq \ell - 1$, and suppose that f is in $\Sigma^{[k]} \text{Sym}$. Let g_1, \dots, g_k be reducible degree 3 homogeneous polynomials and q_1, \dots, q_m be linear such that $f = g_1 + \dots + g_k + q_1^3 + \dots + q_m^3$. For each g_t , let g'_t be linear and g''_t be homogeneous degree two such that $g_t = g'_t g''_t$. We will write

$$g'_t = \sum_{i=1}^n a_i^{(t)} x_i, \quad g''_t = \sum_{i=1}^n \sum_{j=i}^n b_{ij}^{(t)} x_i x_j.$$

We again notice that we can ignore the monomials in $q_1^3 + \dots + q_m^3$.

In $g_1 + \dots + g_k$, the coefficient of $x_i x_j x_r$ is given by

$$\sum_{t=1}^k a_i^{(t)} b_{jr}^{(t)} + a_j^{(t)} b_{ir}^{(t)} + a_r^{(t)} b_{ij}^{(t)},$$

⁴Note that the notation for partitions is slightly different from the notation used in previous sections.

which we will write as c_{ijr} . Then, we claim that, setting $\mathcal{P}_3[n]$ to be the set of all ways to partition n into sets of size three,

$$\sum_{\mathcal{I} \in \mathcal{P}_3[n]} \prod_{\{i,j,r\} \in \mathcal{I}} c_{ijr} \equiv 0 \pmod{2}.$$

To see this, consider one of the monomials formed by this formula, which can be written as $a_{i_1}^{(t_1)} b_{j_1 k_1}^{(t_1)} \dots a_{i_\ell}^{(t_\ell)} b_{j_\ell k_\ell}^{(t_\ell)}$, where $\{i_1, j_1, k_1, \dots, i_\ell, j_\ell, k_\ell\} = [n]$ and $t_1, \dots, t_\ell \in [k]$. The partitions that feature these monomials are exactly characterized by permutations of the $a_i^{(t)}$ with the same value for t . Thus, let n_i be the number of t_j values such that $t_j = i$. Then, the coefficient of this monomial is $n_1! \dots n_k!$. Because $\ell \geq k + 1$, there is at least one $n_i \geq 2$. Thus, this coefficient is zero modulus two.

Finally, we observe that this implies that there is another monomial that is non-zero and that this works in the border setting for the same reasons as in the proof of Claim 3.5. \square

3.2 Higher characteristics

In this section, we will extend our previous arguments from fields of characteristic two to fields of arbitrary, positive characteristic. To begin with, we will extend Claim 3.3 to the case of arbitrary positive field characteristic.

Claim 3.7. *Let $\text{char}(\mathbb{F}) = p \neq 0$. If $f \in \mathbb{F}[x_1, \dots, x_n]$ is homogeneous degree $p + 1$ and is in Sym , then there are reducible homogeneous degree $p + 1$ polynomials $g_1, \dots, g_{p-1} \in \mathbb{F}[x_1, \dots, x_n]$ and linear $q_1, \dots, q_\ell \in \mathbb{F}[x_1, \dots, x_n]$ such that*

$$f = g_1 + \dots + g_{p-1} + q_1^{p+1} + \dots + q_\ell^{p+1}.$$

Proof. Let $L_1, \dots, L_m \in \mathbb{F}[x_1, \dots, x_n]$ be such that $e_{p+1}^m(L_1, \dots, L_m) = f$. Then, by the Newton identities, we have that

$$\begin{aligned} f &= \sum_{i=1}^{p+1} (-1)^{i-1} e_{p+1-i}^m(L_1, \dots, L_m) p_i^m(L_1, \dots, L_m) \\ &= \sum_{i=2}^p (-1)^{i-1} e_{p+1-i}^m(L_1, \dots, L_m) p_i^m(L_1, \dots, L_m) + (e_1^m(L_1, \dots, L_m))^{p+1} + L_1^{p+1} + \dots + L_m^{p+1} \square \end{aligned}$$

Notice that this claim is not as strong as the claim for characteristic two. Currently, it is not known how to extend it, but only one direction is necessary for the rest of the proofs. The biggest part of the problem is that it is not clear how to extend Claim 3.2 to this case, even if the field characteristic is just three.

We will now focus on extending Claim 3.6 to fields of positive characteristic. The main difference for the proof in this case is that it is not necessarily true that each reducible polynomial has a linear factor. But, instead of choosing the linear factor for permutations, we can fix one of the two polynomials to use. Then, the proof will follow similarly.

Claim 3.8. *Let $\text{char}(\mathbb{F}) = p \neq 0$. The polynomial*

$$f = \sum_{i=1}^{\ell} \prod_{j=(p+1)(i-1)+1}^{(p+1)i} x_j \in \mathbb{F}[x_1, \dots, x_n]$$

is not in $\Sigma^{[k]} \text{Sym}$ for $\ell > k \cdot (p - 1)$. Further, this is true in the border setting.

Proof. Assume that $\ell > k \cdot (p - 1)$ and let $g_1, \dots, g_m \in \mathbb{F}[x_1, \dots, x_n]$ be reducible homogeneous degree $p + 1$ polynomials and $q_1, \dots, q_N \in \mathbb{F}[x_1, \dots, x_n]$ be linear polynomials such that

$$f = g_1 + \dots + g_k + q_1^{p+1} + \dots + q_N^{p+1}.$$

We will consider splitting each g_i into the product of two polynomials. For each $i \in [k]$, let d_i be the lower of the degrees of the polynomials that we split g_i into. Hence, letting $S_d \subseteq \mathbb{Z}_{\geq 0}^n$ be the set of n -tuples summing to d , we can write g_i as

$$g_i = \left(\sum_{\alpha \in S_{d_i}} a_{\alpha}^{(i)} x^{\alpha} \right) \left(\sum_{\alpha \in S_{p+1-d_i}} b_{\alpha}^{(i)} x^{\alpha} \right).$$

Consider a fixed monomial $x_{i_1} \dots x_{i_{p+1}}$, and let $M = \{i_1, \dots, i_{p+1}\}$. Observe that the coefficient of this monomial is not influenced by the term $q_1^{p+1} + \dots + q_N^{p+1}$, so we will ignore these terms. We will abuse notation and sometimes write, given a subset $S \subseteq [n]$, $a_S^{(i)}$ or $b_S^{(i)}$ to represent the coefficient corresponding to the multilinear monomial given by the set S . Thus, we have that the coefficient of this monomial in f is given by

$$\sum_{i=1}^k \sum_{S \in \binom{M}{d_i}} a_S^{(i)} b_{M \setminus S}^{(i)},$$

which we will denote by c_M .

Assume that $\ell > k \cdot (p - 1)$ for the sake of reaching a contradiction. We will now show that

$$F = \sum_{\mathcal{I} \in \mathcal{P}_{p+1}[n]} \prod_{I \in \mathcal{I}} c_I \equiv 0 \pmod{p},$$

where $\mathcal{P}_{p+1}[n]$ denotes the set of all ways to partition $[n]$ into groups of size $p + 1$. Once we show this, the proof is clearly complete.

We will fix a monomial in F . Observe that it can be written as $a_{S_1}^{(j_1)} b_{S_1'}^{(j_1)} \dots a_{S_{\ell}}^{(j_{\ell})} b_{S_{\ell}'}^{(j_{\ell})}$, where $S_1 \cup S_1' \cup \dots \cup S_{\ell} \cup S_{\ell}' = [n]$ and $t_1, \dots, t_{\ell} \in [k]$. Notice that the coefficient of this monomial is equal to the number of choices of $\mathcal{I} \in \mathcal{P}_{p+1}[n]$ that could generate it. In fact, a choice of \mathcal{I} is a valid selection if and only if there is a bijection $\pi : [\ell] \rightarrow [\ell]$ such that each $S \in \mathcal{I}$ can be written as $S_i \cup S_{\pi(i)}$ for some $i \in \ell$ and we have that $t_j = t_{\pi(j)}$ for all $j \in [\ell]$. For $i \in [k]$, let n_i be the number of t_j values such that $t_j = i$. Notice that $n_1 + \dots + n_k = \ell$. Then, the number of such selections of bijections is exactly equal to $n_1! \dots n_k!$. Because $\ell > k \cdot (p - 1)$, there is a $i \in [k]$ such that $n_i \geq p$. Thus, we have shown that the coefficient of this monomial is zero modulus p . This then completes the proof by the same argument as the proof of Claim 3.5. \square

3.3 Border Depth-Three Formulas

Now, in this section, we will connect the border symmetric computational model to $\overline{\Sigma^{[k]}\Pi\Sigma}$ formulas. In [Kum20], the main result came from observing we could convert a slightly restrictive extension of the border symmetric model to $\overline{\Sigma^{[2]}\Pi\Sigma}$ formulas. Specifically, for a given homogeneous degree d $f \in \mathbb{F}[x_1, \dots, x_n]$ such that there are linear $L_1, \dots, L_m \in \mathbb{F}(\epsilon)[x_1, \dots, x_n]$ where $e_d^m(L_1, \dots, L_m) \simeq f^5$

⁵Meaning that it approximates in the border setting

and $e_k^m(L_1, \dots, L_m) = 0$ for every $k < d$, then we can write f as a $\overline{\Sigma^{[2]}\Pi\Sigma}$ formula, using (1),

$$\prod_{i=1}^n (1 + \epsilon \cdot L_i) - 1 = \epsilon^d \cdot e_d^n(L_1, \dots, L_m) + \epsilon^{d+1} \sum_{i=d+1}^n \epsilon^{i-d-1} e_i^n(L_1, \dots, L_m).$$

In this section, we will analyze the opposite relationship; namely, if we know a polynomial can be computed by a $\overline{\Sigma^{[k]}\Pi\Sigma}$ circuit, can we say anything about its computability in the symmetric model? We then conclude that the $\overline{\Sigma^{[k]}\Pi\Sigma}$ model is weaker than sums of the border symmetric model.

Theorem 3.9. *If $f \in \mathbb{F}[x_1, \dots, x_n]$ is homogeneous degree d and can be represented using $\overline{\Sigma^{[k]}\Pi\Sigma}$, then we can represent f by $\overline{\Sigma^{[k]}\text{Sym}}$.*

To prove this, let $f_1^{(1)}, \dots, f_{m_k}^{(k)} \in \mathbb{F}(\epsilon)[x_1, \dots, x_n]$ be affine and $c_1, \dots, c_k \in \mathbb{F}(\epsilon)$ be such that $f \simeq \sum_{i=1}^k c_i \prod_{j=1}^{m_i} f_j^{(i)}$. We claim that, if each $f_j^{(i)}$ is not constant-free, then the result is obvious. Notice that, in this case, we can assume that each $f_j^{(i)}(0) = 1$ by dividing out each affine functions constant term. Then, observe that

$$f = H_d[f] \simeq H_d \left[\sum_{i=1}^k c_i \prod_{j=1}^{m_i} f_j^{(i)} \right] = \sum_{i=1}^k c_i \cdot H_d \left[\prod_{j=1}^{m_i} f_j^{(i)} \right] = \sum_{i=1}^k c_i \cdot e_d^{m_i}(f_1^{(i)}, \dots, f_{m_i}^{(i)}).$$

Now, we only need to consider what happens if there is some $f_j^{(i)}$ such that $f_j^{(i)}(0) = 0$. We will show that we can modify this polynomial to make it have a constant part without changing the polynomial we approximate. The proof is then completed from the following lemma.

Lemma 3.10. *Let $F, G, \ell \in \mathbb{F}(\epsilon)[x_1, \dots, x_n]$ be such that ℓ is linear (and hence constant-free). Then, there is an $\alpha \in \mathbb{F}(\epsilon)$ such that, if $F \cdot \ell + G \simeq f$ for $f \in \mathbb{F}[x_1, \dots, x_n]$, then $F \cdot (\ell + \alpha) + G \simeq f$.*

Proof. To prove this, imagine that α is a new independent variable. Then, consider $F \cdot (\ell + \alpha) + G$ as a polynomial over x_1, \dots, x_n, α . Notice that the coefficients of monomials in x_1, \dots, x_n are in $\mathbb{F}(\epsilon)[\alpha]$. Then, observe that there are only a finite number of coefficients in monomials that include α . Therefore, it is obvious that we can select α to make all of these coefficients polynomials (multiplying the denominators) and, by multiplying this α value by ϵ^N (for some large enough N), we ensure that this does not change the approximation. \square

This completes the proof of Theorem 1.1.

4 Future Directions

We end by pondering some open problems.

- When considering Theorem 1.2, we, motivated by [Shp02], analyzed projections of the elementary symmetric polynomials by linear functions⁶. It would be natural to relax this model to allow projections of affine functions. Of course, we can easily homogenize this case by introducing a new independent variable x_0 , so this case can be considered as an extension of the case with linear inputs. We then, unfortunately, face the issue that this homogenization could increase the degree of the polynomial, which is a problem for our results, as they only work with degrees equal to $\text{char}(\mathbb{F}) + 1$. Can we extend our characterizations to work for polynomials of arbitrary degrees?

⁶This is done in their case as linear functions are sufficient to make the model universal

- Recall that the border affine Chow rank of a polynomial f is given by the smallest k such that f can be computed by $\Sigma^{[k]}\Pi\Sigma$. When the characteristic is zero, it is known that this value is at most two, but we have now shown that these results do not extend to positive characteristics (we get lower bounds linear in the number of variables). It would be an interesting line of research to study what sorts of upper bounds we can find when the characteristic is positive.
- To prove Theorem 1.2 in the case of $\text{char}(\mathbb{F}) = 2$, we use Corollary 3.4, which provides a necessary and sufficient condition for being computable by $\Sigma^{[k]}\text{Sym}$. For fields such that $\text{char}(\mathbb{F}) > 2$, we are only able to provide a necessary condition. Is this condition also sufficient for these other fields?
- If we further consider the necessary and sufficient condition given in Corollary 3.4, we can naturally ask if this condition is easily “computable.” In a sense, if provided a degree three polynomial, could we determine in polynomial time if it can be represented in the $\Sigma^{[k]}\text{Sym}$ model?

Acknowledgements

Thank you to my advisor Srikanth Srinivasan for encouraging and helping me throughout this entire line of research and steering me in the right directions through regular chats. A lot of the ideas in this paper came from our long discussions. Also, thank you for helping during the process of writing this paper, where your extensive knowledge of the field was paramount. Further, thank you to Theo Fabris for being involved in some of these aforementioned discussions.

References

- [ABV17] Jarod Alper, Tristram Bogart, and Mauricio Velasco. A Lower Bound for the Determinantal Complexity of a Hypersurface. *Foundations of Computational Mathematics*, 17(3):829–836, June 2017. doi:10.1007/s10208-015-9300-x.
- [And20] Robert Andrews. Algebraic Hardness Versus Randomness in Low Characteristic. In Shubhangi Saraf, editor, *35th Computational Complexity Conference (CCC 2020)*, volume 169 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 37:1–37:32, Dagstuhl, Germany, 2020. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL: <https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.CCC.2020.37>, doi:10.4230/LIPIcs.CCC.2020.37.
- [BKR⁺25] Somnath Bhattacharjee, Mrinal Kumar, Shanthanu Rai, Varun Ramanathan, Ramprasad Saptharishi, and Shubhangi Saraf. Constant-depth circuits for polynomial GCD over any characteristic, 2025. URL: <https://arxiv.org/abs/2506.23220>.
- [BLRS25] Amik Raj Behera, Nutan Limaye, Varun Ramanathan, and Srikanth Srinivasan. New Bounds for the Ideal Proof System in Positive Characteristic. In Keren Censor-Hillel, Fabrizio Grandoni, Joël Ouaknine, and Gabriele Puppis, editors, *52nd International Colloquium on Automata, Languages, and Programming (ICALP 2025)*, volume 334 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 22:1–22:20, Dagstuhl, Germany, 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL: <https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ICALP.2025.22>, doi:10.4230/LIPIcs.ICALP.2025.22.

- [Bü00] Peter Bürgisser. Cook’s versus Valiant’s hypothesis. *Theoretical Computer Science*, 235(1):71–88, 2000. URL: <https://www.sciencedirect.com/science/article/pii/S0304397599001838>, doi:10.1016/S0304-3975(99)00183-8.
- [CGJ⁺18] Mahdi Cheraghchi, Elena Grigorescu, Brendan Juba, Karl Wimmer, and Ning Xie. AC0 MOD2 lower bounds for the Boolean Inner Product. *Journal of Computer and System Sciences*, 97:45–59, 2018. URL: <https://www.sciencedirect.com/science/article/pii/S002200001830518X>, doi:10.1016/j.jcss.2018.04.006.
- [CKSV22] Prerona Chatterjee, Mrinal Kumar, Adrian She, and Ben Lee Volk. Quadratic Lower Bounds for Algebraic Branching Programs and Formulas. *computational complexity*, 31(2):8, July 2022. doi:10.1007/s00037-022-00223-8.
- [DIK⁺24] Pranjal Dutta, Christian Ikenmeyer, Balagopal Komarath, Harshil Mittal, Saraswati Girish Nanoti, and Dhara Thakkar. On the Power of Border Width-2 ABPs over Fields of Characteristic 2. In Olaf Beyersdorff, Mamadou Moustapha Kanté, Orna Kupferman, and Daniel Lokshtanov, editors, *41st International Symposium on Theoretical Aspects of Computer Science (STACS 2024)*, volume 289 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 31:1–31:16, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL: <https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.STACS.2024.31>, doi:10.4230/LIPIcs.STACS.2024.31.
- [Dut25] Pranjal Dutta. A brief survey on de-bordering paradigms and its recent advances, 2025. URL: <https://qi.rub.de/events/wact25/dutta.pdf>.
- [Fis94] Ismor Fischer. Sums of Like Powers of Multivariate Linear Forms. *Mathematics Magazine*, 67(1):59–61, 1994. URL: <http://www.jstor.org/stable/2690560>.
- [FLST24] Hervé Fournier, Nutan Limaye, Srikanth Srinivasan, and Sébastien Tavenas. On the Power of Homogeneous Algebraic Formulas. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, STOC 2024, pages 141–151, New York, NY, USA, 2024. Association for Computing Machinery. event-place: Vancouver, BC, Canada. doi:10.1145/3618260.3649760.
- [For24] Michael A. Forbes. Low-Depth Algebraic Circuit Lower Bounds over Any Field. In Rahul Santhanam, editor, *39th Computational Complexity Conference (CCC 2024)*, volume 300 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 31:1–31:16, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL: <https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.CCC.2024.31>, doi:10.4230/LIPIcs.CCC.2024.31.
- [FSS84] Merrick Furst, James B. Saxe, and Michael Sipser. Parity, circuits, and the polynomial-time hierarchy. *Mathematical systems theory*, 17(1):13–27, December 1984. doi:10.1007/BF01744431.
- [Gat87] Joachim von zur Gathen. Permanent and determinant. *Linear Algebra and its Applications*, 96:87–100, 1987. URL: <https://www.sciencedirect.com/science/article/pii/0024379587903375>, doi:10.1016/0024-3795(87)90337-5.
- [Gat21] Andreas Gathmann. Algebraic Geometry. 2021. URL: <https://agag-gathmann.math.rptu.de/class/alggeom-2021/alggeom-2021.pdf>.

- [GGIL22] Fulvio Gesmundo, Purnata Ghosal, Christian Ikenmeyer, and Vladimir Lysikov. Degree-Restricted Strength Decompositions and Algebraic Branching Programs. In Anuj Dawar and Venkatesan Guruswami, editors, *42nd IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2022)*, volume 250 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 20:1–20:15, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL: <https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.FSTTCS.2022.20>, doi:10.4230/LIPIcs.FSTTCS.2022.20.
- [GP18] Joshua A. Grochow and Toniann Pitassi. Circuit Complexity, Proof Complexity, and Polynomial Identity Testing: The Ideal Proof System. *J. ACM*, 65(6), November 2018. doi:10.1145/3230742.
- [HY11] Pavel Hrubeš and Amir Yehudayoff. Homogeneous Formulas and Symmetric Polynomials. *computational complexity*, 20(3):559–578, September 2011. doi:10.1007/s00037-011-0007-3.
- [KI04] Valentine Kabanets and Russell Impagliazzo. Derandomizing Polynomial Identity Tests Means Proving Circuit Lower Bounds. *computational complexity*, 13(1):1–46, December 2004. doi:10.1007/s00037-004-0182-6.
- [Kum19] Mrinal Kumar. A quadratic lower bound for homogeneous algebraic branching programs. *computational complexity*, 28(3):409–435, September 2019. doi:10.1007/s00037-019-00186-3.
- [Kum20] Mrinal Kumar. On the Power of Border of Depth-3 Arithmetic Circuits. *ACM Trans. Comput. Theory*, 12(1), February 2020. doi:10.1145/3371506.
- [KV22] Mrinal Kumar and Ben Lee Volk. A Lower Bound on Determinantal Complexity. *computational complexity*, 31(2):12, September 2022. doi:10.1007/s00037-022-00228-3.
- [LMP19] Nutan Limaye, Kunal Mittal, and Mukesh Pareek. Homogeneous ABP complexity of Elementary Symmetric polynomials, 2019. URL: <https://www.cse.iitb.ac.in/~nutan/papers/abp-complexity.pdf>.
- [LST24] Nutan Limaye, Srikanth Srinivasan, and Sébastien Tavenas. Superpolynomial Lower Bounds Against Low-Depth Algebraic Circuits. *Commun. ACM*, 67(2):101–108, January 2024. doi:10.1145/3611094.
- [Luc78] Edouard Lucas. Théorie des Fonctions Numériques Simplement Périodiques. *American Journal of Mathematics*, 1(2):184–196, 1878. URL: <http://www.jstor.org/stable/2369308>.
- [Mes14] Romeo Mestrovic. Lucas’ theorem: its generalizations, extensions and applications (1878–2014), 2014. URL: <https://arxiv.org/abs/1409.3820>.
- [MZ17] Izaak Meckler and Gjergji Zaimi. Singular locus of zero locus of elementary symmetric polynomials, 2017. URL: <https://mathoverflow.net/questions/264226/singular-locus-of-zero-set-of-elementary-symmetric-polynomial>.
- [Shp02] Amir Shpilka. Affine projections of symmetric polynomials. *Journal of Computer and System Sciences*, 65(4):639–659, 2002. URL: <https://www.sciencedirect.com/science/article/pii/S002200002000211>, doi:10.1016/S0022-0000(02)00021-1.

[SW01] A. Shpilka and A. Wigderson. Depth-3 arithmetic circuits over fields of characteristic zero. *computational complexity*, 10(1):1–27, November 2001. doi:10.1007/PL00001609.

A The Elementary Symmetric Polynomials

In this section, we will describe some of the basic properties of the elementary symmetric polynomials, which are used throughout the paper. Due to their simplicity, these polynomials possess many nice properties that we will use to simplify them and relate them to each other. For example, given $a_1, \dots, a_n, b_1, \dots, b_m \in \mathbb{F}$, we observe that

$$e_d^{n+m}(a_1, \dots, a_n, b_1, \dots, b_m) = \sum_{k=0}^d e_k^n(a_1, \dots, a_n) e_{d-k}^m(b_1, \dots, b_m). \quad (6)$$

We can also study their partial derivatives and observe that

$$\frac{\partial e_d^n}{\partial x_i}(x) = e_{d-1}^n(x) - x_i \frac{\partial e_{d-1}^n}{\partial x_i}(x) = e_{d-1}^{n-1}(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n). \quad (7)$$

We can then use this fact and a well-known property of homogeneous polynomials to conclude that

$$\sum_{i=1}^n x_i \frac{\partial e_d^n}{\partial x_i}(x) = d \cdot e_d^n(x). \quad (8)$$

Another important property of the elementary symmetric polynomials are Newton’s identities. We will denote $p_d^n(x_1, \dots, x_n) = x_1^d + \dots + x_n^d$. Then, Newton’s identities are given by

$$d e_d^n(x_1, \dots, x_n) = \sum_{k=1}^d (-1)^{k+1} p_k^n(x_1, \dots, x_n) e_{d-k}^n(x_1, \dots, x_n). \quad (9)$$

B Formula Lower Bounds

In this section, we will focus on proving the results of [CKSV22], specifically, we will prove Lemma 2.1. This is done for the sake of completeness and because the statement that we use, while not difficult to see from the proof in the original paper, is slightly different. Further, we provide a minor simplification to the original proof.

We will briefly recall the formal degree of a formula. The formal degree of a leaf node is defined by the degree of the polynomial that the leaf node is labeled with. The formal degree of a sum gate is defined as the maximum of the formal degrees of its children, and the formal degree of a product gate is defined by the sum of the formal degrees of its children. Observe that the formal degree of a formula upper bounds the degree of the polynomial it computes.

Instead of the typical definition, we will define the size of a formula to be the number of leaves whose label is not constant. Observe that this is linearly related to the number of leaves in a formula and its size (noting that we can “collapse” a node where both children are constants). We do this to help simplify the proofs.

The idea behind the following proof will be to iteratively find large sub-trees in our formula whose formal degree is strictly less than the degree of the polynomial we compute. We will then “peel” these sub-trees from our formula and replace them with the constant part of the polynomial our

sub-tree computes, where we will continue our process. We will observe that each step in this process only adds an error term that can be represented as the product of two constant-free polynomials. Finally, we will combine our sub-trees of low formal degree to represent our polynomial by a sum of products of constant-free polynomials summed to a low-degree polynomial. Our conclusion will then follow using Lemma 1.5.

To begin, we will state a simple fact about algebraic circuits, which merely states that every formula has a node with formal degree in the range $[t, 2t - 1]$.

Proposition B.1 (See Lemma 5.11 of [CKSV22]). *Let Φ be a formula of formal degree d . Then for each $t \in [1, d/2]$, there is a vertex v in Φ such that Φ_v has formal degree at least t and at most $2t - 1$.*

Further, there exists polynomials $h, f \in \mathbb{F}[X]$ such that $\Phi = h\Phi_v + f$ and, for every $\gamma \in \mathbb{F}$, $h\gamma + f$ can be computed by a formula of size at most $|\Phi| - |\Phi_v|$.

Proof. First notice that the formal degree of a formula monotonically increases as one goes from a leaf to root. The leaves of the formula have formal degree at most one and the root has formal degree d . Then, we observe that the formal degree of an internal node is at most the sum of the formal degrees of its children. It is, therefore, impossible for a parent node to have formal degree above $2t - 1$ with children of formal degree strictly less than t .

Now, let v be a vertex in Φ that satisfies the previous hypotheses. Notice that Φ is linear in Φ_v , so there are $h, f \in \mathbb{F}[X]$ be such that $\Phi = h\Phi_v + f$. Notice that, for any $\gamma \in \mathbb{F}$, we could replace Φ_v with a leaf node labeled with γ , and it would have size $|\Phi| - |\Phi_v|$. \square

In the next proposition, we represent our process of converting our polynomial to the form we would like. Specifically, we suppose that we have some d' , and we want to represent a polynomial by a formula of formal degree strictly less than d' with some error, represented by the sum of products of constant-free polynomials. We will repeatedly apply Proposition B.1 to complete this simplification.

Proposition B.2 (See Lemma 5.12 of [CKSV22]). *Let Φ be a formula of size s and formal degree d . For every $d' \geq 3$, there is a formula Φ' and polynomials $f_1, \dots, f_k, g_1, \dots, g_k \in \mathbb{F}[X]$ such that*

- $\Phi = \Phi' + \sum_{i=1}^k f_i g_i$,
- Φ' has formal degree less than d' ,
- $f_1, \dots, f_k, g_1, \dots, g_k$ are constant-free polynomials, and
- $k \frac{d'}{3} \leq s$.

Proof. We will prove this inductively on the size of the formula s . We first observe that the claim is trivial if $d < d'$ (which certainly happens when the circuit is sufficiently small), as we can set $\Phi' = \Phi$. Thus, if s is small enough such that $d < d'$, the claim is obvious.

Now, assume the hypothesis is true for all circuit of size strictly smaller than s . We assume that $d \geq d' \geq 3$. Then, we apply Proposition B.1 so that v is a vertex in Φ such that Φ_v has formal degree between $d'/3$ and $2d'/3$ and let $h, f \in \mathbb{F}[X]$ satisfy the rest of the proposition. We will write $h = h' + \alpha$ and $\Phi_v = g' + \beta$, where $h', g' \in \mathbb{F}[X]$ are constant-free polynomials and $\alpha, \beta \in \mathbb{F}$. Then,

$$\Phi = h\Phi_v + f = (h' + \alpha)(g' + \beta) + f = h'g' + \alpha g' + (h\beta + f).$$

Notice that $\alpha g'$ can be computed by a formula of size at most $|\Phi_v|$ and formal degree at most $2d'/3$ and, by Proposition B.1, $h\beta + f$ can be computed by a formula of size at most $|\Phi| - |\Phi_v|$. We can thus apply the inductive hypothesis to $h\alpha + f$ and let Φ' be a formula and $f_1, \dots, f_k, g_1, \dots, g_k \in \mathbb{F}[X]$ be

polynomials that satisfy the hypotheses. We have that h', g' are constant-free, so we let $f_{k+1} = h'$ and $g_{k+1} = g'$. We define Φ'' to be the circuit resulting from summing $\alpha g'$ and Φ' , so that Φ'' has size at most s and formula degree at most d' . Then,

$$\Phi = \Phi'' + \sum_{i=1}^{k+1} f_i g_i.$$

Further notice that (observing that $|\Phi_v| \geq d'/3$)

$$(k+1) \frac{d'}{3} \leq |\Phi| - |\Phi_v| + \frac{d'}{3} \leq |\Phi|. \quad \square$$

We can now use this to conclude the main result of this section.

Proof of Lemma 2.1. Suppose Φ has formal degree D . Then, we apply Proposition B.2 to obtain polynomials $h, f_1, \dots, f_k, g_1, \dots, g_k \in \mathbb{F}[X]$ such that

- $f = p + \sum_{i=1}^k f_i g_i$,
- $\deg(p) < d$,
- $f_1, \dots, f_k, g_1, \dots, g_k$ are constant-free, and
- $k \frac{d}{3} \leq s$.

Then, if we consider Φ as a formula over the algebraic closure of \mathbb{F} , we can apply Proposition 1.5 to conclude that

$$\dim V_2(f) \geq n - 2k \geq n - 2s \frac{3}{d}.$$

Therefore,

$$s \geq \frac{d}{6}(n - \dim V_2(f)). \quad \square$$