Linear Projections of the Vandermonde Polynomial

C. Ramya B. V. Raghavendra Rao

Department of Computer Science and Engineering
IIT Madras, Chennai, INDIA
{ramya,bvrr}@cse.iitm.ac.in

Abstract

An n-variate Vandermonde polynomial is the determinant of the $n \times n$ matrix where the ith column is the vector $(1, x_i, x_i^2, \ldots, x_i^{n-1})^T$. Vandermonde polynomials play a crucial role in the theory of alternating polynomials and occur in Lagrangian polynomial interpolation as well as in the theory of error correcting codes. In this work we study structural and computational aspects of linear projections of Vandermonde polynomials.

Firstly, we consider the problem of testing if a given polynomial is linearly equivalent to the Vandermonde polynomial. We obtain a deterministic polynomial time algorithm to test if f is linearly equivalent to the Vandermonde polynomial when f is given as product of linear factors. In the case when f is given as a black-box our algorithm runs in randomized polynomial time. Exploring the structure of projections of Vandermonde polynomials further, we describe the group of symmetries of a Vandermonde polynomial and show that the associated Lie algebra is simple. Finally, we study arithmetic circuits built over projections of Vandermonde polynomials. We show universality property for some of the models and obtain a lower bounds against sum of projections of Vandermonde determinant.

1 Introduction

The $n \times n$ symbolic Vandermonde matrix is given by

$$V = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ x_1 & x_2 & \cdots & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & \cdots & x_n^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & \cdots & x_n^{n-1} \end{bmatrix} \tag{1}$$

where $x_1, \ldots, x_n$ are variables. The determinant of the symbolic Vandermonde matrix is a homogeneous polynomial of degree $\binom{n}{2}$ given by $\mathsf{VD_n}(\mathsf{x_1}, \ldots, \mathsf{x_n}) \triangleq \mathsf{det}(V) = \prod_{i<j}(x_i - x_j)$ and is known as the n-variate *Vandermonde polynomial*. An *alternating polynomial* is one that changes sign when any two variables of $\{x_1, \ldots, x_n\}$ are swapped. Vandermonde polynomials are central to the theory of alternating polynomials. In fact, any alternating polynomial is divisible by the Vandermonde polynomial [11, 6]. Further, Vandermonde

matrix and Vandermonde polynomial occur very often in the theory of error correcting codes and are useful in Lagrangian interpolation.

Linear projections are the most important form of reductions in Algebraic Complexity Theory developed by Valiant [14]. Comparison between classes of polynomials in Valiant's theory depends on the types of linear projections. (See [1] for a detailed exposition.) Taking a geometric view on linear projections of polynomials, Mulmuley and Shohoni [10] proposed the study of geometry of orbits of polynomials under the action of $\mathsf{GL}(n, \mathbb{F})$, i.e, the group of $n \times n$ non-singular matrices over $\mathbb{F}$. This lead to the development of Geometric Complexity Theory, whose primary objective is to classify families of polynomials based on the geometric and representation theoretic structure of their $\mathsf{GL}(n, \mathbb{F})$ orbits.

In this article, we investigate computational and structural aspects of linear projections of the family $\mathsf{VD} = (\mathsf{VD}_n)_{n \geq 0}$ of Vandermonde polynomials over the fields of real and complex numbers.

Firstly, we consider the polynomial equivalence problem when one of the polynomials is fixed to be the Vandermonde polynomial. Recall that, in the polynomial equivalence problem (POLY-EQUIV) given a pair of polynomials f and g we ask if f is equivalent to g under a non-singular linear change of variables, i.e., is there a $A \in \mathsf{GL}(n, \mathbb{F})$ such that $f(AX) = g(X)$, where $X = (x_1, \ldots, x_n)$? POLY-EQUIV is one of the fundamental computational problems over polynomials and received significant attention in the literature.

POLY-EQUIV can be solved in PSPACE over reals [2] and any algebraically closed field [12], and is in $\mathsf{NP} \cap \mathsf{co\text{-}AM}$ [13] over finite fields. However, it is not known if the problem is even decidable over the field of rational numbers [12]. Saxena [12] showed that POLY-EQUIV is at least as hard as the graph isomorphism problem even in the case of degree three forms. Given the lack of progress on the general problem, authors have focussed on special cases over the recent years. Kayal [8] showed that testing if a given polynomial f is linearly equivalent to the elementary symmetric polynomial, or to the power symmetric polynomial can be done in randomized polynomial time. Further, in [9], Kayal obtained randomized polynomial time algorithms for POLY-EQUIV when one of the polynomials is either the determinant or permanent and the other polynomial is given as a black-box.

We consider the problem of testing equivalence to Vandermonde polynomials:

> **Problem :** VD-EQUIV
> **Input :** $f \in \mathbb{F}[x_1, \ldots, x_n]$
> **Output :** Homogeneous linearly independent linear forms $L_1, L_2, \ldots, L_n$ such that $f = \mathsf{VD}(L_1, L_2, \ldots, L_n)$ if they exist, else output `'No such equivalence exists'`.

Remark 1. *Although Vandermonde polynomial is a special form of determinant, randomized polynomial time algorithm to test equivalence to determinant polynomial due to [9] does not directly give an algorithm for* VD-EQUIV.

We show that VD-EQUIV can be solved in deterministic polynomial time when f is given as a product of linear factors (Theorem 1). Combining this with Kaltofen's factorization algorithm, [7], we get a randomized polynomial time algorithm for VD-EQUIV when f is given as a black-box.

For an n-variate polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$, the group of symmetry $\mathscr{G}_f$ of f is the set of non-singular matrices that fix the polynomial f. The group of symmetry of a polynomial and the associated Lie algebra have significant importance in geometric complexity theory. More recently, Kayal [9] used the structure of Lie algebras of permanent and determinant in his algorithms for special cases of $\mathsf{POLY\text{-}EQUIV}$. Further, Grochow [5] studied the problem of testing conjugacy of matrix Lie algebras. In general, obtaining a complete description of group of symmetry and the associated Lie algebra of a given family of polynomials is an interesting task.

In this paper we obtain a description of the group of symmetry for Vandermonde polynomials (Theorem 3). Further, we show that the associated Lie algebra for Vandermonde polynomials is simple (Lemma 2).

Finally, we explore linear projections of Vandermonde polynomials as a computational model. We prove closure properties (or lack of) and lower bounds for representing a polynomial as sum of projections of Vandermonde polynomials (Section 5).

2 Preliminaries

Throughout the paper, unless otherwise stated, $\mathbb{F} \in \{\mathbb{C}, \mathbb{R}\}$. We briefly review different types of projections of polynomials that are useful for the article. For a more detailed exposition, see [1].

Definition 1. (Projections). *Let $f, g \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. We say that f is projection reducible to g denoted by $f \le g$, if there are linear forms $\ell_1, \ldots, \ell_n \in \mathbb{F}[x_1, \ldots, x_n]$ such that $f = g(\ell_1, \ldots, \ell_n)$. Further, we say*

- $f \le_{\mathsf{proj}} g$ *if* $\ell_1, \ldots, \ell_n \in \mathbb{F} \cup \{x_1, \ldots, x_n\}$.
- $f \le_{\mathsf{homo}} g$ *if $\ell_1, \ldots, \ell_n$ are homogeneous linear forms.*
- $f \le_{\mathsf{aff}} g$ *if $\ell_1, \ldots, \ell_n$ are affine linear forms.*

Based on the types of projections, we consider the following classes of polynomials that are projections of the Vandermonde polynomial.

$$\begin{aligned}
\mathsf{VD} &= \{\mathsf{VD}(x_1, x_2, \ldots, x_n) \mid n \ge 1\};\ \text{and} \\
\mathsf{VD}_{\mathsf{proj}} &= \{\mathsf{VD}(\rho_1, \rho_2, \ldots, \rho_n) \mid \rho_i \in (X \cup \mathbb{F}), \forall i \in [n]\};\ \text{and} \\
\mathsf{VD}_{\mathsf{homo}} &= \{\mathsf{VD}(\ell_1, \ell_2, \ldots, \ell_n) \mid \ell_i \in \mathbb{F}[x_1, x_2, \ldots, x_n],\ \deg(\ell_i) = 1,\ \ell_i(0) = 0\ \ \forall i \in [n]\};\ \text{and} \\
\mathsf{VD}_{\mathsf{aff}} &= \{\mathsf{VD}(\ell_1, \ell_2, \ldots, \ell_n) \mid \ell_i \in \mathbb{F}[x_1, x_2, \ldots, x_n],\ \deg(\ell_i) \le 1\ \ \forall i \in [n]\};
\end{aligned}$$

Among the different types mentioned above, the case when $\ell_1, \ldots, \ell_n$ are homogeneous and linearly independent is particularly interesting. Let $f, g \in \mathbb{F}[x_1, \ldots, x_n]$. f is said to be linearly equivalent to g (denoted by $f \equiv_{\mathsf{lin}} g$) if $g \le_{\mathsf{homo}} f$ via a set of linearly independent homogeneous linear forms $\ell_1, \ldots, \ell_n$. In the language of invariant theory, $f \equiv_{\mathsf{lin}} g$ if and only if g is in the $\mathsf{GL}(n, \mathbb{F})$ orbit of f.

The group of symmetry of a polynomial is one of the fundamental objects associated with a polynomial:

Definition 2. *Let $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. The group of symmetries of f (denoted by $\mathscr{G}_f$) is defined as:*

$$\mathscr{G}_f = \{A \mid A \in \mathsf{GL}(n, \mathbb{F}), f(A\mathsf{x}) = f(\mathsf{x})\}.$$

i.e., the group of invertible $n \times n$ matrices A such that $f(A\mathbf{x}) = A(\mathbf{x})$.

The Lie algebra of a polynomial f is the tangent space of $\mathscr{G}_f$ at the identity matrix and is defined as follows:

Definition 3 ([9]). *Let $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. Let ϵ be a formal variable with $\epsilon^2 = 0$. Then $\mathfrak{g}_f$ is defined to be the set of all matrices $A \in \mathbb{F}^{n \times n}$ such that*

$$f((\mathbf{1}_n + \epsilon A)\mathbf{x}) = f(\mathbf{x}).$$

It can be noted that $\mathfrak{g}_f$ is non-trivial only when $\mathscr{G}_f$ is a continuous group. For a random polynomial, both $\mathscr{G}_f$ as well as $\mathfrak{g}_f$ are trivial.

For a polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$, $k \geq 0$, let $\partial^{=k}(f)$ denote the $\mathbb{F}$-linear span of the set of all partial derivatives of f of order k, i.e.,

$$\partial^{=k}(f) \triangleq \mathbb{F}\text{-}\mathsf{Span}\left\{ \frac{\partial^k f}{\partial x_{i_1} \ldots \partial x_{i_k}} \,\middle|\, i_1, \ldots, i_k \in [n] \right\}.$$

3 Testing Equivalence to Vandermonde Polynomials

Recall the problem $\mathsf{VD} - \mathsf{EQUIV}$ from Section 1. In this section, we obtain an efficient algorithm for $\mathsf{VD} - \mathsf{EQUIV}$. The complexity of the algorithm depends on the input representation of the polynomials. When the polynomial is given as product of linear forms, we show:

Theorem 1. *There is a deterministic polynomial time algorithm for* $\mathsf{VD} - \mathsf{EQUIV}$ *when the input polynomial f is given as a product of homogeneous linear forms.*

The proof of Theorem 1 is based on the correctness of Algorithm 1 described next.

Algorithm 1: $\mathsf{VD} - \mathsf{EQUIV}$

Input : $f = \ell_1 \cdot \ell_2 \cdots \ell_p$
Output: 'f `is linearly equivalent to` $\mathsf{VD}(x_1, \ldots, x_n)$' if $f \equiv_{\mathsf{lin}} \mathsf{VD}$. Else '`No`'

if $p \neq \binom{n}{2}$ *for any* $n < p$ ***or*** $\dim(span\{\ell_1, \ell_2, \ldots, \ell_p\}) \neq n - 1$ **then**
    return '`No such equivalence exists`'
end
else
    $S \leftarrow \{\ell_1, \ell_2, \ldots, \ell_p\}$
    Let $T^{(0)} = \{r_1, r_2, \ldots, r_{n-1}\}$ be $n - 1$ linearly independent linear forms in S.
    $i \leftarrow 1$
    $S' \leftarrow S \setminus T^{(0)}$
    while *true* **do**
        $D_i \leftarrow \{a + b, a - b, b - a \mid a, b \in T^{(i-1)}\}$ ▷ D_i is the set of differences
        $T^{(i)} \leftarrow \{T^{(i-1)} \cup D_i\} \cap S$
        $S' \leftarrow S \setminus T^{(i)}$
        if $|S'| = 0$ **then**
            Output 'f `is linearly equivalent to` $\mathsf{VD}(x_1, \ldots, x_n)$'
            Exit.
        end
        if $T^{(i-1)} = T^{(i)}$ *and* $|S'| \neq 0$ **then**
            Output '`No such equivalence exists`'
            Exit.
        end
    end
end

As a first step, we observe that lines (1)-(3) of algorithm are correct:

Observation 1. *If* $f = \ell_1 \cdot \dots \cdot \ell_p \equiv_{\mathsf{lin}} \mathsf{VD}$ *then* $p = \binom{n}{2}$ *and* $\dim(span\{\ell_1, \ell_2, \dots, \ell_p\}) = n-1$.

Proof. Clearly if $f \equiv_{\mathsf{lin}} \mathsf{VD}$ we have $p = \binom{n}{2}$. For the second part suppose $f = \mathsf{VD}(L_1, \dots, L_n)$, for some linearly independent homogeneous linear forms $L_1, \dots, L_n$. Then $\{\ell_1, \dots, \ell_p\} = \{L_i - L_j \mid i < j\}$, and therefore $\dim(span\{\ell_1, \ell_2, \dots, \ell_p\}) = n-1$. ☐

The following theorem proves the correctness of the Algorithm 1.

Theorem 2. $f \equiv_{\mathsf{lin}} \mathsf{VD}$ *if and only if Algorithm* 1 *outputs '*`f is linearly equivalent to VD`$(x_1, \dots, x_n)$*'.*

Proof. We first argue the forward direction. Suppose there are n homogeneous linearly independent linear forms $L'_1, L'_2, \dots, L'_n$ such that $f = \ell_1 \cdot \ell_2 \cdots \ell_p = \prod_{i<j i,j\in[n]} (L'_i - L'_j)$. Consider the linear forms $L_1 = L'_1 - L'_n, \quad L_2 = L'_2 - L'_n, \cdots, L_{n-1} = L'_{n-1} - L'_n$. Then

$$f = \ell_1 \cdot \ell_2 \cdots \ell_p = \prod_{i=1}^{n-1} L_i \cdot \prod_{i<j} (L_i - L_j). \tag{2}$$

Let $S \triangleq \{\ell_1, \ell_2, \dots, \ell_p\}$ as in line (5) of the algorithm. By equation (2), we have

$$S = \{L_1, L_2, \dots, L_{n-1}\} \cup \{L_i - L_j \mid i < j, \quad i, j \in [n-1]\}.$$

Let $S_1 \triangleq \{L_1, L_2, \dots, L_{n-1}\}$ and $S_2 \triangleq \{L_i - L_j \mid i < j, \quad i, j \in [n-1]\}$. Consider the undirected complete graph G with vertices $\{v_1, v_2, \dots, v_{n-1}\}$. For every vertex $v_i \in V(G)$, let $\mathsf{label}(v_i)$ denote the linear form L_i associated with the vertex v_i. Similarly for every edge $e = (v_i, v_j) \in E(G)$ let $\mathsf{label}(e)$ be defined as follows :

$$\mathsf{label}(e) = \begin{cases} L_i - L_j & \text{if } i < j \\ L_j - L_i & \text{if } j < i \end{cases} \tag{3}$$

Using notations used in line (5) of Algorithm 1, we have $\{r_1, r_2, \dots, r_{n-1}\} \subseteq S$. Observe that for every $i \in [n-1]$ the linear form r_i corresponds to either a vertex or an edge label in G. Let $Q_1 \triangleq \{r_1, r_2, \dots, r_{n-1}\} \cap S_1$ and $Q_2 \triangleq \{r_1, r_2, \dots, r_{n-1}\} \cap S_2$. Suppose $|Q_2| = k$ and $|Q_1| = n - k - 1$, linear forms in Q_1 correspond to labels of vertices in $V(G)$ and linear forms in Q_2 correspond to labels of edges in $E(G)$. For some $k \geq 0$, let

$$\begin{aligned} Q_1 &= \{\mathsf{label}(u_1), \mathsf{label}(u_2), \dots, \mathsf{label}(u_{n-k-1})\} && \text{for } u_1, u_2, \dots, u_{n-k-1} \in V(G) \\ Q_2 &= \{\mathsf{label}(e_1), \mathsf{label}(e_2), \dots, \mathsf{label}(e_k)\} && \text{for } e_1, e_2, \dots, e_k \in E(G) \end{aligned}$$

Let $G[r_1, \dots, r_{n-1}]$ denote the sub-graph $\{u_1, \dots, u_{n-k-1}\} \cup \{e_1, \dots, e_k\}$, i.e., consisting of edges with labels in Q_2 and vertices incident on them and vertices with labels in Q_1.

We need the following claim:

Claim 2.1. *For any choice of linearly independent linear forms* $\{r_1, r_2, \dots, r_{n-1}\}$ *by the algorithm in line* (5)*, any connected component* C *in* $G[r_1, r_2, \dots, r_{n-1}]$ *has exactly one vertex with label in* Q_1*. More formally, if* $Q_C \triangleq \left(\bigcup_{v\in Q_1} \mathsf{label}(v)\right) \bigcap \left(\bigcup_{w\in V(C)} \mathsf{label}(w)\right)$ *then* $|Q_C| = 1$.

Proof of Claim 2.1. Proof is by contradiction. Suppose there is a connected component C in $G[r_1, r_2, \ldots, r_{n-1}]$ with $|Q_C| \geq 2$. Let $v_i, v_j \in Q_C$. Assume without loss of generality that $i < j$. Consider the path $\bar{P} = (v_i, e_{c_1}, e_{c_2}, \ldots, e_{c_{|\bar{P}|-1}}, v_j)$ between v_i and v_j in the connected component C, where $e_{c_1}, \ldots, e_{c_{|\bar{P}|-1}}$ are edges. From the definition of G, we know that there are constants $\alpha_1, \ldots \alpha_{|\bar{P}|-1} \in \{-1, 1\}$ such that

$$\alpha_1 \mathsf{label}(e_{c_1}) + \alpha_2 \mathsf{label}(e_{c_2}) + \cdots + \alpha_{|\bar{P}|-1} \mathsf{label}(e_{c_{|\bar{P}|-1}}) = \mathsf{label}(v_i) - \mathsf{label}(v_j).$$

Therefore, $\{\mathsf{label}(v_i), \mathsf{label}(e_{c_1}), \mathsf{label}(e_{c_2}), \ldots, \mathsf{label}(e_{c_{|\bar{P}|-1}}), \mathsf{label}(v_j)\}$ is a linearly dependent set. Since C is a connected component in $G[r_1, r_2, \ldots, r_{n-1}]$ we have that the set of linear forms $\{\mathsf{label}(v_i), \mathsf{label}(e_{c_1}), \mathsf{label}(e_{c_2}), \ldots, \mathsf{label}(e_{c_{|\bar{P}|-1}}), \mathsf{label}(v_j)\} \subseteq \{r_1, r_2, \ldots, r_{n-1}\}$, hence a contradiction. Now, suppose there exists a connected component C with $Q_C = \emptyset$. Let v be any vertex in C. Clearly, $\{\mathsf{label}(v) \cup \{r_1, \ldots, r_{n-1}\}\}$ is a linearly independent set, a contradiction since $\dim(\mathbb{F}\text{-}\mathsf{span}(S)) = n - 1$. $\square$

Now, the following claim completes the proof of the forward direction:

Claim 2.2. *(i) If $f \equiv_{\mathsf{lin}} \mathsf{VD}$ then there exists an m such that $\{L_1, L_2, \ldots, L_{n-1}\} \subseteq T^{(m)}$.*

(ii) For any m, if $\{L_1, L_2, \ldots, L_{n-1}\} \subseteq T^{(m)}$ then the set $T^{(m+1)} = S$ and the algorithm outputs 'f `is linearly equivalent to` $\mathsf{VD}(x_1, \ldots, x_n)$' *in line 14.*

Proof of Claim 2.2. (i) Let C be a connected component in $G[r_1, \ldots, r_{n-1}]$. By Claim 2.1 we have $|Q_C| = 1$. Let $Q_C = \{b\}$ and $L = \mathsf{label}(b)$. We argue by induction on i that for every vertex $v \in V(C)$ with $dist(L, v) \leq i$, $\mathsf{label}(v) \in T^{(i)}$. Base case is when $i = 0$ and follows from the definition of $T^{(0)}$. For the induction step, let $u \in V(C)$ be such that $(u, v) \in E(G[r_1, \ldots, r_{n-1}])$ and $dist(L, u) \leq i - 1$. By the induction hypothesis, we have $\mathsf{label}(u) \in T^{(i-1)}$. Also, since $\mathsf{label}(u, v) \in \{r_1, \ldots, r_{n-1}\} = T^{(0)}$, we have $\mathsf{label}(u, v) \in T^{(i-1)}$. By line 10 of the algorithm, the linear form $\mathsf{label}(u, v) + \mathsf{label}(u) \in D_i$ where D_i is the set of differences in the i^{th} iteration of the while loop. Now, by the definition of labels in 3, $(L_v - L_u) + L_u \in D_i$ if $v < u$ or $L_u - (L_u - L_v) \in D_i$ if $u < v$. In any case, $L_v = \mathsf{label}(v) \in T^{(i)}$ as required. Now, if $m \geq n - 1$ then we have $\{L_1, \ldots, L_{n-1}\} \subseteq T^{(m)}$. (ii) If $\{L_1, L_2, \ldots, L_{n-1}\} \subseteq T^{(m)}$ then clearly $T^{(m)} \cup D_m = S$. Hence $T^{(m+1)} = S$ and algorithm outputs 'f `is linearly equivalent to` $\mathsf{VD}(x_1, \ldots, x_n)$' in line 14. $\square$

Suppose Algorithm 1 outputs 'f `is linearly equivalent to` $\mathsf{VD}(x_1, \ldots, x_n)$' in k steps. Consider the polynomial $\mathsf{VD}(\ell, r_1, r_2, \ldots, r_{n-1})$ where $\{r_1, r_2, \ldots, r_{n-1}\}$ is the linearly independent set chosen in line 5 of Algorithm 1 and ℓ is an arbitrary linear form such that the set $\{\ell, r_1, r_2, \ldots, r_{n-1}\}$ is linearly independent. Then, we have $\ell_1 \ell_2 \cdots \ell_p = \mathsf{VD}(\ell, \ell - r_1, \ell - r_2, \ldots, \ell - r_{n-1})$. $\square$

Corollary 1. $\mathsf{VD} - \mathsf{EQUIV}$ *is in* RP *when f is given as a black-box.*

Proof. The result immediately follows from Algorithm 2 and Theorem 1.

Algorithm 2: $\mathsf{VD-EQUIV-2}$

Input : $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ as a black-box

Output: 'f `is linearly equivalent to` $\mathsf{VD}(x_1, \ldots, x_n)$' if $f \equiv_{\mathsf{lin}} \mathsf{VD}$. Else '`No such equivalence exists`'

Run Kaltofen's factorization Algorithm [7]
if *f is irreducible* **then**
  Output '`No such equivalence exists`'
end
else
  Let $B_1, B_2, \ldots, B_p$ be black-boxes to the irreducible factors of f obtained from Kaltofen's Algorithm.
  Interpolate the black-boxes $B_1, \ldots, B_p$ to get the explicit linear forms $\ell_1, \ell_2, \ldots, \ell_p$ respectively.
  Run Algorithm 1 with $\ell_1 \ldots \ell_p$ as input.
end

□

Finally, in the black-box setting we show:

Corollary 2. PIT *is polynomial time equivalent to* $\mathsf{VD-EQUIV}$ *in the black-box setting.*

Proof. Since polynomial factorization is polynomial time equivalent to PIT in the black-box setting, by Theorem 1 we have, $\mathsf{VD-EQUIV} \leq_P \mathsf{PIT}$. For the converse direction, let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial of degree d. Given black-box access to f we construct black-box to a polynomial g such that $f \equiv 0$ if and only if $g \equiv_{\mathsf{lin}} \mathsf{VD}$. Consider the polynomial $g = x_1^{\binom{n}{2}+1} f + \mathsf{VD}(x_1, x_2, \ldots, x_n)$. If $f \equiv 0$ then clearly $g = \mathsf{VD}(x_1, x_2, \ldots, x_n)$. If $f \not\equiv 0$ then $\deg(g) > \binom{n}{2}$ and hence g is not linearly equivalent to VD. Observe that given black-box access to f we can construct in polynomial time a black-box for g. □

4 Group of symmetries and Lie algebra of Vandermonde determinant

In this section we characterize the group of symmetries and Lie algebra of the Vandermonde polynomial.

Theorem 3. *Let* VD *denote the determinant of the symbolic $n \times n$ Vandermonde matrix. Then,*

$$\mathscr{G}_{\mathsf{VD}} = \{(I + (v \otimes 1)) \cdot P \mid P \in A_n, v \in \mathbb{F}^n\}$$

where A_n is the alternating group on n elements.

Proof. We first argue the forward direction. Let $A = B + (v \otimes 1)$ where $B \in A_n$ and $v = (v_1, v_2, \ldots, v_n) \in \mathbb{F}^n$. We show that $A \in \mathscr{G}_{\mathsf{VD}}$: Let σ be the permutation defined by the permutation matrix B. Then the transformation defined by A is $A \cdot x_i = x_{\sigma(i)} + \sum_{i=1}^n v_i x_i$. Now it is easy to observe that $\prod_{i<j}(x_i - x_j) = \prod_{i<j}((A \cdot x_i) - (A \cdot x_j))$. Therefore $A \in \mathscr{G}_{\mathsf{VD}}$.

For the converse direction, consider $A \in \mathscr{G}_{\mathsf{VD}}$. To show that $A = B + (v \otimes 1)$ where $B \in A_n$ and $v = (v_1, v_2, \ldots, v_n) \in \mathbb{F}^n$. A defines a linear transformation on the set of variables $\{x_1, x_2, \ldots, x_n\}$ and let $\ell_i = A \cdot x_i$. We have $\prod_{i<j}(x_i - x_j) = \prod_{i<j}(\ell_i - \ell_j)$. By unique factorization of polynomials, we have that there exists a bijection $\sigma : \{(i,j) \mid i < j\} \to \{(i,j) \mid i < j\}$ such that $\sigma(i,j) = (i',j')$ iff $\ell_i - \ell_j = x_{i'} - x_{j'}$.

We now show that the σ is induced by a permutation $\pi \in S_n$:

Claim 3.1. *Let σ be as defined above. Then there exists a permutation π of $\{1,\ldots,n\}$ such that $\sigma(i,j) = (\pi(i), \pi(j))$.*

Proof of Claim 3.1 : Let G be a complete graph on n vertices such that edge (i,j) is labelled by $(\ell_i - \ell_j)$ for $i < j$. Let H be the complete graph on n vertices with the edge (i,j) labelled by $(x_i - x_j)$ for $i < j$. Now σ can be viewed as a bijection from $E(G)$ to $E(H)$. It is enough to argue that for any $1 \leq i \leq n$,

$$\begin{aligned}\sigma(\{(1,i),(2,i),\ldots,(i-1,i),(i,i+1),\ldots,(i,n)\}) = \\ \{(1,k_i),(2,k_i),\ldots,(k_i-1,k_i),(k_i,k_i+1),\ldots,(k_i,n)\}\end{aligned} \quad (4)$$

for some unique $k_i \in [n]$. Then $\pi : i \mapsto k_i$ is the required permutation.
For the sake of contradiction, suppose that (4) is not satisfied for some $i \in [n]$. Then there are distinct $j,k,m \in [n]$ such that the edges $\{(i,j),(i,k),(i,m)\}$ in G under σ map to edges in $\{(\alpha,\beta),(\gamma,\delta),(\eta,\kappa)\}$ in H where the edges $(\alpha,\beta),(\gamma,\delta)$ and (η,κ) do not form a star in H. Note that $\alpha,\beta,\gamma,\delta,\eta,\kappa$ need not be distinct. Various possibilities for the vertices $\alpha,\beta,\gamma,\delta,\eta,\kappa$ and the corresponding vertex-edge incidences in H are depicted in the Figure 1. Observe that in the figure the edges are labelled with a $\pm$ sign to denote that based on whether $i < j$ or $j < i$ one of $+$ or $-$ is chosen.

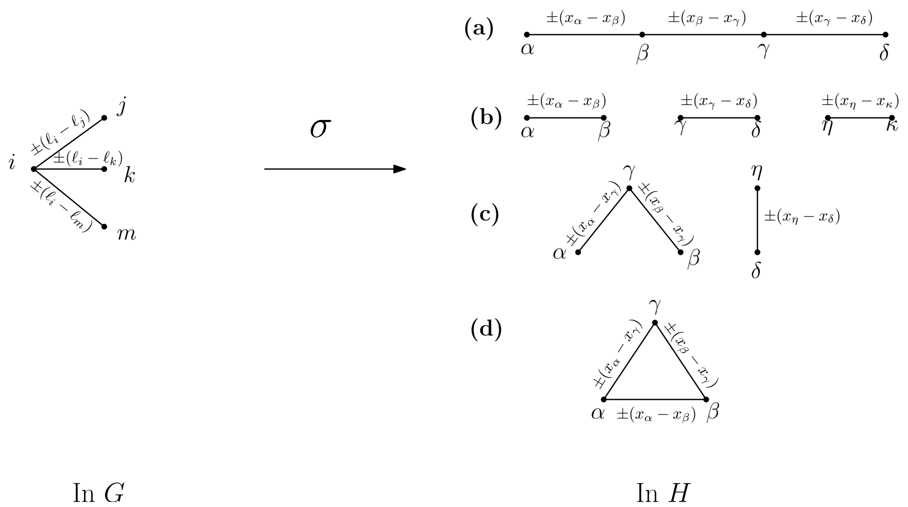

Figure 1: The map σ on vertex i in G

Recall that we have,

$$\forall i < j \quad |\mathsf{var}(\ell_i - \ell_j)| = 2. \quad (5)$$

We denote by P the edges $\{(i,j),(i,k),(i,m)\}$ in G. Consider the following two cases :

Case 1 : P in G maps to one of $(a),(b)$ or (c) in H under σ (see Figure 1). In each of the possibilities, it can be seen that there exist linear forms ℓ' and ℓ'' in $\{\ell_i,\ell_j,\ell_k,\ell_m\}$ such that $|\mathsf{var}(\pm(\ell' - \ell''))| = 4$ which is a contradiction to Equation 5.

Case 2 : P in G maps to (d) in H under σ (see Figure 1). Without loss of generality suppose $\sigma(i,j) = (\alpha, \beta)$, $\sigma(i,k) = (\alpha, \gamma)$ and $\sigma(i,m) = (\beta, \gamma)$. Recall that $\sigma(i,j) = (i', j')$ if and only if $\ell_i - \ell_j = x_{i'} - x_{j'}$. Then we get $\ell_j - \ell_k = x_\beta - x_\gamma$ by the definition of σ. Therefore, we have $\sigma(j,k) = (\beta, \gamma) = \sigma(i,m)$ which is a contradiction since σ is a bijection.

Therefore, for all $1 \le i \le n$, Equation 4 is satisfied and there exists a permutation π such that $\sigma(i,j) = (\pi(i), \pi(j))$. $\triangleleft$

Let P_π be the permutation matrix corresponding to the permutation π obtained from the claim above. To complete the proof, we need to show that $A = P_\pi + (v \otimes 1)$ for $v \in \mathbb{F}^n$. Let

$$\begin{aligned} \ell_1 &= a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ \ell_2 &= a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ &\vdots \\ \ell_n &= a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \end{aligned}$$

Now suppose π is the identity permutation, i.e., $\sigma(i,j) = (i,j)$ for all $i < j$, therefore $\ell_1 - \ell_2 = x_1 - x_2, \ell_1 - \ell_2 = x_1 - x_2, \ldots, \ell_1 - \ell_n = x_1 - x_n$. Now, we have the following system of linear equations

$$\begin{gathered} a_{11} - a_{21} = 1,\ a_{12} - a_{22} = -1,\ a_{13} - a_{23} = 0, a_{14} - a_{24} = 0, \ldots, a_{1n} - a_{2n} = 0 \\ a_{11} - a_{31} = 1,\ a_{12} - a_{32} = 0,\ a_{13} - a_{33} = -1, a_{14} - a_{34} = 0, \ldots, a_{1n} - a_{3n} = 0 \\ \vdots \\ a_{11} - a_{n1} = 1,\ a_{12} - a_{n2} = 0,\ a_{13} - a_{n3} = 0, a_{14} - a_{n4} = 0, \ldots, a_{1n} - a_{nn} = -1. \end{gathered}$$

From the equations above, it follows that when π is the identity permutation, $A - I = v \otimes 1$ for some $v \in \mathbb{F}^n$ where 1 is the vector with all entries as 1. When π is not identity, it follows from the above arguments that $\pi^{-1}A = I + v \otimes 1$ for some $v \in \mathbb{F}^n$. Since $\mathsf{VD}((I + v \otimes 1)X) = \mathsf{VD}(X)$, we conclude that $\pi \in A_n$. $\square$

Now we show that Vandermonde polynomial are characterized by its group of symmetry $\mathscr{G}_{\mathsf{VD}}$.

Lemma 1. *Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a homogeneous polynomial of degree $\binom{n}{2}$. If $\mathscr{G}_f = \mathscr{G}_{\mathsf{VD}}$ then $f(x_1, \ldots, x_n) = \alpha \cdot \mathsf{VD}(x_1, \ldots, x_n)$ for some $\alpha \in \mathbb{F}$.*

Proof. Let $f \in \mathbb{F}[x_1, \ldots, x_n]$. Since $\mathscr{G}_f = \mathscr{G}_{\mathsf{VD}} = \{(I + (v \otimes 1)) \cdot P \mid P \in A_n, v \in \mathbb{F}^n\}$, $\mathscr{G}_f \cap S_n = A_n$. Hence f is an alternating polynomial. By the fundamental theorem of alternating polynomials [4, 11], there exists a symmetric polynomial $g \in \mathbb{F}[x_1, \ldots, x_n]$ such that $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n) \cdot \mathsf{VD}(x_1, \ldots, x_n)$. Since $\deg(f) = \binom{n}{2} = \deg(\mathsf{VD}(x_1, \ldots, x_n))$, $g = \alpha$ for some $\alpha \in \mathbb{F}$. $\square$

Using the description of $\mathscr{G}_{\mathsf{VD}}$ above, we now describe the Lie algebra of $\mathscr{G}_{\mathsf{VD}}$.

Lemma 2. *We have $\mathfrak{g}_{\mathsf{VD}} = \{v \otimes 1 \mid v \in \mathbb{F}^n\}$.*

Proof. We have

$$\begin{aligned} A \in \mathfrak{g}_{\mathsf{VD}} &\iff \prod_{i>j}(x_i - x_j + \epsilon(A(x_i) - A(x_j))) = \prod_{i>j}(x_i - x_j) \\ &\iff A(x_i) = A(x_j) \quad \forall i \neq j \\ &\iff A = v \otimes 1 \quad \text{for some } v \in \mathbb{F}^n. \end{aligned}$$

$\square$

Definition 4. (Simple Lie Algebra). *A lie algebra $\mathfrak{g}$ is said to be simple if it is a non-abelian lie algebra whose only ideals are $\{0\}$ and $\mathfrak{g}$ itself.*

Corollary 3. $\mathfrak{g}_{\mathsf{VD}} = \{v \otimes 1 \mid v \in \mathbb{F}^n\}$ *is a simple Lie Algebra.*

Proof. Let $\mathfrak{g} = \mathfrak{g}_{\mathsf{VD}}$. Suppose , let $I \subseteq \mathfrak{g}$ such that $I \neq \{0\}$ and $I \neq \mathfrak{g}$. Define the Lie bracket

$$[\mathfrak{g}, I] = \{[A, B] \mid A \in \mathfrak{g}, B \in I\} = \{AB - BA \mid A \in \mathfrak{g}, B \in I\} \subseteq I$$

Observe that $\{e_1 \otimes 1, e_2 \otimes 1, \ldots, e_n \otimes 1\}$ is a basis for $[\mathfrak{g}, I]$. Since $[\mathfrak{g}, I] \subseteq I$ we have $n = dim([\mathfrak{g}, I]) \leq dim(I)$. Also $I \subseteq \mathfrak{g}$ implies that $dim(I) \leq dim(\mathfrak{g}) = n$. Hence $dim(I) = n$. As I is a subspace of the vector space $\mathfrak{g}$, and the $dim(I) = dim(\mathfrak{g})$ we have $I = \mathfrak{g}$. □

5 Models of Computation

In this section we study polynomials that can be represented as projections of Vandermonde polynomials. Recall the definitions of the classes $\mathsf{VD}, \mathsf{VD}_{\mathsf{proj}}, \mathsf{VD}_{\mathsf{homo}}$ and $\mathsf{VD}_{\mathsf{aff}}$ from Section 2. For any arithmetic model of computation, universality and closure under addition and multiplication are among the most fundamental and necessary properties to be investigated. Here, we study these properties for projections of the Vandermonde polynomial and their sums. Most of the proofs follow from elementary arguments and can be found in the Appendix.

By definition, $\mathsf{VD}, \mathsf{VD}_{\mathsf{proj}}, \mathsf{VD}_{\mathsf{homo}} \subseteq \mathsf{VD}_{\mathsf{aff}}$. Also, any polynomial with at least one irreducible non-linear factor cannot be written as a projection of VD. As expected, we observe that there are products of linear forms that cannot cannot be written as a projection of VD.

Lemma 3. *Let* $(x_1 - y_1)(x_2 - y_2) \notin \mathsf{VD}_{\mathsf{aff}}$.

Proof. Suppose $f \in \mathsf{VD}_{\mathsf{aff}}$, then there are affine linear forms $\ell_1, \ldots, \ell_n$ such that $(x_1 - y_1)(x_1 - y_2) = \prod_{1 \leq i < j \leq n}(\ell_i - \ell_j)$. Clearly, only two factors of $\prod_{1 \leq i < j \leq n}(\ell_i - \ell_j)$ are non constant polynomials. Without loss of generality, let $\ell_i - \ell_j = x_1 - y_1$ and $\ell_{i'} - \ell_{j'} = x_2 - y_2$. Then, we must have $\ell_{i'} - \ell_i$, $\ell_{j'} - \ell_j$, $\ell_{i'} - \ell_j$ and $\ell_{j'} - \ell_i$ as constant polynomials, as they are factors of $\mathsf{VD}(\ell_1, \ldots, \ell_n)$ and hence $\ell_{i'} - \ell_{j'} = \ell_{i'} - \ell_i - (\ell_{j'} - \ell_i)$ is a constant, which is a contradiction. □

Lemma 4. *The classes* $\mathsf{VD}, \mathsf{VD}_{\mathsf{proj}}, \mathsf{VD}_{\mathrm{hom}}$ *and* $\mathsf{VD}_{\mathsf{aff}}$ *are not closed under addition and multiplication.*

Proof. Since sum of any two variable disjoint polynomials is irreducible, it is clear that $\mathsf{VD}, \mathsf{VD}_{\mathsf{proj}}, \mathsf{VD}_{\mathrm{hom}}$ and $\mathsf{VD}_{\mathsf{aff}}$ are not closed under addition. For multiplication, take $f_1 = x_1 - y_1$, and $f_1 = x_2 - y_2$. By Lemma 3, $f_1 f_2 \notin \mathsf{VD}_{\mathsf{aff}}$ and hence $f_1 f_2 \notin \mathsf{VD} \cup \mathsf{VD}_{\mathsf{proj}} \cup \mathsf{VD}_{\mathrm{hom}}$. Since $f_1, f_2 \in \mathsf{VD} \cap \mathsf{VD}_{\mathsf{proj}} \cap \mathsf{VD}_{\mathrm{hom}} \cap \mathsf{VD}_{\mathsf{aff}}$, we have that $\mathsf{VD}, \mathsf{VD}_{\mathsf{proj}}, \mathsf{VD}_{\mathrm{hom}}$ and $\mathsf{VD}_{\mathsf{aff}}$ are not closed under multiplication. □

It can also be seen that the classes of polynomials $\mathsf{VD}, \mathsf{VD}_{\mathsf{proj}}, \mathsf{VD}_{\mathrm{hom}}$ and $\mathsf{VD}_{\mathsf{aff}}$ are properly separated from each other:

Lemma 5. *(1)* $\mathsf{VD}_{\mathsf{proj}} \subsetneq \mathsf{VD}_{\mathsf{aff}}$ *and* $\mathsf{VD}_{\mathsf{homo}} \subsetneq \mathsf{VD}_{\mathsf{aff}}$.

(2) $\mathsf{VD}_{\mathsf{proj}} \not\subset \mathsf{VD}_{\mathsf{homo}}$ *and* $\mathsf{VD}_{\mathsf{homo}} \not\subset \mathsf{VD}_{\mathsf{proj}}$.

Proof.

- $\mathsf{VD_{proj}} \subsetneq \mathsf{VD_{aff}}$: Let $f = (x_1-y_1)+(x_2-y_2)$.Then $f = \det \begin{bmatrix} 1 & 1 \\ y_2 - x_2 & x_1 - y_1 \end{bmatrix}$. By comparing factors it can be seen that $(x_1 - y_1) + (x_2 - y_2) \notin \mathsf{VD_{proj}}$.

- $\mathsf{VD_{homo}} \subsetneq \mathsf{VD_{aff}}$: Let $f = x_1 + x_2 - 2$. Then $f = \det \begin{bmatrix} 1 & 1 \\ x_2 - 1 & x_1 - 1 \end{bmatrix}$. Suppose $f \in \mathsf{VD_{homo}}$, then there exists an $n \times n$ Vandermonde matrix M' such that $f \leq_{\mathsf{homo}} \det(M')$. In other words, $x_1 + x_2 - 2 = \prod_{i<j \quad i,j\in[n]}(\ell_j - \ell_i)$. where ℓ_i's are homogeneous linear forms which is impossible since $x_1 + x_2 - 2$ is non-homogeneous.

- $\mathsf{VD_{homo}} \subsetneq \mathsf{VD_{proj}}$: Let $f = (x_1 - 1)(x_1 - 2)$. Observe that $f \in \mathsf{VD_{proj}}$. However, since $\mathsf{VD_{homo}}$ consists only of polynomials with homogeneous linear factors, $f \notin \mathsf{VD_{homo}}$.

- $\mathsf{VD_{proj}} \subsetneq \mathsf{VD_{homo}}$: Let $f = (x_1 - y_1) + (x_2 - y_2)$. For $M = \begin{bmatrix} 1 & 1 \\ y_2 - x_2 & x_1 - y_1 \end{bmatrix}$, we have $\det(M) \in \mathsf{VD}_{homo}$ and $f = \det(M)$. It can be seen that $(x_1 - y_1) + (x_2 - y_2) \notin \mathsf{VD_{proj}}$. □

Sum of projections of Vandermonde polynomials

In this section, we consider polynomials that can be expressed as sum of projections of Vandermonde polynomials.

Definition 5. *For a class $\mathcal{C}$ of polynomials, let $\Sigma \cdot \mathcal{C}$ be defined as*

$$\Sigma \cdot \mathcal{C} = \left\{ f \;\middle|\; \begin{array}{l} f = (f_n)_{n\geq 0} \text{ where } \forall n \geq 0 \;\; \exists\, g_1, g_2, \ldots, g_s \in \mathcal{C}, \alpha_1, \ldots, \alpha_s \in \mathbb{F} \\ \text{such that } f \;=\; \alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_s g_s,\, s = n^{O(1)} \end{array} \right\}.$$

Lemma 6. $x_1 \cdot x_2 \notin \Sigma \cdot \mathsf{VD}$.

Proof. Suppose there exists $g_1, g_2, \ldots, g_s \in \mathsf{VD}$. Note that for every i, either $\deg(g_i) \leq 1$ or $\deg(g_i) \geq 3$. Since $\deg(g) = 2$, it is impossible that $x_1x_2 = g_1 + \cdots + g_s$ for any $s \geq 0$. □

Lemma 7. *The class $\Sigma \cdot \mathsf{VD}$ is closed under addition but not under multiplication.*

(i) If $f_1, f_2 \in \Sigma \cdot \mathsf{VD}$ then $f_1 + f_2 \in \Sigma \cdot \mathsf{VD}$.

(ii) There exists $f_1, f_2 \in \Sigma \cdot \mathsf{VD}$ such that $f_1 \cdot f_2 \notin \Sigma \cdot \mathsf{VD}$

Proof. (i) Closure under addition follows by definition.

(ii) Let $f_1 = x_1 - y_1$ and $f_2 = x_2 - y_2$, clearly $f_1, f_2 \in \Sigma \cdot \mathsf{VD}$. since for any $g \in \mathsf{VD}$, $\deg(g) \neq 2$, one can conclude that $f_1 f_2 \notin \Sigma \cdot \mathsf{VD}$. □

We now consider polynomials in the class $\Sigma\mathsf{VD_{proj}}$. Any univariate polynomial f of degree d can be computed by depth-2 circuits of size $\mathsf{poly}(d)$. However there are univariate polynomials not in $\mathsf{VD_{aff}}$ which is a subclass of depth 2 circuits (Consider any univariate polynomial irreducible over $\mathbb{F}$). Here, we show that the class of all univariate polynomials can be computed efficiently by circuits in $\Sigma\mathsf{VD_{proj}}$.

Lemma 8. *Let $f = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$ be a univariate polynomial of degree d. Then there are $g_i \in \mathsf{VD_{proj}}$, $1 \leq i \leq s \leq O(d^2)$ for some $\alpha_i \in \mathbb{F}$ such that $f = g_1 + \cdots + g_s$.*

Proof. Consider the $(d+1) \times (d+1)$ Vandermonde matrix M_0,

$$M_0 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ x & \beta_1 & \cdots & \cdots & \beta_{d-1} \\ x^2 & \beta_1^2 & \cdots & \cdots & \beta_{d-1}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x^{d-1} & \beta_1^{d-1} & \cdots & \cdots & \beta_{d-1}^{d-1} \\ x^d & \beta_1^d & \cdots & \cdots & \beta_{d-1}^d \end{bmatrix}$$

Let $g_0 = \det(M_0) = \gamma_{00} + \gamma_{01}x + \gamma_{02}x^2 + \cdots + \gamma_{0,d-1}x^{d-1} + \gamma_{0d}x^d$ where $\gamma_{00}, \ldots, \gamma_{0d} \in \mathbb{F}$ and $\gamma_{0d} \neq 0$. Note that $g_0 \in \mathsf{VD}_{\mathsf{proj}}$. Setting $\alpha_0 = \frac{a_d}{\gamma_{0d}}$ we get $\alpha_0 f_0 = a_d x^d + \frac{a_d \gamma_{0,d-1}}{\gamma_{0d}} x^{d-1} + \cdots + \frac{a_d \gamma_{01}}{\gamma_{0d}} x + \frac{a_d \gamma_{00}}{\gamma_{0d}}$. Now, let M_1 be the $d \times d$ Vandermonde matrix,

$$M_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ x & \beta_1 & \cdots & \cdots & \beta_{d-1} \\ x^2 & \beta_1^2 & \cdots & \cdots & \beta_{d-1}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x^{d-1} & \beta_1^{d-1} & \cdots & \cdots & \beta_{d-1}^{d-1} \end{bmatrix}$$

Then

$$g_1 = \det(M_1) = \gamma_{10} + \gamma_{11}x + \gamma_{12}x^2 + \cdots + \gamma_{1,d-1}x^{d-1}.$$

where $\gamma_{10}, \ldots, \gamma_{1d} \in \mathbb{F}$. Observe that x^d is not a monomial in $\alpha_1 g_1$. Set $\alpha_1 = \frac{a_{d-1}}{\gamma_{1,d-1}} - \frac{a_d \gamma_{0,d-1}}{\gamma_{0d}}$. Then $\alpha_1 g_1 = a_{d-1}x^{d-1} + \cdots + \frac{a_d \gamma_{01}}{\gamma_{0d}} x + \frac{a_d \gamma_{00}}{\gamma_{0d}}$. Extending this approach : Let M_i be a $(d-(i-1)) \times (d-(i-1))$ Vandermonde matrix,

$$M_i = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ x & \beta_1 & \cdots & \cdots & \beta_{d-i} \\ x^2 & \beta_1^2 & \cdots & \cdots & \beta_{d-i}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x^{d-i} & \beta_1^{d-i} & \cdots & \cdots & \beta_{d-i}^{d-i} \end{bmatrix}$$

Now observe that by setting $\alpha_i = \frac{a_{d-i}}{\gamma_{i,d-i}} - (\alpha_0\gamma_{0,d-i} + \alpha_1\gamma_{1,d-i} + \cdots + \alpha_{i-1}\gamma_{i-1,d-i})$ we ensure that $\sum_{j=0}^{i} \alpha_j g_j$ does not contain any term of the form x^p for $d-i \leq p \leq d-1$. Thus $\sum_{k=0}^{d} \alpha_k g_k = a_d x^d$. Hence to compute $a_d x^d$ we require d summands. Then, using $O(d^2)$ summands f can be obtained. $\square$

Recall that the n-variate power symmetric polynomial of degree d is defined as $\mathsf{Pow}_{\mathsf{n,d}} = x_1^d + x_2^d + \cdots + x_n^d$. From the arguments in Lemma 8, it follows that $\mathsf{Pow}_{\mathsf{n,d}}$ can be expressed by polynomial size circuits in $\Sigma \cdot \mathsf{VD}_{\mathsf{proj}}$.

Corollary 4. *There are polynomials $f_i \in \mathsf{VD}_{\mathsf{proj}}$ $1 \leq i \leq nd$ such that $\mathsf{Pow}_{\mathsf{n,d}} = \sum_{i=1}^{s} \alpha_i f_i$.*

Now, to argue that $\mathsf{VD}_{\mathsf{homo}}$ and $\mathsf{VD}_{\mathsf{aff}}$ are universal, we need the following:

Lemma 9 ([3])**.** *Over any infinite field containing the set of integers, there exists 2^d homogeneous linear forms $L_1, \ldots, L_{2^d}$ such that*

$$\prod_{i=1}^{d} x_i = \sum_{i=1}^{2^d} L_i^d$$

Combining with Corollary 4 with Lemma 9 we establish the universality of the classes $\Sigma \cdot \mathsf{VD}_{\mathsf{homo}}$ and $\Sigma \cdot \mathsf{VD}_{\mathsf{aff}}$.

Lemma 10. *The classes* $\Sigma \cdot \mathsf{VD}_{\mathsf{homo}}$ *and* $\Sigma \cdot \mathsf{VD}_{\mathsf{aff}}$ *are universal.*

Also, in the following, we note that $\mathsf{VD}_{\mathsf{aff}}$ is more powerful than depth three $\Sigma \wedge \Sigma$ circuits:

Lemma 11. $\mathsf{poly}-\mathsf{size}\ \Sigma \wedge \Sigma \subsetneq \mathsf{poly}{-}\mathsf{size}\ \Sigma \cdot \mathsf{VD}_{\mathsf{aff}}$.

Proof. Let $f \in \Sigma \wedge \Sigma$. Then $f = \sum_{i=1}^{s} \ell_i^d$. Then for any $k \geq 1$, $\dim \partial^{=k}(f) \leq s$. Now, for any $1 \leq k \leq n/2$ we have $\dim \partial^{=k}(\mathsf{VD}) \geq \binom{n}{k}$. Therefore, if $f = \mathsf{VD}$ we have $s = 2^{\Omega(n)}$ by setting $k = n/2$. Hence $\mathsf{poly}-\mathsf{size}\ \Sigma \wedge \Sigma \subsetneq \mathsf{poly}{-}\mathsf{size}\ \Sigma \cdot \mathsf{VD}_{\mathsf{aff}}$. ☐

A Lower Bound against $\Sigma \cdot \mathsf{VD}_{\mathsf{proj}}$

Observe that $\Sigma \cdot \mathsf{VD}_{\mathsf{proj}}$ is a subclass of non-homogeneous depth circuits of bottom fan-in 2, i.e., $\Sigma\Pi\Sigma^{[2]}$. It is known that $Sym_{2n,n}$ can be computed by non-homogeneous $\Sigma\Pi\Sigma^{[2]}$ circuits of size $O(n^2)$. We show that any $\Sigma \cdot \mathsf{VD}_{\mathsf{proj}}$ computing $Sym_{n,n/2}$ requires a top fan-in of $2^{\Omega(n)}$ and hence $\Sigma \cdot \mathsf{VD}_{\mathsf{proj}} \subsetneq \Sigma\Pi\Sigma^{[2]}$. The lower bound is obtained by a variant of the evaluation dimension as a complexity measure for polynomials.

Definition 6. (Restricted Evaluation Dimension.) *Let* $f \in \mathbb{F}[x_1, \ldots, x_n]$ *and* $S = \{i_1, \ldots, i_k\} \subseteq [n]$. *Let* $\bar{a} = (a_{i_1}, a_{i_2}, \ldots, a_{i_k}) \in \{0, 1, *\}^k$ *and* $f|_{S=\bar{a}}$ *be the polynomial obtained by substituting for all* $i_j \in S$,

$$x_{i_j} = \begin{cases} 1 & \text{if } a_{i_j} = 1 \\ 0 & \text{if } a_{i_j} = 0 \\ x_{i_j} & \text{if } a_{i_j} = * \end{cases}$$

Let $f|_S \stackrel{\mathsf{def}}{=} \{f|_{S=\bar{a}} \mid \bar{a} \in \{0, 1, *\}^k\}$. *The* restricted evaluation dimension of f *is defined as:*

$$\mathsf{RED_S}(f) \stackrel{\mathsf{def}}{=} dim(\mathbb{F}\text{-}span(f|_S))$$

It is not hard to see that the measure $\mathsf{RED_S}$ is sub-additive:

Lemma 12. *For any* $f, g \in \mathbb{F}[x_1, x_2, \ldots, x_n]$, $\mathsf{RED_S}(f + g) \leq \mathsf{RED_S}(f) + \mathsf{RED_S}(g)$.

In the following, we show that Vandermonde polynomials and their projections have low restricted evaluation dimension:

Lemma 13. *Let* M *be a* $m \times m$ *Vandermonde matrix with entries from* $\{x_1, \ldots, x_n\} \cup \mathbb{F}$ *and* $f = \det(M)$. *Then for any* $S \subset \{1 \ldots, n\}$ *with* $|S| = k$, *we have* $\mathsf{RED_S}(f) \leq (k+1)^2$.

Proof. Without loss of generality suppose $S = \{j_1, j_2, \ldots, j_k\} \subseteq [n]$ and $|S| = k$. Let $T = \{x_{j_1}, x_{j_2}, \ldots, x_{j_k}\} \cap \mathsf{var}(f) = \{i_1, i_2, \ldots, i_m\}$. Observe that $m \leq k$. For a vector $v \in \{0, 1, *\}^n$ and $b \in \{0, 1\}$, let $\#_b(v)$ denote the number of occurrences of b in the vector v. Then, for any $\bar{a} = (a_{j_1}, a_{j_2}, \ldots, a_{j_k}) \in \{0, 1, *\}^k$,

- If $\#_0((a_{i_1}, a_{i_2}, \ldots, a_{i_m})) \geq 2$ or $\#_1((a_{i_1}, a_{i_2}, \ldots, a_{i_m})) \geq 2$ then $f|_{S=\bar{a}} = 0$.
- If $\#_0((a_{i_1}, a_{i_2}, \ldots, a_{i_m})) = \#_1((a_{i_1}, a_{i_2}, \ldots, a_{i_m})) = 1$. Let T_1 be the set of polynomials obtained from such evaluations of f^d. The number of such assignments is at most $\binom{m}{2} \leq \binom{k}{2} \leq k^2$ and hence $|T_1| \leq k^2$.
- If $\#_0(\{a_{i_1}, a_{i_2}, \ldots, a_{i_m}\}) = 1$ or $\#_1(\{a_{i_1}, a_{i_2}, \ldots, a_{i_m}\}) = 1$. Let T_2 denote the set of polynomials obtained from such evaluations. Since number of such assignments is $2\binom{m}{m-1} \leq 2\binom{m}{1} \leq 2\binom{k}{1} \leq 2k$, we have $|T_2| \leq 2k$.
- If, $\#_0(\{a_{i_1}, a_{i_2}, \ldots, a_{i_m}\}) = \#_1(\{a_{i_1}, a_{i_2}, \ldots, a_{i_m}\}) = 0$, in this case, the polynomial f does not change under these evaluations.

From the above case analysis, we have $\mathbb{F}\text{-}span(f|S = a) = \mathbb{F}\text{-}span(T_1 \cup T_2 \cup \{f\})$. Therefore $\mathsf{RED_S}(f) \leq k^2 + 2k + 1 \leq (k+1)^2$. □

Lemma 14. *Let $Sym_{n,k}$ be the elementary symmetric polynomial in n variables of degree k. Then for any $S \subset \{1, \ldots, n\}$, $|S| = k$, we have $\mathsf{RED_S}(Sym_{n,k}) \geq 2^k - 1$.*

Proof. Let $Sym_{n,k}$ be the elementary symmetric polynomial in n variables of degree k. For $T \subseteq S, T \neq \emptyset$, define $\bar{a}_T = (a_1, \ldots, a_k) \in \{1, *\}^k$ as:

$$a_i = \begin{cases} * & \text{if } x_i \in T \\ 1 & \text{if } x_i \in S \setminus T \end{cases}$$

Note that it is enough to prove:

$$dim(\{Sym_{n,k}|_{S=\bar{a}_T} \mid T \subseteq S, T \neq \emptyset\}) \geq 2^k - 1 \tag{6}$$

Since $\{Sym_{n,k}|_{S=\bar{a}_T} \mid T \subseteq S, T \neq \emptyset\} \subseteq \{\mathbb{F}\text{-}span(Sym_{n,k}|_{S=\bar{a}}) \mid \bar{a} = (a_1, \ldots, a_k) \in \{1, *\}^k\}$, by Equation (6) we have

$$\mathsf{RED_S}(Sym_{n,k}) \geq dim(\{Sym_{n,k}|_{S=\bar{a}_T} \mid T \subseteq S, T \neq \emptyset\}) = 2^k - 1.$$

To prove (6), note that for any distinct $T_1, T_2 \subseteq S$, we have $Sym_{n,k}|_{S=\bar{a}_{T_1}}$ and $Sym_{n,k}|_{S=\bar{a}_{T_2}}$ have distinct leading monomials with respect to the lex ordering since they have distinct supports. Since the number of distinct leading monomials in a space of polynomials is a lower bound on its dimension, this concludes the proof of (6). □

Theorem 4. *If $\sum_{i=1}^{s} \alpha_i f_i = Sym_{n,n/2}$ where $f_i \in \mathsf{VD_{proj}}$ then $s = 2^{\Omega(n)}$.*

Proof. The proof is a straightforward application of sub-additivity of $\mathsf{RED_S}$ combined with Lemmas 14 and 13. □

References

[1] Peter Bürgisser. *Completeness and reduction in algebraic complexity theory*, volume 7. Springer Science & Business Media, 2013.

[2] John F. Canny. Some algebraic and geometric computations in PSPACE. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 460–467, 1988.

[3] Ismor Fischer. Sums of like powers of multivariate linear forms. *Mathematics Magazine*, 67(1):59–61, 1994.

[4] Antonio Giambruno and Mikhail Zaicev. *Polynomial identities and asymptotic methods*. American Mathematical Soc., 2005.

[5] Joshua A. Grochow. Matrix isomorphism of matrix lie algebras. In *Proceedings of the 27th Conference on Computational Complexity, CCC 2012, Porto, Portugal, June 26-29, 2012*, pages 203–213, 2012.

[6] I.G.Macdonald. *Symmetric functions and Hall Polynomials*. Oxford Mathematical Monographs, 1998.

[7] Erich Kaltofen. Factorization of polynomials given by straight-line programs. In *Randomness and Computation*, pages 375–412, 1989.

[8] Neeraj Kayal. Efficient algorithms for some special cases of the polynomial equivalence problem. In *Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2011, San Francisco, California, USA, January 23-25, 2011*, pages 1409–1421, 2011.

[9] Neeraj Kayal. Affine projections of polynomials: extended abstract. In *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 643–662, 2012.

[10] Ketan D Mulmuley and Milind Sohoni. Geometric complexity theory i: An approach to the p vs. np and related problems. *SIAM Journal on Computing*, 31(2):496–526, 2001.

[11] Matthieu Romagny. The fundamental theorem of alternating functions. Manuscript, 2005.

[12] Nitin Saxena. *Morphisms of Rings and Applications to Complexity*. PhD thesis, Department of Computer Science, Indian Institute of Technology, Kanpur, India, 2006.

[13] Thomas Thierauf. The isomorphism problem for read-once branching programs and arithmetic circuits. *Chicago J. Theor. Comput. Sci.*, 1998, 1998.

[14] Leslie G. Valiant. Completeness classes in algebra. In *STOC*, pages 249–261, 1979.