




Homogeneous Algebraic Complexity Theory and Algebraic Formulas

Pranjal Dutta   




School of Computing, National University of Singapore (NUS), Singapore

Fulvio Gesmundo   

Institut de Mathématiques de Toulouse, Université Paul Sabatier, Toulouse, France

Christian Ikenmeyer   

University of Warwick, Warwick, UK

Gorav Jindal   

Max Planck Institute for Software Systems, Saarbrücken, Germany

Vladimir Lysikov   

Ruhr-Universität Bochum, Bochum, Germany

Abstract

We study algebraic complexity classes and their complete polynomials under *homogeneous linear* projections, not just under the usual affine linear projections that were originally introduced by Valiant in 1979. These reductions are weaker yet more natural from a geometric complexity theory (GCT) standpoint, because the corresponding orbit closure formulations do not require the padding of polynomials. We give the *first* complete polynomials for \mathbf{VF} , the class of sequences of polynomials that admit small algebraic formulas, under homogeneous linear projections: The sum of the entries of the non-commutative elementary symmetric polynomial in 3 by 3 matrices of homogeneous linear forms.

Even simpler variants of the elementary symmetric polynomial are hard for the topological closure of a large subclass of \mathbf{VF} : the sum of the entries of the non-commutative elementary symmetric polynomial in 2 by 2 matrices of homogeneous linear forms, and homogeneous variants of the continuant polynomial (Bringmann, Ikenmeyer, Zuiddam, JACM '18). This requires a careful study of circuits with arity-3 product gates.

2012 ACM Subject Classification Theory of computation \rightarrow Algebraic complexity theory

Keywords and phrases Homogeneous polynomials, Waring rank, Arithmetic formulas, Border complexity, Geometric Complexity theory, Symmetric polynomials

Funding *Pranjal Dutta*: Funded under the project “Foundation of Lattice-based Cryptography”, by NUS-NCS Joint Laboratory for Cyber Security.

Christian Ikenmeyer: Supported by EPSRC grant EP/W014882/1.

Vladimir Lysikov: Part of the work was done while V.L. was affiliated with the QMATH Centre, University of Copenhagen. V.L. acknowledges financial support from VILLUM FONDEN via the QMATH Centre of Excellence (Grant No. 10059) and the European Union (ERC Grant Agreements 818761 and 101040907). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

1 Motivation: Geometric Complexity Theory and Padding

Geometric Complexity Theory (GCT) is an approach towards proving algebraic variants of the $\mathbf{P} \neq \mathbf{NP}$ conjecture using algebraic geometry and representation theory [27, 28]. Let $\det_n := \sum_{\sigma \in \mathfrak{S}_n} \text{sgn}(\sigma) \prod_{i=1}^n x_{i,\sigma(i)}$ be the determinant polynomial, and let $\text{per}_m := \sum_{\sigma \in \mathfrak{S}_m} \prod_{i=1}^m x_{i,\sigma(i)}$ be the permanent polynomial. An algebraic version of the $\mathbf{P} \neq \mathbf{NP}$ conjecture, often called Valiant’s *determinant vs. permanent* conjecture, states that the smallest size of a matrix

A whose entries are affine linear polynomials such that $\det(A) = \text{per}_m$, is *not polynomially* bounded in m . Mulmuley and Sohoni strengthened the conjecture by allowing the permanent to be approximated arbitrarily closely coefficientwise instead of being computed exactly.

The Mulmuley–Sohoni conjecture can be stated in terms of group orbit closures as $\ell^{n-m}\text{per}_m \notin \overline{\text{GL}_{n^2} \det_n}$, if $n = \text{poly}(m)$; here $\text{GL}_{n^2} := \text{GL}(\mathbb{C}^{n \times n})$ acts on the space of homogeneous degree n polynomials in n^2 variables by (invertible) linear transformations of the variables¹, ℓ is some homogeneous linear polynomial (one can assume $\ell := x_{1,1}$), and the closure can be taken equivalently in the Zariski or the Euclidean topology, see e.g. [24, AI.7.2 Folgerung]. The polynomial $\ell^{m-n}\text{per}_n$ is called the ‘padded permanent’, and the phenomenon of multiplying with a power of a linear form is called *padding*. Note here that the action of GL_{n^2} replaces variables by *homogeneous* linear polynomials. One could formulate this setup without padding, but then the reductive group GL_{n^2} would have to be replaced by the general affine group (see e.g. [26]), which is *not* a reductive group. For reductive groups, every representation decomposes into a direct sum of irreducible representations. This is important for the representation theoretic attack proposed in [27, 28], hence the padding is introduced in those papers. The idea is that $\ell^{n-m}\text{per}_m \in \overline{\text{GL}_{n^2} \det_n}$ if and only if $\overline{\text{GL}_{n^2} \ell^{n-m}\text{per}_m} \subseteq \overline{\text{GL}_{n^2} \det_n}$. Such an inclusion induces a GL_{n^2} -equivariant surjection between the coordinate rings and between their homogeneous degree δ components, see e.g. [12]: $\mathbb{C}[\overline{\text{GL}_{n^2} \det_n}]_\delta \twoheadrightarrow \mathbb{C}[\overline{\text{GL}_{n^2} \ell^{n-m}\text{per}_m}]_\delta$. Now, since the group GL_{n^2} is reductive, both sides decompose into irreducible representations of GL_{n^2} :

$$\underbrace{\mathbb{C}[\overline{\text{GL}_{n^2} \det_n}]_\delta}_{=\bigoplus_\lambda d_\lambda V_\lambda} \twoheadrightarrow \underbrace{\mathbb{C}[\overline{\text{GL}_{n^2} \ell^{n-m}\text{per}_m}]_\delta}_{=\bigoplus_\lambda p_\lambda V_\lambda},$$

where λ is a non-increasing list of n^2 many nonnegative integers, and V_λ is the irreducible GL_{n^2} representation of type λ . Schur’s lemma (see e.g. [16]) implies that $\forall \lambda : d_\lambda \geq p_\lambda$. A λ with $d_\lambda < p_\lambda$ is called a *multiplicity obstruction*. If additionally we have that $d_\lambda = 0$, then λ is called an *occurrence obstruction*. Issues with the padding were known from the beginning, and machinery to carry over information from $\mathbb{C}[\overline{\text{GL}_{m^2} \text{per}_m}]$ to $\mathbb{C}[\overline{\text{GL}_{n^2} \ell^{n-m}\text{per}_m}]$ was discussed, see e.g. [12]. The impact of the padding on λ was first highlighted by Kadish and Landsberg [23], where they use the padding to classify a large class of λ as *not useful*. This was later strengthened in [19, 11], where it was shown that all relevant λ have strictly positive d_λ , so that occurrence obstructions are not sufficient to prove Mulmuley and Sohoni’s conjecture. This is known as the occurrence obstruction no-go result.

However, the padding can be removed by replacing \det_n by the iterated matrix multiplication polynomial in $2n + n^2(d-2)$ variables:

$$\text{IMM}_{n,d} := (x_{1,1,1} \ x_{1,2,1} \ \cdots \ x_{1,n,1}) \begin{pmatrix} x_{1,1,2} & \cdots & x_{1,n,2} \\ \vdots & \ddots & \vdots \\ x_{n,1,2} & \cdots & x_{n,n,2} \end{pmatrix} \cdots \begin{pmatrix} x_{1,1,d-1} & \cdots & x_{1,n,d-1} \\ \vdots & \ddots & \vdots \\ x_{n,1,d-1} & \cdots & x_{n,n,d-1} \end{pmatrix} \begin{pmatrix} x_{1,1,d} \\ \vdots \\ x_{n,1,d} \end{pmatrix}.$$

Again, the task is to show that a surjection cannot exist:

$$\underbrace{\mathbb{C}[\overline{\text{GL}_{2n+n^2(d-2)} \text{IMM}_{n,d}}]_\delta}_{=\bigoplus_\lambda i_\lambda V_\lambda} \twoheadrightarrow \underbrace{\mathbb{C}[\overline{\text{GL}_{2n+n^2(d-2)} \text{per}_d}]_\delta}_{=\bigoplus_\lambda j_\lambda V_\lambda}.$$

Analogously to d_λ vs p_λ , one searches for λ with $i_\lambda < j_\lambda$. In fact, it is known that the j_λ can be determined independently of n via inheritance theorems (see [18]): $\mathbb{C}[\overline{\text{GL}_{d^2} \text{per}_d}]_\delta = \bigoplus_\lambda j_\lambda V_\lambda$.

¹ For a homogeneous polynomial p and $g \in \text{GL}_{n^2}$ define the homogeneous polynomial gp via $(gp)(\vec{x}) := p(g^t \vec{x})$. The orbit is defined as $\text{GL}_{n^2} p := \{gp \mid g \in \text{GL}_{n^2}\}$.

There are no no-go results known for this approach, but no strong equations vanishing on the orbit closure of IMM have been found so far.

Our main contribution in this paper is the discovery of new natural polynomials that serve as much simpler replacements for IMM, which are still powerful enough to imply variants of Valiant’s conjecture, see §3.1.

2 Algebraic Complexity Theory

A sequence of natural numbers $m = (m_n)_{n \in \mathbb{N}}$ is called *polynomially bounded* if there exists a univariate polynomial t such that $\forall n \in \mathbb{N} : m_n \leq t(n)$. Let \mathcal{B} denote the set of all polynomially bounded sequences. Let $\mathbb{S} := \mathbb{C}[x_1, x_2, \dots]$ denote the set of all polynomials, and let \mathbb{S}_d denote the vector space of all homogeneous degree d polynomials (including the zero polynomial). We sometimes use the notation $n \mapsto a(n)$ to denote the function a , for example $n \mapsto n$ is the identity map. For a sequence $g \in \mathbb{S}^{\mathbb{N}}$ of polynomials let $\deg(g) := n \mapsto \deg(g_n)$ be the sequence of degrees. Analogously, for a polynomial p define $\text{nvar}(p)$ to be the number of variables appearing in p , and for a sequence $g \in \mathbb{S}^{\mathbb{N}}$ of polynomials let $\text{nvar}(g) := n \mapsto \text{nvar}(g_n)$. A sequence $g \in \mathbb{S}^{\mathbb{N}}$ is called a *p-family* if $\deg(g) \in \mathcal{B}$ and $\text{nvar}(g) \in \mathcal{B}$. We sometimes call p-families *ungraded* p-families, and we propose a definition of a *graded* p-family in §3, which will be useful for obtaining padding-free orbit closure formulations. The classical complexity classes that we discuss in this section are defined in terms of ungraded p-families.

An algebraic formula is a directed tree with a unique sink vertex. The source vertices are labelled by affine linear combinations of variables, and each internal node of the graph is labelled by either $+$ or \times . Nodes compute polynomials in the natural way by induction. An algebraic circuit is slightly more general: The underlying digraph is required to be acyclic, but not necessarily a tree. The size of a circuit/formula is the number of its vertices. VF is the class of p-families $(f_n)_{n \in \mathbb{N}}$, with required formula size of f_n being polynomially bounded. VP is the class p-families $(f_n)_{n \in \mathbb{N}}$, with required circuit size of f_n being polynomially bounded.

Every homogeneous degree d polynomial p can be written as a product

$$p = (\ell_{1,1,1} \ell_{1,2,1} \cdots \ell_{1,n,1}) \begin{pmatrix} \ell_{1,1,2} & \cdots & \ell_{1,n,2} \\ \vdots & \ddots & \vdots \\ \ell_{n,1,2} & \cdots & \ell_{n,n,2} \end{pmatrix} \cdots \begin{pmatrix} \ell_{1,1,d-1} & \cdots & \ell_{1,n,d-1} \\ \vdots & \ddots & \vdots \\ \ell_{n,1,d-1} & \cdots & \ell_{n,n,d-1} \end{pmatrix} \begin{pmatrix} \ell_{1,1,d} \\ \vdots \\ \ell_{n,1,d} \end{pmatrix}$$

of matrices whose entries are homogeneous linear polynomials. We define $w(p)$ to be the smallest possible such n , and call it the *homogeneous branching program width* of p . For an inhomogeneous polynomial, we define $w(p) := \sum_{d \in \mathbb{N}} w(p_d)$ to be the sum of the widths of its homogeneous components. VBP is the class of p-families whose w is polynomially bounded.

The *permanental complexity* of a polynomial f is the smallest n such that f can be written as the permanent of an $n \times n$ matrix of affine linear polynomials. The class VNP consists of all p-families $(f_n)_{n \in \mathbb{N}}$ for which the permanental complexity is polynomially bounded.

It is known that $\text{VF} \subseteq \text{VBP} \subseteq \text{VP} \subseteq \text{VNP}$ [34, 33]. The conjectures $\text{VF} \neq \text{VNP}$, $\text{VBP} \neq \text{VNP}$, $\text{VP} \neq \text{VNP}$, are known as *Valiant’s conjectures*. Especially $\text{VBP} \neq \text{VNP}$ is known as the *determinant vs permanent* problem. A sequence $(c_n)_{n \in \mathbb{N}}$ of natural numbers is called *quasipolynomially bounded* if there exists a polynomial q with $\forall n \geq 2 : c_n \leq n^{q(\log_2 n)}$. In the definitions of VF, VBP, VP, if we change the upper bound on the complexity to “quasipolynomially bounded” instead of just “polynomially bounded”, then each time we obtain the same class, which we call VQP, see [8]. The conjecture $\text{VNP} \not\subseteq \text{VQP}$ is called Valiant’s *extended* conjecture.

2.1 Border Complexity

The complexity notions mentioned above, such as formula size, circuit size, width w , permanent complexity, have an associated *border complexity* variant: A polynomial has border complexity $\leq k$ if it is the limit of polynomials of complexity at most k . Here, the limit is taken in the Euclidean topology on the coefficient vector space, see e.g. [20]. Border complexity measures are usually indicated by an underlined symbol: e.g., \underline{w} is the border homogeneous algebraic branching program width. Clearly $\underline{w}(p) \leq w(p)$ for all polynomials p .

The border complexity analogues of the classical classes are denoted by an overline, e.g., $\overline{\text{VF}}$ is the class of p-families with polynomially bounded border formula complexity². While Valiant's conjecture states that $w(\text{per})$ grows superpolynomially ($\text{VBP} \neq \text{VNP}$), the Mulmuley-Sohoni conjecture states that $\underline{w}(\text{per})$ grows superpolynomially ($\text{VNP} \not\subseteq \overline{\text{VBP}}$). The extended Valiant's conjecture states that $w(\text{per})$ grows superquasipolynomially ($\text{VNP} \not\subseteq \text{VQP}$), and it is natural to merge these to the extended Mulmuley-Sohoni conjecture: $\underline{w}(\text{per})$ grows superquasipolynomially ($\text{VNP} \not\subseteq \overline{\text{VQP}}$).

Border complexity is an old area of study in algebraic geometry. In theoretical computer science it was introduced in [3, 2] in the context of fast matrix multiplication. In algebraic complexity theory, border complexity was first discussed independently in [27, 9].

3 Graded p-families and Homogeneous Reductions

In this section we generalize known concepts from algebraic complexity theory from univariate to bivariate by adding a degree parameter. This gives the correct setting for homogeneous linear projections, which is the natural setting for *padding-free* geometric complexity theory. We are very formal in this section, because the readers are used to affine projections, and some steps might seem very subtle.

For the connections between the homogeneous and inhomogeneous setting, see §4.2.

As usual, for a set A , we identify sequences $a \in A^{\mathbb{N}}$ with functions $\mathbb{N} \rightarrow A$, and we write $a_n = a(n)$. We use the same notation for functions $\mathbb{N} \times \mathbb{N} \rightarrow A$, i.e., $a_{n,d} = a(n, d)$.

A function $m : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ is called *bivariately polynomially bounded* if there exists a bivariate polynomial t such that $\forall (n, d) \in \mathbb{N} \times \mathbb{N} : m_{n,d} \leq t(n, d)$. We propose the following definition of a *graded* p-family in order to work with the weak reduction notion of homogeneous linear projections, which enables padding-free orbit closure formulations.

► **Definition 3.1.** A graded p-family f is a map $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{S}$ such that

- $(n, d) \mapsto \text{nvar}(f_{n,d})$ is bivariately polynomially bounded, and
- every $f_{n,d}$ is either zero or homogeneous of degree d .

For example, $\text{IMM}(n, d) = \text{IMM}_{n,d}$ is a graded p-family. The natural reduction notion for graded p-families are *homogeneous linear projections*, which are defined as follows. Suppose U, W are finite dimensional complex vector spaces and $p \in \mathbb{C}[U]_d, q \in \mathbb{C}[W]_d$ are homogeneous degree d (where $d > 0$) polynomials. We say that p is a homogeneous linear projection of q , and write $p \leq_{\text{homlin}} q$, if $p \in \{q \circ A \mid A : U \rightarrow W \text{ linear}\}$. For degree $d = 0$ we define that for any nonzero q we have $p \leq_{\text{homlin}} q$. For graded p-families f and h we write $f \leq_{\text{p-homlin}} h$ if there exists $m \in \mathbb{B}$ such that for all n, d we have $f_{n,d} \leq_{\text{homlin}} h_{m_{n,d}}$. The border complexity version is analogous: $p \trianglelefteq_{\text{homlin}} q$, if $p \in \overline{\{q \circ A \mid A : U \rightarrow W \text{ linear}\}}$, and $f \trianglelefteq_{\text{p-homlin}} h$, if

² see [20] for the definition of the closure of sets of p-families in general.

$\exists m \in \mathcal{B} \forall n, d : f_{n,d} \trianglelefteq_{\text{homlin}} h_{m_n,d}$. If m is only quasipolynomially bounded, we obtain the analogous quasipolynomial variants $f \leq_{\text{qp-homlin}} h$ and $f \trianglelefteq_{\text{qp-homlin}} h$.

Ungraded p-families g are graded p-families in the natural way, by setting $g_{n,d}$ to be the homogeneous degree d component of g_n . In particular, the permanent can be interpreted in this way as a graded p-family. This allows us to phrase the four conjectures in this language:

$\text{VNP} = \text{VBP}$	if and only if	$\text{per} \leq_{\text{p-homlin}} \text{IMM}$,
$\text{VNP} \subseteq \overline{\text{VBP}}$	if and only if	$\text{per} \trianglelefteq_{\text{p-homlin}} \text{IMM}$,
$\text{VNP} \subseteq \text{VQP}$	if and only if	$\text{per} \leq_{\text{qp-homlin}} \text{IMM}$,
$\text{VNP} \subseteq \overline{\text{VQP}}$	if and only if	$\text{per} \trianglelefteq_{\text{qp-homlin}} \text{IMM}$.

Since per is a p-family of homogeneous polynomials, the question $\text{per} \trianglelefteq_{\text{p-homlin}} \text{IMM}$ is about the existence of an $m \in \mathcal{B}$ such that $\forall d : \text{per}_d \trianglelefteq_{\text{homlin}} \text{IMM}_{m(d),d}$. This has a padding-free orbit closure formulation under the general linear group, which is reductive:

$$\text{per}_d \trianglelefteq_{\text{homlin}} \text{IMM}_{m,d} \quad \text{iff} \quad \overline{\text{GL}_{d^2} \text{per}_d} \subseteq \overline{\text{GL}_{2m_d+m_d^2(d-2)} \text{IMM}_{m,d}}.$$

This is the main advantage of using homogeneous linear projections as the reduction notion. Our main contribution is to replace IMM by simpler graded p-families that capture VF or the large subset V3F of VF ; see Definition 6.7 in §6.3. This has two advantages: The orbit closures become simpler, and the separations from VNP become easier than $\text{VBP} \neq \text{VNP}$, because $\text{V3F} \subseteq \text{VF} \subseteq \text{VBP}$, while the quasipolynomial versions of V3F , VF , VBP all coincide with VQP .

3.1 Main Results

Let $\text{nce}_d(X_1, \dots, X_n) := \sum_{1 \leq I_1 < I_2 < \dots < I_d \leq n} X_{I_1} \dots X_{I_d}$, denote the elementary symmetric polynomial in noncommuting variables X_1, \dots, X_n . Let $L : \mathbb{C}^{3 \times 3} \rightarrow \mathbb{C}$ be the sum of all 9 entries. Let $\text{nce}_{3,n,d} := L \circ \text{nce}_d(A_1, A_2, \dots, A_n)$, where each A_i is a 3×3 matrix of 9 fresh variables. We denote by nce_3 the corresponding graded p-family.

► Theorem 3.2.

$\text{VNP} = \text{VF}$	if and only if	$\text{per} \leq_{\text{p-homlin}} \text{nce}_3$,
$\text{VNP} \subseteq \overline{\text{VF}}$	if and only if	$\text{per} \trianglelefteq_{\text{p-homlin}} \text{nce}_3$,
$\text{VNP} \subseteq \text{VQP}$	if and only if	$\text{per} \leq_{\text{qp-homlin}} \text{nce}_3$,
$\text{VNP} \subseteq \overline{\text{VQP}}$	if and only if	$\text{per} \trianglelefteq_{\text{qp-homlin}} \text{nce}_3$.

Note that $\text{per}_d \trianglelefteq_{\text{homlin}} \text{nce}_{3,n,d}$ iff $\overline{\text{GL}_{d^2} \text{per}_d} \subseteq \overline{\text{GL}_{9n} \text{nce}_{3,n,d}}$. In the border setting, we manage to get the same results even for nce_2 , we simplify the orbit closure on the right hand side even further by introducing a new class $\text{V3F} \subseteq \text{VF}$ (see §6.3), whose quasipolynomial version is still VQP . The parity-alternating elementary symmetric polynomial $C_{n,d}$ is defined via $C_{n,d} := \sum_{(i_1, i_2, \dots, i_d) \in I} x_{i_1} x_{i_2} \dots x_{i_d}$, where I is the set of length d increasing sequences of numbers $i_1 < i_2 < \dots < i_d$ from $\{1, \dots, n\}$ in which for all j the parity of i_j differs from the parity of i_{j+1} , and i_1 is odd, in other words, $i_j \equiv j \pmod{2}$.

► Theorem 3.3.

$\text{VNP} \subseteq \overline{\text{V3F}}$	\implies	$\text{per} \trianglelefteq_{\text{p-homlin}} C$,
$\text{VNP} \subseteq \overline{\text{VF}}$	\longleftarrow	$\text{per} \trianglelefteq_{\text{p-homlin}} C$,
$\text{VNP} \subseteq \overline{\text{VQP}}$	if and only if	$\text{per} \trianglelefteq_{\text{qp-homlin}} C$.

Note that “ $\text{per}_d \leq_{\text{homlin}} C_{n,d}$ iff $\overline{\text{GL}_{d^2} \text{per}_d} \subseteq \overline{\text{GL}_n C_{n,d}}$ ”

is a formulation with an intriguingly simple orbit closure. Moreover, it seems reasonable to try to prove $\text{VNP} \not\subseteq \sqrt{3}\text{F}$ or $\text{VNP} \not\subseteq \sqrt{\text{V}}$ before proving the more difficult $\text{VNP} \not\subseteq \text{VBP}$.

4 Related Concepts

4.1 Classical homogeneous complexity measures: Waring rank, Chow rank, tensor rank

In classical algebraic geometry, homogeneous linear projections are the standard way to compare homogeneous polynomials and tensors.

We list some of the classical examples in this subsection.

Given a homogeneous degree d polynomial f , the *Waring rank* of f , denoted $\text{WR}(f)$, is the smallest r such that there exist homogeneous linear polynomials ℓ_1, \dots, ℓ_r , with $f = \sum_{i=1}^r \ell_i^d$.

The *border Waring rank* of f , denoted $\underline{\text{WR}}(f)$, is the smallest r such that f can be written as limit of a sequence of polynomials f_ϵ with $\text{WR}(f_\epsilon) \leq r$. Given the graded p-family $P_{n,d} := x_1^d + \dots + x_n^d$, we see that $\text{WR}(p) \leq r$ iff $p \leq_{\text{homlin}} P_{n,d}$ and $\underline{\text{WR}}(p) \leq r$ iff $p \leq_{\text{homlin}} P_{n,d}$, which is equivalent to $p \in \overline{\text{GL}_n P_{n,d}}$, provided p is defined in the variables x_1, \dots, x_n . Waring rank was studied already in the eighteenth century [13, 31, 14] in the context of invariant theory, with the aim to determine normal forms for homogeneous polynomials. We mention the famous Sylvester Pentahedral Theorem, stating that a generic cubic form in four variables can be written uniquely as sum of five cubes. At the beginning of the twentieth century, the early work on secant varieties in classical algebraic geometry [29, 32] implicitly commenced the study of border Waring rank. In the algebraic complexity theory literature, Waring rank is called the homogeneous $\Sigma\Lambda\Sigma$ -circuit complexity.

The *Chow rank* of f , denoted $\text{CR}(f)$, is the smallest r such that there exist homogeneous linear polynomials $\ell_{1,1}, \dots, \ell_{r,d}$, with $f = \sum_{i=1}^r \ell_{i,1} \dots \ell_{i,d}$. The *border Chow rank* of f , denoted $\underline{\text{CR}}(f)$, is the smallest r such that f can be written as limit of a sequence of polynomials f_ϵ with $\text{CR}(f_\epsilon) \leq r$. Given the graded p-family $Q_{n,d} := x_{1,1} \dots x_{1,d} + \dots + x_{n,1} \dots x_{n,d}$, we see that $\text{CR}(p) \leq r$ iff $p \leq_{\text{homlin}} Q_{n,d}$ and $\underline{\text{CR}}(p) \leq r$ iff $p \leq_{\text{homlin}} Q_{n,d}$, which is equivalent to $p \in \overline{\text{GL}_{nd} Q_{n,d}}$, provided p is defined in the variables $x_{1,1}, \dots, x_{n,d}$. In the algebraic complexity literature, Chow rank is called the homogeneous $\Sigma\Pi\Sigma$ -circuit complexity.

The noncommutative analog (i.e., variables do not commute) of Chow rank is the classical tensor rank. The notion of border rank for tensors was introduced in [3] to construct faster-than-Strassen matrix multiplication algorithms. In [2], Bini proved that tensor border rank and tensor rank define the same matrix multiplication exponent. Today this theory is deeply related to the study of Gorenstein algebras [17, 6], the Hilbert scheme of points [21], and deformation theory [7, 22]. Homogeneous linear projections are used to compare not only the rank of tensors, but they are used to define a partial order on the set of all tensors, see e.g. [10, Ch 14.6]. This is also a common concept in quantum information theory.

4.2 Homogeneous vs Inhomogeneous

In this subsection we work out the relation to classical (i.e., ungraded) algebraic complexity theory. In order to define the notion of completeness of graded p-families for the classical algebraic complexity classes we use the following map φ . Given $d \in \mathcal{B}$, $m \in \mathcal{B}$ and $a \in \mathbb{C}^{\mathbb{N} \times \mathbb{N}}$, then a graded p-family f can be converted into an ungraded p-family $\varphi(f, a, m, d)$ by setting

$\varphi(f, a, m, d)_n := \sum_{i=0}^{d_n} a_{n,i} \cdot f_{m_n,i}$. For a graded p -family f we define the set $\varphi(f)$ of associated ungraded p -families as $\varphi(f) := \{\varphi(f, a, m, d) \mid m \in \mathcal{B}, d \in \mathcal{B}, a \in \mathbb{C}^{\mathbb{N} \times \mathbb{N}}\}$.

► **Definition 4.1.** Let $\mathcal{C} \subseteq \mathbb{S}^{\mathbb{N}}$ be a class of ungraded p -families. We say that a graded p -family f is \mathcal{C} -hard if for all $g \in \mathcal{C}$ we have $g \leq_{\text{p-homlin}} f$.

We say that f is \mathcal{C} -complete if f is \mathcal{C} -hard and $\varphi(f) \subseteq \mathcal{C}$.

There are analogous variants for completeness under border projections ($g \leq_{\text{p-homlin}} f$) and quasipolynomial projections ($g \leq_{\text{qp-homlin}} f$), and quasipolynomial border projections ($g \leq_{\text{qp-homlin}} f$).

The main example is that the graded p -family IMM is VBP-complete under homogeneous linear p -projections. From §4.1, P is complete for the class of p -families with polynomially bounded Waring rank, and Q is complete for the class of p -families with polynomially bounded Chow rank.

While for ungraded p -families we have to allow affine linear projections as reductions, for graded p -families we can (and always will) use the *weaker* notion of homogeneous linear projections. Hence, it is *not obvious* how to turn a \mathcal{C} -complete ungraded p -family (under affine linear projections) into a \mathcal{C} -complete graded p -family (under homogeneous linear projections)! We illustrate this scenario by an example below.

Let us consider a ungraded p -family g , which is VF-complete under affine linear projections; then g interpreted as a graded p -family is *not necessarily* VF-complete under homogeneous linear projections, as the following example illustrates. The ungraded p -family IMM₃ defined via $(\text{IMM}_3)_n = \text{IMM}_{3,n}$ is an ungraded VF-complete p -family. The constant ungraded p -family with each element $x_1^2 + \dots + x_7^2$ is in VF, but by construction IMM_{3,2} is nonzero only for exactly $n = 2$, and there is no homogeneous linear projection of IMM_{3,2} to $x_1^2 + \dots + x_7^2$ (because every homogeneous linear projection of IMM_{3,2} has only at most 6 essential variables, i.e., its GL-orbit has dimension at most 6). However, the reverse works under mild conditions on self-reducibility of f under affine projections and on being able to simulate sums; as an example we refer to the following claim.

▷ **Claim 4.2.** We write $p \leq_{\text{affin}} q$ if p can be obtained from q by replacing variables in q by affine linear polynomials. Let f be a graded p -family that is \mathcal{C} -complete under homogeneous linear projections, and assume that $\forall n, d : f_{n,d-1} \leq_{\text{affin}} f_{n,d}$ and $f_{n-1,d} \leq_{\text{homlin}} f_{n,d}$. Let $g := \varphi(f, \text{diag}(1, \dots, 1), \text{id}_{\mathbb{N}}, \text{id}_{\mathbb{N}})$ with the property that there exists a bivariate polynomially bounded q such that $\forall n, k$: if $h_1, \dots, h_k \leq_{\text{affin}} g_n$, then $h_1 + \dots + h_k \leq_{\text{affin}} g_{q(k,n)}$. Then g is \mathcal{C} -complete under affine linear projections.

Proof. From $\varphi(f) \subseteq \mathcal{C}$ it follows that $g \in \mathcal{C}$. Now, let $h \in \mathcal{C}$ be an ungraded p -family. We have $h \leq_{\text{p-homlin}} f$, hence

$$\forall n, d : h_{n,d} \leq_{\text{homlin}} f_{m_n,d} \leq_{\text{affin}} f_{\max\{m_n, \deg(h_n)\}, \max\{m_n, \deg(h_n)\}} = g_{\max\{m_n, \deg(h_n)\}}.$$

Therefore, $\forall n : h_n \leq_{\text{affin}} g_{q(\deg(h_n)+1, \max\{m_n, \deg(h_n)\})}$. Define

$$a(n) := q(\deg(h_n) + 1, \max\{m_n, \deg(h_n)\}).$$

Thus, $\forall n : h_n \leq_{\text{affin}} g_{a(n)}$, which proves the claim, because $a \in \mathcal{B}$. ◀

While IMM is a VBP-complete graded p -family and IMM₃ is a VF-complete ungraded p -family, our paper is the *first to introduce* a VF-complete graded p -family nce_3 , see Theorem 3.2. It is unclear if graded complete p -families for VP or for VNP *exist*, and we leave this as an open question. For example, it is not obvious if a universal circuit family for VP can be used to construct a VP-complete graded p -family under homogeneous linear projections.

5 Proof Ideas

In this section, we briefly sketch the overall proof idea of Theorem 3.2 and Theorem 3.3.

5.1 Proof idea of Theorem 3.2

The recent paper [15, Section 3] introduced a notion of complexity with a rigid interplay between homogeneous linear entries and fixed constants, which they call Kumar’s complexity. It is modeled after Kumar’s construction in [25]. For a polynomial f , Kumar’s complexity of f is the smallest m such that there exists a constant α and homogeneous linear polynomials ℓ_i such that

$$f = \alpha \left(\left(\prod_{i=1}^m (1 + \ell_i) \right) - 1 \right). \quad (1)$$

We study an analogous notion for matrices. Let $E_{n,d}$ be the homogeneous degree d part of the sum of the entries of

$$\begin{pmatrix} 1 & x_{1,1,2} & x_{1,1,3} \\ x_{1,2,1} & 1 & x_{1,2,3} \\ x_{1,3,1} & x_{1,3,2} & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & x_{n,1,2} & x_{n,1,3} \\ x_{n,2,1} & 1 & x_{n,2,3} \\ x_{n,3,1} & x_{n,3,2} & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

In the expansion, the noncommutative elementary symmetric polynomials appear. Our study of this setup leads to a homogenized version of the result by Ben-Or & Cleve [1]. Here we have to pay close attention on how to deal with field constants, and we define the notion of *input-homogeneous-linear computation* (IHL), see §6.1. In particular, we prove an input-homogeneous-linear version of Brent’s depth reduction, see Lemma 6.2. Theorem 3.2 appears in §6 as Corollary 6.6.

5.2 Proof idea of Theorem 3.3

From 3×3 matrices, we turn to 2×2 matrices. Note that (for odd d) $C_{n,d}$ is the homogeneous degree d part of the $(1, 2)$ entry of $\begin{pmatrix} 1 & x_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ x_2 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & x_n \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Theorem 3.3 appears in §6 as Theorem 6.10. Its proof is based on the construction of [5], which is, however inherently *affine*. To circumvent this, we convert the product gate into an arity 3 homogeneous product gate. The resulting analysis of arithmetic circuits and formulas allowing only arity 3 homogeneous product gates is surprisingly subtle. The graded p-family $C_{n,d}$ can be seen as a homogeneous variant of the continuant in [5].

For the last part of Theorem 3.3, we prove that $\text{VQ3F} = \text{VQP}$. The rest of the hardness proof follows then completely analogously via quasipolynomial homogeneous linear border projections. The proof of $\text{VQ3F} = \text{VQP}$ proceeds in two steps: We first show that VF lies in V3P (the circuit analog of V3F), see Theorem 6.11, where we first “parity-homogenize” the formula (every gate has only even or only odd nonzero homogeneous components), and then compute $z \cdot f$ at each even-degree gate instead of f , where z is a new variable. This additional factor z is then later replaced, which is the main reason why the output of this construction is a *circuit* and not a formula. Since we know that $\text{V3F} \subseteq \text{VF}$, we are now in this situation:

$$\text{V3F} \subseteq \text{VF} \subseteq \text{V3P} \cap \text{VBP} \subseteq \text{VP}.$$

Our proof does not give $\text{V3F} = \text{VF}$, see Remark 6.12. We conclude our proof by showing that $\text{VQ3F} = \text{VQ3P}$, which implies that both classes are equal to $\text{VQ3F} = \text{VQF} = \text{VQ3P}$, but we already know $\text{VQF} = \text{VQP}$. For details, see (2) and Theorem 6.14.

To achieve this, we use an arity-3 basis variant of the Valiant-Skyum-Berkowitz-Rackoff circuit depth reduction [35], which is a bit more involved than the original proof.

6 Input-homogenization and Arity 3 Products

In this section, f is a polynomial, and not a graded p-family.

6.1 Input-homogeneous-linear Computation

We start with a technicality in the definition of arithmetic circuits. In this section every edge of an arithmetic circuit is labelled with a field constant. Instead of just forwarding the computation result of a gate to another gate, these edges rescale the polynomial along the way. For arithmetic *formulas* we do *not* allow this, as we will see that it is unnecessary. In other words, we allow $g + h$ gates for formulas, while we allow a $\alpha \cdot g + \beta \cdot h$ gates in circuits, and analogously for multiplication.

The *depth* of an arithmetic circuit/formula is the length of the longest path from the source to a leaf.

► **Definition 6.1.** *An arithmetic formula/circuit is called input-homogeneous-linear (IHL) if all its leaves are labelled with homogeneous linear polynomials.*

In particular (contrary to ordinary arithmetic formulas/circuits) in an IHL formula/circuit we *do not* allow any leaf to be labelled with a field constant. It now becomes clear why we needed the technicality: For any $\alpha \in \mathbb{C}$, if an IHL circuit with s gates computes a polynomial f , then using the scalars on the edges there exists an IHL circuit computing αf with also only s many gates. For formulas this rescaling can be simulated by rescaling a subset of the leaves. Indeed, we rescale the root of the formula by induction: we rescale a summation gate by rescaling both children, we rescale a product gate by rescaling an arbitrary child. Alternatively, if f is homogeneous, one can rescale the input gates by the $\sqrt[d]{\alpha}$. The latter technique works for formulas and circuits alike, but we will not use this method.

It is easy to see that IHL formulas/circuits can only compute polynomials f with $f(0) = 0$. But other than that, being IHL is not a strong restriction, as the following simple lemma shows. We write $\widehat{f} := f - f(0)$.

► **Lemma 6.2.** *Given an arithmetic circuit of size s computing a polynomial f , then there exists an IHL arithmetic circuit of size $6s$ and depth $3s$ computing \widehat{f} .*

There exists a polynomial p such that: Given any arithmetic formula of size s computing a polynomial f , then there exists an IHL arithmetic formula of size $p(s)$ and depth $O(\log(s))$ computing \widehat{f} .

Proof. We treat the case of formulas first. We first use Brent's depth reduction [4] to ensure that the size is $\text{poly}(s)$ and the depth is $O(\log(s))$. We now proceed in a way that is similar to the homogenization of arithmetic circuits. Let F be the formula computing f . We replace every computation gate (that computes some polynomial g) by a pair of gates (and some auxiliary gates), one computing $g(0)$ and one computing \widehat{g} . Clearly,

$$\begin{aligned} ((g + h)(0), \widehat{g + h}) &= (g(0) + h(0), \widehat{g} + \widehat{h}) && \text{(addition gate)}, \\ ((g \cdot h)(0), \widehat{g \cdot h}) &= (g(0) \cdot h(0), g(0) \cdot \widehat{h} + \widehat{g} \cdot h(0) + \widehat{g} \cdot \widehat{h}) && \text{(multiplication gate)}. \end{aligned}$$

Therefore, an addition gate is just replaced by 2 addition gates, while a multiplication gate is replaced by 4 multiplication gates and 2 addition gates (and this gadget has depth 3). We copy the subformulas of $g(0)$, $h(0)$, \widehat{g} , and \widehat{h} , which maintains the depth, and it keeps the size $\text{poly}(s)$. In this construction additions happen only between constants or between non-constants, but never between a constant and a non-constant. Therefore each maximal subformula of constant gates can be evaluated and replaced with a single constant gate, and these gates are multiplied with non-constant gates (with the one exception of the gate for $f(0)$). But in a formula, scaling a non-constant gate by a field element *does not* require a multiplication gate, and instead we can recursively pass this scaling operation down to the children, as explained before this lemma. At the end we remove the one remaining constant gate for $f(0)$ and are done.

For circuits we proceed similarly. We skip the depth reduction step. Let C be the formula computing f . We replace every computation gate (that computes some polynomial g) by a pair of gates (and some auxiliary gates), one computing $g(0)$ and one computing \widehat{g} . Clearly, for addition and multiplication gates, we can do the following:

$$\begin{aligned} ((\alpha g + \beta h)(0), \widehat{\alpha g + \beta h}) &= (\alpha g(0) + \beta h(0), \alpha \widehat{g} + \beta \widehat{h}), \\ ((\alpha g \cdot \beta h)(0), \widehat{\alpha g \cdot \beta h}) &= (\alpha g(0) \cdot \beta h(0), \alpha g(0) \cdot \beta \widehat{h} + \alpha \widehat{g} \cdot \beta h(0) + \alpha \widehat{g} \cdot \beta \widehat{h}). \end{aligned}$$

Therefore, an addition gate is just replaced by 2 addition gates, while a multiplication gate is replaced by 4 multiplication gates and 2 addition gates (and this gadget has depth 3). Here we have no need to copy subformulas, and we re-use the computation instead. In this construction additions happen only between constants or between non-constants, but never between a constant and a non-constant. Therefore each maximal subcircuit of constant gates can be evaluated and replaced with a single constant gate v , and each of these gates is multiplied with a non-constant gate w (with the one exception of the gate for $f(0)$). This rescaling of the polynomial computed at w can be simulated by just rescaling all the edge labels of the outgoing edges of w , so v can be removed. At the end we also remove the one remaining constant gate for $f(0)$ and are done. ◀

A circuit/formula that is the sum of an IHL circuit/formula and a field constant is called an IHL^+ circuit/formula. The following corollary is obvious.

► **Corollary 6.3.** *VP is the set of p -families for which the IHL^+ circuit size is polynomially bounded. VF is the set of p -families for which the IHL^+ formula size is polynomially bounded.*

Proof. Use Lemma 6.2 to compute \widehat{f} . The missing constant $f(0)$ can be added to the IHL circuit/formula as the very last operation. ◀

6.2 IHL Ben-Or and Cleve is Exactly Kumar's complexity for 3×3 Matrices

Quite surprisingly, the 3×3 matrix analogue of Kumar's complexity model (see (1)) turns out to be the homogeneous version of Ben-Or and Cleve's construction [1], as the proof of the following Proposition 6.4 shows. Let $E_{i,j}$ denote the 3×3 matrix with a 1 at the entry (i, j) and zeros elsewhere. Let id_3 denote the 3×3 identity matrix.

► **Proposition 6.4.** *Fix $i, j \in \{1, 2, 3\}$, $i \neq j$. Let f be a polynomial admitting an IHL formula of depth δ . Then there exist 3×3 matrices A_1, \dots, A_r with $r \leq 4^\delta$ having homogeneous linear entries such that*

$$f \cdot E_{i,j} = (\text{id}_3 + A_1)(\text{id}_3 + A_2) \cdots (\text{id}_3 + A_r) - \text{id}_3.$$

Proof. Consider the six positions $\{(i, j) \mid 1 \leq i, j \leq 3, i \neq j\}$ of the zeros in the 3×3 unit matrix. Given an IHL formula, to each input gate and to each computation gate we assign one of the 6 positions in the following way. We start at the root and assign it position (i, j) . We proceed by assigning position labels recursively: For a summation gate with position (i', j') , both summands get position (i', j') . For a product gate with position (i', j') , one factor gets position (i', k) and the other gets position (k, j') , $k \neq i', k \neq j'$. We now prove by induction on the depth D of the gate g (the depth of a gate is the depth of its subformula: the input have depth 0; the root has the highest depth) with position (i', j') that for each gate there is a list of at most 4^D matrices (A_1, \dots, A_r) such that

$$(\text{id}_3 + A_1)(\text{id}_3 + A_2) \cdots (\text{id}_3 + A_r) = \text{id}_3 + gE_{(i', j')}$$

and the same number of matrices B_1, \dots, B_r such that

$$(\text{id}_3 + B_1)(\text{id}_3 + B_2) \cdots (\text{id}_3 + B_r) = \text{id}_3 - gE_{(i', j')}.$$

For an input gate (i.e., depth 0) with position (i', j') and input label ℓ , we set $A_1 := \ell \cdot E_{i', j'}$ and $B_1 := -\ell \cdot E_{i', j'}$. For an addition gate with position (i', j') let (A_1, \dots, A_r) , (B_1, \dots, B_r) and $(A'_1, \dots, A'_{r'})$, $(B'_1, \dots, B'_{r'})$ be the lists coming from the induction hypothesis. We define the list for the addition gate as the concatenations $(A_1, \dots, A_r, A'_1, \dots, A'_{r'})$ and $(B_1, \dots, B_r, B'_1, \dots, B'_{r'})$. Observe that

$$(\text{id}_3 + fE_{(i', j')}) \cdot (\text{id}_3 + gE_{(i', j')}) = \text{id}_3 + (f + g)E_{(i', j')},$$

and

$$(\text{id}_3 - fE_{(i', j')}) \cdot (\text{id}_3 - gE_{(i', j')}) = \text{id}_3 - (f + g)E_{(i', j')}.$$

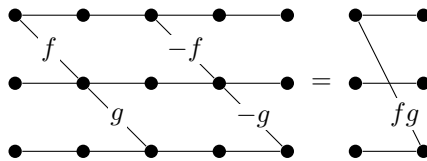
so this case is correct. For a product gate with position (i', j') let (A_1, \dots, A_r) , (B_1, \dots, B_r) and $(A'_1, \dots, A'_{r'})$, $(B'_1, \dots, B'_{r'})$ be the lists coming from the induction hypothesis, i.e., $(\text{id}_3 + A_1)(\text{id}_3 + A_2) \cdots (\text{id}_3 + A_r) = \text{id}_3 + fE_{(i', k)}$, $(\text{id}_3 + B_1)(\text{id}_3 + B_2) \cdots (\text{id}_3 + B_r) = \text{id}_3 - fE_{(i', k)}$, $(\text{id}_3 + A'_1)(\text{id}_3 + A'_2) \cdots (\text{id}_3 + A'_{r'}) = \text{id}_3 + gE_{(k, j')}$, $(\text{id}_3 + B'_1)(\text{id}_3 + B'_2) \cdots (\text{id}_3 + B'_{r'}) = \text{id}_3 - gE_{(k, j')}$. Observe that

$$(\text{id}_3 + fE_{(i', k)})(\text{id}_3 + gE_{(k, j')})(\text{id}_3 - fE_{(i', k)})(\text{id}_3 - gE_{(k, j')}) = \text{id}_3 + fgE_{(i', j')}$$

and analogously

$$(\text{id}_3 - fE_{(i', k)})(\text{id}_3 + gE_{(k, j')})(\text{id}_3 + fE_{(i', k)})(\text{id}_3 - gE_{(k, j')}) = \text{id}_3 - fgE_{(i', j')}.$$

For illustration, in the notation of [5] the product with position $(1,3)$ can be depicted as follows.



Since $4 \cdot 4^{D-1} = 4^D$, the size bound is satisfied. ◀

Since the trace of a matrix can sometimes be preferable to the (i, j) -entry, we present the result with the trace, provided approximations are allowed.

► **Proposition 6.5.** *For every IHL formula of depth δ there exist $\leq 4^\delta$ many 3×3 matrices A_i with homogeneous linear entries over $\mathbb{C}[\epsilon, \epsilon^{-1}]$ and $\alpha \in \mathbb{C}[\epsilon, \epsilon^{-1}]$ such that*

$$E_{1,1} \cdot f = \lim_{\epsilon \rightarrow 0} \left(\alpha \left((\text{id}_3 + A_1)(\text{id}_3 + A_2) \cdots (\text{id}_3 + A_r) - \text{id}_3 \right) \right)$$

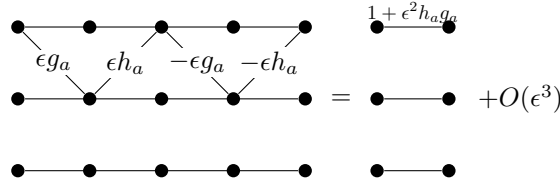
and hence

$$f = \lim_{\epsilon \rightarrow 0} \text{tr} \left(\alpha \left((\text{id}_3 + A_1)(\text{id}_3 + A_2) \cdots (\text{id}_3 + A_r) - \text{id}_3 \right) \right).$$

Proof. The IHL formula is a sum of products of subformulas $g_1 \cdot h_1, g_2 \cdot h_2, \dots, g_r \cdot h_r$, and $r \leq 2^\delta$ by induction. We compute subformulas for $\epsilon g_1, -\epsilon g_1, \epsilon h_1, -\epsilon h_1, \epsilon g_2, -\epsilon g_2, \dots, -\epsilon h_r$ as in the proof of Proposition 6.4 with position (1, 2) for each $\pm \epsilon g_i$ and position (2, 1) for each $\pm \epsilon h_i$. It turns out that

$$M_a := (\text{id}_3 + \epsilon g_a E_{1,2})(\text{id}_3 + \epsilon h_a E_{2,1})(\text{id}_3 - \epsilon g_a E_{1,2})(\text{id}_3 - \epsilon h_a E_{2,1}) = \text{id}_3 + \epsilon^2 f_a g_a E_{1,1} + O(\epsilon^3).$$

Pictorially:



Hence $M_1 M_2 \cdots M_r = \text{id}_3 + \epsilon^2 (h_1 g_1 + h_2 g_2 + \cdots + h_r g_r) E_{1,1} + O(\epsilon^3)$. We choose $\alpha = \epsilon^{-2}$. ◀

Recall, $\text{nce}_{n,d}(X_1, \dots, X_n) := \sum_{1 \leq I_1 < I_2 < \cdots < I_d \leq n} X_{I_1} \cdots X_{I_d}$, is the elementary symmetric polynomial in noncommuting variables X_1, \dots, X_n . For any $L : \mathbb{C}^{3 \times 3} \rightarrow \mathbb{C}$, let $\text{nce}_{L,n,d} := L \circ \text{nce}_d(A_1, A_2, \dots, A_n)$, where each $A_i = \begin{pmatrix} 0 & x_{1,2,i} & x_{1,3,i} \\ x_{2,1,i} & 0 & x_{2,3,i} \\ x_{3,1,i} & x_{3,2,i} & 0 \end{pmatrix}$ is a 3×3 matrix of 6 fresh variables. We denote by nce_L the corresponding graded p-family. To be formally precise, we set $\text{nce}_{L,n,0} = 1$. In particular, L can be taken to be the trace.

► **Corollary 6.6.** *Fix any nonzero linear form L on the space of 3×3 matrices. If L is supported outside the main diagonal, then the graded p-family nce_L is VF-complete under homogeneous linear projections. If L is supported on the main diagonal, then the graded p-family nce_L is VF-complete under homogeneous linear border projections.*

Proof. Given a ungraded p-family $g \in \text{VF}$. We apply Brent's depth reduction and then Lemma 6.2 to every homogeneous component of every g_n to obtain IHL formulas $f_{n,d}$ of logarithmic depth and polynomial size in n (d is polynomial in n). The first case is treated with Proposition 6.4, the second is treated completely analogously with Proposition 6.5. We only handle the slightly more difficult second case. We obtain $4^{O(\log n)} = \text{poly}(n)$ many matrices A_i with

$$f_n = \lim_{\epsilon \rightarrow 0} L \left(\alpha \left((\text{id}_3 + A_1)(\text{id}_3 + A_2) \cdots (\text{id}_3 + A_r) - \text{id}_3 \right) \right)$$

Note that $\alpha \in \mathbb{C}[\epsilon, \epsilon^{-1}]$ can be assumed to be a scalar times a power of ϵ , because lower order terms have no effect on the limit. Since $f_{n,d}$ is homogeneous of degree d , we have

$$f_{n,d} = \lim_{\epsilon \rightarrow 0} L \left(\alpha \text{nce}_{n,d}(A_1, \dots, A_r) \right) = \lim_{\epsilon \rightarrow 0} L \left(\text{nce}_{n,d}(\sqrt[d]{\beta} \epsilon^k A'_1, \dots, \alpha \sqrt[d]{\beta} \epsilon^k A'_r) \right)$$

where A'_i arises from A_i by replacing every ϵ by ϵ^d . ◀

While Corollary 6.6 gives the first collection that is VF-complete under homogeneous linear projection, we found simpler polynomials with similar properties. In the next sections we will prove that the parity-alternating elementary symmetric polynomial is hard for the class V3F under homogeneous linear projections, which gives a polynomial that is just barely more complicated than the elementary symmetric polynomial.

6.3 IHL Computation with Arity 3 Products

In the light of [5] we now study the 2×2 analogues of Proposition 6.4, Proposition 6.5, Corollary 6.6. In order to do so, in this section we study IHL formulas and circuits where the additions have arity 2, but the products have *arity exactly 3*. We call this basis the *arity 3 basis*. This turns out to be rather subtle, because one would usually want to simulate an arity 2 product by an arity 3 product in which one of the factors is a constant 1, but that violates the IHL property. A circuit/formula of this type is called an *IHL circuit/formula over the arity 3 basis*. If a polynomial is computed by an IHL formula or circuit over the arity 3 basis, then all its homogeneous even-degree components are zero, hence we have to adjust this definition slightly: For an even degree homogeneous polynomial we want to compute all partial derivatives instead. Formally, a *graded IHL circuit/formula over the arity 3 basis* is a circuit/formula of the following syntactic structure:

$$f = f(0) + \sum_{d \in 2\mathbb{N}+1} \underbrace{f_d}_{\text{IHL, arity 3}} + \sum_{\substack{d \in 2\mathbb{N} \\ d \geq 2}} \frac{1}{d} \sum_{i=1}^m x_i \cdot \underbrace{\partial f_d / \partial x_i}_{\text{IHL, arity 3}},$$

where each homogeneous f_d and homogeneous $\partial f_d / \partial x_i$ is computed by an IHL circuit/formula over the arity 3 basis. Euler's homogeneous function theorem ensures that the right-hand side actually computes f . We define V3P and V3F as follows:

► **Definition 6.7** (V3P and V3F). *V3P (respectively, V3F) is the class of p -families for which the graded IHL circuit (respectively, formula) complexity over the arity 3 basis is polynomially bounded.*

We have the following inclusion among the classes:

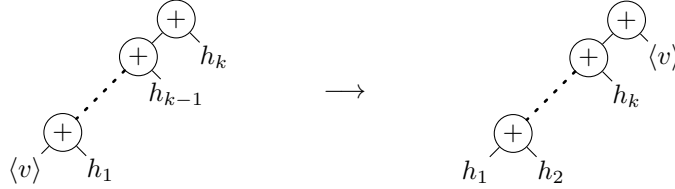
$$\text{V3F} \subseteq \text{VF} \subseteq \text{V3P} \cap \text{VBP} \subseteq \text{VP}, \tag{2}$$

where $\text{V3F} \subseteq \text{VF}$ is obvious, and we prove the first inclusion in Theorem 6.11, while it is well-known that $\text{VF} \subseteq \text{VBP}$. It is known that if we go to quasipolynomial complexity instead of polynomial complexity, the three classical classes coincide: $\text{VQF} = \text{VQBP} = \text{VQP}$, which is an immediate corollary of the circuit depth reduction result of Valiant-Berkowitz-Skyum-Rackoff [35]. We prove in Theorem 6.14 that our two new classes also belong to this set: All classes in (2) coincide if we go to quasipolynomial complexity instead of polynomial complexity, see (6).

The following proposition is an adaption of Brent's depth reduction [4] and it shows that instead of polynomially sized formulas we can work with formulas of logarithmic depth. Both properties, IHL and the arity 3 basis, require some modifications to Brent's original argument.

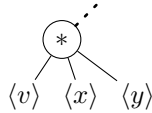
► **Proposition 6.8** (Brent's depth reduction for graded IHL formulas over the arity 3 basis). *Let f be a polynomial computed by a graded IHL formula of size s over the arity 3 basis. Then there exists a graded IHL formula over the arity 3 basis of size $\text{poly}(s)$ and depth $O(\log(s))$ computing f .*

Proof. We discuss only the homogeneous odd-degree case, because the more general case directly follows from it. The construction is recursive, just as in Brent's original argument. We follow the description in [30]. We start at the root and keep picking the child with the larger subformula until we reach a vertex v with $\frac{1}{3}s \leq |\langle v \rangle| \leq \frac{2}{3}s$, where $\langle v \rangle$ is the subformula at the gate v . We make a case distinction. In the first case we assume that on the path from v to the root (excluding v) there is no product gate. We reorder the gates as follows:



The construction applied to a size s formula gives $\text{Depth}(s) \leq \text{Depth}(\frac{2}{3}s) + 1$. The resulting size is $\text{Size}(s) \leq 2 \cdot \text{Size}(\frac{2}{3}s) + 1$.

In the second case we assume that v is the child of a product gate.

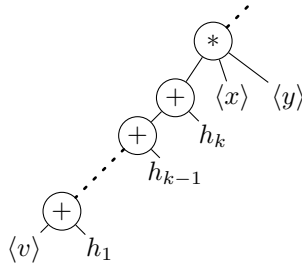


We now replace $\langle v \rangle$ by a new variable α and $\langle x \rangle$ by a new variable β . We observe that the resulting polynomial F (interpreted as a bivariate polynomial in α and β) is *linear* in the product $\alpha\beta$. Therefore $F(\alpha, \beta) = \alpha\beta(F(1, 1) - F(0, 0)) + F(0, 0)$. Both $F(0, 0)$ and $F(1, 1)$ can be realized as an IHL formula over the arity 3 basis (because an arity 3 product gate with two 1s as inputs can be replaced by just the third input, and an arity 3 product gate with two 0s as input can be replaced by a constant 0, which can be simulated by removing gates), so we obtain:



The construction on a size s formula gives $\text{Depth}(s) \leq \text{Depth}(\frac{2}{3}s) + 2$. The resulting size is: $\text{Size}(s) \leq 5 \cdot \text{Size}(\frac{2}{3}s) + 3$.

In the third case we assume that on the path from v to the root (excluding v) there are addition gates and then a product gate, so



Proof. Let id_2 denote the 2×2 identity matrix. $\varphi(C) \subseteq \mathbf{VF}$ follows from the fact that $C_{n,d}$ is the homogeneous degree d component of the product $(\text{id}_2 + X_1) \cdots (\text{id}_2 + X_n)$ of 2×2 matrices.

We prove $\forall 3F$ -hardness. Given a logdepth formula for a homogeneous degree d polynomial f . Let $E_{\text{odd}} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and let $E_{\text{even}} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. We are given a formula for a homogeneous degree d polynomial f . We can assume that the gates are additions and negative cubes ($x \mapsto -x^3$), because $xyz = \frac{1}{24}((x+y+z)^3 - (x+y-z)^3 - (x-y+z)^3 + (x-y-z)^3)$, and the rescalings by $(\pm 24)^{-\frac{1}{3}}$ can be pushed to the input gates. We first treat the case of d being odd. We write $A \simeq B$ if A and B are parametrized by ϵ and both limits $\lim_{\epsilon \rightarrow 0} A$ and $\lim_{\epsilon \rightarrow 0} B$ exist and coincide with each other. We prove by induction on the depth D of a gate that there exist $\leq 3^D$ homogeneous linear forms ℓ_1, \dots, ℓ_r over $\mathbb{C}[\epsilon, \epsilon^{-1}, \alpha]$ such that

$$\alpha f \cdot E_{\text{odd}} \simeq (\text{id}_2 + \ell_1 E_{\text{odd}})(\text{id}_2 + \ell_2 E_{\text{even}}) \cdots (\text{id}_2 + \ell_r E_{\text{odd}}) - \text{id}_2$$

The induction starting at an input gate with label ℓ is done by $\ell_1 = \alpha \ell$. The addition gate is handled as follows. By induction hypothesis there exist ℓ_1, \dots, ℓ_r and $\ell'_1, \dots, \ell'_{r'}$ with

$$\alpha f \cdot E_{\text{odd}} + \text{id}_2 \simeq (\text{id}_2 + \ell_1 E_{\text{odd}})(\text{id}_2 + \ell_2 E_{\text{even}}) \cdots (\text{id}_2 + \ell_r E_{\text{odd}}) \quad \text{and}$$

$$\alpha g \cdot E_{\text{odd}} + \text{id}_2 \simeq (\text{id}_2 + \ell'_1 E_{\text{odd}})(\text{id}_2 + \ell'_2 E_{\text{even}}) \cdots (\text{id}_2 + \ell'_{r'} E_{\text{odd}})$$

Therefore $\alpha(f+g) \cdot E_{\text{odd}} + \text{id}_2 = (\alpha f \cdot E_{\text{odd}} + \text{id}_2)(\alpha g \cdot E_{\text{odd}} + \text{id}_2) \simeq$

$$(\text{id}_2 + \ell_1 E_{\text{odd}})(\text{id}_2 + \ell_2 E_{\text{even}}) \cdots (\text{id}_2 + \ell_r E_{\text{odd}})(\text{id}_2 + \ell'_1 E_{\text{odd}})(\text{id}_2 + \ell'_2 E_{\text{even}}) \cdots (\text{id}_2 + \ell'_{r'} E_{\text{odd}})$$

Handling the negative cube gates is more subtle (the negative squaring gates are also the subtle cases in [5]). By induction hypothesis we have ℓ_1, \dots, ℓ_r such that

$$\alpha f \cdot E_{\text{odd}} \simeq (\text{id}_2 + \ell_1 E_{\text{odd}})(\text{id}_2 + \ell_2 E_{\text{even}}) \cdots (\text{id}_2 + \ell_r E_{\text{odd}}) - \text{id}_2 \quad (5)$$

We replace each ϵ by ϵ^k in each ℓ_i , with k so large that even when we replace α by ϵ^{-1} or $-\epsilon^{-1}$, we still have the equivalence of the LHS and RHS mod ϵ^2 .

We call the resulting linear forms ℓ'_i . It follows that

$$\alpha f \cdot E_{\text{odd}} \equiv ((\text{id}_2 + \ell'_1 E_{\text{odd}})(\text{id}_2 + \ell'_2 E_{\text{even}}) \cdots (\text{id}_2 + \ell'_r E_{\text{odd}}) - \text{id}_2) \pmod{\epsilon^k}$$

Setting α to ϵ^{-1} we obtain

$$\epsilon^{-1} f \cdot E_{\text{odd}} \equiv ((\text{id}_2 + \ell''_1 E_{\text{odd}})(\text{id}_2 + \ell''_2 E_{\text{even}}) \cdots (\text{id}_2 + \ell''_r E_{\text{odd}}) - \text{id}_2) \pmod{\epsilon^2}$$

Analogously with $\alpha = -\epsilon^{-1}$:

$$-\epsilon^{-1} f \cdot E_{\text{odd}} \equiv ((\text{id}_2 + \tilde{\ell}'_1 E_{\text{odd}})(\text{id}_2 + \tilde{\ell}'_2 E_{\text{even}}) \cdots (\text{id}_2 + \tilde{\ell}'_r E_{\text{odd}}) - \text{id}_2) \pmod{\epsilon^2}$$

The induction hypothesis (5) also implies (set ϵ to ϵ^3 and α to $\epsilon^2 \alpha$) that

$$\epsilon^2 \alpha f \cdot E_{\text{odd}} \equiv ((\text{id}_2 + \ell'''_1 E_{\text{odd}})(\text{id}_2 + \ell'''_2 E_{\text{even}}) \cdots (\text{id}_2 + \ell'''_r E_{\text{odd}}) - \text{id}_2) \pmod{\epsilon^3}$$

Transposing gives

$$\epsilon^2 \alpha f \cdot E_{\text{even}} \equiv ((\text{id}_2 + \ell'''_r E_{\text{even}})(\text{id}_2 + \ell'''_{r-1} E_{\text{odd}}) \cdots (\text{id}_2 + \ell'''_1 E_{\text{even}}) - \text{id}_2) \pmod{\epsilon^3}$$

We now observe:

$$(\epsilon^{-1} f E_{\text{odd}} + \text{id}_2 + \epsilon^2 g_1)(\epsilon^2 \alpha f E_{\text{even}} + \text{id}_2 + \epsilon^3 g_2)(-\epsilon^{-1} f E_{\text{odd}} + \text{id}_2 + \epsilon^2 g_3) \simeq -\alpha f^3 E_{\text{odd}} + \text{id}_2.$$

Pictorially:

At the end, setting $\alpha = 1$ we obtain

$$\alpha f \cdot E_{\text{odd}} \simeq (\text{id}_2 + \ell_1 E_{\text{odd}})(\text{id}_2 + \ell_2 E_{\text{even}}) \cdots (\text{id}_2 + \ell_r E_{\text{odd}}) - \text{id}_2.$$

Observe that r is only polynomially large, because we started with a formula of logarithmic depth. Since f is homogeneous of degree d , this implies

$$f \simeq \text{nce}_{r,d}(\ell_1 E_{\text{odd}}, \ell_2 E_{\text{even}}, \dots, \ell_r E_{\text{odd}})_{1,2} = C_{r,d}(\ell_1, \dots, \ell_r).$$

We now treat the case where f has even degree, using an argument similar to the one from Proposition 6.5. By the above construction, for each i we find

$$\alpha \left(\frac{1}{d} \partial f / \partial x_i \right) \cdot E_{\text{odd}} \simeq (\text{id}_2 + \ell_{i,1} E_{\text{odd}})(\text{id}_2 + \ell_{i,2} E_{\text{even}}) \cdots (\text{id}_2 + \ell_{i,r_i} E_{\text{odd}}) - \text{id}_2.$$

We replace all ϵ by ϵ^3 , replace all α by ϵ , and lastly add id_2 :

$$\epsilon \left(\frac{1}{d} \partial f / \partial x_i \right) \cdot E_{\text{odd}} + \text{id}_2 \equiv ((\text{id}_2 + \ell'_{i,1} E_{\text{odd}})(\text{id}_2 + \ell'_{i,2} E_{\text{even}}) \cdots (\text{id}_2 + \ell'_{i,r_i} E_{\text{odd}})) \pmod{\epsilon^3}.$$

Analogously, when replacing α by $-\epsilon$ instead:

$$-\epsilon \left(\frac{1}{d} \partial f / \partial x_i \right) \cdot E_{\text{odd}} + \text{id}_2 \equiv ((\text{id}_2 + \ell''_{i,1} E_{\text{odd}})(\text{id}_2 + \ell''_{i,2} E_{\text{even}}) \cdots (\text{id}_2 + \ell''_{i,r_i} E_{\text{odd}})) \pmod{\epsilon^3}.$$

We also find corresponding linear forms for the transposes. Now observe that for any polynomials a, b we have

$$\begin{aligned} & (-\epsilon a \cdot E_{\text{odd}} + \text{id}_2 + O(\epsilon^3))(-\epsilon b \cdot E_{\text{even}} + \text{id}_2 + O(\epsilon^3))(\epsilon a \cdot E_{\text{odd}} + \text{id}_2 + O(\epsilon^3))(\epsilon b \cdot E_{\text{even}} + \text{id}_2 + O(\epsilon^3)) \\ & \equiv \begin{pmatrix} 1 + \epsilon^2 a \cdot b & 0 \\ 0 & 1 - \epsilon^2 a \cdot b \end{pmatrix} \pmod{\epsilon^3}. \end{aligned}$$

Pictorially:

Let $M(c) := \begin{pmatrix} 1 + \epsilon^2 c & 0 \\ 0 & 1 - \epsilon^2 c \end{pmatrix}$. Now note that

$$(M(a_1 b_1) + O(\epsilon^3)) \cdots (M(a_n b_n) + O(\epsilon^3)) \equiv M(a_1 b_1 + a_2 b_2 + \cdots + a_n b_n) \pmod{\epsilon^3}.$$

Setting $a_i = x_i$ and $b_i = \frac{1}{d} \partial f / \partial x_i$, and using Euler's homogeneous function theorem, we obtain polynomially many linear forms ℓ_1, \dots, ℓ_r so that

$$M(f) \equiv ((\text{id}_2 + \ell_1 E_{\text{odd}})(\text{id}_2 + \ell_2 E_{\text{even}}) \cdots (\text{id}_2 + \ell_r E_{\text{even}})) \pmod{\epsilon^3}$$

Subtracting id_2 on both sides and taking the degree d homogeneous part of the $(1, 1)$ entry:

$$\epsilon^2 f \equiv \underbrace{\text{nce}_{r,d}(\ell_1 E_{\text{odd}}, \ell_2 E_{\text{even}}, \dots, \ell_r E_{\text{even}})_{1,1}}_{=C_{r,d}(\ell_1, \dots, \ell_r)} \pmod{\epsilon^3}$$

We replace all ϵ by $\epsilon^{d/2}$, to get $\epsilon^d f \equiv C_{r,d}(\ell'_1, \dots, \ell'_r) \pmod{\epsilon^{3d/2}}$. Therefore, $f \simeq C_{r,d}(\epsilon^{-1} \cdot \ell'_1, \dots, \epsilon^{-1} \cdot \ell'_r)$. Both cases together prove that $C_{n,d}$ is V3F-hard under homogeneous linear border projections. The VQP-hardness under quasipolynomial homogeneous linear border projections now follows from Theorem 6.14. \blacktriangleleft

6.5 Converting Formulas to Circuits Over the Arity 3 Basis

In this section we prove the following theorem.

► **Theorem 6.11.** $\text{VF} \subseteq \text{V3P}$.

Proof. Let $h \in \text{VF}$, i.e., by Brent's depth reduction, h has formulas of polynomial size and logarithmic depth. We treat the homogeneous components f of g_n independently. If f is of even degree, observe that if f has a formula of depth δ , then $\partial f / \partial x_i$ has a formula of depth 2δ (by induction, using the sum and product rules of derivatives), which by Lemma 6.2 implies the existence of an IHL formula of depth $O(\delta)$ (note that $\partial f / \partial x_i$ is homogeneous of odd degree). Now we apply the odd-degree argument below for each partial derivative independently.

Let f be of odd degree. As a first step we convert the IHL formula into an IHL formula for which at each gate either all even homogeneous components vanish or all odd homogeneous components vanish. The construction is similar to the Lemma 6.2 and works as follows. We replace each gate v by two gates v_{odd} and v_{even} , where at v_{even} the sum of the even degree components is computed, and at v_{odd} the sum of the odd degree components is computed. Let $f = f_{\text{even}} + f_{\text{odd}}$ be the decomposition of f into the even homogeneous parts and the odd homogeneous parts. $((f + g)_{\text{even}}, (f + g)_{\text{odd}}) = (f_{\text{even}} + g_{\text{even}}, f_{\text{odd}} + g_{\text{odd}})$ so a sum gate is replaced by two sum gates. Moreover, $((f \cdot g)_{\text{even}}, (f \cdot g)_{\text{odd}}) = (f_{\text{even}} \cdot g_{\text{even}} + f_{\text{odd}} \cdot g_{\text{odd}}, f_{\text{even}} \cdot g_{\text{odd}} + f_{\text{odd}} \cdot g_{\text{even}})$, so a product gate is replaced by 4 product gates and 2 summation gates. Here we use that the depth was logarithmic.

We now convert such a formula to an IHL circuit with the same number of gates, but over the arity 3 basis. This part is a bit subtle, and therefore we do it more formally below. We replace each even degree gate v that computes g with a gate that computes $z \cdot g$, where z is a dummy variable. Addition gates are not changed. For product gates there are three cases.

- A product gate v of two odd-degree polynomials f and g . By induction we have an IHL circuit over the arity 3 basis for f and for g . We construct the arity 3 product $z \times f \times g$.
- A product gate v that has an odd-degree polynomial f at its child w , and that has an even-degree polynomial g at its child u . By induction we have IHL circuits C and D over the arity 3 basis for f and for zg , respectively. We take C and D , delete all instances of z in D , and feed there the output of C instead. The resulting circuit computes fg .
- A product of an even-degree polynomial f and an even-degree polynomial g . By induction we have IHL circuits C and D over the arity 3 basis for zf and for zg , respectively. We take C and D , delete all instances of z in D , and feed there the output of C instead. The resulting circuit computes zfg .

The size of the resulting circuit is less or equal to the size of the formula (even though the depth can increase in this construction). ◀

► **Remark 6.12.** Even when starting with a formula of logarithmic depth, the resulting circuit does not necessarily have logarithmic depth, hence we do not obtain $\text{VF} = \text{V3F}$. This is because in the second bullet point we rearrange the circuit structure when we replace z .

► **Remark 6.13.** We also do not get $\text{VP} = \text{V3P}$, because note that the replacements of z in the second and third bullet point can only be done, because in a formula the outdegree of each gate is at most 1, i.e., we do not reuse computation results. After we replace z by f in a subcircuit that computes zg , the original subcircuit computing zg will be gone and cannot be reused.

6.6 Valiant-Skyum-Berkowitz-Rackoff Over the Arity 3 Basis

► **Theorem 6.14.** $VQ3F = VQ3P$.

Proof. The entire argument is over the arity 3 basis and each homogeneous component is treated separately. Given a size s circuit that computes an odd-degree polynomial, we use Theorem 6.15 below to obtain a circuit of size $\text{poly}(s)$ and depth $O(\log^2(s))$ that computes the same polynomial. We unfold the circuit to a formula of the same depth. The size is hence $3^{O(\log^2(s))} = s^{O(\log s)}$. If $s = n^{\text{poly}(\log(n))}$, then $s^{O(\log s)} = n^{\text{poly}(\log(n))}$ ³. The even-degree case is done by treating each partial derivative independently. ◀

Since we know that $VQF = VQBP = VQP$ and $VQ3F = VQF = VQ3P$, the situation of (2) simplifies:

$$VQ3F = VQF = VQBP = VQP = VQ3P. \quad (6)$$

The following Theorem 6.15 is needed in the proof of Theorem 6.14. It lifts the classical Valiant-Skyum-Berkowitz-Rackoff [35] circuit depth reduction to the arity 3 basis. The argument is an adaption of the original argument.

► **Theorem 6.15** (VSBR depth reduction for IHL circuits over the arity 3 basis). *Let f be a polynomial computed by a graded IHL circuit of size s over the arity 3 basis, $\deg(f) = d$. Then there exists a graded IHL circuit over the arity 3 basis of size $O(\text{poly}(s))$ and depth $O(\log(s) \cdot \log d)$ computing f .*

Proof. We adapt the proof from [30]. We treat only the homogeneous odd case, because all summands can be treated independently, and in the even degree case we can treat each partial derivative independently. We work entirely over the arity 3 basis (and hence compute a polynomial whose even degree homogeneous parts all vanish), so every circuit and subcircuit is over the arity 3 basis, and every product is of arity 3.

A circuit whose root is an arity 3 product gate is denoted by $x \times y \times z$. A circuit whose root is an arity 2 addition gate is denoted by $x + y$, just as usual. Notationally, we use the same notation for gates, for their subcircuits, and for the polynomials they compute. If we want to specifically highlight that we talk about the circuit with root w , then we write $\langle w \rangle$. We write $v \leq u$ if v is contained in the subcircuit with root u . We write $C \equiv C'$ to denote that the circuits C and C' compute the same polynomial.

Let z be a new dummy variable. Let the circuit $[u : v]$ be defined via $[u : v] := z$ if $u = v$, and if $u \neq v$ we have

$$[u : v] := \begin{cases} 0 & \text{if } u \text{ is a leaf} \\ [u_1 : v] + [u_2 : v] & \text{if } u = u_1 + u_2 \\ [u_1 : v] \times u_2 \times u_3 & \text{if } u = u_1 \times u_2 \times u_3 \text{ and } u_1 \text{ has the highest degree} \\ & \text{among } \{[u_1], [u_2], [u_3]\} \end{cases}$$

It can be seen by induction that $[u : v]$ is zero or a homogeneous polynomial of degree $\deg u - \deg v + 1$, and $[u : v]$ is zero or is homogeneous linear in z . If $w \not\leq u$, then $[u : w] = 0$. For a circuit C we write $[u : v]_C := [u : v](z \leftarrow C)$, where \leftarrow means that all leaves labelled z are replaced by the output of the circuit C .

We define a set of gates that is called the m -frontier \mathcal{F}_m via $\mathcal{F}_m := \{u \mid u = u_1 \times u_2 \times u_3 \text{ with } \deg u_1, \deg u_2, \deg u_3 \leq m \text{ and } \deg(u) > m\}$.

³ $(n^{\log^i(n)})^{\log^j(n^{\log^i(n)})} = n^{\log^{i+j}(n)}$

► **Lemma 6.16.** Fix a pair (u, m) with $\deg u > m$. Let $\mathcal{F} := \mathcal{F}_m$. Then $u \equiv \sum_{w \in \mathcal{F}} [u : w]_{\langle w \rangle}$.

Proof. For the proof we fix m and do induction on the *depth* of u , i.e., the position of u in any fixed topological ordering of the gates. Since for every gate u with $\deg(u) > m$ there exists some gate $u' \in \mathcal{F} \cap \langle u \rangle$, the induction start is the case $u \in \mathcal{F}$. In this case, since \mathcal{F} is an antichain, it follows that $\sum_{w \in \mathcal{F}} [u : w] = 0 + [u : u] = z$, and hence $\sum_{w \in \mathcal{F}} [u : w]_{\langle w \rangle} = [u : u]_{\langle u \rangle} = z_{\langle u \rangle} = u$. This proves that case $u \in \mathcal{F}$. Now, let $u \notin \mathcal{F}$. If u is an addition gate:

$$\begin{aligned} u &= u_1 + u_2 \stackrel{\text{I.H.}}{\equiv} \sum_{w \in \mathcal{F}} [u_1 : w]_{\langle w \rangle} + \sum_{w \in \mathcal{F}} [u_2 : w]_{\langle w \rangle} \equiv \sum_{w \in \mathcal{F}} \left([u_1 : w]_{\langle w \rangle} + [u_2 : w]_{\langle w \rangle} \right) \\ &= \sum_{w \in \mathcal{F}} \left([u_1 : w] + [u_2 : w] \right)_{\langle w \rangle} \stackrel{\text{Def.}}{\equiv} \sum_{w \in \mathcal{F}} [u : w]_{\langle w \rangle} \end{aligned}$$

If u is a multiplication gate, note that $u \notin \mathcal{F}$, so one of the children has degree $> m$ (w.l.o.g. that child is called u_1):

$$\begin{aligned} u &= u_1 \times u_2 \times u_3 \stackrel{\text{I.H.}}{\equiv} \left(\sum_{w \in \mathcal{F}} [u_1 : w]_{\langle w \rangle} \right) \times u_2 \times u_3 \equiv \sum_{w \in \mathcal{F}} \left([u_1 : w]_{\langle w \rangle} \times u_2 \times u_3 \right) \\ &= \sum_{w \in \mathcal{F}} \left([u_1 : w] \times u_2 \times u_3 \right)_{\langle w \rangle} \stackrel{\text{Def.}}{\equiv} \sum_{w \in \mathcal{F}} [u : w]_{\langle w \rangle} \blacktriangleleft \end{aligned}$$

► **Lemma 6.17.** Fix a pair (u, m, v) with $\deg u > m \geq \deg v$. Let $\mathcal{F} := \mathcal{F}_m$.

$$[u : v] \equiv \sum_{w \in \mathcal{F}} [u : w]_{[w:v]}.$$

Proof. For the proof we fix m and v and do induction on the *depth* of u , i.e., the position of u in any fixed topological ordering of the gates. Since for every gate u with $\deg(u) > m$ there exists some gate $u' \in \mathcal{F} \cap \langle u \rangle$, the induction start is the case $u \in \mathcal{F}$. In this case, since \mathcal{F} is an antichain, it follows that $\sum_{w \in \mathcal{F}} [u : w]_{[w:v]} \equiv z_{[u:v]} = [u : v]$. This proves that case $u \in \mathcal{F}$. Now, let $u \notin \mathcal{F}$. Since $\deg u > m$ and $m \geq \deg v$ we have $u \neq v$. If u is an addition gate:

$$\begin{aligned} [u : v] &\stackrel{\text{Def. } (u \neq v)}{\equiv} [u_1 : v] + [u_2 : v] \stackrel{\text{I.H.}}{\equiv} \sum_{w \in \mathcal{F}} [u_1 : w]_{[w:v]} + \sum_{w \in \mathcal{F}} [u_2 : w]_{[w:v]} \\ &\equiv \sum_{w \in \mathcal{F}} \left([u_1 : w]_{[w:v]} + [u_2 : w]_{[w:v]} \right) = \sum_{w \in \mathcal{F}} \left([u_1 : w] + [u_2 : w] \right)_{[w:v]} \\ &\stackrel{\text{Def.}}{\equiv} \sum_{w \in \mathcal{F}} [u : w]_{[w:v]} \end{aligned}$$

If u is a multiplication gate, note that $u \notin \mathcal{F}$, so one of the children has degree $> m$ (w.l.o.g. that child is called u_1):

$$\begin{aligned} [u : v] &\stackrel{\text{Def. } (u \neq v)}{\equiv} [u_1 : v] \times u_2 \times u_3 \stackrel{\text{I.H.}}{\equiv} \left(\sum_{w \in \mathcal{F}} [u_1 : w]_{[w:v]} \right) \times u_2 \times u_3 \\ &\equiv \sum_{w \in \mathcal{F}} \left([u_1 : w]_{[w:v]} \times u_2 \times u_3 \right) = \sum_{w \in \mathcal{F}} \left([u_1 : w] \times u_2 \times u_3 \right)_{[w:v]} \\ &\stackrel{\text{Def.}}{\equiv} \sum_{w \in \mathcal{F}} [u : w]_{[w:v]} \blacktriangleleft \end{aligned}$$

We now construct the shallow circuit so that the degree of each child in a multiplication gate decreases from δ to $\lceil \frac{2}{3}\delta \rceil$, so the multiplication depth (i.e., the number of multiplications on a path from leaf to root) is at most $O(\log d)$. Here we allow arity 5 multiplication gates. These can be simulated by two arity 3 multiplication gates. We construct the circuit by induction on the degree, and we construct it in a way that each u and each $[u : w]_{\langle v \rangle}$ are computed at some gate, so the size of the resulting circuit is at most $O(s^3)$. The addition gates between the multiplications can be balanced, so that we have at most $O(\log s)$ depth in each addition tree. This gives a total depth of $\log d \cdot \log s$.

6.7 The construction for u .

$$\begin{aligned} u &\stackrel{\text{Lem. 6.16}}{\equiv} \sum_{w \in \mathcal{F}} [u : w]_{\langle w \rangle} = \sum_{w \in \mathcal{F}} [u : w]_{\langle w_1 \rangle} \times w_2 \times w_3 \\ &= \sum_{\substack{w \in \mathcal{F} \\ \deg(u) \geq \deg(w)}} [u : w]_{\langle w_1 \rangle} \times w_2 \times w_3 \equiv \sum_{\substack{w \in \mathcal{F} \\ \deg(u) \geq \deg(w)}} [u : w]_{\langle w_3 \rangle} \times w_2 \times w_1 \end{aligned}$$

This explicit rearrangement of w_1 and w_3 is necessary and goes beyond [35]. Choose $m = \lceil \frac{2}{3} \deg u \rceil$. Recall $\deg w_i \leq m$, so we already have two of the three cases: $\deg w_1 \leq \lceil \frac{2}{3} \deg u \rceil$ and $w_2 \leq \lceil \frac{2}{3} \deg u \rceil$. But we also know $\deg(u) \geq \deg(w) = \deg(w_1) + \deg(w_2) + \deg(w_3)$, hence w.l.o.g. $\deg(w_3) \leq \lfloor \frac{1}{3} \deg(u) \rfloor$. Therefore $\deg u - \deg w + \deg w_3 \leq \underbrace{\lfloor \frac{4}{3} \deg u - \deg w \rfloor}_{> m} < \frac{2}{3} \deg u$.

6.8 The construction for $[u : v]$.

We use fractions and “.” multiplication signs when we do not have a circuit implementation in the intermediate equalities on polynomials. We write $w = w_1 \times w_2 \times w_3$ for $w \in \mathcal{F}$.

$$\begin{aligned} [u : v] &\stackrel{\text{Lem. 6.17}}{\equiv} \sum_{w \in \mathcal{F}} [u : w]_{[w : v]} = \sum_{\substack{w \in \mathcal{F} \\ \deg(u) \geq \deg(w)}} \frac{[u : w]}{z} \cdot [w : v] \\ &= \frac{1}{z} \sum_{\substack{w \in \mathcal{F} \\ \deg(u) \geq \deg(w)}} [u : w] \cdot [w_1 : v] \cdot w_2 \cdot w_3 \equiv \sum_{\substack{w \in \mathcal{F} \\ \deg(u) \geq \deg(w)}} [u : w]_{\langle w_3 \rangle} \times [w_1 : v] \times w_2 \\ &\stackrel{\text{Lem. 6.16}}{\equiv} \sum_{\substack{w \in \mathcal{F} \\ \deg(u) \geq \deg(w)}} [u : w]_{\langle w_3 \rangle} \times [w_1 : v] \times \left(\sum_{\substack{y \in \mathcal{F}' \\ \deg(w_2) \geq \deg(y)}} [w_2 : y]_{\langle y_3 \rangle} \times y_2 \times y_1 \right) \\ &\equiv \sum_{\substack{w \in \mathcal{F} \\ \deg(u) \geq \deg(w)}} \sum_{\substack{y \in \mathcal{F}' \\ \deg(w_2) \geq \deg(y)}} [u : w]_{\langle w_3 \rangle} \times [w_1 : v] \times ([w_2 : y]_{\langle y_3 \rangle} \times y_2 \times y_1) \end{aligned}$$

We set $m = \lceil \frac{2}{3}(\deg u + \deg v) \rceil$ and $m' = \lceil \frac{2}{3} \deg w_2 \rceil$. We calculate the degrees of the five factors:

- $\deg u - \deg w + \deg w_3 \leq (\deg u - \deg w) + \lfloor \frac{1}{3} \deg u \rfloor \leq \lfloor \frac{4}{3} \deg u \rfloor - m \leq \lceil \frac{2}{3}(\deg u - \deg v) \rceil$
- $\deg w_1 - \deg v + 1 \leq \deg w_1 \leq m \leq \lceil \frac{2}{3}(\deg u - \deg v) \rceil$
- $\deg w_2 - \deg y + \deg y_3 \leq \lfloor \frac{4}{3} \deg w_2 \rfloor - \lceil \frac{2}{3} \deg w_2 \rceil \leq \lceil \frac{2}{3} \deg w_2 \rceil \leq \lceil \frac{2}{3}(\deg u - \deg v) \rceil$
- $\deg y_2 \leq \lceil \frac{2}{3} \deg w_2 \rceil \leq \lceil \frac{2}{3}(\deg u - \deg v) \rceil$, and analogously for $\deg y_1$.

The rescaling constants on the edges can be set in the straightforward way. ◀

References

- 1 M. Ben-Or and R. Cleve. Computing algebraic formulas using a constant number of registers. *SIAM J. Comput.*, 21(21):54–58, 1992. doi:10.1137/0221006.
- 2 D. Bini. Relations between exact and approximate bilinear algorithms. Applications. *Calcolo*, 17(1):87–97, 1980. doi:10.1007/BF02575865.
- 3 D. Bini, M. Capovani, G. Lotti, and F. Romani. $O(n^{2.7799})$ complexity for $n \times n$ approximate matrix multiplication. *Inform. Process. Lett.*, 8(5):234–235, 1979. doi:10.1016/0020-0190(79)90113-3.
- 4 R. P. Brent. The Parallel Evaluation of General Arithmetic Expressions. *J. Assoc. Comput. Mach.*, 21(2):201–206, 1974. doi:10.1145/321812.321815.
- 5 K. Bringmann, C. Ikenmeyer, and J. Zuiddam. On Algebraic Branching Programs of Small Width. *J. ACM*, 65(5):32:1–32:29, 2018. doi:10.1145/3209663.
- 6 W. Buczyńska and J. Buczyński. Secant varieties to high degree Veronese reembeddings, catalecticant matrices and smoothable Gorenstein schemes. *J. Alg. Geom.*, 23(1):63–90, 2014.
- 7 W. Buczyńska and J. Buczyński. Apolarity, border rank, and multigraded Hilbert scheme. *Duke Math. J.*, 170(16):3659 – 3702, 2021. doi:10.1215/00127094-2021-0048.
- 8 P. Bürgisser. *Completeness and Reduction in Algebraic Complexity Theory*, volume 7 of *Algorithms and Computation in Mathematics*. Springer Verlag, 2000.
- 9 P. Bürgisser. The Complexity of Factors of Multivariate Polynomials. *Found. Comp. Math.*, 4(4):369–396, 2004. doi:10.1007/s10208-002-0059-5.
- 10 P. Bürgisser, M. Clausen, and M. A. Shokrollahi. *Algebraic complexity theory*, volume 315 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1997.
- 11 P. Bürgisser, C. Ikenmeyer, and G. Panova. No occurrence obstructions in geometric complexity theory. *J. Amer. Math. Soc.*, 32(1):163–193, 2019. doi:10.1090/jams/908.
- 12 P. Bürgisser, J. M. Landsberg, L. Manivel, and J. Weyman. An overview of mathematical issues arising in the Geometric Complexity Theory approach to $VP \neq VNP$. *SIAM J. Comput.*, 40(4):1179–1209, 2011. doi:10.1137/090765328.
- 13 A. Cayley. On the theory of linear transformations. *Cambridge Math. J.*, iv:193–209, 1845.
- 14 A. Clebsch. Zur Theorie der algebraischen Flächen. *J. Reine Angew. Math.*, 58:93–108, 1861.
- 15 P. Dutta, F. Gesmundo, C. Ikenmeyer, G. Jindal, and V. Lysikov. De-bordering and Geometric Complexity Theory for Waring rank and related models. arXiv:2211.07055, 2022.
- 16 W. Fulton and J. Harris. *Representation theory: a first course*, volume 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991.
- 17 A. Iarrobino and V. Kanev. *Power sums, Gorenstein algebras, and determinantal loci*, volume 1721 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1999. doi:10.1007/BFb0093426.
- 18 C. Ikenmeyer. *Geometric complexity theory, tensor rank, and Littlewood-Richardson coefficients*. PhD thesis, Universität Paderborn, 2013.
- 19 C. Ikenmeyer and G. Panova. Rectangular Kronecker coefficients and plethysms in geometric complexity theory. *Adv. Math.*, 319:40–66, 2017. doi:10.1016/j.aim.2017.08.024.
- 20 C. Ikenmeyer and A. Sanyal. A note on VNP-completeness and border complexity. *Information Processing Letters*, 176:106243, 2022.
- 21 J. Jelisiejew. Pathologies on the Hilbert scheme of points. *Inventiones mathematicae*, 220(2):581–610, 2020.
- 22 J. Jelisiejew and T. Mańdziuk. Limits of saturated ideals. arXiv:2210.13579, pages 1–31, 2022.
- 23 H. Kadish and J. M. Landsberg. Padded polynomials, their cousins, and geometric complexity theory. *Comm. Algebra*, 42(5):2171–2180, 2014. doi:10.1080/00927872.2012.758268.
- 24 H. Kraft. *Geometrische Methoden in der Invariantentheorie*. Aspects of Mathematics, D1. Friedr. Vieweg & Sohn, Braunschweig, 1984.
- 25 M. Kumar. On the power of border of depth-3 arithmetic circuits. *ACM Trans. Comput. Theory*, 12(1):5:1–5:8, 2020. doi:10.1145/3371506.

- 26 D. Medini and A. Shpilka. Hitting Sets and Reconstruction for Dense Orbits in VP_e and $\Sigma\Pi\Sigma$ Circuits. *36th Computational Complexity Conference (CCC 2021)*, 200:19:1–19:27, 2021. doi:10.4230/LIPIcs.CCC.2021.19.
- 27 K. D. Mulmuley and M. Sohoni. Geometric Complexity Theory I: An Approach to the P vs. NP and Related Problems. *SIAM J. Comput.*, 31(2):496–526, 2001. doi:10.1137/S009753970038715X.
- 28 K. D. Mulmuley and M. Sohoni. Geometric Complexity Theory II: Towards explicit obstructions for embeddings among class varieties. *SIAM J. Computing*, 38(3):1175–1206, 2008.
- 29 F. Palatini. Sulle superficie algebriche i cui $S_h(h+1)$ -seganti non riempiono lo spazio ambiente. *Atti della R. Acc. delle Scienze di Torino*, 41:634–640, 1906.
- 30 R. Saptharishi. *A survey of lower bounds in arithmetic circuit complexity*. Github Survey, 2021. URL: <https://github.com/dasarpmar/lowerbounds-survey/releases/tag/v9.0.3>.
- 31 J. J. Sylvester. On the principles of the calculus of forms. *J. Cambridge and Dublin Math.*, 7:52–97, 1852.
- 32 A. Terracini. Sulle v_k per cui la varietà degli $s_h(h+1)$ -seganti ha dimensione minore dell'ordinario. *Rend. Circ. Mat.*, 31:392–396, 1911.
- 33 S. Toda. Classes of arithmetic circuits capturing the complexity of computing the determinant. *IEICE Transactions on Information and Systems*, 75(1):116–124, 1992.
- 34 L. G. Valiant. Completeness classes in algebra. In *Proceedings of the 11th Annual ACM Symposium on Theory of Computing*, pages 249–261, 1979. doi:10.1145/800135.804419.
- 35 L. G. Valiant, S. Skyum, S. Berkowitz, and C. Rackoff. Fast parallel computation of polynomials using few processors. *SIAM J. Comput.*, 12(4):641–644, 1983. doi:10.1137/0212043.