Electronic Colloquium on Computational Complexity, Report No. 164 (2018)

On the symmetries of design polynomials

Nikhil Gupta
Indian Institute of Science
nikhilg@iisc.ac.in

Chandan Saha
Indian Institute of Science
chandan@iisc.ac.in

September 18, 2018

Abstract

In a Nisan-Wigderson design polynomial (in short, a design polynomial), the gcd of every pair of monomials has a low degree. A useful example of such a polynomial, introduced in [KSS14], is the following:

$$\mathsf{NW}_{d,k}(\mathbf{x}) = \sum_{h \in \mathbb{F}_d[z],\ \deg(h) \le k} \ \prod_{i=0}^{d-1} x_{i,h(i)},$$

where d is a prime, $\mathbb{F}_d$ is the finite field with d elements, and $k \ll d$. The degree of the gcd of every pair of monomials in $\mathsf{NW}_{d,k}$ is at most k. For concreteness, let us fix $k = \lceil \sqrt{d} \rceil$. The family of polynomials $\mathcal{NW} := \{\mathsf{NW}_{d,k} : d \text{ is a prime}\}$ and close variants of it have been used as hard explicit polynomial families in several recent arithmetic circuit lower bound proofs. But, unlike the permanent, very little is known about the various complexity and structural aspects of $\mathcal{NW}$ beyond the fact that $\mathcal{NW} \in \mathsf{VNP}$. Is $\mathcal{NW}$ VNP-complete? Is $\mathsf{NW}_{d,k}$ characterized by its symmetries? Is it circuit-testable, i.e., given a circuit C can we check efficiently if C computes $\mathsf{NW}_{d,k}$? Characterization of polynomials by their symmetries plays a central role in the geometric complexity theory program. Here, we answer the last two questions.

We show that $\mathsf{NW}_{d,k}$ is characterized by its group of symmetries over $\mathbb{C}$. We also show that $\mathsf{NW}_{d,k}$ is characterized by circuit identities which implies that $\mathsf{NW}_{d,k}$ is circuit-testable in randomized polynomial time. As another implication, we obtain the "flip theorem" for $\mathcal{NW}$: Suppose $\mathsf{NW}_{d,k}$ is not computable by circuits of size s. Then, there exist $\mathrm{poly}(s)$ many points $\mathbf{a}_1, \ldots, \mathbf{a}_m$ such that for every circuit C of size s, there is an $\ell \in [m]$ satisfying $\mathsf{C}(\mathbf{a}_\ell) \neq \mathsf{NW}_{d,k}(\mathbf{a}_\ell)$. These points can be computed deterministically in $\mathrm{poly}(s)$ time if black-box polynomial identity testing for size-s circuits can be derandomized in $\mathrm{poly}(s)$ time. It is well-known that the permanent polynomial has the above-mentioned features.

We also show a structural similarity between the group of symmetries of the permanent and that of $\mathsf{NW}_{d,k}$: If A is in the group of symmetries of $\mathsf{NW}_{d,k}$ then $A = D \cdot P$, where D and P are diagonal and permutation matrices respectively. This is proved by completely characterizing the Lie algebra of $\mathsf{NW}_{d,k}$, and using an interplay between the Hessian of $\mathsf{NW}_{d,k}$ and the evaluation dimension.

ISSN 1433-8092

1 Introduction

Proving super-polynomial lower bounds for Boolean and arithmetic circuits computing explicit functions is the holy grail of circuit complexity. Over the past few decades, research on lower bounds has gradually pushed the frontier by bringing in novel methods in the arena and carefully building upon the older ones. Some of the notable achievements are – lower bounds for AC^0 circuits [FSS81, Ajt83, Hås86], monotone circuits [Raz85, AB87], $\mathsf{ACC}(p)$ circuits [Raz87, Smo87] and ACC circuits [Wil14, MW18] in the Boolean case, and lower bounds for homogeneous depth three circuits [NW97], multilinear formulas [Raz09, RY09], homogeneous depth four circuits [GKKS14, KLSS17, KS17b] and the lower bound on the depth of circuits for MaxFlow [Mul99] in the arithmetic case. The slow progress in circuit lower bounds is explained by a few "barrier" type results, particularly by the notion of natural proofs [RR97] for Boolean circuits, and the notion of algebraically natural proofs [FSV17, GKSS17] for arithmetic circuits [1]. Most lower bound proofs, but not all [2], do fit in the natural proof framework.

It is apparent from the concept of natural proofs and its algebraic version that in order to avoid this barrier, we need to develop an approach that violates the so called *constructivity* criterion or the *largeness* criterion. Focusing on the latter criterion, it means, if an explicit function has a special property that random functions do not have, and if a lower bound proof for circuits computing this explicit function uses this special property critically, then such a proof circumvents the natural proof barrier automatically. For polynomial functions (simply polynomials), *characterization by symmetries* is such a special property[3], and the geometric complexity theory (GCT) program [MS01] is an approach to proving super-polynomial arithmetic circuit lower bound by crucially exploiting this property of the permanent and the determinant polynomials. From hereon, our discussion will be restricted to polynomial functions and arithmetic circuits.

The permanent family is complete for the class VNP and the determinant family is complete for the class VQP under p-projections. Class $\mathsf{VQP} \subseteq \mathsf{VP}$ consists of polynomial families that are computable by poly-size algebraic branching programs; this class has another interesting complete family, namely the iterated matrix multiplication (IMM) family. These three polynomial families have appeared in quite a few lower bound proofs [NW97, GK98, MR04, Raz09, RY09, GKKS14, FLMS15, KS17b, KST16b, CLS18] in the arithmetic circuit literature. That permanent and determinant are characterized by their respective groups of symmetries are classical results [MM62, Fro97]. It has also been shown that IMM is characterized by its symmetries [Ges16, KNST17]. There are two other polynomial families in VP, the power symmetric polynomials and the sum-product polynomials, that are known to possess this rare property (see Section 2 in [CKW11]). However, the elementary symmetric polynomial is not characterized by its symmetries [Hüt16].

In the recent years, another polynomial, namely the Nisan-Wigderson design polynomial (in

[1] Presently, the evidences in favor of existence of one-way functions (which implies the natural proof barrier) are much stronger than that of existence of succinct hitting-set generators (which implies the algebraically natural proof barrier). However, there are a few results in algebraic complexity that exhibit, unconditionally [EGdOW18] or based on more plausible complexity theoretic assumptions [BIJL18], the limitations of some of the current techniques in proving lower bounds for certain restricted arithmetic models.

[2] like the lower bounds for monotone and ACC circuits

[3] A random polynomial is not characterized by its symmetries with high probability (see Proposition 3.4.9 in [Gro12])

short, design polynomial), and close variants of it have been used intensely as hard explicit polynomials in several lower bound proofs for depth three, depth four and depth five circuits [KSS14, CM14, KS14a, KS14b, KLSS17, KS17b, KS16a, KS16c, KS16b, KST16a, FKS16, KS17a]. In some cases, the design polynomial (Definition 2.2) yielded lower bounds that are not known yet for the permanent, determinant and IMM (as in [KS16a, KS16b, FKS16, KS17a]). It can be easily shown that the design polynomial defines a family in VNP (see Observation A.1). But, very little is otherwise known about the various complexity and structural aspects of this family. Like the permanent, is it VNP-complete? Is it characterized by its symmetries? Is it circuit testable? It is reasonable to seek answers to these fundamental questions for a natural family like the design polynomials. Moreover, in the light of some recent developments in GCT [IP16, BIP16, IMW17], it may be worth studying other polynomial families (like the design polynomials and the IMM) that have some of the "nice features" of the permanent and the determinant and that may also fit in the GCT framework. We refer the reader to [Gro12, Aar17, Mul12, Reg02] for an overview of GCT. If the design polynomial family turns out to be in VP then that would be an interesting result by itself with potentially important complexity theoretic and algorithmic consequences.

In this article, we answer some of the questions on the design polynomial pertaining to its group of symmetries. Our results accord a fundamental status to this polynomial family.

1.1 Our results

Some of the basic definitions and notations are given in Section 2. The design polynomial $\mathsf{NW}_{d,k}$ is defined (in Definition 2.2) using two parameters, d (the degree) and k (the "intersection" parameter). Our results hold for any $k \in [1, \frac{d}{2} - 2]$, but (from the lower bound point of view) it is best to think of k as d^ϵ for some arbitrarily chosen constant $\epsilon \in (0, 1)$. The number of variables in $\mathsf{NW}_{d,k}$ is $n = d^2$. Any polynomial can be expressed as an affine projection of $\mathsf{NW}_{d,k}$, for a possibly large d (see Observation A.2). For notational convenience, we will drop the subscripts d and k whenever they are clear from the context. Let $\mathscr{G}_f$ be the group of symmetries of a polynomial f over an underlying field $\mathbb{F}$ (see Definition 2.6).

Theorem 1 (Characterization by symmetries)**.** *Let $\mathbb{F} = \mathbb{C}$ be the underlying field and f be a homogeneous degree-d polynomial in $n = d^2$ variables. If $\mathscr{G}_{\mathsf{NW}} \subseteq \mathscr{G}_f$ then $f = \alpha \cdot \mathsf{NW}$ for some $\alpha \in \mathbb{C}$.*

The theorem, proven in Section 3, holds over any field $\mathbb{F}$ that has a d-th root of unity $\zeta \neq 1$ and $|\mathbb{F}| \neq d + 1$. We do not know if NW is characterized by its symmetries over $\mathbb{R}$ or $\mathbb{Q}$ (more on this later). The symmetries of NW have a nice algorithmic application: Although, it is not known if NW is computable by a $\mathrm{poly}(d)$ size circuit (which is defined in Definition 2.1), the following theorem shows that checking if a given circuit computes NW can be done efficiently. In this article, whenever we mention size-s circuit, we mean size-s circuit with degree bounded by $\delta(s)$, which is an arbitrarily fixed polynomial function[4] of s. Let $\mathbf{x}$ be the set of n variables of NW. We will identify a circuit with the polynomial computed by it.

Theorem 2 (Circuit testability)**.** *There is a randomized algorithm that takes input black-box access to a circuit $\mathtt{C}(\mathbf{x})$ of size s over a finite field $\mathbb{F}$, where $|\mathbb{F}| \geq 4 \cdot \delta(s)$, and determines correctly whether or not $\mathtt{C}(\mathbf{x}) = \mathsf{NW}$ with probability $1 - \exp(-s)$, using $\mathrm{poly}(s)$ field operations.*

[4] This is the interesting scenario in algebraic complexity theory as polynomial families in VP admit circuits with degree bounded by a polynomial function of size.

A suitable version of the theorem also holds over $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$. Such a theorem is known for the permanent with two different proofs, one using self-reducibility of the permanent [Lip89] and the other using its symmetries [Mul10]. We do not know if NW has a self-reducible property like the permanent, but its symmetries are powerful enough to imply the above result. The theorem is proven in Section 4 by showing that NW is characterized by circuit identities over *any* field (see Definition 2.10). This characterization, which uses the symmetries of NW, also implies the following result. For this result, we can assume $\delta(s) \geq d$, without any loss of generality.

Theorem 3 (Flip theorem)**.** *Suppose* NW *is not computable by circuits of size s over a finite field $\mathbb{F}$, where $|\mathbb{F}| \geq 4 \cdot \delta(s)$. Then, there exist points $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{F}^n$, where $m = \mathrm{poly}(s)$, such that for every circuit $\mathtt{C}$ over $\mathbb{F}$ of size at most s, there is an $\ell \in [m]$ satisfying $\mathtt{C}(\mathbf{a}_\ell) \neq \mathsf{NW}(\mathbf{a}_\ell)$. A set of randomly generated points $\mathbf{a}_1, \ldots, \mathbf{a}_m \in_r \mathbb{F}^n$ has this property with probability $1 - \exp(-s)$. Moreover, black-box derandomization of polynomial identity testing for size-$(10s)$ circuits over $\mathbb{F}$ using $\mathrm{poly}(s)$ field operations implies that the above-mentioned points can be computed deterministically using $\mathrm{poly}(s)$ field operations.*

An appropriate version of the theorem also holds over $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$. The flip theorem is known for the permanent [Mul10, Mul11] [5]. Similar theorems have also been shown for the $3SAT$ problem [FPS08, Ats06]. Results of this kind show that if a certain function ($3SAT$ or permanent or NW) is not computable by small circuits then there exists a short list of efficiently computable "hard instances" that fail all small circuits. Finally, we show a structural similarity between the symmetries of permanent and NW.

Theorem 4 (Structure of $\mathscr{G}_{\mathsf{NW}}$)**.** *Let $\mathbb{F}$ be the underlying field of size greater than $\binom{d}{2}$ and $\mathrm{char}(\mathbb{F}) \neq d$. If $A \in \mathscr{G}_{\mathsf{NW}}$ then $A = D \cdot P$, where $D, P \in \mathscr{G}_{\mathsf{NW}}$ are diagonal and permutation matrices respectively.*

The group of symmetries of the permanent has a similar structure [MM62]. The proof of the above theorem is more technical than the other proofs and is given in Section 5. It involves a complete characterization of the Lie algebra of NW, and an interplay between the Hessian of NW and the evaluation dimension measure. Finally, in Section 6, we analyze the diagonal and permutation symmetries of NW. Our analysis along with the above structure of $\mathscr{G}_{\mathsf{NW}}$ seem to indicate that NW is *not* characterized by its symmetries over $\mathbb{R}$.

2 Preliminaries

Notations. The set of natural numbers is $\mathbb{N} = \{0, 1, 2 \ldots\}$ and $\mathbb{N}^\times = \mathbb{N} \backslash \{0\}$. For $r \in \mathbb{N}^\times$, $[r] = \{0, \ldots, r-1\}$. The general linear group $\mathrm{GL}_r(\mathbb{F})$ is the group of all $r \times r$ invertible matrices over $\mathbb{F}$. Throughout this article, $\mathrm{poly}(r)$ means $r^{O(1)}$ and $\exp(r)$ means 2^r. For a prime d, $\mathbb{F}_d$ is the finite field of order d whose elements are naturally identified with $[d] = \{0, 1, \ldots, d-1\}$. Let $\mathbf{x}$ be the following disjoint union of variables,

$$\mathbf{x} := \biguplus_{i \in [d]} \mathbf{x}_i, \tag{1}$$

where $\mathbf{x}_i := \{x_{i,0}, \ldots, x_{i,d-1}\}$. The total number of variables in $\mathbf{x}$ is $n = d^2$. $\mathbb{F}[\mathbf{x}]$ and $\mathbb{F}_d[z]$ denote the rings of multivariate and univariate polynomials over $\mathbb{F}$ and $\mathbb{F}_d$ in $\mathbf{x}$ and z variables respectively,

[5] We have borrowed the name 'flip theorem' from these work.

and the set $\mathbb{F}_d[z]_k := \{h \in \mathbb{F}_d[z] : \deg(h) \leq k\}$. We will represent elements of $\mathbb{F}$ by lower case Greek alphabets $(\alpha, \beta, ...)$, elements of $\mathbb{F}_d$ by lower case Roman alphabets $(a, b, ...)$, multivariate polynomials over $\mathbb{F}$ by f, g and q, univariate polynomials over $\mathbb{F}_d$ by p and h, matrices over $\mathbb{F}$ by capital letters $(A, B, C, ...)$, and the set of variables by $\mathbf{x}, \mathbf{y}, \mathbf{z}$ and vectors over $\mathbb{F}$ by $\mathbf{a}, \mathbf{b}$. Variable sets are interpreted as column vectors when left multiplied to a matrix. For instance, in $A \cdot \mathbf{x}$, $\mathbf{x}$ is the vector $(x_{0,0}\ x_{0,1} \dots\ x_{0,d-1}\ \dots\ x_{d-1,0}\ x_{d-1,1} \dots\ x_{d-1,d-1})^T$, and we say A is applied on $\mathbf{x}$.

2.1 Algebraic preliminaries

A polynomial f is homogeneous if the degree of all the monomials of f are the same. Polynomial $f \in \mathbb{F}[\mathbf{x}]$ is set-multilinear in the sets $\mathbf{x}_0, \dots, \mathbf{x}_{d-1}$ (as defined in Equation (1)) if every monomial contains exactly one variable from each set $\mathbf{x}_i$ for $i \in [d]$.

Definition 2.1 (Arithmetic circuit)**.** An arithmetic circuit $\mathtt{C}$ over $\mathbb{F}$ is a directed acyclic graph in which a node with in-degree zero is labelled with either a variable or a $\mathbb{F}$-element, an edge is labelled with a $\mathbb{F}$-element, and other nodes are labelled with $+$ and $\times$. Computation proceeds in a natural way: a node with in-degree zero computes its label, an edge scales a polynomial by its label, and a node labelled with $+/\times$ computes the sum/product of the polynomials computed at the end of the edges entering the node. The polynomials computed by nodes with out-degree zero are the output of $\mathtt{C}$. The *size* of $\mathtt{C}$ is the sum of the number of nodes and edges in the graph. The *degree* of $\mathtt{C}$ is the maximum over the degree of the polynomials computed at all nodes of $\mathtt{C}$.

Definition 2.2 (Nisan-Wigderson polynomial)**.** Let $d > 2$ be a prime and $k \in \mathbb{N}$. The Nisan-Wigderson design polynomial is defined as in [KSS14] (which is inspired by the Nisan-Wigderson set-systems [NW94]),

$$\mathsf{NW}_{d,k}(\mathbf{x}) := \sum_{h \in \mathbb{F}_d[z]_k} \prod_{i \in \mathbb{F}_d} x_{i,h(i)}.$$

It is a degree-d homogeneous and set-multilinear polynomial in $n = d^2$ variables, having d^{k+1} monomials. We drop the subscripts d, k for notational convenience. NW satisfies the 'low intersection' property, meaning any two monomials of NW have at most k variables in common. This follows from the fact that the monomials are obtained from polynomials in $\mathbb{F}_d[z]_k$.

Definition 2.3 (Block-permuted matrix)**.** A matrix $A \in \mathbb{F}^{d^2 \times d^2}$ is a block-permuted matrix with block size d if $A = B \cdot (P \otimes I_d)$, where $B \in \mathbb{F}^{d^2 \times d^2}$ is a block-diagonal matrix with block size d, $P \in \mathbb{F}^{d \times d}$ is a permutation matrix, and I_d is the $d \times d$ identity matrix.

Definition 2.4 (Evaluation dimension)**.** Let $f \in \mathbb{F}[\mathbf{y}]$ and $\mathbf{z} \subseteq \mathbf{y}$. The evaluation dimension of f with respect to $\mathbf{z}$ is,

$$\text{evalDim}_{\mathbf{z}}(f) := \dim(\ \mathbb{F}\text{-span}\ \{f(\mathbf{y})|_{\mathbf{z}=\mathbf{a}} : \mathbf{a} \in \mathbb{F}^{|\mathbf{z}|}\}\ ).$$

Definition 2.5 (Hessian)**.** Let $f \in \mathbb{F}[\mathbf{y}]$ be a polynomial in $\mathbf{y} = \{y_1, y_2, \dots, y_n\}$ variables. The Hessian of f is the following matrix in $(\mathbb{F}[\mathbf{y}])^{n \times n}$,

$$H_f(\mathbf{y}) := \left(\frac{\partial^2 f}{\partial y_i \cdot \partial y_j}\right)_{i,j \in [n]}.$$

We would need the following property of $H_f(\mathbf{y})$ that can be proved using chain-rule of derivatives.

Lemma 2.1 (Lemma 2.6 of [CKW11]). *Let $g \in \mathbb{F}[\mathbf{y}]$ and $f = g(A \cdot \mathbf{y})$ for some $A \in \mathbb{F}^{n\times n}$. Then,*

$$H_f(\mathbf{y}) = A^T \cdot H_g(A \cdot \mathbf{y}) \cdot A.$$

Definition 2.6 (Group of symmetries)**.** Let $f \in \mathbb{F}[\mathbf{y}]$ be an n-variate polynomial. The set $\mathscr{G}_f = \{A \in \mathrm{GL}_n(\mathbb{F}) : f(A \cdot \mathbf{y}) = f(\mathbf{y})\}$ forms a group under matrix multiplication and it is called the group of symmetries of f over $\mathbb{F}$.

Definition 2.7 (Lie algebra)**.** Let $f \in \mathbb{F}[\mathbf{y}]$ be a polynomial in $\mathbf{y} = \{y_1, y_2, \ldots, y_n\}$ variables. The Lie algebra of f, denoted by $\mathfrak{g}_f$, is the set of matrices $B = (b_{i,j})_{i,j\in[n]} \in \mathbb{F}^{n\times n}$ satisfying the relation,

$$\sum_{i,j\in[n]} b_{i,j} \cdot y_j \cdot \frac{\partial f}{\partial y_i} = 0.$$

It is easy to check that $\mathfrak{g}_f$ is a vector space over $\mathbb{F}$. The following property relates the Lie algebras of $f(\mathbf{y})$ and $f(A \cdot \mathbf{y})$ for $A \in \mathrm{GL}_n(\mathbb{F})$. See Proposition 58 of [Kay12] for a proof of this fact.

Lemma 2.2 (Conjugacy of Lie algebras)**.** *Let $g \in \mathbb{F}[\mathbf{y}]$ be an n-variate polynomial. If $f(\mathbf{y}) = g(A \cdot \mathbf{y})$ for $A \in GL_n(\mathbb{F})$, then $\mathfrak{g}_f = A^{-1} \cdot \mathfrak{g}_g \cdot A$.*

Over $\mathbb{C}$, the Lie algebra $\mathfrak{g}_f$ is related to the group of symmetries $\mathscr{G}_f$ as stated in the following definition. For $B \in \mathbb{C}^{n\times n}$, let $e^B := \sum_{i\in\mathbb{N}} \frac{B^i}{i!} \in \mathbb{C}^{n\times n}$ (the series always converges).

Definition 2.8 (Continuous and discrete symmetries)**.** Let $f \in \mathbb{C}[\mathbf{y}]$. If $A \in \mathfrak{g}_f$ then $e^{tA} \in \mathscr{G}_f$ for every $t \in \mathbb{R}$ (see [Hal15] for a proof of this fact). Elements of the set $\{e^{tA} : A \in \mathfrak{g}_f \text{ and } t \in \mathbb{R}\}$ are the continuous symmetries of f. All the other symmetries in $\mathscr{G}_f$ are the discrete symmetries of f.

Definition 2.9 (Characterization by symmetries)**.** A homogeneous degree-d polynomial $g \in \mathbb{F}[\mathbf{y}]$ is said to be *characterized by its symmetries* if for every degree-d homogeneous polynomial $f \in \mathbb{F}[\mathbf{y}]$, $\mathscr{G}_g \subseteq \mathscr{G}_f$ implies that $f(\mathbf{y}) = \alpha \cdot g(\mathbf{y})$ for some $\alpha \in \mathbb{F}$.

Definition 2.10 (Characterization by circuit identities)**.** Let $g \in \mathbb{F}[\mathbf{y}]$ be an n-variate polynomial, and $\mathbf{z}, \mathbf{u}$ be two sets of constantly many variables and $|\mathbf{z}| = c$. Suppose that there exist $m = \mathrm{poly}(n)$ polynomials $q_1(\mathbf{z}, \mathbf{u}), \ldots, q_m(\mathbf{z}, \mathbf{u})$ over $\mathbb{F}$ such that for every $i \in [m]$, q_i is computable by a constant size circuit and there are matrices $A_{i1}, \ldots, A_{ic} \in \mathbb{F}[\mathbf{u}]^{n\times n}$ computable by $\mathrm{poly}(n)$ size circuits, and the following condition is satisfied: For $f \in \mathbb{F}[\mathbf{y}]$, $q_i(f(A_{i1} \cdot \mathbf{y}), \ldots, f(A_{ic} \cdot \mathbf{y}), \mathbf{u}) = 0$ for every $i \in [m]$ if and only if $f = \alpha \cdot g$ for some $\alpha \in \mathbb{F}$. Then, g is *characterized by circuit identities* over $\mathbb{F}$.

The above definition is taken (after slight modifications to suit our purpose) from Definition 3.4.7 in [Gro12] and is attributed to an article by Mulmuley [Mul07].

3 Symmetry characterization of the NW polynomial

Let $\mathbb{F}$ be a field having a d-th root of unity $\zeta \neq 1$ and $|\mathbb{F}| \neq d + 1$.[6] As d is a prime, ζ is primitive, i.e., $\zeta^d = 1$ and $\zeta^t \neq 1$ for $0 < t < d$. For a polynomial $p \in \mathbb{F}_d[z]$, m_p would refer to the monomial $\prod_{i\in[d]} x_{i,p(i)}$. The rows and columns of a matrix in $\mathscr{G}_{\mathsf{NW}}$ are indexed by the set $\{(i, j) : i, j \in \mathbb{F}_d\}$.

[6] For a prime d, $|\mathbb{F}| = d + 1$ if and only if d is a Mersenne prime.

Claim 3.1. *The following matrices in $\mathbb{F}^{n\times n}$ are in $\mathscr{G}_{\mathsf{NW}}$:*

1. *$A_{\boldsymbol{\beta}}$, a diagonal matrix with $((i,j),(i,j))$-th entry as $\beta_i \in \mathbb{F}^\times$ for $i,j \in [d]$, such that $\prod_{i\in[d]} \beta_i = 1$.*
2. *A_ℓ, a diagonal matrix with $((i,j),(i,j))$-th entry as $\zeta^{i^\ell \cdot j}$ for $i,j \in [d]$, where $\ell \in [d-k-1]$.* [7]
3. *A_h, where $h \in \mathbb{F}_d[z]_k$, the $((i,j),(i,j+h(i)))$-th entry of A_h is 1 for $i,j \in [d]$ and other entries are 0.*

Proof. By definition, $A_{\boldsymbol{\beta}}, A_\ell \in \mathrm{GL}_n(\mathbb{F})$. Also, $A_h \in \mathrm{GL}_n(F)$ as it is a permutation matrix. Observe that the polynomials $\mathsf{NW}(A_{\boldsymbol{\beta}}\cdot\mathbf{x}), \mathsf{NW}(A_\ell\cdot\mathbf{x})$ and $\mathsf{NW}(A_h\cdot\mathbf{x})$ are obtained from $\mathsf{NW}(\mathbf{x})$ by replacing the variable $x_{i,j}$ with $\beta_i\cdot x_{i,j}$, $\zeta^{i^\ell\cdot j}\cdot x_{i,j}$ and $x_{i,j+h(i)}$ respectively, for $i,j\in[d]$. When $A_{\boldsymbol{\beta}}$ is applied on $\mathbf{x}$, a monomial m_p gets mapped to $\prod_{i\in[d]}\beta_i\cdot m_p = m_p$ as $\prod_{i\in[d]}\beta_i = 1$, implying $\mathsf{NW}(A_{\boldsymbol{\beta}}\cdot\mathbf{x}) = \mathsf{NW}$. When A_h is applied on $\mathbf{x}$, a monomial m_p gets mapped to m_{p+h}; in other words, the monomials of NW are 'shifted around' and so $\mathsf{NW}(A_h\cdot\mathbf{x}) = \mathsf{NW}$. When A_ℓ is applied on $\mathbf{x}$, a monomial m_p is mapped to $\prod_{i\in[d]}\zeta^{i^\ell\cdot p(i)}\cdot m_p$. We show below that $\prod_{i\in[d]}\zeta^{i^\ell\cdot p(i)} = 1$ for every $\ell\in[d-k-1]$, thereby implying $\mathsf{NW}(A_\ell\cdot\mathbf{x}) = \mathsf{NW}$.

Observation 3.1. *For every $p\in\mathbb{F}_d[\mathbf{x}]_k$ and $\ell\in[d-k-1]$, $\prod_{i\in[d]}\zeta^{i^\ell\cdot p(i)} = 1$.*

Proof. As $\zeta\neq 1$ is a d-th root of unity, $\prod_{i\in[d]}\zeta^{i^\ell\cdot p(i)} = \zeta^{\sum_{i\in\mathbb{F}_d} i^\ell\cdot p(i)}$ and so it is sufficient to show that $\sum_{i\in\mathbb{F}_d} i^\ell\cdot p(i) = 0$. Suppose $p(z) = a_r z^r + \cdots + a_0$, where $r\le k$ and $a_r,\ldots,a_0\in\mathbb{F}_d$. Then

$$\sum_{i\in\mathbb{F}_d} i^\ell\cdot p(i) = a_r\left(\sum_{i\in\mathbb{F}_d} i^{r+\ell}\right) + \cdots + a_0\left(\sum_{i\in\mathbb{F}_d} i^\ell\right).$$

Each summand in the RHS of the above equation is of the form $a\cdot\left(\sum_{i\in\mathbb{F}_d} i^s\right)$, where $0\le s\le d-2$. As $\sum_{i\in\mathbb{F}_d} i^0 = 0$, assume that $1\le s\le d-2$. Let b be a generator of $\mathbb{F}_d^\times$. Then

$$\sum_{i\in\mathbb{F}_d} i^s = \sum_{i\in\mathbb{F}_d^\times} i^s = \sum_{t\in[d-1]} b^{t\cdot s} = \frac{1-b^{(d-1)\cdot s}}{1-b^s} = 0, \quad \text{as } b^{d-1} = 1 \text{ in } \mathbb{F}_d. \tag{2}$$

Hence, $\sum_{i\in\mathbb{F}_d} i^\ell\cdot p(i) = 0$ implying $\prod_{i\in[d]}\zeta^{i^\ell\cdot p(i)} = 1$. □

Thus, $A_{\boldsymbol{\beta}}$, A_ℓ and A_h belong to $\mathscr{G}_{\mathsf{NW}}$ over $\mathbb{F}$. □

3.1 Proof of Theorem 1

Claim 3.2. *Let f be a homogeneous degree-d polynomial in $\mathbb{F}[\mathbf{x}]$. If $\mathscr{G}_f$ contains the matrices $A_{\boldsymbol{\beta}}$, A_ℓ and A_h (for all choices of $\boldsymbol{\beta}$, ℓ and h, as mentioned in Claim 3.1) then $f = \alpha\cdot\mathsf{NW}$ for some $\alpha\in\mathbb{F}$.*

Proof. Let $f\neq 0$, otherwise we have nothing to prove. The presence of $A_{\boldsymbol{\beta}}$ in $\mathscr{G}_f$ implies that f is a set-multilinear polynomial with respect to the partition $\biguplus_{i\in[d]}\mathbf{x}_i$. If not then there is a term $\alpha\cdot m$ in f, where $\alpha\in\mathbb{F}^\times$ and m is a degree-d monomial with no $\mathbf{x}_t$-variables for some $t\in[d]$. Pick a $\gamma\in\mathbb{F}^\times$ such that $\gamma^d\neq 1$ [8]. Now, set $\beta_i = \gamma$ for $i\in[d]\backslash\{t\}$ and $\beta_t = \gamma^{-(d-1)}$ so that

[7] Recall, $[d-k-1] = \{0,1,\ldots,d-k-2\}$

[8] As $|\mathbb{F}|\neq d+1$, such a γ always exists.

$\prod_{i\in[d]} \beta_i = 1$ is satisfied. When A_β is applied on $\mathbf{x}$, the term $\alpha \cdot m$ maps to $\alpha\gamma^d \cdot m \neq \alpha \cdot m$, implying that $f(A_\beta \cdot \mathbf{x}) \neq f(\mathbf{x})$.

As f is set-multilinear, every term of f is of the kind $\alpha_p \cdot m_p$, where $\alpha_p \in \mathbb{F}^\times$ and $p \in \mathbb{F}_d[z]$ with $\deg(p) \leq d-1$. This is because any function from $\mathbb{F}_d$ to $\mathbb{F}_d$ can be represented by a univariate polynomial of degree at most $d-1$. We now show that $\deg(p) \leq k$ for every term $\alpha_p \cdot m_p$ in f. Suppose not. Then, there is a term $\alpha_p \cdot m_p$ such that $p = a_r z^r + \cdots + a_0$, $r > k$ and $a_r \neq 0$. When A_ℓ is applied on $\mathbf{x}$, the term $\alpha_p \cdot m_p$ gets mapped to $\prod_{i\in[d]} \zeta^{i^\ell \cdot p(i)} \cdot \alpha_p \cdot m_p$. Now choose $\ell = d-r-1 \leq d-k-2$. That $\prod_{i\in[d]} \zeta^{i^\ell \cdot p(i)} \neq 1$ for this choice of ℓ can be argued as follows: Since $\prod_{i\in[d]} \zeta^{i^\ell \cdot p(i)} = \zeta^{\sum_{i\in\mathbb{F}_d} i^\ell \cdot p(i)}$, it is sufficient to show that $\sum_{i\in\mathbb{F}_d} i^\ell \cdot p(i) \neq 0$. Expanding the sum,

$$\sum_{i\in\mathbb{F}_d} i^\ell \cdot p(i) = a_r \left(\sum_{i\in\mathbb{F}_d} i^{d-1}\right) + a_{r-1}\left(\sum_{i\in\mathbb{F}_d} i^{d-2}\right) + \cdots + a_0\left(\sum_{i\in\mathbb{F}_d} i^{d-r-1}\right).$$

As argued in Equation (2), the above sum is $a_r \cdot (d-1) \neq 0$, implying $f(A_\ell \cdot \mathbf{x}) \neq f(\mathbf{x})$. Hence, every term $\alpha_p \cdot m_p$ of f must have $\deg(p) \leq k$.

When A_h is applied on $\mathbf{x}$, a term $\alpha_p \cdot m_p$ maps to $\alpha_p \cdot m_{p+h}$ which implies $\alpha_p = \alpha_{p+h}$. Running over all $h \in \mathbb{F}_d[z]_k$, we get $\alpha_p = \alpha$ for every $p \in \mathbb{F}_d[z]_k$, for some $\alpha \in \mathbb{F}^\times$. Hence, $f = \alpha \cdot \mathsf{NW}$.

□

4 Circuit testability for the NW polynomial and the flip theorem

In the following lemma, we show that NW is characterized by circuit identities (as defined in Definition 2.10). The proofs of Theorem 2 and 3 would follow from this characterization.

4.1 Characterization by circuit identitites

Lemma 4.1. *Polynomial* NW *is characterized by circuit identities over any field* $\mathbb{F}$.

Proof. Recall, $n = |\mathbf{x}| = d^2$. We show that if an n-variate polynomial $f \in \mathbb{F}[\mathbf{x}]$ satisfies the following polynomial identities then $f = \alpha \cdot \mathsf{NW}$ for some $\alpha \in \mathbb{F}$. The rows and columns of the $n \times n$ matrices in the identities below are indexed by the set $\{(i,j) : i,j \in \mathbb{F}_d\}$.

1. $q_1(f(A_i(u)\cdot\mathbf{x}), f(\mathbf{x}), u) = 0$, for $i \in [d]$, where $q_1(z_1,z_2,u) := z_1 - u\cdot z_2$. Here, $A_i(u) \in \mathbb{F}[u]^{n\times n}$ is a diagonal matrix with the $((i,j),(i,j))$-th entry as u, for every $j \in [d]$, and the other diagonal entries as 1.

2. $q_2(f(A_{a,r}\cdot\mathbf{x}), f(\mathbf{x})) = 0$, for $a \in \mathbb{F}_d^\times$ and $r \in [k+1]$, where $q_2(z_1,z_2) := z_1 - z_2$. Here, $A_{a,r} \in \mathbb{F}^{n\times n}$ with the $((i,j),(i,j+a\cdot i^r))$-th entry as 1, for every $i,j \in \mathbb{F}_d$, and the other entries as 0.

3. $q_3(f(A_t\cdot\mathbf{x})) = 0$, for $t \in [d]\backslash[k+1]$, where $q_3(z) := z$. Here, $A_t \in \mathbb{F}^{n\times n}$ is a diagonal matrix with the $((t,0),(t,0))$-th and the $((i,j),(i,j))$-th entries as 0, for every $i \in [k+1], j \in [d]\backslash\{0\}$, and the remaining diagonal entries as 1.

Observe that there are poly(n) many identities above: d many under item 1, $(d-1)(k+1)$ many under item 2, and $(d-k-1)$ many under item 3. Also, it is clear that every q_i is computable by a constant size circuit, and the matrices $A_i(u), A_{a,r}$ and A_t are computable by poly(n) size circuits. The identities under item 1 imply that f is a set-multilinear, homogeneous, degree-d polynomial. If not then f contains a term $\beta \cdot m$, where the degree of the $\mathbf{x}_i$-variables in m is $e \neq 1$ for some $i \in [d]$. On applying $A_i(u)$ to $\mathbf{x}$, the term $\beta \cdot m$ gets mapped to $u^e \beta \cdot m \neq u\beta \cdot m$, implying $f(A_i(u) \cdot \mathbf{x}) \neq u \cdot f(\mathbf{x})$, i.e., $q_1(f(A_i(u) \cdot \mathbf{x}), f(\mathbf{x}), u) \neq 0$.

As f is set-multilinear and homogeneous, every term of f looks like $\alpha_p \cdot m_p$, where $\alpha_p \in \mathbb{F}^\times$ and $m_p = \prod_{i \in \mathbb{F}_d} x_{i,p(i)}$ for some $p \in \mathbb{F}_d[z]$ with $\deg(p) \leq d-1$. When $A_{a,r}$ is applied on $\mathbf{x}$, for some $a \in \mathbb{F}_d^\times$ and $r \in [k+1]$, a term $\alpha_p \cdot m_p$ maps to $\alpha_p \cdot m_{p+h}$, where $h = az^r \in \mathbb{F}_d[z]_k$. Since, f satisfies the identities in item 2, $f(A_{a,r} \cdot \mathbf{x}) = f(\mathbf{x})$ and so $\alpha_p \cdot m_{p+h}$ is also a term in f. By varying $a \in \mathbb{F}_d^\times$ and $r \in [k+1]$, we see that f contains the term $\alpha_p \cdot m_{p+h}$ for every $h \in \mathbb{F}_d[z]_k$. Thus, there is a set $\mathcal{S} \subseteq \mathbb{F}_d[z]_{d-1}$ such that f is of the form,

$$f = \sum_{p \in \mathcal{S}} \alpha_p \cdot \sum_{h \in \mathbb{F}_d[z]_k} m_{p+h}. \tag{3}$$

If $f \neq \alpha \cdot \mathsf{NW}$ for all $\alpha \in \mathbb{F}$, then there is a $p \in \mathbb{F}_d[z]$ with $\deg(p) > k$ such that f contains a term $\alpha_p \cdot m_p$ for some $\alpha_p \in \mathbb{F}^\times$. Let h be the polynomial in $\mathbb{F}_d[z]_k$ such that $h(i) = -p(i)$ for all $i \in [k+1]$. From Equation (3), f contains the term $\alpha_p \cdot m_{p+h}$. As $\deg(p) > k$, $h(z) \neq -p(z)$. So, there is a $t \in [d] \backslash [k+1]$ such that $p(t) + h(t) \neq 0$. On applying A_t to $\mathbf{x}$, only those terms of f survive that contain the variables $x_{0,0}, \ldots, x_{k,0}$ but do not contain $x_{t,0}$, and $\alpha_p \cdot m_{p+h}$ is such a term. Hence, $q_3(f(A_t \cdot \mathbf{x})) = f(A_t \cdot \mathbf{x}) \neq 0$. This contradicts f satisfying the identities in item 3. Therefore, $f = \alpha \cdot \mathsf{NW}$, for some $\alpha \in \mathbb{F}$. On the other hand, any $f = \alpha \cdot \mathsf{NW}$ satisfies all the identities. □

4.2 Proof of Theorem 2

Let $\mathtt{C}$ be a given circuit of size s over $\mathbb{F}$ that computes a n-variate polynomial $f = \mathtt{C}(\mathbf{x})$. Naturally, $\deg(f) \leq \delta(s)$. Algorithm 1 intends to check, in steps 2 and 3, if f satisfies the identities given in the proof of Lemma 4.1. If $f \neq \alpha \cdot \mathsf{NW}$ for all $\alpha \in \mathbb{F}$, then at least one of the identities is not satisfied. Observe that the polynomial $q_1(f(A_i(u) \cdot \mathbf{x}), f(\mathbf{x}), u)$ has degree bounded by $2 \cdot \delta(s)$, whereas the degrees of $q_2(f(A_{a,r} \cdot \mathbf{x}), f(\mathbf{x}))$ and $q_3(f(A_t \cdot \mathbf{x}))$ are at most $\delta(s)$. As $|\mathbb{F}| \geq 4 \cdot \delta(s)$, by Schwartz-Zippel lemma [Zip79, Sch80], step 4 returns 'False' with probability at least $\frac{1}{2}$. If $f = \alpha \cdot \mathsf{NW}$ for some $\alpha \in \mathbb{F}$ then all the identities are satisfied, and step 7 ensures that $\alpha = 1$. Clearly, the algorithm uses poly(s) field operations. The success probability can be boosted from $\frac{1}{2}$ to $1 - \exp(-s)$ by repeating the algorithm poly(s) times.

4.3 Proof of Theorem 3

Let $\mathtt{C}$ be a circuit of size s over a finite field $\mathbb{F}$. As NW is not computable by size-s circuits over $\mathbb{F}$ (by assumption), $\mathtt{C}(\mathbf{x}) - \mathsf{NW} \neq 0$. The polynomial $\mathtt{C}(\mathbf{x}) - \mathsf{NW}$ has degree bounded by $\delta(s)$, as $\delta(s) \geq d$. By Schwartz-Zippel lemma, for any $m \in \mathbb{N}$,

$$\Pr_{\mathbf{a}_1, \ldots, \mathbf{a}_m \in_r \mathbb{F}^n} [\mathtt{C}(\mathbf{a}_\ell) = \mathsf{NW}(\mathbf{a}_\ell), \text{ for all } \ell \in [m]] \leq \left(\frac{\delta(s)}{|\mathbb{F}|}\right)^m.$$

Algorithm 1 Circuit testing for NW

Input: Black-box access to a circuit $\mathtt{C}$ of size s over $\mathbb{F}$.
Output: 'True' if $\mathtt{C}(\mathbf{x}) = \mathsf{NW}$, else 'False'.

1. Pick $\mathbf{a} \in_r \mathbb{F}^n$ and $\mu \in_r \mathbb{F}$.
2. **for** $i \in [d], a \in \mathbb{F}_d^{\times}, r \in [k+1], t \in [d] \backslash [k+1]$ **do**
3. **if** $(\mathtt{C}(A_i(\mu) \cdot \mathbf{a}) - \mu \cdot \mathtt{C}(\mathbf{a}) \neq 0)$ or $(\mathtt{C}(A_{a,r} \cdot \mathbf{a}) - \mathtt{C}(\mathbf{a}) \neq 0)$ or $(\mathtt{C}(A_t \cdot \mathbf{a}) \neq 0)$ **then**
4. **return** 'False'.
5. **end if**
6. **end for**
7. Let $\mathbf{b} \in \mathbb{F}^n$ be an assignment obtained by setting $x_{i0} = 1$, for $i \in [d]$, and all other variables to zero. If $f(\mathbf{b}) \neq 1$, return 'False'. Else, return 'True'.

The number of size-s circuits over $\mathbb{F}$ is at most $2^{s^2+s} \cdot |\mathbb{F}|^s$ (as there are 2^s ways to label the nodes as $+$ and $\times$ gates, at most 2^{s^2} ways to choose the adjacency matrix of the underlying directed graph, and $|\mathbb{F}|^s$ ways to label the edges of a given graph). Therefore,

$$\Pr_{\mathbf{a}_1,\ldots,\mathbf{a}_m \in_r \mathbb{F}^n} [\exists \text{ a size-}s \text{ circuit } \mathtt{C} \text{ such that } \mathtt{C}(\mathbf{a}_\ell) = \mathsf{NW}(\mathbf{a}_\ell), \text{ for all } \ell \in [m]] \leq |\mathbb{F}|^s \cdot 2^{s^2+s} \cdot \left(\frac{\delta(s)}{|\mathbb{F}|}\right)^m.$$

By fixing $m = s^2 + 2s$, the above probability can be upper bounded by $\exp(-s)$ as $|\mathbb{F}| \geq 4 \cdot \delta(s)$.

Now, let us show that black-box derandomization of identity testing implies that such points $\mathbf{a}_1, \ldots, \mathbf{a}_m$ can be computed deterministically. Consider the class $\mathcal{C}$ of size-$(10s)$ circuits over $\mathbb{F}$ on $n+1$ variables $\mathbf{x} \uplus u$. Assume that $\mathcal{H} = \{(\mathbf{b}_0, \mu_0), \ldots, (\mathbf{b}_{w-1}, \mu_{w-1})\} \subseteq \mathbb{F}^{n+1}$ is a hitting set[9] for the circuit class $\mathcal{C}$, and $\mathcal{H}$ is computable using $\mathrm{poly}(s)$ field operations. Let $\mathcal{P} \subseteq \mathbb{F}^n$ be the set of points that includes $\mathbf{b}_0, \ldots \mathbf{b}_{w-1}$ along with $A_i(\mu_\ell) \cdot \mathbf{b}_\ell$, $A_{a,r} \cdot \mathbf{b}_\ell$ and $A_t \cdot \mathbf{b}_\ell$ for every $\ell \in [w], i \in [d], a \in \mathbb{F}_d^{\times}, r \in [k+1]$ and $t \in [d] \backslash [k+1]$. Finally, $\mathcal{P}$ also contains the point $\mathbf{b} \in \mathbb{F}^n$ obtained by setting $x_{i0} = 1$, for $i \in [d]$, and all other variables to zero. Observe that $|\mathcal{P}| = \mathrm{poly}(s)$ as $|\mathcal{H}| = \mathrm{poly}(s)$.

Claim 4.1. *For every size-s circuit $\mathtt{C}$ on n inputs, there is a point $\mathbf{a}$ in $\mathcal{P}$ such that $\mathtt{C}(\mathbf{a}) \neq \mathsf{NW}(\mathbf{a})$.*

Proof. As NW is not computable by size-s circuits, $f = \mathtt{C}(\mathbf{x}) \neq \alpha \cdot \mathsf{NW}$ for all $\alpha \in \mathbb{F}^{\times}$ [10]. Hence, at least one of the identities, in the proof of Lemma 4.1, is not satisfied by f unless $f = 0$. If $f = 0$ then $f(\mathbf{b}) \neq \mathsf{NW}(\mathbf{b}) = 1$, and so let $f \neq 0$. The degrees of the polynomials $q_1(f(A_i(u) \cdot \mathbf{x}), f(\mathbf{x}), u)$, $q_2(f(A_{a,r} \cdot \mathbf{x}), f(\mathbf{x}))$ and $q_3(f(A_t \cdot \mathbf{x}))$ are upper bounded by $2 \cdot \delta(s)$. Also, it can be verified that the polynomials $q_1(f(A_i(u) \cdot \mathbf{x}), f(\mathbf{x}), u)$, $q_2(f(A_{a,r} \cdot \mathbf{x}), f(\mathbf{x}))$ and $q_3(f(A_t \cdot \mathbf{x}))$ are computable by size-$(10s)$ circuits on $n+1$ variables $\mathbf{x} \uplus u$. Hence, $\mathcal{H}$ is a hitting-set for these polynomials. Without loss of generality, let $q_1(f(A_i(u) \cdot \mathbf{x}), f(\mathbf{x}), u) = 0$ be an identity that is not satisfied by f. Then, there is a $(\mathbf{b}_\ell, \mu_\ell) \in \mathcal{H}$ such that $q_1(f(A_i(\mu_\ell) \cdot \mathbf{b}_\ell), f(\mathbf{b}_\ell), \mu_\ell) \neq 0$ implying $f(A_i(\mu_\ell) \cdot \mathbf{b}_\ell) \neq \mu_\ell \cdot f(\mathbf{b}_\ell)$. On the other hand, $\mathsf{NW}(A_i(\mu_\ell) \cdot \mathbf{b}_\ell) = \mu_\ell \cdot \mathsf{NW}(\mathbf{b}_\ell)$ as NW satisfies all the identities. Therefore, either $f(A_i(\mu_\ell) \cdot \mathbf{b}_\ell) \neq \mathsf{NW}(A_i(\mu_\ell) \cdot \mathbf{b}_\ell)$ or $f(\mathbf{b}_\ell) \neq \mathsf{NW}(\mathbf{b}_\ell)$. This implies the claim as $A_i(\mu_\ell) \cdot \mathbf{b}_\ell$ and $\mathbf{b}_\ell$ belong to $\mathcal{P}$. □

[9] A set of points $\mathcal{H}$ is a hitting-set for a circuit class $\mathcal{C}$ if for every circuit $\mathtt{C} \in \mathcal{C}$ computing a non-zero polynomial, there exists a point $\mathbf{b} \in \mathcal{H}$ such that $\mathtt{C}(\mathbf{b}) \neq 0$. Black-box derandomization of identity testing for a circuit class amounts to constructing a hitting-set for the class.

[10] If $\alpha \cdot \mathsf{NW}$ is computable by a size-s circuit $\mathtt{C}$, for some $\alpha \in \mathbb{F}^{\times}$, then NW is also computable by a size-s circuit by appropriately scaling some of the edges feeding into the output gate of $\mathtt{C}$ by α^{-1}.

The proof of the theorem follows from the above claim and by observing that $\mathcal{P}$ can be constructed from $\mathcal{H}$ using $\text{poly}(s)$ field operations.

5 Structure of the group of symmetries of NW

The Lie algebra $\mathfrak{g}_{\mathsf{NW}}$ is a useful tool in investigating the symmetries of NW. In this section, we give a complete description of $\mathfrak{g}_{\mathsf{NW}}$ by giving an explicit $\mathbb{F}$-basis. The rows and columns of a $n \times n$ matrix in $\mathfrak{g}_{\mathsf{NW}}$ and $\mathscr{G}_{\mathsf{NW}}$ are indexed by the set $\{(i,j) : i,j \in \mathbb{F}_d\}$, which is naturally identified with the $\mathbf{x}$-variables, where $\mathbf{x} = (x_{0,0}\ x_{0,1} \dots\ x_{0,d-1}\ \dots\ x_{d-1,0}\ x_{d-1,1} \dots\ x_{d-1,d-1})^T$.

5.1 Lie algebra of NW

Lemma 5.1. *Let $\mathbb{F}$ be a field and $\text{char}(\mathbb{F}) \neq d$. The dimension of $\mathfrak{g}_{\mathsf{NW}}$ over $\mathbb{F}$ is $d-1$, and the diagonal matrices $B_1, \dots, B_\ell$ (defined below) form a $\mathbb{F}$-basis of $\mathfrak{g}_{\mathsf{NW}}$. For $\ell \in \{1, \dots, d-1\}$,*

$$(B_\ell)_{(i,j),(i,j)} = \begin{cases} 1, & \text{if } i = 0, j \in [d] \\ -1, & \text{if } i = \ell, j \in [d] \\ 0, & \text{otherwise.} \end{cases}$$

The lemma is proven in Section A.2 by carefully analysing a system of linear equations obtained from the monomials of NW. It follows that every $B \in \mathfrak{g}_{\mathsf{NW}}$ is of the form $\text{diag}(\alpha_0, \dots, \alpha_{d-1}) \otimes I_d$, where each $\alpha_i \in \mathbb{F}$ and $\sum_{i\in[d]} \alpha_i = 0$. It also follows that the continuous symmetries of NW consist of matrices of the form $A = \text{diag}(\beta_0, \dots, \beta_{d-1}) \otimes I_d$, where each $\beta_i \in \mathbb{C}$ and $\prod_{i\in[d]} \beta_i = 1$.

Corollary 5.1. *If $|\mathbb{F}| > \binom{d}{2}$ then there exists a $B = \text{diag}(\alpha_0, \dots, \alpha_d) \otimes I_d \in \mathfrak{g}_{\mathsf{NW}}$ such that $\alpha_0, \dots, \alpha_{d-1}$ are distinct elements of $\mathbb{F}$ and $\sum_{i\in[d]} \alpha_i = 0$.*

Proof. Treat $\alpha_0, \dots, \alpha_{d-2}$ as formal variables and let $\alpha_{d-1} = -(\alpha_0 + \dots + \alpha_{d-2})$. By the Schwartz-Zippel lemma,

$$\Pr_{\alpha_0,\dots,\alpha_{d-2} \in_r \mathbb{F}} [\text{there exist } i,l \in [d] \text{ such that } i \neq l \text{ and } \alpha_i = \alpha_l] \leq \frac{\binom{d}{2}}{|\mathbb{F}|} < 1.$$

Hence, there exists such a $B \in \mathfrak{g}_{\mathsf{NW}}$. □

Let $A \in \mathscr{G}_{\mathsf{NW}}$. For $i,l \in [d]$, the (i,l)-th *block of* A, denoted A_{il}, is a sub-matrix of A whose rows are indexed by the set $\{(i,j) : j \in [d]\}$ (called the i-th block of rows) and columns indexed by $\{(l,j) : j \in [d]\}$ (called the l-th block of columns).

Corollary 5.2. *Every $A \in \mathscr{G}_{\mathsf{NW}}$ is a block-permuted matrix with block size d.*

Proof. Choose a $B \in \mathfrak{g}_{\mathsf{NW}}$ arbitrarily. From Lemma 2.2, there exists a $C \in \mathfrak{g}_{\mathsf{NW}}$ such that

$$A \cdot C = B \cdot A.$$

From Lemma 5.1, $B = \text{diag}(\alpha_0, \dots, \alpha_{d-1}) \otimes I_d$ and $C = \text{diag}(\gamma_0, \dots, \gamma_{d-1}) \otimes I_d$, where $\sum_{i\in[d]} \alpha_i = \sum_{i\in[d]} \gamma_i = 0$. The above equation implies, for every $i,l \in [d]$,

$$\gamma_l \cdot A_{il} = \alpha_i \cdot A_{il},$$

where A_{il} is the (i,l)-th block of A. If A is not block-permuted then for some $l \in [d]$, there are non-zero blocks A_{il} and $A_{i'l}$ such that $i \neq i'$ (as A is non-singular). For this choice of l, i and i', the last equation implies $\gamma_l = \alpha_i = \alpha_{i'}$. This contradicts Corollary 5.1, as B is chosen arbitrarily. □

5.2 Proof of Theorem 4

Let $A \in \mathscr{G}_{\mathsf{NW}}$. The goal is to show that $A = D \cdot P$, where $D, P \in \mathscr{G}_{\mathsf{NW}}$ are diagonal and permutation matrices respectively. As A is block-permuted (by Corollary 5.2), there is a permutation μ on $[d]$ such that the only non-zero blocks of A are the $(i, \mu(i))$-th blocks for $i \in [d]$. Lemma 2.1 implies,

$$H_{\mathsf{NW}}(\mathbf{x}) = A^T \cdot H_{\mathsf{NW}}(A \cdot \mathbf{x}) \cdot A. \tag{4}$$

The rows and columns of $H_{\mathsf{NW}}(\mathbf{x})$ and $H_{\mathsf{NW}}(A \cdot \mathbf{x})$ are indexed by the $\mathbf{x}$-variables, and the i-th block of rows and columns by the $\mathbf{x}_i$-variables for $i \in [d]$. We can also view $H_{\mathsf{NW}}(\mathbf{x})$ and $H_{\mathsf{NW}}(A \cdot \mathbf{x})$ as block matrices with the (i, l)-th block defined by the i-th block of rows and l-th block of columns. Let C_{il} and B_{il} be the (i, l)-th blocks of $H_{\mathsf{NW}}(\mathbf{x})$ and $H_{\mathsf{NW}}(A \cdot \mathbf{x})$ respectively. Then

$$C_{il} = \left(\frac{\partial^2 \mathsf{NW}}{\partial x_{i,j} \partial x_{l,r}}\right)_{j,r \in [d]} \quad \text{and} \quad B_{il} = \left(\frac{\partial^2 \mathsf{NW}}{\partial x_{i,j} \partial x_{l,r}}(A \cdot \mathbf{x})\right)_{j,r \in [d]}. \tag{5}$$

Observation 5.1. *Let $\pi = \mu^{-1}$. Then, for every $i, l \in [d]$,*

$$(A^T_{\pi(i)i})^{-1} \cdot C_{il} \cdot (A_{\pi(l)l})^{-1} = B_{\pi(i)\pi(l)}. \tag{6}$$

Proof. The only non-zero block among the i-th block of rows in A^T is $A^T_{\pi(i)i}$, and the only non-zero block among the l-th block of columns in A is $A_{\pi(l)l}$. Hence, from Equation (4), we have $C_{il} = A^T_{\pi(i)i} \cdot B_{\pi(i)\pi(l)} \cdot A_{\pi(l)l}$. As A is block-permuted and invertible, $A^T_{\pi(i)i}$, $A_{\pi(l)l}$ are also invertible. □

For contradiction, suppose A is not a product of a diagonal matrix and a permutation matrix. As A is block-permuted, there is a $l \in [d]$ such that $A_{\pi(l)l}$ has a column containing more than one non-zero entries which implies $(A_{\pi(l)l})^{-1}$ also has a column containing more than one non-zero entries; let this be the r-th column of $(A_{\pi(l)l})^{-1}$, where $r \in [d]$. We work with this choice of l and r, and fix $i \in [d] \setminus \{l\}$ arbitrarily, in Equation (6). For $j \in [d]$, let g_{jr} and f_{jr} be the (j, r)-th entries of the matrices in the LHS and RHS of Equation (6) respectively. As $g_{jr} = f_{jr}$, the evaluation dimensions of g_{jr} and f_{jr} must be equal with respect to every $\mathbf{z} \subseteq \mathbf{x}$. However, the following claim shows that this is false. Thus, A is a product of a diagonal matrix and a permutation matrix.

Claim 5.1. *Let $d \geq 2k + 4$. For every $j \in [d]$, there exists $\mathbf{z} \subseteq \mathbf{x}$ such that* $\text{evalDim}_{\mathbf{z}}(g_{jr}) > \text{evalDim}_{\mathbf{z}}(f_{jr})$.

The proof of Claim 5.1 is given in Section A.3. It is a simple exercise to show that if $A \in \mathscr{G}_{\mathsf{NW}}$ and $A = D \cdot P$, where D and P are diagonal and permutation matrices respectively, then $D, P \in \mathscr{G}_{\mathsf{NW}}$.

6 Is NW characterized by its symmetries over $\mathbb{R}$?

The permanent is characterized by its symmetries over reals. It is natural to ask if this is also true for the NW polynomial. To answer the question, we need a detailed understanding of the diagonal and permutation symmetries of NW. As mentioned in the last section, the set of continuous symmetries of NW consists of diagonal matrices of the form $A = \text{diag}(\beta_0, \ldots, \beta_{d-1}) \otimes I_d$, where each $\beta_i \in \mathbb{C}$ and $\prod_{i \in [d]} \beta_i = 1$. We have seen, in Claim 3.1, that NW has discrete diagonal symmetries over $\mathbb{C}$ (obtained from a d-th root of unity) which play a crucial role in its symmetry characterization over $\mathbb{C}$. However, we show in the following lemma that NW does not have any discrete diagonal symmetry over $\mathbb{R}$. The proof of the lemma is given in Appendix A.4.

Lemma 6.1. *If $D \in \mathscr{G}_{\mathsf{NW}}$ is a diagonal matrix with real entries then D is a continuous symmetry of* NW*. In other words, D is of the form $D = diag(\beta_0, \ldots, \beta_{d-1}) \otimes I_d$, where each $\beta_i \in \mathbb{R}$ and $\prod_{i\in[d]} \beta_i = 1$.*

Any set-multilinear polynomial with respect to the partition $\uplus_{i\in[d]}\mathbf{x}_i$ has the above kind of diagonal symmetries. As the diagonal symmetries of NW over $\mathbb{R}$ are not special, we turn to the permutation symmetries. Could it be that the permutation symmetries of NW imply a symmetry characterization over $\mathbb{R}$?

Let $P \in \mathscr{G}_{\mathsf{NW}}$ be a permutation matrix, and σ the corresponding permutation on $\mathbf{x}$, i.e. $\sigma(x_{i,j}) = (P \cdot \mathbf{x})(i,j)$. As P is block-permuted (by Corollary 5.2), there exist a permutation μ on $\mathbb{F}_d$ and a permutation ψ on $\mathbb{F}_d[z]_k$ such that for every $h \in \mathbb{F}_d[z]_k$, $\sigma(x_{i,h(i)}) = x_{\mu(i),\psi(h)(\mu(i))}$. It can be easily verified that a (μ,ψ) pair (where μ is a permutation on $\mathbb{F}_d$ and ψ is a permutation on $\mathbb{F}_d[z]_k$) *yields a permutation symmetry* of NW via the map $\sigma : x_{i,h(i)} \mapsto x_{\mu(i),\psi(h)(\mu(i))}$ if and only if for every $i \in \mathbb{F}_d$ and $h, p \in \mathbb{F}_d[z]_k$, the following is satisfied:

$$h(i) = p(i) \quad \text{implies} \quad \psi(h)(\mu(i)) = \psi(p)(\mu(i)) \quad \text{and vice versa.} \tag{7}$$

The task now boils down to understanding which (μ,ψ) pairs satisfy the above condition. Towards this, we have the following observation, which is easy to prove using Equation (7).

Observation 6.1. *Fix $a, b \in \mathbb{F}_d^\times$, $c \in \mathbb{F}_d$ and $h_0 \in \mathbb{F}_d[z]_k$ arbitrarily. Let $\mu(i) = bi + c$ for all $i \in \mathbb{F}_d$ and $\psi(h) = a \cdot h(\frac{z-c}{b}) + h_0$ for all $h \in \mathbb{F}_d[z]_k$. Then, μ is a permutation on $\mathbb{F}_d$, ψ is a permutation on $\mathbb{F}_d[z]_k$ and the (μ,ψ) pair yields a permutation symmetry of* NW *via the map $\sigma : x_{i,h(i)} \mapsto x_{\mu(i),\psi(h)(\mu(i))}$, i.e., $x_{i,j} \mapsto x_{\mu(i),aj+h_0(\mu(i))}$ for every $i, j \in [d]$.*

Are all permutation symmetries of NW obtained from the (μ,ψ) pairs given in the above observation? We have a partial answer: If there exist $b \in \mathbb{F}_d^\times$ and $c \in \mathbb{F}_d$ such that $\mu(i) = bi + c$ for all $i \in \mathbb{F}_d$ then ψ has to be of the form given in Observation 6.1 for the (μ,ψ) pair to yield a permutation symmetry of NW (we omit the proof of this fact here). If the answer to the question turns out to be yes unconditionally, then NW is not symmetry characterized over $\mathbb{R}$. For example, the polynomial $\mathsf{NW}'_{d,k} := \sum_{e\in\mathbb{F}_d^\times,\, h\in\mathbb{F}_d[z]_k} \prod_{i\in\mathbb{F}_d} x_{i,\, e.i^{k+1}+h(i)}$ also has these permutation symmetries.

7 Few problems

In conclusion, we state a few problems on the NW polynomial which, if resolved, would shed more light on this fundamental polynomial family.

1. Is the $\mathcal{NW} = \{\mathsf{NW}_{d,k} : d \text{ is a prime}\}$ family VNP-complete for a suitable choice of k (say, $k = d^\epsilon$ for a constant $\epsilon > 0$)?
2. Is there an efficient algorithm to check if $\mathsf{NW}(\mathbf{a}) = 0$ for a given point $\mathbf{a} \in \{0,1\}^n$?
3. Is there an efficient algorithm to do equivalence testing for NW, i.e. given black-box access to an n-variate polynomial f, check if there exists a $A \in \mathrm{GL}_n(\mathbb{F})$ such that $f = \mathsf{NW}(A \cdot \mathbf{x})$?
4. Give a complete description of the permutation symmetries of NW. In other words, are all the permutation symmetries captured in Observation 6.1?

For the permanent polynomial, the answers to the first three questions are known to be positive.

Acknowledgment

We would like to thank Neeraj Kayal and Meena Mahajan for some insightful discussions on the design polynomial family.

References

[Aar17] Scott Aaronson. P=?NP. *Electronic Colloquium on Computational Complexity (ECCC)*, 24:4, 2017.

[AB87] Noga Alon and Ravi B. Boppana. The monotone circuit complexity of boolean functions. *Combinatorica*, 7(1):1–22, 1987.

[Ajt83] Miklós Ajtai. Σ_1^1-formulae on finite structures. *Annals of Pure and Applied Logic*, 24(1):1–48, 1983.

[Ats06] Albert Atserias. Distinguishing SAT from polynomial-size circuits, through black-box queries. In *21st Annual IEEE Conference on Computational Complexity (CCC 2006), 16-20 July 2006, Prague, Czech Republic*, pages 88–95, 2006.

[BÖ0] Peter Bürgisser. *Completeness and Reduction in Algebraic Complexity Theory*, volume 7 of *Algorithms and Computation in Mathematics*. Springer-Verlag Berlin Heidelberg, 2000.

[BIJL18] Markus Bläser, Christian Ikenmeyer, Gorav Jindal, and Vladimir Lysikov. Generalized matrix completion and algebraic natural proofs. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 1193–1206, 2018.

[BIP16] Peter Bürgisser, Christian Ikenmeyer, and Greta Panova. No Occurrence Obstructions in Geometric Complexity Theory. In *IEEE 57th Annual Symposium on Foundations of Computer Science, FOCS 2016, 9-11 October 2016, Hyatt Regency, New Brunswick, New Jersey, USA*, pages 386–395, 2016.

[CKW11] Xi Chen, Neeraj Kayal, and Avi Wigderson. Partial derivatives in arithmetic complexity and beyond. *Foundations and Trends in Theoretical Computer Science*, 6(1-2):1–138, 2011.

[CLS18] Suryajith Chillara, Nutan Limaye, and Srikanth Srinivasan. Small-depth multilinear formula lower bounds for iterated matrix multiplication, with applications. In *35th Symposium on Theoretical Aspects of Computer Science, STACS 2018, February 28 to March 3, 2018, Caen, France*, pages 21:1–21:15, 2018.

[CM14] Suryajith Chillara and Partha Mukhopadhyay. Depth-4 lower bounds, determinantal complexity: A unified approach. In *31st International Symposium on Theoretical Aspects of Computer Science (STACS 2014), STACS 2014, March 5-8, 2014, Lyon, France*, pages 239–250, 2014.

[EGdOW18] Klim Efremenko, Ankit Garg, Rafael Mendes de Oliveira, and Avi Wigderson. Barriers for Rank Methods in Arithmetic Complexity. In *9th Innovations in Theoretical Computer Science Conference, ITCS 2018, January 11-14, 2018, Cambridge, MA, USA*, pages 1:1–1:19, 2018.

[FKS16] Michael A. Forbes, Mrinal Kumar, and Ramprasad Saptharishi. Functional lower bounds for arithmetic circuits and connections to boolean circuit complexity. In *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*, pages 33:1–33:19, 2016.

[FLMS15] Hervé Fournier, Nutan Limaye, Guillaume Malod, and Srikanth Srinivasan. Lower Bounds for Depth-4 Formulas Computing Iterated Matrix Multiplication. *SIAM J. Comput.*, 44(5):1173–1201, 2015.

[FPS08] Lance Fortnow, Aduri Pavan, and Samik Sengupta. Proving SAT does not have small circuits with an application to the two queries problem. *J. Comput. Syst. Sci.*, 74(3):358–363, 2008.

[Fro97] Georg Frobenius. Ueber die darstellung der endlichen gruppen durch linearc substitutionen. *Sitzungber. der Berliner Akademie*, 7:994–1015, 1897.

[FSS81] Merrick L. Furst, James B. Saxe, and Michael Sipser. Parity, circuits, and the polynomial-time hierarchy. In *22nd Annual Symposium on Foundations of Computer Science, Nashville, Tennessee, USA, 28-30 October 1981*, pages 260–270, 1981.

[FSV17] Michael A. Forbes, Amir Shpilka, and Ben Lee Volk. Succinct hitting sets and barriers to proving algebraic circuits lower bounds. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 653–664, 2017.

[Ges16] Fulvio Gesmundo. Gemetric aspects of iterated matrix multiplication. *Journal of Algebra*, 461:42–64, 2016.

[GK98] Dima Grigoriev and Marek Karpinski. An exponential lower bound for depth 3 arithmetic circuits. In *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, May 23-26, 1998*, pages 577–582, 1998.

[GKKS14] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Approaching the Chasm at Depth Four. *J. ACM*, 61(6):33:1–33:16, 2014.

[GKSS17] Joshua A. Grochow, Mrinal Kumar, Michael E. Saks, and Shubhangi Saraf. Towards an algebraic natural proofs barrier via polynomial identity testing. *CoRR*, abs/1701.01717, 2017.

[Gro12] Joshua Abraham Grochow. *Symmetry and equivalence relations in classical and geometric complexity theory*. PhD thesis, Department of Computer Science, The University of Chicago, Chicago, Illinois, 2012.

[Hal15] Brian C Hall. *Lie Groups, Lie Algebras and Representations An Elementary introduction*. Springer, second edition, 2015.

[Hås86] Johan Håstad. Almost optimal lower bounds for small depth circuits. In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing, May 28-30, 1986, Berkeley, California, USA*, pages 6–20, 1986.

[Hüt16] Jesko Hüttenhain. The Stabilizer of Elementary Symmetric Polynomials. *CoRR*, abs/1607.08419, 2016.

[IMW17] Christian Ikenmeyer, Ketan D. Mulmuley, and Michael Walter. On vanishing of kronecker coefficients. *Computational Complexity*, 26(4):949–992, 2017.

[IP16] Christian Ikenmeyer and Greta Panova. Rectangular kronecker coefficients and plethysms in geometric complexity theory. In *IEEE 57th Annual Symposium on Foundations of Computer Science, FOCS 2016, 9-11 October 2016, Hyatt Regency, New Brunswick, New Jersey, USA*, pages 396–405, 2016.

[Kay12] 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.

[KLSS17] Neeraj Kayal, Nutan Limaye, Chandan Saha, and Srikanth Srinivasan. An Exponential Lower Bound for Homogeneous Depth Four Arithmetic Formulas. *SIAM J. Comput.*, 46(1):307–335, 2017.

[KNST17] Neeraj Kayal, Vineet Nair, Chandan Saha, and Sébastien Tavenas. Reconstruction of Full Rank Algebraic Branching Programs. In *32nd Computational Complexity Conference, CCC 2017, July 6-9, 2017, Riga, Latvia*, pages 21:1–21:61, 2017.

[KS14a] Mrinal Kumar and Shubhangi Saraf. The limits of depth reduction for arithmetic formulas: it's all about the top fan-in. In *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 136–145, 2014.

[KS14b] Mrinal Kumar and Shubhangi Saraf. Superpolynomial lower bounds for general homogeneous depth 4 arithmetic circuits. In *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part I*, pages 751–762, 2014.

[KS16a] Neeraj Kayal and Chandan Saha. Lower Bounds for Depth-Three Arithmetic Circuits with small bottom fanin. *Computational Complexity*, 25(2):419–454, 2016.

[KS16b] Mrinal Kumar and Shubhangi Saraf. Arithmetic circuits with locally low algebraic rank. In *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*, pages 34:1–34:27, 2016.

[KS16c] Mrinal Kumar and Shubhangi Saraf. Sums of products of polynomials in few variables: Lower bounds and polynomial identity testing. In *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*, pages 35:1–35:29, 2016.

[KS17a] Mrinal Kumar and Ramprasad Saptharishi. An exponential lower bound for homogeneous depth-5 circuits over finite fields. In *32nd Computational Complexity Conference, CCC 2017, July 6-9, 2017, Riga, Latvia*, pages 31:1–31:30, 2017.

[KS17b] Mrinal Kumar and Shubhangi Saraf. On the Power of Homogeneous Depth 4 Arithmetic Circuits. *SIAM J. Comput.*, 46(1):336–387, 2017.

[KSS14] Neeraj Kayal, Chandan Saha, and Ramprasad Saptharishi. A super-polynomial lower bound for regular arithmetic formulas. In *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 146–153, 2014.

[KST16a] Neeraj Kayal, Chandan Saha, and Sébastien Tavenas. An Almost Cubic Lower Bound for Depth Three Arithmetic Circuits. In *43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 11-15, 2016, Rome, Italy*, pages 33:1–33:15, 2016.

[KST16b] Neeraj Kayal, Chandan Saha, and Sébastien Tavenas. On the size of homogeneous and of depth four formulas with low individual degree. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, pages 626–632, 2016.

[Lip89] Richard J. Lipton. New directions in testing. In *Distributed Computing And Cryptography, Proceedings of a DIMACS Workshop, Princeton, New Jersey, USA, October 4-6, 1989*, pages 191–202, 1989.

[MM62] Marvin Marcus and Francis May. The permanent function. *Canadian Journal of Mathematics*, 14:177–189, 1962.

[MR04] Thierry Mignon and Nicolas Ressayre. A quadratic bound for the determinant and permanent problem. *International Mathematics Research Notes*, 2004(79):4241–4253, 2004.

[MS01] Ketan Mulmuley and Milind A. Sohoni. Geometric complexity theory I: an approach to the P vs. NP and related problems. *SIAM J. Comput.*, 31(2):496–526, 2001.

[Mul99] Ketan Mulmuley. Lower bounds in a parallel model without bit operations. *SIAM J. Comput.*, 28(4):1460–1509, 1999.

[Mul07] Ketan Mulmuley. On P vs. NP, Geometric Complexity Theory, and the Flip I: a high level view. *CoRR*, abs/0709.0748, 2007.

[Mul10] Ketan Mulmuley. Explicit proofs and the flip. *CoRR*, abs/1009.0246, 2010.

[Mul11] Ketan Mulmuley. On P vs. NP and geometric complexity theory: Dedicated to Sri Ramakrishna. *J. ACM*, 58(2):5:1–5:26, 2011.

[Mul12] Ketan Mulmuley. The GCT program toward the *P* vs. *NP* problem. *Commun. ACM*, 55(6):98–107, 2012.

[MW18] Cody Murray and R. Ryan Williams. Circuit lower bounds for nondeterministic quasi-polytime: an easy witness lemma for NP and NQP. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 890–901, 2018.

[NW94] Noam Nisan and Avi Wigderson. Hardness vs randomness. *J. Comput. Syst. Sci.*, 49(2):149–167, 1994.

[NW97] Noam Nisan and Avi Wigderson. Lower Bounds on Arithmetic Circuits Via Partial Derivatives. *Computational Complexity*, 6(3):217–234, 1997.

[Raz85] Alexander A. Razborov. Lower bounds on the monotone complexity of some Boolean functions. *Soviet Mathematics Doklady*, 31:354–357, 1985.

[Raz87] Alexander A. Razborov. Lower bounds on the size of bounded-depth networks over a complete basis with logical addition. *Mathematical Notes of the Academy of Sciences of the USSR*, 41(4):333–338, 1987.

[Raz09] Ran Raz. Multi-linear formulas for permanent and determinant are of super-polynomial size. *J. ACM*, 56(2):8:1–8:17, 2009.

[Reg02] Kenneth W. Regan. Understanding the mulmuley-sohoni approach to P vs. NP. *Bulletin of the EATCS*, 78:86–99, 2002.

[RR97] Alexander A. Razborov and Steven Rudich. Natural Proofs. *J. Comput. Syst. Sci.*, 55(1):24–35, 1997.

[RY09] Ran Raz and Amir Yehudayoff. Lower Bounds and Separations for Constant Depth Multilinear Circuits. *Computational Complexity*, 18(2):171–207, 2009.

[Sch80] Jacob T. Schwartz. Fast Probabilistic Algorithms for Verification of Polynomial Identities. *J. ACM*, 27(4):701–717, 1980.

[Smo87] Roman Smolensky. Algebraic Methods in the Theory of Lower Bounds for Boolean Circuit Complexity. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA*, pages 77–82, 1987.

[Val79] Leslie G. Valiant. Completeness classes in algebra. In *Proceedings of the 11h Annual ACM Symposium on Theory of Computing, April 30 - May 2, 1979, Atlanta, Georgia, USA*, pages 249–261, 1979.

[Wil14] Ryan Williams. Nonuniform ACC Circuit Lower Bounds. *J. ACM*, 61(1):2:1–2:32, 2014.

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *Symbolic and Algebraic Computation, EUROSAM '79, An International Symposiumon Symbolic and Algebraic Computation, Marseille, France, June 1979, Proceedings*, pages 216–226, 1979.

A Appendix

A.1 Two observations on the design polynomial family

Observation A.1. *Let $k = k(d) \in [d]$ be an arbitrarily fixed,* poly(d)*-time computable, function of d. The design polynomial family $\mathcal{NW} := \{\mathsf{NW}_{d,k} : d \text{ is a prime}\}$ is in* VNP.

Proof. Owing to the density of primes, $\mathcal{NW}$ is a p-bounded family [Val79] as the number of variables and the degree of $\mathsf{NW}_{d,k}$ are both polynomial functions of d. By Proposition 2.20 of [BÖ0], a p-bounded family $\{f_i\}_{i\in\mathbb{N}}$ is in VNP (i.e. p-definable) if the *coefficient computing function* for f_i is in #P. The coefficient computing function for f_i takes input a monomial in the variables of f_i and outputs the coefficient of the monomial in f_i. The coefficient computing function for $\mathsf{NW}_{d,k}$ can be shown to be in P as follows: Given a monomial m, check if it is set-multilinear in the sets $\mathbf{x}_0, \ldots, \mathbf{x}_{d-1}$. If not, the coefficient of m is 0 in $\mathsf{NW}_{d,k}$. Otherwise, let $m = x_{0,j_0} \cdots x_{d-1,j_{d-1}}$. Obtain a polynomial $h \in \mathbb{F}_d[z]_{d-1}$ by interpolating the points $(0, j_0), \ldots, (d-1, j_{d-1})$. Compute k from d. If $\deg(h) \leq k$ then coefficient of m in $\mathsf{NW}_{d,k}$ is 1 else it is 0. □

Observation A.2. *Suppose $f \in \mathbb{F}[\mathbf{y}]$ is a degree-r polynomial having s monomials. Then, for $d \geq s$ and $d - k \geq r$, f is an affine projection of $\mathsf{NW}_{d,k}$.*

Proof. Fix a univariate $h \in \mathbb{F}_d[z]_k$ and set the variables $x_{0,h(0)}, \ldots, x_{k-1,h(k-1)}$ to 1 and other variables of $\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}$ to 0. The low-intersection property of $\mathsf{NW}_{d,k}$ ensures that under this setting, exactly d monomials remain in $\mathsf{NW}_{d,k}$. Moreover, these d monomials are pairwise variable disjoint and each monomial contains $d - k$ variables. As $d \geq s$ and $d - k \geq r$, we can map these d monomials to monomials of f via a simple substitution map from $\mathbf{x}$ to $\mathbf{y} \cup \mathbb{F}$. Hence, there is a $A \in \mathbb{F}^{n\times|\mathbf{y}|}$ and $\mathbf{b} \in \mathbb{F}^n$ such that $\mathsf{NW}_{d,k}(A \cdot \mathbf{y} + \mathbf{b}) = f$; in other words, f is an affine projection of $\mathsf{NW}_{d,k}$. □

A.2 Proof of Lemma 5.1

Recall that the rows and columns of a matrix in $\mathfrak{g}_{\mathsf{NW}}$ are indexed by the set $\{(i,j) : i,j \in \mathbb{F}_d\}$. By Definition 2.7, $B = (\alpha_{(i,j),(l,r)})_{i,j,l,r\in[d]} \in \mathfrak{g}_{\mathsf{NW}}$ if and only if the following equation is satisfied:

$$\sum_{i,j,l,r\in[d]} \alpha_{(i,j),(l,r)} \cdot x_{l,r} \cdot \partial_{ij}\mathsf{NW} = 0, \qquad \text{where } \partial_{ij}\mathsf{NW} := \frac{\partial \mathsf{NW}}{\partial x_{i,j}}. \tag{8}$$

Claim A.1. *Every $B = (\alpha_{(i,j),(l,r)})_{i,j,l,r\in[d]} \in \mathfrak{g}_{\mathsf{NW}}$ is a diagonal matrix.*

Proof. Let $i,j,l,r \in [d]$, such that $(i,j) \neq (l,r)$. It follows from the low-intersection property of NW that the terms $x_{l,r} \cdot \partial_{ij}\mathsf{NW}$ and $x_{u,v} \cdot \partial_{st}\mathsf{NW}$ in Equation (8) are monomial disjoint for every $s,t,u,v \in [d]$ satisfying $(s,t) \neq (i,j)$ or $(u,v) \neq (l,r)$. Hence, $\alpha_{(i,j),(l,r)} = 0$ and B is diagonal. □

Thus, $\mathfrak{g}_{\mathsf{NW}}$ can be viewed as a subspace of $\mathbb{F}^n$ by associating a column vector $\mathbf{w}_B := B \cdot \mathbf{1} \in \mathbb{F}^n$ with every $B \in \mathfrak{g}_{\mathsf{NW}}$, where $\mathbf{1}$ is the all-one column vector in $\mathbb{F}^n$. The coordinates of $\mathbf{w}_B$ are indexed by $\{(l,r) : l,r \in \mathbb{F}_d\}$ and $\mathbf{w}_B(l,r) = \alpha_{(l,r),(l,r)}$ is its (l,r)-th coordinate. Now, we construct a matrix $D \in \mathbb{F}^{n\times n}$ using degree-0 and degree-1 polynomials in $\mathbb{F}_d[z]_k$, such that $\mathfrak{g}_{\mathsf{NW}}$ (viewed as a subspace of $\mathbb{F}^n$) is contained in $\mathrm{Ker}_{\mathbb{F}}(D)$, the kernel of D [11]. This would help us find $\dim_{\mathbb{F}}(\mathfrak{g}_{\mathsf{NW}})$.

[11] Matrix D would just be a part of the coefficient matrix of the linear system obtained from the equations $\sum_{l\in[d]} \alpha_{(l,h(l)),(l,h(l))} = 0$, for all $h \in \mathbb{F}_d[z]_k$. Here, $\{\alpha_{(l,r),(l,r)} : l,r \in \mathbb{F}_d\}$ are the d^2 variables of the system.

Construction of matrix D. The rows of D are indexed by $\{(a,b) : a,b \in \mathbb{F}_d\}$, where (a,b) corresponds to the univariate $bz + a \in \mathbb{F}_d[z]$. The columns are indexed by $\{(l,r) : l,r \in \mathbb{F}_d\}$, where (l,r) corresponds to the variable $x_{l,r}$ (as before). D is a $0/1$ matrix. The $((a,b),(l,r))$-th entry of D is 1 if $x_{l,r}$ is present in the monomial $\prod_{i\in\mathbb{F}_d} x_{i,bi+a}$, else it is 0. Denote the (a,b)-th row of D by R_{ab}. We record a few easy-to-verify properties of D below:

1. For $a,b \in [d]$, R_{ab} contains d many 1.
2. For every $a \in [d]$, the rows $\{\mathsf{R}_{ab} : b \in [d]\}$ contain 1 in the $(0,a)$-th column and 0 in the columns indexed by $(0,r)$ where $r \neq a$.
3. Let $B \in \mathfrak{g}_{\mathsf{NW}}$ and $\mathbf{w}_B(l,r) = \alpha_{(l,r),(l,r)}$ for $l,r \in \mathbb{F}_d$. Then, $(D \cdot \mathbf{w}_B)(a,b) = \sum_{l\in[d]} \alpha_{(l,bl+a),(l,bl+a)}$, which is the coefficient of monomial $\prod_{l\in\mathbb{F}_d} x_{l,bl+a}$ in the LHS of Equation (8). This implies $(D \cdot \mathbf{w}_B)(a,b) = 0$ for every $a,b \in [d]$, and hence, $\mathbf{w}_B \in \mathrm{Ker}_{\mathbb{F}}(D)$.

We argue that the rank of D is at least $d^2 - d + 1$, by showing the $\mathbb{F}$-linear independence of the rows indexed by $\{(a,b) : a \in [d-1], b \in [d]\}$ and $(d-1,0)$. This, along with property 3, would imply that $\dim_{\mathbb{F}}(\mathfrak{g}_{\mathsf{NW}}) \leq d-1$. Property 2 implies that it is sufficient to show the $\mathbb{F}$-linear independence of the $d^2 - d$ rows indexed by $\{(a,b) : a \in [d-1], b \in [d]\}$, as the row indexed by $(d-1,0)$ contains 1 in the column indexed by $(0,d-1)$ and this column contains 0 in the rows indexed by $\{(a,b) : a \in [d-1], b \in [d]\}$.

Claim A.2. *The rows $\{\mathsf{R}_{ab} : a \in [d-1], b \in [d]\}$ are $\mathbb{F}$-linearly independent, if $\mathrm{char}(\mathbb{F}) \neq d$.*

Proof. We multiply these rows with formal variables $\Gamma := \{\gamma_{ab} : a \in [d-1], b \in [d]\}$, and show that if the following equation holds then each $\gamma_{ab} = 0$. The number of Γ-variables is $|\Gamma| = d^2 - d$.

$$\sum_{a\in[d-1],b\in[d]} \gamma_{ab} \cdot \mathsf{R}_{ab} = 0.$$

From the above equation, we get d^2 linear equations in the Γ-variables, one for every coordinate of the rows. Fix $a \in [d-1]$ and $b \in [d]$ arbitrarily. From property 1, there are exactly d equations (one for each $l \in [d]$) containing the variable γ_{ab}. We can naturally identify these d equations with $l \in [d]$. The variables γ_{ab} and $\gamma_{a'b'}$ are present in the equation corresponding to a $l \in [d]$ if and only if $bl + a = b'l + a'$ over $\mathbb{F}_d$. Equation (9) corresponds to $l = 0$ and Equation (10) corresponds to a $l \in [d]\backslash\{0\}$.

$$\gamma_{a\,0} + \cdots + \gamma_{a\,b} + \cdots + \gamma_{a\,d-1} = 0, \tag{9}$$

$$\left(\sum_{a'\in[d-1]\backslash\{a\}} \gamma_{a'b'}\right) + \gamma_{ab} = 0, \qquad \text{where } b' = b + \frac{a-a'}{l}. \tag{10}$$

For $a \in [d-1]$ and $b,l \in [d]$, denote the linear forms at the LHS of these equations as 'Equation $(9)_{a,b}$' and 'Equation $(10)_{a,b,l}$'. A simple counting argument imply the following.

Observation A.3. *Let $a \in [d-1]$ and $b \in [d]$. Consider the d linear forms, Equation $(9)_{a,b}$ and Equation $(10)_{a,b,l}$ for $l \in [d]\backslash\{0\}$. Every pair of these d linear forms has γ_{ab} as the only common Γ-variable. Further, these d linear forms together contain all the Γ-variables except the variables in $\{\gamma_{a'b} : a' \in [d-1] \setminus \{a\}\}$.*

The next two observations will help us conclude that $\gamma_{ab} = 0$.

Observation A.4. *Let $a \in [d-1]$, $b \in [d]$ and $b' \in [d] \setminus \{b\}$. There is exactly one linear form in $\{$Equation $(10)_{a,b',l} : l \in [d] \setminus \{0\}\}$ that contains no Γ-variable from $\{\gamma_{a'b} : a' \in [d-1] \setminus \{a\}\}$. This unique linear form is Equation $(10)_{a,b',l(b')}$, where $l(b') = \frac{(d-1)-a}{b'-b}$.*

Proof. The linear form Equation $(10)_{a,b',l}$ contains a variable $\gamma_{a'b}$ if and only if $l = \frac{a'-a}{b'-b}$. If we choose $l = l(b') = \frac{(d-1)-a}{b'-b}$ then a' is forced to take value $d-1$. Thus, Equation $(10)_{a,b',l(b')}$ contains no variable from $\{\gamma_{a'b} : a' \in [d-1] \setminus \{a\}\}$. On the other hand, for $l \in [d] \setminus \{0\}$ and $l \neq l(b')$, there is exactly one variable in $\{\gamma_{a'b} : a' \in [d-1] \setminus \{a\}\}$ that belongs to Equation $(10)_{a,b',l}$. □

With $l(b')$ defined as above, we have the following observation.

Observation A.5. *Let $a \in [d-1]$, $b \in [d]$ and b', b'' be two distinct elements in $[d] \setminus \{b\}$. The linear forms Equation $(10)_{a,b',l(b')}$ and Equation $(10)_{a,b'',l(b'')}$ do not have any Γ-variable in common.*

Proof. For contradiction, suppose $\gamma_{\tilde{a}\tilde{b}}$ appears in both Equation $(10)_{a,b',l(b')}$ and Equation $(10)_{a,b'',l(b'')}$. Then, $\tilde{b} = b' + \frac{a-\tilde{a}}{l(b')} = b'' + \frac{a-\tilde{a}}{l(b'')}$. Hence,

$$b' - b'' = (a - \tilde{a}) \cdot \left(\frac{1}{l(b'')} - \frac{1}{l(b')} \right) = (a - \tilde{a}) \cdot \frac{b'' - b'}{(d-1) - a} \quad ,$$

by plugging in the values of $l(b')$ and $l(b'')$. As $\tilde{a} \neq d-1$, the above equality cannot hold. □

Finally, consider the following equation, which is implied from Equations (9) and (10),

$$\text{Equation } (9)_{a,b} \; + \sum_{l \in [d] \setminus \{0\}} \text{Equation } (10)_{a,b,l} \; - \sum_{b' \in [d] \setminus \{b\}} \text{Equation } (10)_{a,b',l(b')} \; = \; 0.$$

By Observation A.3, Equation $(9)_{a,b} + \sum_{l \in [d] \setminus \{0\}}$ Equation $(10)_{a,b,l}$ is the sum of $d \cdot \gamma_{ab}$ and all the Γ-variables barring $\{\gamma_{a'b} : a' \in [d-1] \setminus \{a\}\} \uplus \{\gamma_{ab}\}$. On the other hand, Observations A.4 and A.5 and a simple counting argument, imply that $\sum_{b' \in [d] \setminus \{b\}}$ Equation $(10)_{a,b',l(b')}$ is the sum of all the Γ-variables barring $\{\gamma_{a'b} : a' \in [d-1] \setminus \{a\}\} \uplus \{\gamma_{ab}\}$. Therefore, $\gamma_{ab} = 0$ as $\mathrm{char}(\mathbb{F}_d) \neq d$. This proves the $\mathbb{F}$-linear independence of $\{\mathsf{R}_{ab} : a \in [d-1], b \in [d]\}$. □

Thus, we have shown that $\dim_{\mathbb{F}}(\mathfrak{g}_{\mathsf{NW}}) \leq d-1$. This immediately implies that $\dim_{\mathbb{F}}(\mathfrak{g}_{\mathsf{NW}}) = d-1$, as the matrices $B_1, \ldots, B_{d-1}$ (in the statement of Lemma 5.1) are $\mathbb{F}$-linearly independent and they belong to $\mathfrak{g}_{\mathsf{NW}}$ (as they satisfy Equation (8)).

A.3 Proof of Claim 5.1

Recall the choice of l, r and i from the paragraph before the statement of Claim 5.1.

Observation A.6. *For every $j, s \in [d]$, the (j,s)-th entry of C_{il} equals*

$$\sum_{\substack{h \in \mathbb{F}_d[z]_k \\ h(i)=j,\, h(l)=s}} \; \prod_{t \in [d] \setminus \{i,l\}} x_{t,h(t)}.$$

The number of monomials in the above polynomial is d^{k-1}.

Proof. The proof follows directly from Equation (5). □

Observation A.7. *The polynomials in two distinct entries of C_{il} are monomial disjoint.*

Proof. Let $(j,s) \neq (j',s')$. The monomials of the polynomial at the (j,s)-th entry of C_{il} correspond to univariate polynomials $h \in \mathbb{F}_d[z]_k$ such that $h(i) = j$ and $h(l) = s$, whereas the monomials of the polynomial at the (j',s')-th entry of C_{il} correspond to univariate polynomials $h' \in \mathbb{F}_d[z]_k$ such that $h'(i) = j'$ and $h'(l) = s'$. As two distinct degree-k univariates share at most k roots over $\mathbb{F}_d$ and $d - 2 \geq k + 1$, the two polynomials must be monomial disjoint. □

Recall that g_{jr} is the (j,r)-th entry of $(A^T_{\pi(i)i})^{-1} \cdot C_{il} \cdot (A_{\pi(l)l})^{-1}$ and f_{jr} is the (j,r)-th entry of $B_{\pi(i)\pi(l)}$.

Observation A.8. *For every $j \in [d]$, $g_{jr} \neq 0$ is a $\mathbb{F}$-linear combination of at least two entries of C_{il}.*

Proof. The proof follows immediately from the choice of l and r, and by observing that none of the rows of $(A^T_{\pi(i)i})^{-1}$ has all zero entries. □

Now, pick an arbitrary set $T \subseteq [d] \setminus \{i,l\}$ such that $|T| = k + 1$; this is possible as $d - 2 \geq k + 1$. Fix $\mathbf{z} = \biguplus_{w \in T} \mathbf{x}_w$.

Observation A.9. *For every $j \in [d]$, $\text{evalDim}_{\mathbf{z}}(f_{jr}) \leq d^{k-1}$.*

Proof. From Equation (5), we have

$$f_{jr} = \frac{\partial^2 \mathsf{NW}}{\partial x_{\pi(i),j} \partial x_{\pi(l),r}}(A \cdot \mathbf{x}).$$

Thus, f_{jr} is computed by a depth three circuit having top fan-in d^{k-1}. Further, as A is block-permuted, the circuit is set-multilinear with respect to the partition $\biguplus_{t \in [d] \setminus \{i,l\}} \mathbf{x}_t$. In other words, f_{jr} can be expressed as a sum of d^{k-1} many products of linear forms such that each product term is of the form $\prod_{t \in [d] \setminus \{i,l\}} \ell_t(\mathbf{x}_t)$, where ℓ_t is a linear form. The proof is immediate from this point. □

Observation A.10. *For every $j \in [d]$, $\text{evalDim}_{\mathbf{z}}(g_{jr}) \geq 2 \cdot d^{k-1}$.*

Proof. From Observations A.6, A.7 and A.8, we can infer that there exists a set $P \subseteq \mathbb{F}_d[z]_k$ of size $|P| \geq 2 \cdot d^{k-1}$ such that

$$g_{jr} = \sum_{h \in P} \beta_h \cdot \prod_{t \in [d] \setminus \{i,l\}} x_{t,h(t)}, \quad \text{where } \beta_h \in \mathbb{F} \setminus \{0\}.$$

Now, we argue that $\text{evalDim}_{\mathbf{z}}(g_{jr}) = |P|$. Clearly, $\text{evalDim}_{\mathbf{z}}(g_{jr}) \leq |P|$. For a fixed $h \in P$ and every $w \in T$, set the variables $x_{w,h(w)} = 1$ and the remaining variables of $\mathbf{z}$ to 0. This substitution reduces the above sum to a single term $\beta_h \cdot \prod_{t \in [d] \setminus (\{i,l\} \uplus T)} x_{t,h(t)}$, as $d - 2 \geq k + 1$. Moreover,

$$\prod_{t \in [d] \setminus (\{i,l\} \uplus T)} x_{t,h(t)} \neq \prod_{t \in [d] \setminus (\{i,l\} \uplus T)} x_{t,h'(t)},$$

for distinct $h, h' \in P$, as $(d-2) - (k+1) \geq k + 1$ (by assumption). Hence, under various similar substitutions of the $\mathbf{z}$-variables, we get $|P|$ distinct monomials implying $\text{evalDim}_{\mathbf{z}}(g_{jr}) \geq |P|$. □

A.4 Proof of Lemma 6.1

Evidently, the proof of Lemma 5.1 gives a proof of the following fact.

Fact 1. *Suppose* $\mathrm{char}(\mathbb{F}) \neq d$. *Consider the linear system over* $\mathbb{F}$ *obtained from the equations* $\sum_{i\in[d]} y_{i,h(i)} = 0$ *for all* $h \in \mathbb{F}_d[z]_k$, *where* $\{y_{ij} : i, j \in [d]\}$ *are the variables. The solution space of the system consists of the solutions* $y_{i,0} = y_{i,1} = \ldots = y_{i,d-1} = \alpha_i$ *for every* $i \in [d]$, *where* $\alpha_0, \ldots, \alpha_{d-1} \in \mathbb{F}$ *satisfy* $\sum_{i\in[d]} \alpha_i = 0$, *and these are the only solutions.*

Let $D \in \mathscr{G}_{\mathsf{NW}}$ be a diagonal matrix with real entries, and the $((i,j),(i,j))$-th entry of D be $\beta_{i,j} \in \mathbb{R}$ for $i, j \in [d]$. We can express $\beta_{i,j}$ as $\beta_{i,j} = (-1)^{\lambda_{i,j}} \cdot 2^{\gamma_{i,j}}$, where $\lambda_{i,j} \in \{0,1\}$ and $\gamma_{i,j} \in \mathbb{R}$. When D is applied on $\mathbf{x}$, a monomial $m_h = \prod_{i\in\mathbb{F}_d} x_{i,h(i)}$ of NW gets mapped to $\left(\prod_{i\in\mathbb{F}_d} (-1)^{\lambda_{i,h(i)}} \cdot 2^{\gamma_{i,h(i)}}\right) \cdot m_h$, implying $\prod_{i\in\mathbb{F}_d} (-1)^{\lambda_{i,h(i)}} = \prod_{i\in\mathbb{F}_d} 2^{\gamma_{i,h(i)}} = 1$. In other words,

$$\begin{aligned} \sum_{i\in[d]} \lambda_{i,h(i)} &= 0 \quad \text{over } \mathbb{F}_2, \text{ for all } h \in \mathbb{F}_d[z]_k, \text{ and} \\ \sum_{i\in[d]} \gamma_{i,h(i)} &= 0 \quad \text{over } \mathbb{R}, \text{ for all } h \in \mathbb{F}_d[z]_k. \end{aligned}$$

By invoking Fact 1 (over $\mathbb{F} = \mathbb{F}_2$ and over $\mathbb{F} = \mathbb{R}$) for the above two linear systems, we get $\lambda_{i,0} = \ldots = \lambda_{i,d-1} = \lambda_i$ and $\gamma_{i,0} = \ldots = \gamma_{i,d-1} = \gamma_i$ for every $i \in [d]$, where $\lambda_0, \ldots, \lambda_{d-1} \in \mathbb{F}_2$ (similarly, $\gamma_0, \ldots, \gamma_{d-1} \in \mathbb{R}$) satisfy $\sum_{i\in[d]} \lambda_i = 0$ in $\mathbb{F}_2$ (similarly, $\sum_{i\in[d]} \gamma_i = 0$ in $\mathbb{R}$). This implies $\beta_{i,0} = \ldots = \beta_{i,d-1} = \beta_i$ for every $i \in [d]$, where $\beta_0, \ldots, \beta_{d-1} \in \mathbb{R}$ satisfy $\prod_{i\in[d]} \beta_i = 1$.

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il