Towards a characterization of the symmetries of the Nisan-Wigderson polynomial family

A THESIS

SUBMITTED FOR THE DEGREE OF

Master of Science (Engineering)

IN THE

Faculty of Engineering

BY

Nikhil Gupta

Computer Science and Automation
Indian Institute of Science
Bangalore – 560 012 (INDIA)

August, 2017

Declaration of Originality

I, **Nikhil Gupta**, with SR No. **04-04-00-10-21-15-1-12618** hereby declare that the material presented in the thesis titled

Towards a characterization of the symmetries of the Nisan-Wigderson polynomial family

represents original work carried out by me in the **Department of Computer Science and Automation** at **Indian Institute of Science** during the years **2015-2017**.
With my signature, I certify that:

- I have not manipulated any of the data or results.
- I have not committed any plagiarism of intellectual property. I have clearly indicated and referenced the contributions of others.
- I have explicitly acknowledged all collaborative research and discussions.
- I have understood that any false claim will result in severe disciplinary action.
- I have understood that the work may be screened for any form of academic misconduct.

Date: Student Signature

In my capacity as supervisor of the above-mentioned work, I certify that the above statements are true to the best of my knowledge, and I have carried out due diligence to ensure the originality of the report.

Advisor Name: Advisor Signature

DEDICATED TO

My parents, Mukund and Chaitanya

who love and support me unconditionally.

Acknowledgements

First of all I want to thank my adviser Chandan Saha for his support in the past two years. Working with Chandan has been a great learning experience for me. His way of solving problems, command on the literature and excellent presentation skills have always been a source of inspiration for me. I am indebted for everything I learnt from him. I thank him for tolerating my silly mistakes and motivating me to be on the right track always. I am very fortunate to have a guide like him.

My interest in algebraic complexity theory emanated from the training in algebra provided by professor Dilip Patil. Dilip is like a father to me, who always motivates me to learn. His knowledge and way of teaching has influenced me to a great extent. I thank Dilip for all the formal and informal discussions on algebra, which helped me a lot in my research. I am also grateful to Arnab Bhattacharya and Pandurangan Chandrashekharan (IIT Madras) for teaching me algorithms, Chandan Saha for teaching computational complexity and algebraic geometry, and Dilip Patil and R. Vittal Rao for teaching linear algebra. I am also thankful to the staff of CSA department for their help. I am grateful to Neeraj Kayal (Microsoft Research India) for providing some insights on the discrete symmetries of Nisan-Wigderson polynomial mentioned in Chapter 5. I also want to acknowledge the organisers of *Mysore park workshop* for giving me an opportunity to attend the four days workshop on 'recent trends in complexity and algorithms' at Infosys Mysore.

My stay at IISc became more enjoyable because of my friends. Heartfelt thanks to Ishan Rastogi, Parth Verma, Lokesh Mohan and Anubhav Guleria for their wonderful company. I am grateful to Vineet Nair, for all the help. I also thank Sumant Hedge and Abhijat Sharma for wonderful discussions in the lab. I also want to thank Shweta Makhija for her help and support. I am thankful to Hemang Chaitanya Das for his love and care during the last two years and Srila Prabhupada for his value able teachings, that helped me a lot in the tough times.

Acknowledgements

Finally, I am extremely thankful to my family and relatives for having a firm belief on me. I am indebted to the unconditional and uninterrupted love and support from them. I thank my grandmother for her love, care and blessings, my mother for every thing she did for me and my father for inspiring me to follow my dreams. I also want to express my gratitude to Mukund and Chaitanya for constantly accompanying me and helping me in every difficulty. Without your support I would not have been here.

Abstract

Understanding the structure and complexity of a polynomial family is a fundamental problem of arithmetic circuit complexity. There are various approaches like studying the lower bounds, which deals with finding the smallest circuit required to compute a polynomial, studying the orbit and stabilizer of a polynomial with respect to an invertible transformation etc to do this. We have a rich understanding of some of the well known polynomial families like determinant, permanent, IMM etc. In this thesis we study some of the structural properties of the polynomial family called the Nisan-Wigderson polynomial family. This polynomial family is inspired from a well known combinatorial design called Nisan-Wigderson design and is recently used to prove strong lower bounds on some restricted classes of arithmetic circuits ([KSS14],[KLSS14], [KST16]). But unlike determinant, permanent, IMM etc, our understanding of the Nisan-Wigderson polynomial family is inadequate. For example we do not know if this polynomial family is in VP or VNP complete or VNP-intermediate assuming VP $\neq$ VNP, nor do we have an understanding of the complexity of its equivalence test. We hope that the knowledge of some of the inherent properties of Nisan-Wigderson polynomial like group of symmetries and Lie algebra would provide us some insights in this regard.

A matrix $A \in GL_n(\mathbb{F})$ is called a symmetry of an n-variate polynomial f if $f(A \cdot \boldsymbol{x}) = f(\boldsymbol{x})$. The set of symmetries of f forms a subgroup of $GL_n(\mathbb{F})$, which is also known as group of symmetries of f, denoted $\mathscr{G}_f$. A vector space is attached to $\mathscr{G}_f$ to get the complete understanding of the symmetries of f. This vector space is known as Lie algebra of group of symmetries of f (or Lie algebra of f), represented as $\mathfrak{g}_f$. Lie algebra of f contributes some elements of $\mathscr{G}_f$, known as continuous symmetries of f. Lie algebra has also been instrumental in designing efficient randomized equivalence tests for some polynomial families like determinant, permanent, IMM etc ([Kay11], [KNST17]).

In this work we completely characterize the Lie algebra of Nisan-Wigderson polynomial family. We show that $\mathfrak{g}_{NW}$ contains diagonal matrices of a specific type. The knowledge of $\mathfrak{g}_{NW}$

not only helps us to completely figure out the continuous symmetries of the Nisan-Wigderson polynomial family, but also gives some crucial insights into the other symmetries of Nisan-Wigderson polynomial (i.e. the discrete symmetries). Thereafter using *Hessian matrix* of Nisan-Wigderson polynomial and the concept of *evaluation dimension*, we are able to almost completely identify the structure of $\mathscr{G}_{NW}$. In particular we prove that any $A \in \mathscr{G}_{NW}$ is a product of diagonal and permutation matrices of certain kind that we call *block-permuted permutation matrix*. Finally, we give explicit examples of nontrivial block-permuted permutation matrices using the Frobenius automorphisms that establishes the richness of the discrete symmetries of the Nisan-Wigderson polynomial family.

Contents

List of Figures

Chapter 1

Introduction

Algebraic complexity theory (ACT) is a branch of computational complexity theory that seeks to understand the power and limitation of algebraic/arithmetic computation. The main objective of this area is to either give efficient algorithms for tractable problems using algebraic techniques, or show the limitation of solving a problem by algebraic means. Based on this, ACT is classified into two subareas namely *computational algebra* and *arithmetic circuit complexity*. Computational algebra deals with designing of fast algorithms using a number of tools from algebra, number theory, geometry, combinatorics etc, whereas arithmetic circuit complexity aims to give tight lower bounds for hard problems. Some of the important problems in computational algebra literature are polynomial factorization, matrix multiplication, computation of inverse and determinant of a matrix, primality testing, large integer multiplication and factorization. There has been a lot of development in this area in the last few decades and some of the well known results are matrix multiplication algorithm by Strassen[Str69], Discrete Fourier Transform by Cooley and Tukey [CT65], RSA algorithm used for encryption and decryption of messages [RSA78], parallel computation of determinant by Cshanky [Csa79], polynomial factorization ([Kal89], [LLL82]), deterministic primality testing ([AKS04]), graph isomorphism ([Bab16]) etc. These algorithms rely on various mathematical concepts, tools and techniques like Euler's totient function, Euclidean algorithm, elliptic curves, Chinese remaindering, Hensel lifting, group theory and many more. The utilization of such algorithms can be seen in the diverse areas of mathematics and computer science like cryptography, combinatorial geometry, coding theory, quantum computing etc.

Arithmetic circuit complexity is concerned with computation of polynomials[1]. Polynomials are

[1] primarily multivariate polynomials

very widely used in many branches of mathematics and theoretical computer science and they can be computed/represented using a succinct model known as *arithmetic circuit*. An arithmetic circuit accepts variables as input and outputs a polynomial using the operations $+$, $\times$ and field constants. An example is shown in 1.1. The number of operations required for computing a polynomial is captured by the *size* of arithmetic circuit. Size of the circuit is a vital measure of complexity of computation and computing a polynomial using smallest size circuit is an important question. Based on this, Leslie Valiant classified polynomials in two classes namely *VP* and *VNP* in his seminal work [Val79a] [1]. VP is an algebraic analog of (nonuniform) P and consists of all those families of polynomials of low degree which can be computed by circuits of small size [2]. An example of VP polynomial family (in short VP polynomial) is the symbolic determinant. On the other hand, VNP is an algebraic analog of (nonuniform) NP and contains a family of polynomial $\{f_n\}_{n\geq 1}$, if there is a polynomial time algorithm to compute coefficient of a given monomial in f_n [3]. Like NP complete problems, there are *VNP complete* polynomials families (simply, VNP complete polynomials). It was shown by Valiant that the symbolic permanent family is VNP complete [Val79b]. He further conjectured that permanent can not be computed by a circuit of small size. This is popularly known as *Valiant's hypothesis*. Apart from this, there is also an evidence of existence of polynomial families which are neither in VP nor VNP complete. These are called *VNP intermediate polynomials*. However the existence of such polynomial families is based on the assumption that Valiant's hypothesis is true (Corollary 5.19 of [B̈98]). Cut enumerator polynomial is one such polynomial [B̈98].

In the spirit of proving Valiant's conjecture, researchers started studying lower bounds for the arithmetic circuits with an objective to come up with an explicit polynomial f that requires a circuit of super polynomial size in the number of variables. Unfortunately we are still far from the desired goal as the best known lower bound for general arithmetic circuit is $\Omega(n \log n)$ given by Baur and Strassen in [BS83]. To get more insights, people started studying lower bounds for restricted circuits like constant depth [4] circuits. In a breakthrough result [AV08], Agrawal and Vinay showed that to prove exponential lower bound on general circuits it is enough to give exponential lower bound on *depth 4* circuit. Thereafter Gupta, Kamath, Kayal and Saptharishi showed in [GKKS13] that if a degree d polynomial over the field of characteristic zero is computed by a general arithmetic circuit of size s then the same polynomial can also be computed by a depth three circuit of size $s^{O(\sqrt{d})}$. This means proving strong lower bounds on depth three

[1] Leslie Valiant used the terms *p-bounded* and *p-definable* for VP and VNP respectively.
[2] By low degree and small size, we mean degree and size are polynomial in the number of variables.
[3] In fact, for membership in VNP, it is sufficient that the coefficient computation problem in in #P.
[4] *depth* of the circuit is the largest path from input to output node of the circuit.

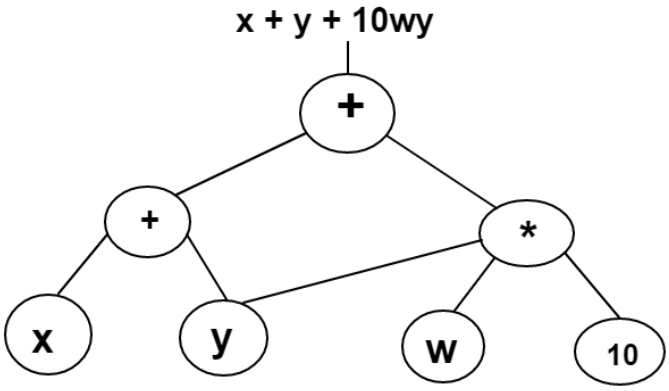

Figure 1.1: Arithmetic circuit computing polynomial $x + y + 10wy$

circuit will imply strong lower bound on general circuit also.

Apart from lower bounds there are a variety of interesting problems in arithmetic circuit complexity theory like *Polynomial identity testing (PIT)*, *Circuit reconstruction* and *Polynomial equivalence test*. In *PIT* we check if a given circuit computes formally zero polynomial [1]. There is a randomized algorithm for PIT due to *Schwartz-Zippel lemma* ([Zip79] and [Sch80]) but to give a polynomial time deterministic algorithm for this is a long standing open problem. However for some restricted arithmetic circuits PIT is solved in deterministic polynomial time, for example depth-3 circuit of bounded top fan-in ([DS06],[KS07], [KS08], [SS13]), diagonal circuits [Sax08], depth-4 multilinear circuits with bounded top fan-in ([SKMV10],[ASSS12]), read-once oblivious algebraic branching programs ([AGKS14]). PIT is strongly connected to arithmetic circuit lower bounds. Kabanets and Impaliazzo showed that if PIT admits a polynomial time deterministic algorithm then either Permanent is not computed by polynomial size arithmetic circuit or NEXP not in P/poly [KI04].

In *circuit reconstruction* we are given black box access to a circuit C and the main objective is to come up with a circuit D of size polynomial in the size of C such that the polynomials computed by C and D are same. The aim is to design a reconstruction algorithm (even randomized) whose running time is polynomial in the size of C. It is analogous to the learning problem of boolean functions.

Another problem called *Affine projection of polynomials* was studied in [Kay11]. We say a

[1] A polynomial f is called formally zero polynomial if f does not contain a monomial with non zero coefficient.

polynomial g is an affine projection of f if there exists a matrix A and a vector b such that $g(\mathbf{x}) = f(A \cdot \mathbf{x} + b)$. Many interesting problems like VP vs VNP, matrix multiplication etc are related to this problem. [Kay11] showed that the problem of checking if a given polynomial f is an affine projection of another given polynomial g is NP-hard. Then he considered the restricted version of this problem called *polynomial equivalence*, where matrix A is invertible and b is a zero vector. Even this problem is also not easy. In [AS06], Agrawal and Saxena showed that this problem is at least as hard as *Graph Isomorphism*. They also showed in the same paper that the complexity of polynomial equivalence test depends on the base field. If the base field is algebraically closed field or $\mathbb{R}$ or finite field then polynomial equivalence is decidable and has different complexities, but if the base field is $\mathbb{Q}$ then it is not clear if this problem is even decidable. However there are some instances of polynomial equivalence that can be solved using randomized polynomial time algorithms. If we fix the polynomial f as some of the well known polynomials like permanent, IMM [1] then the equivalence test can be done in randomized polynomial time ([Kay11], [KNST17]) over $\mathbb{Q}$ and the same for determinant over $\mathbb{C}$.

Equivalence test is interesting as (besides being a natural problem) it provides us a different view of the complexity of a polynomial family. The algorithms of equivalence test of permanent, determinant (over $\mathbb{C}$) and IMM used a tool called *Lie algebra*. It is an important concept used in representation theory. We discuss Lie algebra in Chapter 2. Designing equivalence test for a polynomial family has some connections to understand the group of *symmetries* of the polynomials in the family. Symmetries of polynomial families also play an important role in *Geometric complexity theory*.

Geometric Complexity Theory. A matrix $A \in GL_n(\mathbb{F})$ is a symmetry of an n-variate polynomial f if $f(\mathbf{x}) = f(A \cdot \mathbf{x})$. The set of symmetries of f forms a group with respect to matrix multiplication and it provides a lot of information about f. Inspired by this, Mulmuley and Sohoni introduced a new approach namely *Geometric Complexity Theory (GCT)* in 2001 to tackle the VP vs VNP problem [MS01]. The starting point of GCT was a famous result from *representation theory*, which says that permanent and determinant can be uniquely characterized by their group of symmetries. It means that if the symmetries of any degree n homogeneous polynomial f is same as the symmetries of Permanent (or Determinant) then f is a constant multiple of Permanent (or Determinant). GCT attempts to resolve VP vs VNP using tools from algebraic geometry and representation theory.

[1] IMM stands for iterated matrix multiplication. It is the polynomial defined as the first entry of product of variable matrices.

An initial task in GCT is to study the symmetries and *orbit closure* of a given polynomial, which can perhaps be helpful to give lower bounds on circuit computing that polynomial. The property of symmetry characterization for determinant and permanent has helped in identifying their orbit closures. Mulmuley and Sohoni conjectured [1] that the permanent is not contained in the orbit closure of polynomial size determinant. In other words it says that if there exist an $n \times n$ matrix X and an $m \times m$ matrix Y with entries as affine forms in n^2 variables such that permanent(X)= determinant(Y) then m is a super polynomial in n.

1.1 Previous works

The group of symmetries of the permanent was studied by Marcus and May ([MM62]),which provided many insights to understand the Lie algebra of permanent and design an efficient randomized equivalence test for it over $\mathbb{Q}$ ([Kay11]). For determinant polynomial, the efficient equivalence test is known only when the underlined field is $\mathbb{C}$ ([Kay11]). This algorithm was inspired from the Lie algebra of determinant, which was identified using its group of symmetries. The group symmetries of the determinant was given by Frobenius ([Fro97]). In [Ges16], the group of symmetries of a variant of IMM was given. Later Kayal, Nair, Saha and Tavenas figured out the group of symmetries of IMM, using which they identified the Lie algebra of IMM and gave an efficient randomized equivalence test for it ([KNST17]).

1.2 Motivation

In [KSS14] a polynomial named *Nisan-Wigderson polynomial* was introduced, which was used to prove strong lower bounds on a special class of arithmetic circuits called *regular arithmetic formula*. A variant of the same polynomial was used in the recent work by Kayal, Saha and Tavenas [KST16] to give an almost cubic lower bound for general depth three circuit. This polynomial family is inspired from a well known combinatorial design known as *Nisan-Wigderson design*. This design was introduced by Nisan and Wigderson in [NW94] and they called it (k, m) design. It is defined as a collection of subsets of a universe set such that each subset is of size m and any two subsets can have intersection of at most k (value of k is small as compared to m). Nisan-Wigderson design is one of the fundamental concept used in pseudo random number generation and randomness extraction. Apart from this, in arithmetic circuit complexity also this design is used to show the connections between circuit lower bounds and PIT [KI04]. In a Nisan-Wigderson polynomial (defined formally in the next section) the monomials are treated

[1] This is the restatement of Valiant's hypothesis.

as the subsets of (k, m) design.

It was shown in [KSS14] that Nisan-Wigderson polynomial is in VNP, but its exact computational complexity is not known. Like other well known polynomials (Permanent, Determinant, IMM) we are interested to know if this polynomial is in VP, or VP-intermediate (under some plausible assumptions) or VNP complete. This motivates us to study some of the structural properties of Nisan-Wigderson polynomial like group of symmetries and Lie algebra. In the spirit of GCT, we hope that the knowledge of group of symmetries of Nisan-Wigderson polynomial (and equivalence test for this family) will provide us some insights about the hardness of this polynomial. We also want to know if Nisan-Wigderson polynomial can also be uniquely characterized by its group of symmetries.

Another question that motivates us is the equivalence test of Nisan-Wigderson polynomial. We want to know if Nisan-Wigderson polynomial also admits a randomized equivalence test or is it that the test can not be done efficiently even with the help of randomness. Even a *no* answer will give us an explicit polynomial which is "harder" than permanent, determinant and IMM from the *perspective of equivalence test*. The Lie algebra of Nisan-Wigderson polynomial may provide us with some useful information that help us in doing an equivalence test for this family efficiently as it did in the case of permanent, determinant (over $\mathbb{C}$) and IMM.

1.3 Our Results

In this thesis we completely characterize the Lie algebra of Nisan-Wigderson polynomial and give the structure and some nontrivial elements of its group of symmetries. Before stating these results as theorems, we define Nisan-Wigderson polynomial.

Definition 1.1 *(Nisan-Wigderson polynomial)*
Let $k, q \in \mathbb{N}^*$, where q is a power of a prime number, then Nisan-Wigderson polynomial (denoted $NW_{q,k}(\boldsymbol{x})$) is defined as

$$NW_{q,k}(\boldsymbol{x}) = \sum_{h \in \mathbb{F}_q[t]_k} x_{0\,h(0)} \cdot x_{1\,h(1)} \cdots x_{q-1\,h(q-1)},$$

where $\mathbb{F}_q[t]_k := \{f \in \mathbb{F}_q[t] \mid \deg(f) \leq k\}$. Nisan-Wigderson polynomial is a set-multilinear (Definition 2.10) and homogeneous polynomial (Definition 2.9) of degree q. For brevity we drop the subscripts of $NW_{q,k}(\boldsymbol{x})$.

Theorem 1.1 ***(Lie algebra of Nisan-Wigderson polynomial)***

The Lie algebra of Nisan-Wigderson polynomial has dimension $(q-1)$ *over the field* $\mathbb{F}$[1] *for every* $k \geq 1$.

We give the proof of this theorem in Chapter 3. We show that its Lie algebra consists of diagonal matrices of a special type and give an explicit $\mathbb{F}$-basis of the Lie algebra. The next theorem gives the structure of group of symmetries of Nisan-Wigderson polynomial.

Theorem 1.2 ***(Structure of group of symmetries of Nisan-Wigderson polynomial)*** *Every element A of group of symmetries of Nisan-Wigderson polynomial is a product of a diagonal matrix and a permutation $q^2 \times q^2$ matrix.*

The proof of this theorem is given in Chapter 4. There we show that the permutation matrices in the above theorem have got to be *block-permuted* matrices (Definition 2.8). In the next theorem we show that this group contains discrete symmetries, that are elements other than the continuous symmetries of Nisan-Wigderson polynomial family. It would follow from Theorem 1.1 that the continuous symmetries of $NW(\boldsymbol{x})$ consist of diagonal matrices. Whereas we show in the proof of the following theorem that there are block-permuted permutation matrices[2] with non-trivial block permutation [3] in the group of symmetries of $NW(\boldsymbol{x})$. We will explain continuous and discrete symmetries of a polynomial in Chapter 2.

Theorem 1.3 ***(Discrete symmetries of Nisan-Wigderson polynomial)*** *The group of symmetries of Nisan-Wigderson polynomial has discrete symmetries. Moreover, there are discrete symmetries where the matrices are block-permuted permutation matrices with non trivial block permutation.*

The proof of this theorem is in Chapter 5. In this chapter we give some explicit discrete symmetries of $NW(\boldsymbol{x})$. We show that there are symmetries A of $NW(\boldsymbol{x})$ such that A is a non trivial block permutation matrix and A is a product of a diagonal and a permutation matrices.

1.4 Organization of the thesis

We present here the road map of our thesis. We state all the required definitions and preliminary results in Chapter 2. In Chapter 3 we give the proof of Theorem 1.1 and give an $\mathbb{F}$-basis of Lie algebra of the Nisan-Wigderson polynomial. The proof is obtained by a careful analysis of

[1] Characteristic of $\mathbb{F}$ is either zero or large enough.
[2] It is a permutation matrix, which is block permuted.
[3] the permutation σ in Definition 2.10 is not identity.

certain system of linear equations. Chapter 4 contains the proof of Theorem 1.2. The proof uses concepts of the *Hessian of a polynomial* and *evaluation dimension*. Thereafter in Chapter 5 we explicitly give some of the nontrivial discrete symmetries of $NW(\boldsymbol{x})$. Finally in Chapter 6 we discuss the future directions.

Chapter 2

Preliminaries

In this chapter we note the basic results that have been used in our work. Along with this we also touch on the required concepts of algebra very succinctly. In the first section, we specify the notations that are used in the thesis. The second section is devoted to the introduction of basic algebraic structure and in the third section we introduce some tools required to prove our results.

2.1 Notations and Terminology

Throughout the thesis, $[n]$ represents the set $\{0, \ldots, n-1\}$. However, at many places in the literature, $[n]$ is defined as $\{1, \ldots, n\}$ but here we are using this definition for our convenience. $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$. Unless specified, $\mathbb{F}$ denotes a field of characteristic zero or sufficiently large and $\mathbb{F}_q$ is the finite field of size q. The set of variables $\boldsymbol{x}$ is

$$\boldsymbol{x} = \biguplus_{\boldsymbol{i} \in [\boldsymbol{q}]} \boldsymbol{x_i},$$

where $\boldsymbol{x_i} := \{x_{i\,0}, \ldots, x_{i\,q-1}\}$, i.e. the variables $\boldsymbol{x_i}$ get precedence over the variables $\boldsymbol{x_j}$ if $i < j$ and within a set $\boldsymbol{x_i}$ the variable x_{ir} gets precedence over x_{il} if $r < l$. We impose the ordering $x_{0\,0} \prec \cdots \prec x_{0\,q-1} \prec \cdots \prec x_{q-1\,q-1}$ on $\boldsymbol{x}$. The set $\mathbb{F}[\boldsymbol{x}]$ is the ring of multivariate polynomials with coefficients from $\mathbb{F}$ and the set $\mathbb{F}_q[t]_k$ comprises of all the univariate polynomials of degree at most k with coefficients from $\mathbb{F}_q$. Let $f \in \mathbb{F}_q[t]_k$ and $\mathbf{v}_f$ be its coefficient vector defined as $\mathbf{v}_f = (a_0, a_1, \ldots, a_k)$, where a_i is the coefficient of t^i in f. We order the polynomials of $\mathbb{F}_q[t]_k$ using the lexicographic ordering on their coefficient vectors. We denote this ordered set as $(\mathbb{F}_q[t]_k, \preceq)$. Further $\mathrm{GL}_n(\mathbb{F})$ is the group of all $n \times n$ size invertible matrices over $\mathbb{F}$.

A polynomial family is a set of 'related' polynomials indexed by $n \in \mathbb{N}$. For example $\{Det_n\}$ contains the determinant of an $n \times n$ size variable matrix for all $n \in \mathbb{N}$.

2.2 Algebraic Preliminaries

In this section we give very concise introduction of basic algebraic structures and some of their properties. We refer the interested readers to [Her75], [Art91] for more details.

Definition 2.1 *(Permutation)*
Let S be any set. A bijective map on S is called a permutation on S.

If S is a finite set with cardinality n then there are $n!$ permutations on S.

Fact 2.1 *(Pigeonhole principle)*
Let S be a finite set and $\sigma : S \to S$ be a function. Then the following statements are equivalent

1. *σ is injective.*
2. *σ is surjective.*
3. *σ is bijective.*

Pigeonhole principle is stated in different forms and is one of the most widely used counting tool in mathematics.

Definition 2.2 *(Group)*
A set G with the binary operation $\cdot$ is called a group if it satisfies the following properties

1. *(Closure) For all $x, y \in G$, $x \cdot y$ is also in G.*
2. *(Associativity) For all $x, y, z \in G$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.*
3. *(Identity) There exists $1 \in G$ such that for all $x \in G, x \cdot 1 = 1 \cdot x = x$.*
4. *(Inverse) For every $x \in G$ there exists $x^{-1} \in G$ such that $x \cdot x^{-1} = x^{-1} \cdot x = 1$.*

G is called an abelian group or commutative group if for all $x, y \in G, x \cdot y = y \cdot x$. Examples of groups are $(\mathbb{Z}, +), (\mathbb{R}, \cdot)$ etc.

Definition 2.3 *(Field) A set $\mathbb{F}$ with the binary operations $+$ and $\cdot$ is called a field if*

1. *$(\mathbb{F}, +)$ is an abelian group.*

2. $(\mathbb{F}, \cdot)$ *is an abelian group.*

3. *(Distributivity) For* $x, y, z \in \mathbb{F}$, $x \cdot (y + z) = x \cdot y + x \cdot z$.

Examples of fields are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ and finite fields[1].

Characteristic of $\mathbb{F}$ is defined as the smallest natural number n such that $n \cdot 1 = 0$. If no such n exists then we say that $\mathbb{F}$ has characteristic zero. It is easy to show that the characteristic of a field is either 0 or a prime number.

Fact 2.2 *The cardinality of a finite field* $\mathbb{F}_q$ *is* q*, where* q *is equal to* p^n *for some prime number* p *and natural number* n*.*

The characteristic of $\mathbb{F}_q$ is p.

Definition 2.4 *(Field homomorphism)*
Let $\mathbb{F}$ *and* $\mathbb{K}$ *be fields. The map* $\psi : \mathbb{F} \to \mathbb{K}$ *is called a field homomorphism if for all* $a, b \in \mathbb{F}$*,*

1. $\psi(a + b) = \psi(a) + \psi(b)$,

2. $\psi(a \cdot b) = \psi(a) \cdot \psi(b)$.

In addition if ψ is bijective then it is called field isomorphism. Further, if $\mathbb{K} = \mathbb{F}$ then field isomorphism is also known as field automorphism.

Claim 2.2.1 *Let* $\mathbb{F}_q$ *be a finite field of characteristic* p *and* $q = p^n$*. Then the following map is a field automorphism.*

$$\begin{aligned} \sigma : \mathbb{F}_q &\to \mathbb{F}_q \\ a &\mapsto a^{p^i} \end{aligned}$$

for $i = 0, \ldots, n - 1$.

Proof: Let $a, b \in \mathbb{F}_p$. Then

$$\begin{aligned} \sigma(a + b) &= (a + b)^{p^i} \\ &= a^{p^i} + (p^i \cdot 1) \cdot a^{p^i - 1} b + \cdots + b^{p^i} && \text{(using Binomial theorem)} \\ &= a^{p^i} + b^{p^i} && \text{(Characteristic of } \mathbb{F}_q \text{ is } p) \\ &= \sigma(a) + \sigma(b). \end{aligned}$$

[1] It is a field having finite number of elements.

Also, $\sigma(ab) = \sigma(a) \cdot \sigma(b)$. Thus σ is a field homomorphism. Now we argue that σ is a bijective map. Since $\mathbb{F}_q$ is finite, it is enough to show that σ is injective. We prove this by showing that $\text{Ker}(\sigma) = \{0\}$. Let $a \in \text{Ker}(\sigma)$, $\sigma(a) = 0$, which means $a^{p^i} = 0$ thus $a = 0$. □

The automorphisms in the above claim are known as Frobenius automorphisms.

Fact 2.3 *Let $\mathbb{F}_{p^n}$ be a field of size p^n. Then the number of distinct Frobenius automorphisms of $\mathbb{F}_{p^n}$ are n.*

Fact 2.4 *Let $Aut(\mathbb{F}_{p^n})$ denote the group of all automorphisms of $\mathbb{F}_{p^n}$. Then the cardinality of $Aut(\mathbb{F}_{p^n})$ is n.*

In other words, Fact 2.4 says that the only automorphisms on finite fields are Frobenius automorphisms. The proof of these facts can be found in any elementary book on Galois theory or finite fields. Now we give a very brief introduction to vector spaces.

Definition 2.5 *(Vector Space)*
A set V with a binary operation $+$ is called a vector space over a field $\mathbb{F}$ if $(V, +)$ is an abelian group and there exists a map [1] $\cdot : \mathbb{F} \times V \to V$ such that for every $c \in \mathbb{F}$ and $v \in V$, $c \cdot v \in V$. In addition for every $x, y \in V$ and $a, b \in \mathbb{F}$ the following properties hold

1. $a \cdot (x + y) = a \cdot x + a \cdot y$.
2. $(a + b) \cdot x = a \cdot x + b \cdot x$.
3. $a \cdot (b \cdot x) = (a \cdot b) \cdot x$.
4. $1 \cdot x = x$.

Remarks 2.1 *In property 3 on the right hand side $\cdot$ is the multiplication operation of $\mathbb{F}$.*

An example of vector space is the set of $n \times n$ matrices with entries from $\mathbb{F}$, denoted by $M_n(\mathbb{F})$ or $\mathbb{F}^{n \times n}$. The elements of a vector space are called vectors and the elements of the base field $\mathbb{F}$ are called scalars. The set of vectors $S = \{v_1, \ldots, v_n\}$ is called a *generating set* of V if for any $x \in V$ there exist $a_1, \ldots, a_n \in \mathbb{F}$ such that $x = a_1 \cdot v_1 + \cdots + a_n \cdot v_n$. S is called *linearly independent over* $\mathbb{F}$ if $b_1 \cdot v_1 + \cdots + b_n \cdot v_n = 0$ with $b_1, \ldots, b_n \in \mathbb{F}$ implies $b_1 = \cdots = b_n = 0$. The set S is called an $\mathbb{F}$-basis of V if S is linearly independent over $\mathbb{F}$ and generating system of V.

[1] This is called scalar multiplication

Fact 2.5 *Every vector space over the field $\mathbb{F}$ has an $\mathbb{F}$-basis.*

Fact 2.6 *Any two basis of an $\mathbb{F}$-vector space V have same cardinalities. This cardinality is known as* dimension *of V.*

The proofs of these facts can be found in any basic book on linear algebra.

Definition 2.6 *(Block matrix)*
A matrix A is called a block matrix if A can be written using same size sub matrices or blocks. For example let

$$A = \begin{bmatrix} 1 & 0 & 3 & 9 \\ 0 & 2 & 4 & 8 \\ 4 & 6 & 7 & 5 \\ 8 & 3 & 9 & 2 \end{bmatrix}.$$

Then A can be written as a block matrix like

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix},$$

where

$$A_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, A_{12} = \begin{bmatrix} 3 & 9 \\ 4 & 8 \end{bmatrix}, A_{21} = \begin{bmatrix} 4 & 6 \\ 8 & 3 \end{bmatrix} A_{22} = \begin{bmatrix} 7 & 5 \\ 9 & 2 \end{bmatrix}$$

We can view every matrix as a block matrix by viewing every element as a block. Let T be a matrix of size $q^2 \times q^2$ and the rows and columns be divided into q sets, each of size q. The (i, j)-th block of T, denoted T_{ij} is indexed by i-th row block and j-th column block as shown in Figure 4.1. The blocks T_{ii} for $i \in q$ are known as diagonal blocks of T.

Definition 2.7 *(Block diagonal matrix)*
A block matrix $A \in M_{n^2}(\mathbb{F})$ with block size $n \times n$ is called a block diagonal matrix if all the off diagonal blocks of A are zero.

For example the following matrix A is a block diagonal matrix.

$$A = \begin{bmatrix} 1 & 4 & 0 & 0 \\ 2 & 3 & 0 & 0 \\ 0 & 0 & 4 & 8 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

Definition 2.8 *(Block permuted matrix)*
Let $A \in M_{n^2}(\mathbb{F})$ be a block matrix with block size $n \times n$. Then A is called a block permuted matrix if there exists a permutation σ on $[n]$ such that the blocks other than $A_{i,\sigma(i)}$ are zero for $i \in [n]$. $A_{i\sigma(i)}$ is the block of A indexed by i-th block of rows and $\sigma(i)$-th block of columns.

For example the following matrix A is a block permuted matrix .

$$A = \begin{bmatrix} 0 & 0 & 1 & 4 \\ 0 & 0 & 2 & 3 \\ 4 & 8 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{bmatrix}$$

2.3 Some tools and concepts

In this section we list some of the tools and concepts used in our results. We have divided this section into a number of subsections for clarity.

2.3.1 Nisan-Wigderson polynomial

In this section we first define homogeneous and set-multilinear polynomial and then state low intersection property of Nisan-Wigderson polynomial (Definition 1.1).

Definition 2.9 *(Homogeneous polynomial) Let $f \in \mathbb{F}[\boldsymbol{x}]$ be an n-variate polynomial. f is called a homogeneous polynomial of degree d if degree of every monomial of f is d.*

Definition 2.10 *(Set-multilinear polynomial)*
Let the set of variables $\boldsymbol{x}$ be partitioned into subsets as mentioned in Section 2.1. A polynomial f is called set-multilinear *with respect to the partition on $\boldsymbol{x}$ if every monomial of f contains exactly one variable from each set of the partition of $\boldsymbol{x}$.*

For example let $\boldsymbol{x} = \{x_{00}, x_{01}\} \cup \{x_{10}, x_{11}\}$. Then $f = x_{00}x_{10} + x_{01}x_{11}$ is a set-multilinear polynomial.

Nisan-Wigderson polynomial is a set-multilinear homogenous polynomial. It has a very interesting property called *low intersection property*. This property is stated as the following claim.

Claim 2.3.1 *Let m_1, m_2 be distinct monomials of $NW(\boldsymbol{x})$. Then m_1 and m_2 can have at most k variables in common.*

Proof: From the definition of $NW(\boldsymbol{x})$ we know that there exist distinct polynomials $h_1, h_2 \in \mathbb{F}_q[t]_k$ such that $m_1 = x_{0\,h_1(0)} \cdots x_{q-1\,h_1(q-1)}$ and $m_2 = x_{0\,h_2(0)} \cdots x_{q-1\,h_2(q-1)}$. Since $h_1 \neq h_2$ and their degrees are bounded by k, $h_1 - h_2$ can have at most k roots in $\mathbb{F}_q$, which implies that m_1 and m_2 can have at most k common variables. □

2.3.2 Partial derivatives

Let $g \in \mathbb{F}[y_0, \ldots, y_{n-1}]$ be a degree d polynomial. Then g can be written as follows

$$g = f_{i\,0} + f_{i\,1} \cdot y_i + f_{i\,2} \cdot y_i^2 \cdots + f_{i\,d} y_i^d,$$

where $f_{i\,0}, \ldots, f_{i\,d} \in \mathbb{F}[y_0, \cdots, y_{i-1}, y_{i+1}, \ldots y_{n-1}]$. *Partial derivative* of f with respect to y_i denoted $\frac{\partial f}{\partial y_i}$ is defined as

$$\frac{\partial f}{\partial y_i} := f_{i\,1} + 2 \cdot f_{i\,2} \cdot y_i + \cdots + (d-1) \cdot f_{i\,d} y_i^{d-1}.$$

Let $f, g \in \mathbb{F}[\boldsymbol{y}]$ and $a, b \in \mathbb{F}$. Then partial derivatives satisfy the following properties.

1. Linearity of derivatives:

$$\frac{\partial}{\partial y_i}(a \cdot f + b \cdot g) = a \cdot \frac{\partial(f)}{\partial y_i} + b \cdot \frac{\partial(g)}{\partial y_i}.$$

2. Derivative of product:

$$\frac{\partial}{\partial y_i}(f \cdot g) = \frac{\partial(f)}{\partial y_i} \cdot g + \frac{\partial(g)}{\partial y_i} \cdot f.$$

3. Chain Rule of partial derivatives: Let $f \in \mathbb{F}[y_0, \ldots, y_{r-1}]$ and $\boldsymbol{g} = (g_0, \ldots, g_{r-1})$, such that every $j \in [r]$, $g_j \in \mathbb{F}[\boldsymbol{z}]$, where $\boldsymbol{z} = \{z_0, \ldots, z_{n-1}\}$. The composition $f \circ \boldsymbol{g}$, which is a polynomial in $\mathbb{F}[\boldsymbol{z}]$ defined as

$$f \circ \boldsymbol{g} := f(g_0(\boldsymbol{z}), \ldots, g_{r-1}(\boldsymbol{z})).$$

   Then *chain rule* is stated as follows. For every $j \in [n]$,

$$\frac{\partial}{\partial z_j}(f \circ \boldsymbol{g}) = \sum_{i=0}^{r-1} \frac{\partial f}{\partial g_i} \cdot \frac{\partial g_i}{\partial z_j},$$

   where $\frac{\partial f}{\partial g_i}$ denotes $(\frac{\partial f}{\partial y_i} \circ \boldsymbol{g}) \in \mathbb{F}[\boldsymbol{z}]$ for all $i \in [r]$.

For more details on the applications of partial derivatives in arithmetic circuit complexity, the reader can refer to [CKW11].

2.3.3 Hessian of a polynomial

Definition 2.11 *(Hessian of a polynomial)*
Let $\boldsymbol{y}= (y_0, \ldots, y_{n-1})$ *be a set of* n *variables and* $f \in \mathbb{F}[\boldsymbol{y}]$*. Hessian of* f*, denoted* $H_f(\boldsymbol{y})$ *is an* $n \times n$ *matrix with entries from* $\mathbb{F}[\boldsymbol{y}]$ *defined as*

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

The rows and columns of $H_f(\boldsymbol{y})$ are indexed by $\boldsymbol{y}$. We here note an important property of $H_f(\boldsymbol{y})$, which will be used in the proof of Theorem 1.2.

Lemma 2.1 *(Lemma 2.6 of [CKW11])*
Let $f \in \mathbb{F}[\boldsymbol{y}]$ *be an* n*-variate polynomial and* $A \in \mathbb{F}^{n\times n}$ *be a linear transformation. Let* $g(\boldsymbol{y}) := f(A \cdot \boldsymbol{y})$*. Then*

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

Proof: Let $A = (a_{ij})_{i,j\in[n]}$. Then

$$g(\boldsymbol{y}) = f\left(\sum_{j=0}^{n-1} a_{0\,j} \cdot y_j, \ldots, \sum_{j=0}^{n-1} a_{n-1\,j} \cdot y_j\right).$$

Using chain rule of partial derivatives, we can write

$$\frac{\partial g}{\partial y_j} = \sum_{i=0}^{n-1} a_{i\,j} \cdot \frac{\partial f}{\partial y_i}(A \cdot \mathbf{y}),$$

for $j \in [n]$. Now for all $j, l \in [n]$,

$$\begin{aligned}\frac{\partial^2 g}{\partial y_j \cdot \partial y_l} &= \sum_{i=0}^{n-1} a_{ij} \cdot \left(\sum_{r=0}^{n-1} a_{rl} \cdot \frac{\partial^2 f}{\partial y_i \cdot \partial y_r}(A \cdot \boldsymbol{y})\right) \\ &= \sum_{i,r\in[n]} a_{ij} \cdot \frac{\partial^2 f}{\partial y_i \cdot \partial y_r}(A \cdot \boldsymbol{y}) \cdot a_{rl}\,.\end{aligned}$$

The above equation leads to the desired result. □

2.3.4 Evaluation dimension of a polynomial

Definition 2.12 *(Evaluation dimension)*
Let $f \in \mathbb{F}[\boldsymbol{y}]$ be an n-variate polynomial and $\boldsymbol{z} \subseteq \boldsymbol{y}$. Let V be the vector space defined as

$$V := \mathbb{F}\text{-}span\ \{f(\boldsymbol{a},\ \boldsymbol{y} \setminus \boldsymbol{z}) \mid \boldsymbol{a} \in \mathbb{F}^{|\boldsymbol{z}|}\}.$$

Evaluation dimension of f, denoted $evalDim_{\boldsymbol{z}}(f)$ is the dimension of V.

Remarks 2.2 *In the above definition $f(\boldsymbol{a},\ \boldsymbol{y} \setminus \boldsymbol{z})$ denotes polynomial f after substituting the variables of set $\boldsymbol{z}$ with $\boldsymbol{a}$ in f.*

For example let $f = y_1y_2^2 + y_3y_4$ and $\boldsymbol{z}$= $\{y_1, y_3\}$. Then after setting $\boldsymbol{z}$ to different values from field $\mathbb{F}$, $f = \alpha y_2^2 + \beta y_4$, where $\alpha, \beta \in \mathbb{F}$ and $\text{evalDim}_{\boldsymbol{z}}(f) = 2$.

Claim 2.3.2 *$evalDim_{\boldsymbol{z}}(f)$ is always finite for any $\boldsymbol{z} \subseteq \boldsymbol{y}$ and is upper bounded by the number of monomials in f .*

Proof: Let f has r monomials. Once the set $\boldsymbol{z}$ is fixed, every monomial in $f(\mathbf{a}\,, \boldsymbol{y} \setminus \boldsymbol{z})$ is either fixed to a constant or remains a monomial in the variables of $\boldsymbol{y} \setminus \boldsymbol{z}$ after the substitution of $\boldsymbol{z}$ with $\boldsymbol{a}$. Thus the $\text{evalDim}_{\boldsymbol{z}}(f)$ is upper bounded by r.

□

2.3.5 Lie group and Group of symmetries of a polynomial

In this subsection we give a brief overview of the matrix Lie group and symmetries of a polynomial. We state here the important lemmas and refer the reader to [Hal03] for proofs. In this subsection, we assume that the underlying field $\mathbb{F}$ is $\mathbb{C}$.

Definition 2.13 *(Convergence of a sequence of matrices)*
Let $(A_m)_{m\in\mathbb{N}}$ be a sequence of $n \times n$ matrices over the field $\mathbb{F}$. This sequence converges *to a matrix A if the sequence defined by the (i,j)-th entries of A_m for $m \in \mathbb{N}$ converges to the (i,j)-th entry of A for $i, j \in [n]$.*

In the above definition, A can be written as $A = \lim_{m\to\infty} A_m$.

Definition 2.14 *(Matrix Lie group)*
A subgroup G of $GL_n(\mathbb{F})$ is called matrix Lie group *if G satisfies the following property: If A_m is a sequence of matrices in G and it converges to A then either $A \in G$ or $A \notin GL_n(\mathbb{F})$.*

Matrix Lie group is also known as *continuous group* or *Lie group*. An example of matrix Lie group is special linear group, denoted $\mathrm{SL}_n(\mathbb{F})$. It is the group of all invertible matrices over $\mathbb{F}$ with determinant equal to one.

Definition 2.15 *(Matrix Exponential)*
Let $M \in \mathbb{F}^{n\times n}$. Exponential *of M, denoted e^M is defined as the following power series*

$$e^M = \sum_{i=0}^{\infty} \frac{M^i}{i!},$$

where M^0 is $n \times n$ identity matrix and M^i is the product of M with itself i times. The above power series converges for every M.

Claim 2.3.3 *Let $X = diag(a_0, \ldots, a_{n-1})$[1] be a diagonal matrix with $a_i \in \mathbb{F}, i \in [n]$. Then $e^X = diag(e^{a_0}, \ldots, e^{a_{n-1}})$.*

Definition 2.16 *(Symmetry of a polynomial)*
Let $f \in \mathbb{F}[\boldsymbol{y}]$ be an n-variate polynomial and $A \in GL_n(\mathbb{F})$. A is called a symmetry of f *if $f(\boldsymbol{y}) = f(A \cdot \boldsymbol{y})$.*

Claim 2.3.4 *Let $f \in \mathbb{F}[\boldsymbol{y}]$ be an n-variate polynomial. The set of all symmetries of f forms a group under matrix multiplication.*

Proof: Let A, B, C be the symmetries of f.

1. (Closure): $f(A \cdot (B \cdot \mathbf{y})) = f(B \cdot \mathbf{y}) = f(\mathbf{y})$. This shows that $A \cdot B$ is also a symmetry of f.
2. (Associativity): $f((A \cdot (B \cdot C)) \cdot \mathbf{y}) = f(((A \cdot B) \cdot C) \cdot \mathbf{y})$.
3. (Identity): The identity matrix I_n is the identity of this group.
4. (Inverse): $f(A^{-1} \cdot \mathbf{y}) = f(\mathbf{y})$, which means A^{-1} is also a symmetry of f.

□

This is called group of symmetries of f and is denoted by $\mathscr{G}_f$.

Remarks 2.3 *The group of symmetry of a polynomial f is also called the isotropy subgroup of f, group of automorphism of f or stabilizer of f.*

[1] diag(...) is used to denote a diagonal matrix.

Now we show that the group of symmetries of a polynomial is a Lie group.

Lemma 2.2 *(Theorem 4.1 of [Wel16])*
Let $f \in \mathbb{F}[\boldsymbol{y}]$ be an n-variate polynomial. Then $\mathscr{G}_f$ is a Lie group.

Proof: Let the sequence $(A_m)_m$ of matrices in $\mathscr{G}_f$ converges to a matrix A i.e. $A = \lim_{m\to\infty} A_m$. To show that $\mathscr{G}_f$ is a Lie group, we have to either show that $A \in \mathscr{G}_f$ or A is not invertible. The fact that polynomials are continuous function implies the following

$$\begin{aligned} f(A \cdot \mathbf{y}) &= f(\lim_{m\to\infty} A_m \cdot \mathbf{y}) \\ &= \lim_{m\to\infty} f(A_m \cdot \mathbf{y}) \\ &= \lim_{m\to\infty} f(\mathbf{y}) \\ &= f(\mathbf{y}). \end{aligned}$$

This shows that $A \in \mathscr{G}_f$ and $\mathscr{G}_f$ is a Lie group. □

Definition 2.17 *(Continuous and discrete symmetries)*
Let f be an n-variate polynomial. The symmetries obtained from the Lie algebra of f are known as the continuous symmetries of f and the other symmetries are called discrete symmetries of f.

2.3.6 Lie algebra of a polynomial

We can study some of the properties of a Lie group by attaching a vector space to it and using the tools of linear algebra. This vector space is known as *Lie algebra*. Since the group of symmetries of a polynomial is a Lie group, we can talk about the Lie algebra of the group of symmetries of a polynomial (we call it Lie algebra of polynomial). Lie algebras of some of the well known polynomial families in arithmetic complexity like determinant, permanent, IMM have been completely characterized ([Kay11], [KNST17]). The definition we present here is taken from [Kay11] and is not the abstract definition of Lie algebra. The abstract definition of Lie algebra is given in [Hal03] and Theorem 2.27 in the same book shows the equivalence of two definitions.

Definition 2.18 *(Lie algebra of a polynomial)*
Let $f \in \mathbb{F}[\boldsymbol{y}]$ be an n-variate polynomial and ϵ be a variable such that $\epsilon^2 = 0$. Then a matrix

$A \in \mathbb{F}^{n \times n}$ is in the Lie algebra of the group of symmetries of f [1]*, denoted $\mathfrak{g}_f$, if the following condition is satisfied*

$$f((I_n + \epsilon A) \cdot \boldsymbol{y}) = f(\boldsymbol{y}),$$

where I_n is $n \times n$ size identity matrix.

Now we state a result about the computation of Lie algebra of a polynomial in the following lemma. We omit the proof here and the reader can refer Lemma 26 of [Kay11].

Lemma 2.3 *There exists a randomized polynomial time algorithm that computes a basis of $\mathfrak{g}_f$ from black box access to f, where f is an n-variate polynomial.*

The proof of Lemma 2.3 includes an important component which we state explicitly in the following claim. This gives us an alternate definition of Lie algebra of a polynomial.

Claim 2.3.5 *(Claim 58 of [Kay11])*
Let $f \in \mathbb{F}[\boldsymbol{y}]$ be an n-variate polynomial. Then $A = (a_{ij})_{i,j \in [q]}$ is in $\mathfrak{g}_f$ if the following relation holds.

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

Proof: Suppose for simplicity f is a monomial. Then we can write

$$f((I_n + \epsilon A) \cdot \boldsymbol{y}) - f(\boldsymbol{y}) = \epsilon \cdot \left(\sum_{i,j \in [n]} a_{ij}\, y_j \cdot \frac{\partial f}{\partial y_i} \right)$$

Now because of linearity of partial derivatives, the same result holds for any polynomial f. Since $A \in \mathfrak{g}_f$, we get

$$f((I_n + \epsilon A) \cdot \boldsymbol{y}) - f(\boldsymbol{y}) = 0,$$

which implies

$$\epsilon \cdot \left(\sum_{i,j \in [n]} a_{ij}\, y_j \cdot \frac{\partial f}{\partial y_i} \right) = 0.$$

Since $\epsilon \neq 0$, we get

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

□

[1] For brevity, we call it Lie algebra of f

This gives a nice characterization of Lie algebra of f that also helps in computing its basis in Lemma 2.3. Since Claim 2.3.5 captures the essence of $\mathfrak{g}_f$, we take this as the *working definition* of Lie algebra of a polynomial throughout this thesis.

Definition 2.19 *(Working definition of Lie algebra of a polynomial)*
The set of matrices $A = (a_{ij})_{i,j\in[q]} \in \mathbb{F}^{n\times n}$ is called the Lie algebra of an n-variate polynomial $f \in \mathbb{F}[\boldsymbol{y}]$ if

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

Now we show the relation between the Lie algebras of equivalent polynomials. We say an n-variate polynomial $h \in \mathbb{F}[\boldsymbol{y}]$ is *equivalent* to $f \in \mathbb{F}[\boldsymbol{y}]$ if there exists $A \in \mathrm{GL}_n(\mathbb{F})$ such that $h(\boldsymbol{y}) = f(A \cdot \boldsymbol{y})$.

Claim 2.3.6 *(Proposition 58 of [Kay11])*
If $h(\boldsymbol{y}) = f(A \cdot \boldsymbol{y})$ then

$$\mathfrak{g}_h = A^{-1} \cdot \mathfrak{g}_f \cdot A.$$

Proof: Let $B \in \mathfrak{g}_f$. Then

$$f(\boldsymbol{y}) = f((I_n + \epsilon B) \cdot \boldsymbol{y}).$$

Since $f(\boldsymbol{y}) = h(A^{-1} \cdot \boldsymbol{y})$, we get

$$h(A^{-1} \cdot \boldsymbol{y}) = h(A^{-1} \cdot (I_n + \epsilon B) \cdot \boldsymbol{y}),$$

which implies

$$\begin{aligned} h(\boldsymbol{y}) &= h(A^{-1} \cdot (I_n + \epsilon B) \cdot A \cdot \boldsymbol{y}) \\ &= h((I_n + \epsilon(A^{-1} \cdot B \cdot A)) \cdot \boldsymbol{y}). \end{aligned}$$

This means $A^{-1} \cdot B \cdot A \in \mathfrak{g}_h$, which means $A^{-1} \cdot \mathfrak{g}_f \cdot A \subseteq \mathfrak{g}_h$. Now Suppose $C \in \mathfrak{g}_h$. Then

$$h(\boldsymbol{y}) = h((I_n + \epsilon C) \cdot \boldsymbol{y}).$$

We know that $f(A \cdot \boldsymbol{y}) = h(\boldsymbol{y})$, which implies

$$f(A \cdot \boldsymbol{y}) = f(A \cdot (I_n + \epsilon C) \cdot \boldsymbol{y}).$$

This gives us the following relation

$$\begin{aligned} f(\boldsymbol{y}) &= f(A \cdot (I_n + \epsilon C) \cdot A^{-1} \cdot \boldsymbol{y}) \\ &= f((I_n + \epsilon(A \cdot C \cdot A^{-1})) \cdot \boldsymbol{y}). \end{aligned}$$

This implies $A \cdot C \cdot A^{-1} \in \mathfrak{g}_f$, meaning $\mathfrak{g}_h \subseteq A^{-1} \cdot \mathfrak{g}_f \cdot A$. □

The relationship between $\mathfrak{g}_f$ and $\mathfrak{g}_h$ is called *conjugacy relation*. In other words, Lie algebra of g is called *conjugate* of Lie algebra of f via A. Now we define Lie algebra of a matrix Lie group. Here our underlying field $\mathbb{F}$ is $\mathbb{C}$.

Definition 2.20 *(Lie algebra of a matrix Lie group)*
Let $\mathscr{G}$ be a matrix Lie group. The set of matrices $A \in \mathbb{F}^{n\times n}$ such that e^{tA} is in $\mathscr{G}$ for all real number t is called the Lie algebra of $\mathscr{G}$.

The above definition shows how can we get a Lie algebra from a Lie group. The following definition immediately shows how to get element of Lie group from Lie algebra through exponential map.

Definition 2.21 *(Exponential map)*
Let $G \subseteq GL_n(\mathbb{F})$ be a Lie group and $\mathfrak{g}$ be the Lie algebra associated with it. We define the exponential map exp_t for any real number t as follows

$$exp_t : \mathfrak{g} \to G,$$

where $A \in \mathfrak{g}$ is mapped to e^{tA} in G.

All the concepts mentioned in this chapter would be directly or indirectly used in the following chapters.

Chapter 3

Lie algebra of Nisan-Wigderson polynomial

In this chapter we present the proof of Theorem 1.1. Along with this we also give an $\mathbb{F}$-basis of the Lie algebra of Nisan-Wigderson polynomial. Using this information, we give the continuous symmetries of $NW(\boldsymbol{x})$ and show how it helps in tracking the discrete symmetries in Chapter 4. We also hope that it will be helpful in designing an equivalence test for $NW(\boldsymbol{x})$.

3.1 Proof of Theorem 1.1

In this section, we give the structure of proof of Theorem 1.1, pushing several details to the subsequent sections. We present the proof idea in the form of a flowchart in Figure 3.1. The different blocks are formally stated here and proved in the subsequent sections. Let $A \in \mathfrak{g}_{NW}$, then A is $q^2 \times q^2$ matrix, where q is the parameter used in the definition of Nisan-Wigderson polynomial. In the following lemma, we identify the structure of A.

Lemma 3.1 *Every $A \in \mathfrak{g}_{NW}$ is a diagonal matrix with entries from $\mathbb{F}$.*

The proof of this lemma uses the crucial *low intersection property* of $NW(\boldsymbol{x})$. We defer the proof to Section 3.2 and discuss the rest of proof structure of Theorem 1.1 assuming Lemma 3.1. Since A is a diagonal matrix, it can be identified with a vector in $\mathbb{F}^{q^2}$ containing the diagonal entries of A. Therefore, from now onwards we treat every element of $\mathfrak{g}_{NW}$ as a vector in $\mathbb{F}^{q^2}$ instead of a matrix. After this we construct a matrix $D \in \mathbb{F}^{q^{k+1} \times q^2}$ using the monomials of $NW(\boldsymbol{x})$ such that $\mathfrak{g}_{NW}$ (viewed as a space of vectors in $\mathbb{F}^{q^2}$) is contained as an $\mathbb{F}$-subspace in the Kernel of D, denoted $\mathrm{Ker}_{\mathbb{F}}(D)$ [1]. The rows and columns of D are indexed by monomials of

[1] $\mathrm{Ker}_{\mathbb{F}}(D) = \{v \in \mathbb{F}^{q^2} \mid D \cdot v = 0\}$.

$NW(\boldsymbol{x})$ and variable set $\boldsymbol{x}$ respectively.

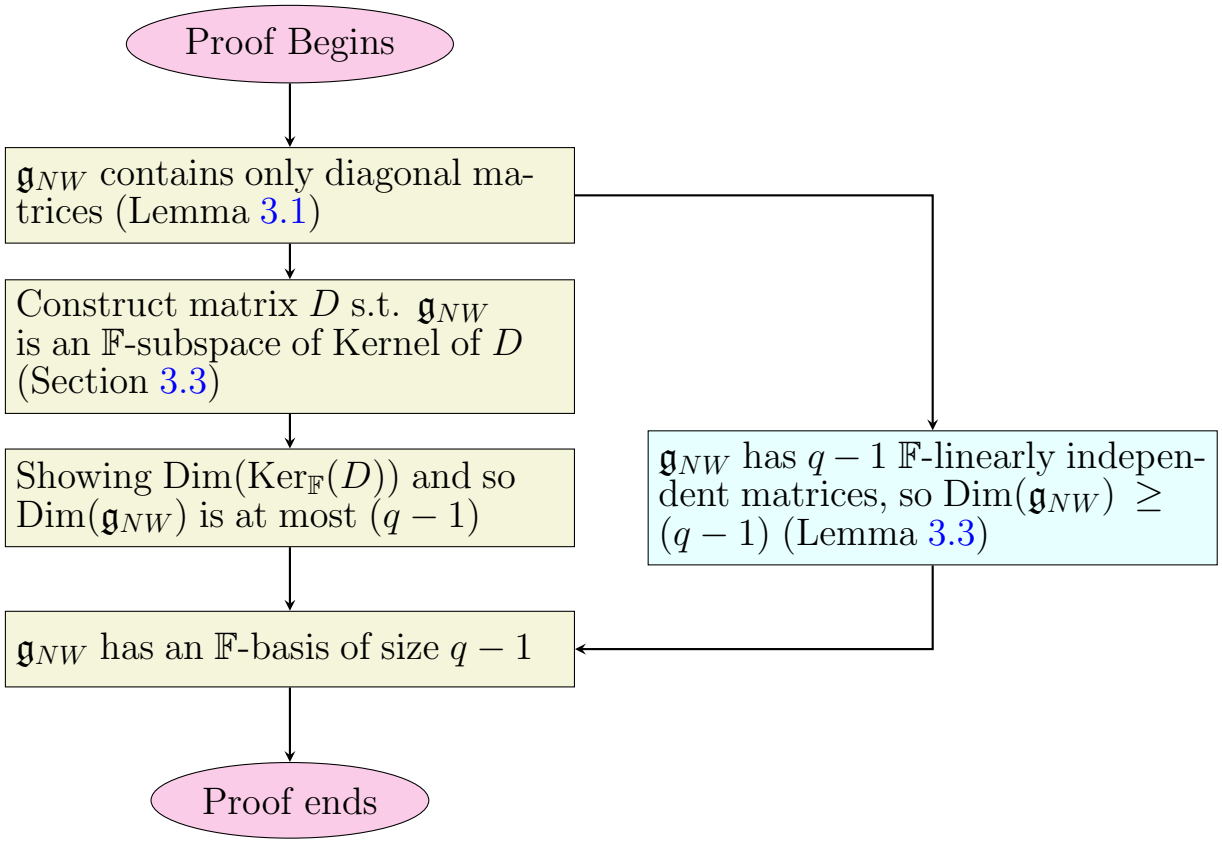

Figure 3.1: Proof idea of Theorem 1.1

Description of matrix D. From the construction, D turns out to be a $0,1$ matrix, with the (i,j)-th entry $d_{ij} = 1$ if the monomial indexing the i-th row contains the variable indexing the j-th column of D otherwise $d_{ij} = 0$. Since rows of D are identified with the monomials of $NW(\boldsymbol{x})$, every row of D contains exactly q many 1s. We present the other details about the construction of D in Section 3.3.

Thereafter we divide the rows and columns of D into blocks of size $q \times q$ and do some preprocessing on D. Then we choose special $q^2 - q$ rows of D. The matrix shown in Figure 3.2 gives a glimpse of these rows. The sub matrices indexed by the rows blocks and column blocks indexed by the sets $\boldsymbol{x_1}, \ldots, \boldsymbol{x_{q-1}}$ are permutation matrices of size $q \times q$. As shown in the figure, in these rows the column indexed by $x_{0\,q-1}$ does not have a 1, the other columns of $\boldsymbol{x_0}$ have exactly q many 1s and every other column of D has exactly $q-1$ many 1s. We give full detail of this restructuring of D in Section 3.4. Along with these $q^2 - q$ rows, we take in one row from D,

whose entry in the column indexed by $x_{0\,q-1}$ is 1, the entries in the columns indexed by $x_{r\,i_r}$ are 1 for some $i_r \in [q]$ and $r \in \{1, \ldots, q-1\}$ and the entries in the other columns are 0, thereby getting a total of $q^2 - q + 1$ rows.

We prove that these $q^2 - q + 1$ rows are $\mathbb{F}$-linearly independent in the following lemma which is proved in Section 3.5.

Lemma 3.2 *There are at least $q^2 - q + 1$ $\mathbb{F}$-linearly independent rows in D.*

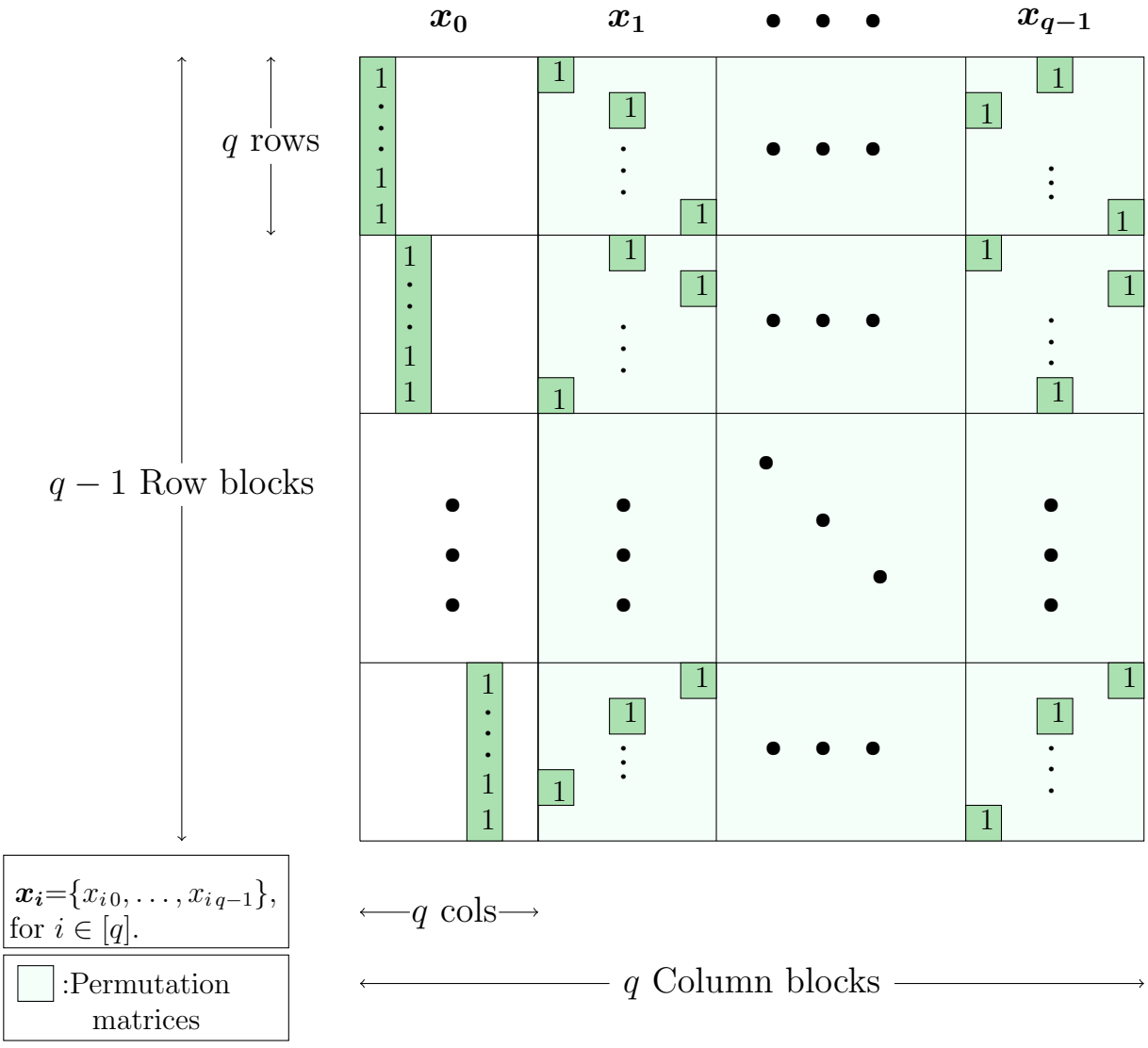

Figure 3.2: $q^2 - q$ rows of D

Lemma 3.2 is the heart of the proof of Theorem 1.1. This immediately implies that dimension of $\mathrm{Ker}_{\mathbb{F}}(D)$, denoted $\mathrm{Dim}(\mathrm{Ker}_{\mathbb{F}}(D))$, and $\mathrm{Dim}_{\mathbb{F}}(\mathfrak{g}_{NW})$ is upper bounded by $q-1$. The following lemma shows that there are at least $q-1$ $\mathbb{F}$-linear independent matrices in $\mathfrak{g}_{NW}$, proving that $\mathrm{Dim}(\mathfrak{g}_{NW}) \geq q-1$. In the lemma, R_l is a $q^2 \times q^2$ matrix in $\mathfrak{g}_{NW}$ with rows and columns indexed by q^2 variables. Thus, $(R_l)_{ij,pr}$ refers to the entry of R_l with row indexed by x_{ij} and column by x_{pr}.

Lemma 3.3 *The following $q-1$ matrices $R_1, \ldots, R_{q-1}$ are $\mathbb{F}$-linearly independent in $\mathfrak{g}_{NW}$. For $l = 1, \ldots, q-1$*

$$(R_l)_{ij,ij} = \begin{cases} 1, & \text{if } i = 0, j \in [q] \\ -1, & \text{if } i = l, j \in [q] \\ 0, & \text{otherwise} \end{cases}$$

Section 3.6 is devoted for the proof of Lemma 3.3. Together with Lemma 3.1 and 3.2, this immediately shows $\dim_{\mathbb{F}}(\mathfrak{g}_{NW}) = q-1$ and gives us an $\mathbb{F}$-basis of $\mathfrak{g}_{Nw}$.

3.2 Proof of Lemma 3.1

Our goal here is to show if $A \in \mathfrak{g}_{NW}$ then A is a diagonal matrix.

Proof: Recall $A \in \mathfrak{g}_{NW}$ is a $q^2 \times q^2$ matrix with rows and columns indexed by the q^2 variables. Let $a_{i_1 j_1, i_2 j_2}$ be the $((i_1, j_1), (i_2, j_2))$-th entry of A for $i_1, i_2, j_1, j_2 \in [q]$. Since $A \in \mathfrak{g}_{NW}$, we have the following equation from Definition 2.19.

$$\sum_{i_1, i_2, j_1, j_2 \in [q]} a_{i_1 j_1, i_2 j_2} \cdot x_{i_2 j_2} \cdot \frac{\partial NW(\boldsymbol{x})}{\partial x_{i_1 j_1}} = 0.$$

We prove that $a_{i_1 j_1, i_2 j_2} \neq 0$ if and only if $(i_1, j_1) = (i_2, j_2)$. We do this by showing that if $(i_1, j_1) \neq (i_2, j_2)$[1] then the monomials in $x_{i_2 j_2} \cdot \frac{\partial NW(\boldsymbol{x})}{\partial x_{i_1 j_1}}$ are not present in $x_{i_4 j_4} \cdot \frac{\partial NW(\boldsymbol{x})}{\partial x_{i_3 j_3}}$ for $(i_1, j_1) \neq (i_3, j_3)$ or $(i_2, j_2) \neq (i_4, j_4)$. This immediately implies $a_{i_1 j_1, i_2 j_2} = 0$, as there is no way to cancel out the monomial in the term $x_{i_2 j_2} \cdot \frac{\partial NW(\boldsymbol{x})}{\partial x_{i_1 j_1}}$.

Suppose for contradiction there exists a monomial m such that

$$m = x_{i_2, j_2} \cdot \frac{\partial m_1}{\partial x_{i_1, j_1}} = x_{i_4, j_4} \cdot \frac{\partial m_2}{\partial x_{i_3, j_3}}, \tag{3.1}$$

[1] $(i_1, j_1) \neq (i_2, j_2)$ means either $i_1 \neq i_2$ or $j_1 \neq j_2$.

where m_1, m_2 are monomials of $NW(\boldsymbol{x})$. We show using the following claim that this is only possible if $m_1 = m_2$.

Claim 3.2.1 *Let m_1, m_2 be two distinct monomials of $NW(\boldsymbol{x})$ used to define the monomials m_1' and m_2' respectively as follow*

$$m_1' = x_{i_2,j_2} \cdot \frac{\partial m_1}{\partial x_{i_1,j_1}} \quad \text{and} \quad m_2' = x_{i_4,j_4} \cdot \frac{\partial m_2}{\partial x_{i_3,j_3}},$$

where $i_1, i_2, j_1, j_2, i_3, j_3, i_4, j_4 \in [q]$. Then m_1' and m_2' can have at most $k+2$ common variables.

Proof: From the *low intersection property* of $NW(\boldsymbol{x})$, m_1 and m_2 can have at most k variables in common. This implies that the number of common variables in $\frac{\partial m_1}{\partial x_{i_1,j_1}}$ and $\frac{\partial m_2}{\partial x_{i_3,j_3}}$ is also upper bounded by k. Now the following can happen

$$x_{i_4,j_4} \in \frac{\partial m_1}{\partial x_{i_1,j_1}}^{1} \quad \text{and} \quad x_{i_2,j_2} \in \frac{\partial m_1}{\partial x_{i_3,j_3}},$$

which proves that the number of common variables in m_1' and m_2' is at most $k+2$. □

Thus in Equation (3.1), $m_1 = m_2$. Now we multiply both sides of Equation (3.1) by $x_{i_1 j_1}$ and $x_{i_3 j_3}$. This implies the following

$$x_{i_1,j_1} \cdot x_{i_4,j_4} = x_{i_3,j_3} \cdot x_{i_2,j_2}$$

But we know that $(i_1, j_1) \neq (i_2, j_2)$, hence $x_{i_1,j_1} = x_{i_3,j_3}$ and $x_{i_2,j_2} = x_{i_4,j_4}$. This contradicts our assumption $(i_1, j_1) \neq (i_3, j_3)$ or $(i_2, j_2) \neq (i_4 j_4)$. □

3.3 Construction of matrix D

As promised in Section 3.1, we show in this section how to construct matrix D using the monomials of $NW(\boldsymbol{x})$ such that $\mathfrak{g}_{NW}$ (viewed as a space of vectors in $\mathbb{F}^{q^2}$) is an $\mathbb{F}$-subspace of $\mathrm{Ker}_{\mathbb{F}}(D)$. We noted in the same section that any $A \in \mathfrak{g}_{NW}$ can be identified with a vector $\boldsymbol{v}_A \in \mathbb{F}^{q^2}$ such that for $i, j \in [q]$, the (i,j)-th entry of $\boldsymbol{v}_A$, denoted a_{ij}, is the $((i,j),(i,j))$-th diagonal entry of A and the entries of $\boldsymbol{v}_A$ are ordered as $a_{00} \prec a_{01} \prec \cdots \prec a_{q-1\,q-1}$. For a moment, pretend that $a_{ij}, i, j \in [q]$ are formal variables. Since A is diagonal (Lemma 3.1), we have

$$\sum_{i,j \in [q]} a_{ij}\, x_{ij} \cdot \frac{\partial NW(\boldsymbol{x})}{\partial x_{ij}} = 0. \tag{3.2}$$

[1] It means $x_{i_4 j_4}$ is in the monomial $\frac{\partial m_1}{\partial x_{i_1,j_1}}$

By focusing on the coefficient of a monomial, we arrive at the following observation, which will be helpful later.

Observation 3.1 *Let $h \in \mathbb{F}_q[t]_k$ and $m_h = x_{0\,h(0)} \cdots x_{q-1\,h(q-1)}$ a monomial of $NW(\boldsymbol{x})$. Then we can attach the following equation with m_h.*

$$a_{0\,h(0)} + \cdots + a_{q-1\,h(q-1)} = 0 \tag{3.3}$$

This equation is called 'equation of m_h obtained from $\mathfrak{g}_{NW}$' and denoted e_h. Since m_h occurs only in $x_{i\,h(i)} \cdot \frac{\partial NW(\boldsymbol{x})}{\partial x_{i\,h(i)}}$ for $i \in [q]$, the coefficient of m_h in Equation (3.2) is $(a_{0\,h(0)} + \cdots + a_{q-1\,h(q-1)})$ and Equation (3.3) follows from Equation(3.2). Now using these equations, matrix D is formed.

For $l \in [q^{k+1}]$, the l-th row of D is the coefficient vector of e_{h_l} in the variables $a_{ij}, i, j \in [q]$, where the variables are ordered as $a_{00} \prec a_{01} \prec \cdots \prec a_{q-1\,q-1}$. Here h_l is the l-th polynomial of the ordered set $(\mathbb{F}_q[t]_k, \preceq)$.[1] A snippet of l-th row of D is given in Figure 3.3. Every row of D is a 0,1 vector. The rows of D are indexed by monomials of $NW(\boldsymbol{x})$ following the ordering on $(\mathbb{F}_q[t]_k, \preceq)$ and columns of D are indexed by $a_{ij}, i, j \in [q]$ with the ordering $a_{00} \prec a_{01} \cdots \prec a_{q-1\,q-1}$.

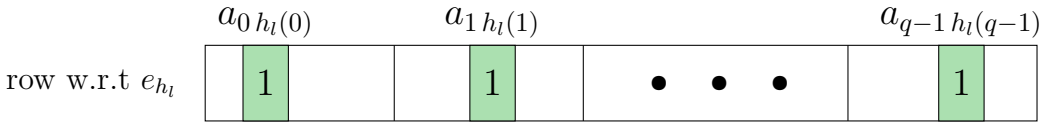

Figure 3.3: l-th row of D

It clearly follows from the construction of D that $D \cdot \boldsymbol{v}_A = 0$. Thus $\boldsymbol{v}_A \in \ker_{\mathbb{F}}(D)$ implying $\mathfrak{g}_{NW}$ is an $\mathbb{F}$-subspace of $\ker_{\mathbb{F}}(D)$. We note one more observation about D as follows.

Observation 3.2 *The columns of D can be indexed by the variable set $\boldsymbol{x}$ with the variable ordering $x_{00} \prec \cdots \prec x_{q-1\,q-1}$.*

As stated in the observation above, from now we consider the columns of D being indexed by $\boldsymbol{x}$. Now the l-th row of D like the following structure.

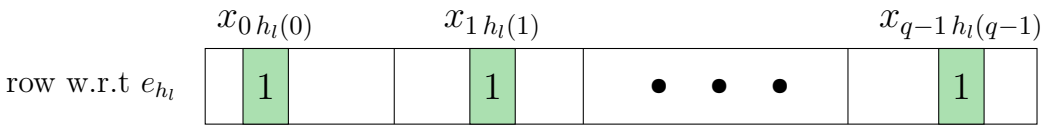

Figure 3.4: l-th row of D

[1] The ordering was defined in Section 2.1.

3.4 Restructuring matrix D

In this section we note some properties of the rows of D and choose the special $q^2 - q$ rows of D as mentioned in Section 3.1. Since a row of D is indexed by a monomial of $NW(\boldsymbol{x})$ (equivalently indexed by a univariate polynomial from $\mathbb{F}_q[t]_k$), every row of D contains exactly q 1s with exactly one column from the set $\boldsymbol{x_i}$ containing a 1 for $i \in [q]$. We now restrict D to the first q^2 rows and represent this sub matrix as $D_{|q^2}$. The rows of $D_{|q^2}$ correspond to the degree 0 and degree 1 polynomials of $\mathbb{F}_q[t]_k$ and for $a, b \in [q]$ the (a, b)-th row of $D_{|q^2}$ is indexed with monomial m_{at+b}. Now we do the following preprocessing in the matrix $D_{|q^2}$.

1. Swap the rows such that the column indexed by x_{00} contains 1 in the first q rows of $D_{|q^2}$. Similarly, the column indexed by x_{01} contains 1 in the next q rows of $D_{|q^2}$ and so on. After swapping, we name these q^2 rows as R_{00} to $R_{q-1\,q-1}$. Further, let $\boldsymbol{R_l} := \{R_{l0}, \ldots, R_{l\,q-1}\}$ for $l \in [q]$. It means in every R_l, the rows correspond to the polynomials of type $at+l, a \in \mathbb{F}_q$.

2. Perform the row exchange operation in each $\boldsymbol{R_l}$ for $l \in [q]$, such that for $j \in [q]$, the row R_{lj} corresponds to the polynomial $jt + l$, i.e. it is indexed by e_{jt+l}. It is easy to observe that for any fixed $j \in [q]$, the j-th rows of the blocks $\boldsymbol{R_l}, l \in [q]$ corresponds to the set $\{jt + l \mid l \in [q]\}$. We now note a property of this set in Claim 3.4.1.

Let subset $S \subseteq \mathbb{F}_q[t]_k$ and $f, g \in S$. Then f, g are called *evaluation disjoint polynomials over* $\mathbb{F}_q$ if for every $c \in \mathbb{F}_q$, $f(c) \neq g(c)$. For example $f = t, g = t + 1$ are evaluation disjoint over $\mathbb{F}_q$.

Claim 3.4.1 *Let $S := \{at + b \mid a, b \in \mathbb{F}_q\}$ and $g = at + b$ and $f = a't + b'$ be two distinct elements in S. Then f and g are evaluation disjoint over $\mathbb{F}_q$ if and only if $a = a'$.*

Proof: Let f, g be evaluation disjoint over $\mathbb{F}_q$. Then $(f - g)(c) \neq 0,\ c \in [q]$. If $a \neq a'$ then for $c = \frac{b-b'}{a'-a}$ we get $(f - g)(c) = 0$ and f, g are not evaluation disjoint over $\mathbb{F}_q$. Let $a = a'$. Then clearly f, g are evaluation disjoint over $\mathbb{F}_q$. □

Let $f, g \in \{jt + l \mid l \in [q]\}$ for any fixed $j \in [q]$. Since f, g are evaluation disjoint polynomials, the rows of $D_{|q^2}$ indexed by f, g can not have 1 in the same column. Now we select first $q^2 - q + 1$ rows of $D_{|q^2}$ and show in Section 3.5 that these are $\mathbb{F}$-linear independent. In fact, as $(q^2 - q + 1)$-th row is the only row in this set of rows having 1 in the column indexed by $x_{0\,q-1}$, it is enough to show that first $q^2 - q$ rows are linear independent over $\mathbb{F}$. A snapshot of these rows is already given in Figure 3.2. We record a property of these rows in the following observation.

Observation 3.3 *Restricted to the first $q^2 - q$ rows of $D_{|q^2}$, each of the columns indexed by $x_{1\,0}, \ldots, x_{q-1\,q-1}$ have exactly $q-1$ ones, with exactly one 1 among the rows in $\boldsymbol{R_l}$ for $l \in [q-1]$.*

Proof: Suppose there exist a block $\boldsymbol{R_l}$ and a variable x_{ij} with $i \neq 0$ such that $\boldsymbol{R_l}$ has two rows R_{lr} and R_{ls} having 1 in the column indexed by $x_{i\,j}$. We know that R_{lr}, R_{ls} correspond to the univariate polynomials $rt + l$ and $st + l$ respectively for $r \neq s$. Thus, $ri + l = si + l = j$. But this can not happen as $r \neq s$ and $i \neq 0$. Thus the column indexed by $x_{i\,j}$ can not have 1 in both R_{lr} and R_{ls}. □

This observation will help us in proving that these $q^2 - q$ rows are linearly independent over $\mathbb{F}$. This also explains why the blocks in Figure 3.2 (excluding the columns indexed by $\boldsymbol{x_0}$) are permutation matrices.

3.5 Proof of Lemma 3.2

As argued in the previous section, proving first $q^2 - q$ rows of $D_{|q^2}$ are $\mathbb{F}$-linearly independent implies linear independence of first $q^2 - q + 1$ rows. We multiply first $q^2 - q$ rows of $D_{|q^2}$ with the formal variables α_{lj} with $l \in [q-1]$ and $j \in [q]$ and show that if the following equation holds then all α_{lj} are 0.

$$\sum_{l \in [q-1], j \in [q]} \alpha_{lj} \cdot R_{lj} = 0. \tag{3.4}$$

In Equation (3.4) the addition is column wise and we get q^2 equations in total, one for every column of $D_{|q^2}$. In this set of equations, there are q equations containing the variable α_{lj}. The following observation is immediate from Claim 3.4.1.

Observation 3.4 *No two variables of the set $\{\alpha_{0\,j}, \ldots, \alpha_{q-1\,j}\}$ can be together in any equation obtained from Equation (3.4), for a fixed $j \in [q]$.*

Now we select a variable α_{lj} (arbitrarily) and show that $\alpha_{lj} = 0$ by manipulating the q equations obtained from Equation (3.4) containing α_{lj}. This will imply that all these rows are $\mathbb{F}$-linearly independent. In the following observation we note when can the variables α_{lj} and $\alpha_{l'j'}$ be in the same equation obtained from Equation (3.4).

Observation 3.5 *An equation obtained from Equation (3.4) contains the variables α_{lj} and $\alpha_{l'j'}$ if the polynomials $jt + l$ and $j't + l'$ are equal on some value of $t \in [q]$.*

We can identify the q equations obtained from Equation (3.4) containing the variable α_{lj} with q values of t as follows.

For $t = 0$, we get

$$\alpha_{l\,0} + \cdots + \alpha_{l\,j} + \cdots + \alpha_{l\,q-1} = 0. \tag{3.5}$$

For the remaining $q-1$ values of t, we have the following relation between j and j'

$$j' = j + \frac{l - l'}{t},$$

and the equations containing α_{lj} obtained for each of $t \in \{1, \ldots, q-1\}$ look like

$$\sum_{l' \in [q-1], l \neq l'} \alpha_{l'j'} + \alpha_{lj} = 0, \tag{3.6}$$

where $j' = j + \frac{l-l'}{t}$. Observe that j' can not be j as $l \neq l'$ and $t \neq 0$. We note again that Equation (3.6) is actually a system of $q-1$ equations for $t \in \{1, \ldots, q-1\}$. It follows from Observation 3.3 that every equation of the type Equation (3.6) has $q-1$ variables. Also, observe that other than α_{lj}, there are $(q-1)\cdot(q-2)$ different variables in these $q-1$ equations.

Observation 3.6 *There are $q^2 - 2q + 2$ distinct variables (including α_{lj}) in the q equations stated in Equation (3.6) and (3.5) containing α_{lj}. In other words, all the $q^2 - q$ variables other than $\alpha_{l'j}$ for $l \in [q-1], l' \neq l$ are present in these q equations. Moreover, the $(q-1)(q-2)$ variables in the system defined by Equation (3.6) are exactly the variables $\alpha_{l'j'}$ for $j' \neq j$ and $l' \in [q-1] \setminus \{l\}$.*

A legitimate substitution in Equation (3.5). Now we select all the variable $\alpha_{l\,r}, r \neq j$ from Equation (3.5) and replace it with some linear expressions such that after substitution Equation (3.5) becomes

$$\alpha_{lj} + \sum_{l' \in [q], l' \neq l} (-\alpha_{l',j'}) = 0, \tag{3.7}$$

where $j' = j + \frac{l-l'}{t}$ as t runs over $\{1, \ldots, q-1\}$. Observe that the above equation contains all the variables in Equation (3.6) for $t = 1, \ldots, q-1$ with negative sign. Thereafter if we add the above equation with Equations (3.6) for all $t = 1, \ldots, q-1$ then get $q \cdot \alpha_{lj} = 0$, which implies $\alpha_{lj} = 0$, if characteristic of $\mathbb{F}$ is equal to zero or greater than q.

Now we show that such a legitimate substitution is indeed possible. Let $r \in [q], r \neq j$. Choose the q equations containing the variable α_{lr}. As mentioned in Observation 3.5, we can identify these equations with $t = 0, \ldots, q-1$. For $t = 0$, we get Equation (3.5). Now out of remaining

$q-1$ equations we choose 'the' equation that does not contain $\alpha_{l'j}, l' \in [q-1], l \neq l'$. This is so because from Observation 3.6, we know that for $l' \neq l$, the equations containing α_{lj} contain all the α variables except $\alpha_{l'j}$ for $l' \neq l$. The following claim shows that there exists such an equation and it is 'unique'.

Claim 3.5.1 *Let $r \in [q]$ and $r \neq j$. Then in the following $q-1$ equations containing α_{lr}, there exists exactly one equation that does not contain any of the variable $\alpha_{l'j}$ for $l' \in [q-1], l' \neq l$. This one unique equation corresponds to $t = \frac{(q-1)-l}{r-j}$.*

$$\sum_{l' \in [q-1], l' \neq l} \alpha_{l'r'} + \alpha_{lr} = 0, \text{ for } t \in \{1, \ldots, q-1\},$$

where $r' = r + \frac{l-l'}{t}$.

Proof: We want an equation that is free from $a_{l'j}$ for $l' \neq l$. It is clear from Claim 3.4.1 that the polynomials $rt + l$ and $jt + l'$ are not evaluation disjoint for $j \neq r$. Suppose in the above set of equations, the equation corresponding to $t = \tau$ contains $\alpha_{l'j}$. Then $l' = l - \tau \cdot (j - r)$. As $l' \neq l$ can take $(q-2)$ values and t can take $(q-1)$ values, there is one t (say, t_r) for which the equation above will be free from any $\alpha_{l'j}$. Observe that as t takes different values in the set $\{1, \ldots, q-1\}$ so does $l' \in \{0, \ldots, q-1\} \setminus \{l\}$. Since l' is disallowed to take value $q-1$, t_r must be

$$t_r = \frac{(q-1) - l}{r - j}.$$

□

We choose the equation corresponding to $t = \frac{(q-1)-l}{r-j} = t_r$ (say, as in the above claim) for the following legitimate substitution

$$\alpha_{lr} = \sum_{l' \in [q-1], l \neq l'} -\alpha_{l'r'},$$

where $r' = r + \frac{l-l'}{t_r}$. In this manner, we substitute all the variables except α_{lj} in Equation (3.5) to obtain,

$$\alpha_{lj} + \sum_{r \in [q], r \neq j} (-\alpha_{l'r'}) = 0, \tag{3.8}$$

where $r' = r + \frac{l-l'}{t_r}$. By construction every $r' \neq j$ and every $l' \in [q-1] \setminus \{l\}$ in the above equation.

Now the following claim implies that if a variable $\alpha_{l'j'}$ is in some equation containing α_{lj} in

the system defined by Equation (3.8) then $\alpha_{l'j'}$ appears exactly once in Equation (3.5) with a negative sign.

Claim 3.5.2 *Let r, p be two distinct elements in the set $[q]$, such that $p \neq j, r \neq j$ and following are the substitutions for α_{lr} and α_{lp} in Equation (3.5) respectively:*

$$\alpha_{lr} = \sum_{l_1 \in [q-1], l \neq l_1} -\alpha_{l_1\, r'},$$

$$\alpha_{lp} = \sum_{l_2 \in [q-1], l \neq l_2} -\alpha_{l_2\, p'},$$

where $r' = r + \frac{l-l_1}{t_r}, p' = p + \frac{l-l_2}{t_p}$. Then there is no common variable in the above two equations.

Proof: We know

$$t_r = \frac{(q-1)-l}{r-j},$$
$$t_p = \frac{(q-1)-l}{p-j}$$

Suppose for the contradiction a variable $a_{l'j'}$ is present in both the equations. Then $l' = l_1 = l_2$ and

$$j' = r + \frac{l-l_1}{t_r} = p + \frac{l-l_1}{t_p}, \text{ as } l_1 = l_2$$

This implies

$$(r-p) = \frac{l-l_1}{q-1-l} \cdot (p-r)$$
$$(l-l_1) = l-q+1, \text{ as } r \neq p$$
$$l_1 = q-1.$$

But this is a contradiction because l_1 can only take values in $[q-1]$. □

For any $l \in [q-1], j \in [q]$ the variable $\alpha_{lj} = 0$. Thus the first $q^2 - q$ rows of matrix D are $\mathbb{F}$-linearly independent. This implies that $\text{Rank}(D) \geq q^2 - q + 1$ and dimensions of $\text{Ker}_{\mathbb{F}}(D)$ and of $\mathfrak{g}_{NW}$ is at most $q-1$.

3.6 Proof of Lemma 3.3

In the last section we show that the following $q-1$ matrices are elements of $\mathfrak{g}_{NW}$ and they are $\mathbb{F}$-linearly independent. For $l = 1, \ldots, q-1$

$$(R_l)_{ij,ij} = \begin{cases} 1, \text{ if } i = 0, j \in [q] \\ -1, \text{ if } i = l, j \in [q] \\ 0, \text{ otherwise} \end{cases}$$

Proof: Let $(R_l)_{ij,ij} = r^l_{ij}$ for fixed $i, j \in [q]$. We want to show that the following equation is satisfied

$$\sum_{i,j \in [q]} r^l_{ij}\, x_{ij} \cdot \frac{\partial NW(\boldsymbol{x})}{\partial x_{ij}} = 0, \tag{3.9}$$

implying $R_l \in \mathfrak{g}_{NW}$. Let $m = x_{0\,i_0} \cdots x_{q-1\,i_{q-1}}$ be a monomial of $NW(\boldsymbol{x})$. The coefficient of m in Equation (3.9) is $(r^l_{0\,i_0} + \cdots + r^l_{l\,i_l} + \cdots + r^l_{q-1\,i_{q-1}})$, which is equal to 0 because $r^l_{0\,i_0} = 1, r^l_{l\,i_l} = -1$ and other entries are zero. This show $R_l \in \mathfrak{g}_{NW}$ for $l \in \{1, \ldots, q-1\}$. Now it is also easy to show that these matrices are $\mathbb{F}$-linearly independent. □

This shows $\mathrm{Dim}(\mathfrak{g}_{NW}) \geq q-1$ and in Section 3.5 we noted $\mathrm{Dimension}(\mathfrak{g}_{NW}) \leq q-1$. Thus the dimension of Lie algebra of $NW(\boldsymbol{x})$ is $q-1$ and $R_l, l \in \{1, \ldots, q-1\}$ is an $\mathbb{F}$-basis of $\mathfrak{g}_{NW}$.

Chapter 4

Structure of group of symmetries of Nisan-Wigderson polynomial

In this chapter we first give an elaborate statement of Theorem 1.2 and then prove it.

Theorem 4.1 *(Restatement of Theorem 1.2)*
Let $A \in \mathscr{G}_{NW}$. There exist a diagonal matrix $S \in \mathbb{F}^{q^2 \times q^2}$ and a permutation matrix $P \in \mathbb{F}^{q^2 \times q^2}$ such that P is a block permuted matrix and

$$A = P \cdot S.$$

Observe that if $A = P \cdot S$ then $A = S' \cdot P$, where S' is another diagonal matrix. We begin the proof of the theorem by first showing (in Lemma 4.1) that every $A \in \mathscr{G}_{NW}$ is a block diagonal matrix.

Before presenting the proof, we state a terminology here. Let $T \in \mathbb{F}^{q^2 \times q^2}$. By the term 'viewing T as a block matrix of size $q \times q$' we mean T is a block matrix with block size $q \times q$ (see Definition 2.6) and the (i, j)-th block of T, denoted T_{ij}, is identified by the i-th block of rows and j-th block of columns as shown in Figure 4.1.

Lemma 4.1 *Let $A \in \mathscr{G}_{NW}$. Then A is a block permuted matrix.*

The proof of lemma uses the property of *conjugacy of Lie algebras of equivalent polynomials*. Then using the concepts of *Hessian matrix* and *evaluation dimension of polynomials*, we prove Theorem 1.2 in the next sections.

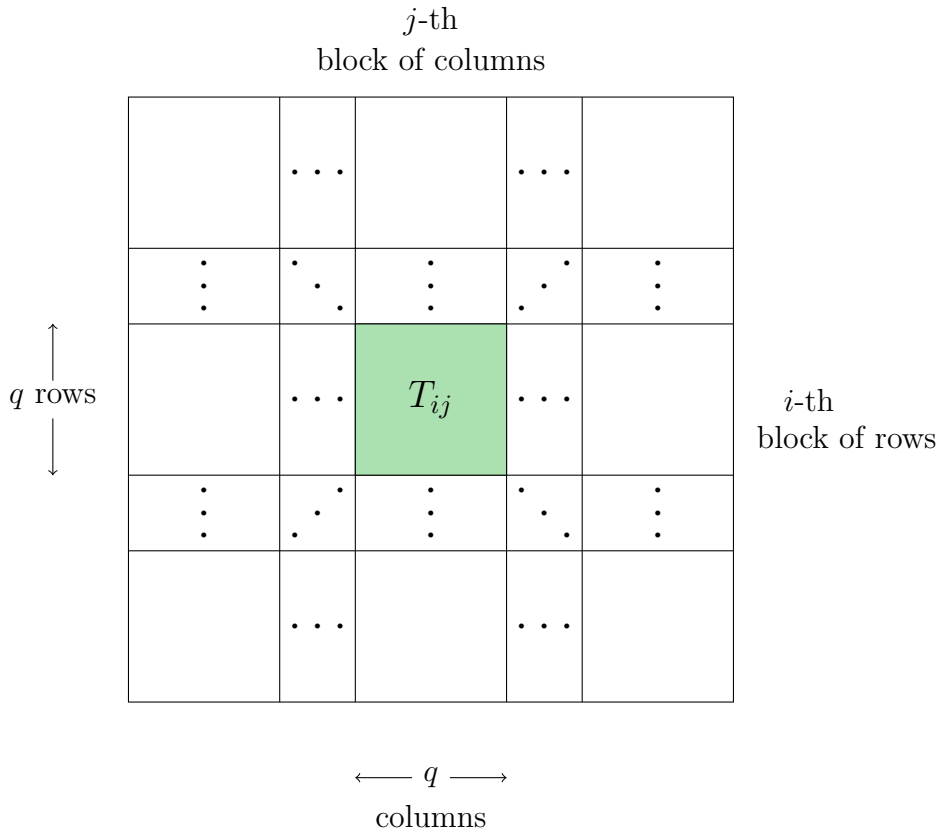

Figure 4.1: Block matrix

4.1 Proof of Lemma 4.1

Proof: As $A \in \mathscr{G}_{NW}$, from Claim 2.3.6, we have

$$\mathfrak{g}_{NW} = \{A^{-1} \cdot B \cdot A \mid B \in \mathfrak{g}_{NW}\}. \tag{4.1}$$

We know that the following matrices form an $\mathbb{F}$-basis of $\mathfrak{g}_{NW}$ (Theorem 1.1 and Lemma 3.3). For $l = 1, \ldots, q-1$

$$(R_l)_{ij,ij} = \begin{cases} 1, & \text{if } i = 0, j \in [q] \\ -1, & \text{if } i = l, j \in [q] \\ 0, & \text{otherwise} \end{cases}$$

It is easy to observe that every $R \in \mathfrak{g}_{NW}$ looks like

$$R = \text{diag}(r_0, \ldots, r_0, \ldots, r_{q-1}, \ldots, r_{q-1}),$$

where $r_1, \ldots, r_{q-1}$ are arbitrary elements of $\mathbb{F}$ and $r_0 = -(r_1 + \cdots + r_{q-1})$. Each r_i for $i \in [q]$ appears exactly q times. From Equation (4.1) we know that there exists a matrix $C \in \mathfrak{g}_{NW}$, such that

$$C = A^{-1} \cdot B \cdot A$$

or

$$A \cdot C = B \cdot A, \text{ for every } B \in \mathfrak{g}_{NW}. \tag{4.2}$$

We view the matrices A, B, C as block matrices with block size $q \times q$. Let there exist $c_j, b_j \in \mathbb{F}$ for $j = 1, \ldots, q-1$, such that matrices $C = \text{diag}(c_0, \ldots, c_0, \ldots, c_{q-1}, \cdots, c_{q-1})$ and $B = \text{diag}(b_0, \ldots, b_0, \ldots, b_{q-1}, \ldots, b_{q-1})$, where $c_0 = -(c_1 + \cdots + c_{q-1})$ and $b_0 = -(b_1 + \cdots + b_{q-1})$. One can observe that Equation (4.2) can be written as

$$(c_j \cdot A_{ij})_{i,j \in [q]} = (b_i \cdot A_{ij})_{i,j \in [q]}, \tag{4.3}$$

where A_{ij} is the (i,j)-th block of A, indexed by i-th block of rows and j-th block of columns of A. We assume for the contradiction that matrix A is not block permuted i.e. there are two non zero blocks $A_{i_1 j}$ and $A_{i_2 j}$ for $i_1 \neq i_2$ in A (as A is invertible). Then from Equation (4.3) we have

$$c_j \cdot A_{i_1 j} = b_{i_1} \cdot A_{i_1 j}$$

and

$$c_j \cdot A_{i_2 j} = b_{i_2} \cdot A_{i_2 j} \ ,$$

which implies

$$c_j = b_{i_1} = b_{i_2}.$$

This should hold true for every $B \in \mathfrak{g}_{NW}$. Now, if we select matrix B as mentioned in the following Claim then that leads to a contradiction and so A is a block permuted matrix.

Claim 4.1.1 *There exists $B \in \mathfrak{g}_{NW}$ such that*

$$B = \mathit{diag}(b_0, \ldots, b_0, \ldots, b_{q-1}, \ldots, b_{q-1}),$$

where $b_0, b_1, \ldots, b_{q-1}$ are distinct elements of the field $\mathbb{F}$ and $b_0 = -(b_1 + \cdots, b_{q-1})$, if size of $\mathbb{F}$ is larger than $\binom{q}{2}$.

Proof: Think of $b_1, \ldots, b_{q-1}$ as formal variables. Consider

$$B = -b_1 \cdot R_1 + \cdots + (-b_{q-1}) \cdot R_{q-1},$$

where $R_1, \ldots, R_{q-1}$ form an $\mathbb{F}$-basis of $\mathfrak{g}_{NW}$ as mentioned in Section 3.6. Observe that matrix $B = \text{diag}(b_0, \ldots, b_0, \ldots, b_{q-1}, \ldots, b_{q-1})$, where $b_0 = -(b_1 + \cdots, b_{q-1})$. As $b_0, \ldots, b_{q-1}$ are distinct linear forms in the variables $b_1, \ldots, b_{q-1}$, a random substitution of field elements in place of $b_1, \ldots, b_{q-1}$ (basically an application of Schwartz-Zippel lemma) ensures that B is the kind of matrix we want. □

If A is not a block permuted matrix then we get $b_{i_1} = b_{i_2}$ for $i_1 \neq i_2$, which is a contradiction, for the above B. Hence every element of $\mathscr{G}_{NW}$ is a block permuted matrix. □

4.2 Proof of Theorem 1.2

Let $A = (a_{iu,jv})_{i,u,j,v \in [q]} \in \mathscr{G}_{NW}$, where the entry in row indexed by x_{iu} and column indexed by x_{jv} is $a_{iu,jv}$. Now we show that A can be written as

$$A = P \cdot S,$$

where $S \in \mathbb{F}^{q^2 \times q^2}$ is a diagonal matrix and $P \in \mathbb{F}^{q^2 \times q^2}$ is a permutation matrix that is also block permuted. As $A \in \mathscr{G}_{NW}$,

$$NW(\boldsymbol{x}) = NW(A \cdot \boldsymbol{x}).$$

From Lemma 4.1 we know that A is a block permuted matrix. First we show the result when A is a block diagonal matrix and then in the next section we point out the necessary alterations in the argument to handle arbitrary block permuted matrix. All the essential ingredients of the proof can be found in the case when A is block diagonal.

Assume that A is a block diagonal matrix

From Lemma 2.1, we know

$$H_{NW}(\boldsymbol{x}) = A^T \cdot H_{NW}(A \cdot \boldsymbol{x}) \cdot A. \tag{4.4}$$

We view the matrices $H_{NW}(\boldsymbol{x})$ and $H_{NW}(A \cdot \boldsymbol{x})$ as block matrices with the block size $q \times q$. For $i, j \in [q]$, the i-th block of rows and j-th block of columns of these matrices are indexed by the sets $\boldsymbol{x_i}$ and $\boldsymbol{x_j}$ respectively. Let the (i, j)-th blocks of $H_{NW}(\boldsymbol{x})$ and $H_{NW}(A \cdot \boldsymbol{x})$ be denoted as C_{ij} and B_{ij} respectively, which are

$$C_{ij} = \left(\frac{\partial^2 NW(\boldsymbol{x})}{\partial x_{il} \partial x_{jp}} \right)_{l,p \in [q]} \tag{4.5}$$

and

$$B_{ij} = \left(\frac{\partial^2 NW}{\partial x_{il} \partial x_{jp}} \right)_{l,p \in [q]} (A \cdot \boldsymbol{x}). \tag{4.6}$$

Each entry of C_{ij} is the Nisan-Wigderson polynomial derived by a couple of variables, so we can view an entry as a sum of monomials. On the other hand, every entry of B_{ij} is the Nisan-Wigderson polynomial derived by a couple of variables and then the variables are replaced by linear forms from the column vector $A \cdot \boldsymbol{x}$. So we can view an entry of B_{ij} as a sum of products of linear forms.[1] Observe that the diagonal blocks of $H_{NW}(\boldsymbol{x})$ and $H_{NW}(A \cdot \boldsymbol{x})$ are equal to zero because Nisan-Wigderson polynomial is a set-multilinear polynomial. The following relation is immediate from Equation 4.4.

$$C_{ij} = A_i^T \cdot B_{ij} \cdot A_j, \text{ for every } i \neq j$$

or

$$(A_i^T)^{-1} \cdot C_{ij} \cdot A_j^{-1} = B_{ij}. \tag{4.7}$$

We record some observations about an entry of C_{ij}.

Observation 4.1 *Let $l, p, l', p' \in [q]$. If $(l, p) \neq (l', p')$ then the polynomials in the (l, p)-th and (l', p')-th entries of C_{ij} $(i \neq j)$ do not have any common monomial.*

Proof: The (l, p)-th and (l', p')-th entries of C_{ij} are $\frac{\partial^2 NW(\mathbf{x})}{\partial x_{il} \partial x_{jp}}$ and $\frac{\partial^2 NW(\mathbf{x})}{\partial x_{il'} \partial x_{jp'}}$ respectively, which can be written as

$$\frac{\partial^2 NW(\boldsymbol{x})}{\partial x_{il} \partial x_{jp}} = \sum_{\substack{h \in \mathbb{F}_q[t]_k, \\ h(i)=l, \\ h(j)=p}} \prod_{r \in [q] \setminus \{i,j\}} x_{r\, h(r)},$$

$$\frac{\partial^2 NW(\boldsymbol{x})}{\partial x_{il'} \partial x_{jp'}} = \sum_{\substack{h \in \mathbb{F}_q[t]_k, \\ h(i)=l', \\ h(j)=p'}} \prod_{r \in [q] \setminus \{i,j\}} x_{r\, h(r)}.$$

Suppose there exists a common monomial m in both $\frac{\partial^2 NW(\mathbf{x})}{\partial x_{il} \partial x_{jp}}$ and $\frac{\partial^2 NW(\mathbf{x})}{\partial x_{il'} \partial x_{jp'}}$. This means there exist polynomials $h_1, h_2 \in \mathbb{F}_q[t]_k$ such that $h_1(i) = l, h_1(j) = p$, $h_2(i) = l', h_2(j) = p'$ and

$$m = \prod_{r \in [q] \setminus \{i,j\}} x_{r\, h_1(r)} = \prod_{r \in [q] \setminus \{i,j\}} x_{r\, h_2(r)}.$$

Since h_1 and h_2 are same on more than $k+1$ evaluations (assuming $q-2 > k+1$), $h_1(i) = h_2(i)$

[1] It is a depth 3 set-multilinear circuit, as A is a block permuted matrix.

(i.e. $l = l'$) and $h_1(j) = h_2(j)$ (i.e. $p = p'$), which is a contradiction. □

Observation 4.2 *There are q^{k-1} monomials in every entry of C_{ij} for $i \neq j$.*

Proof: For $l, p \in [q]$, we know that each monomial of the (l,p)-th entry of C_{ij} is obtained from a polynomial $h \in \mathbb{F}_q[t]_k$ such that

$$h(i) = l \text{ and } h(j) = p.$$

We claim that there are q^{k-1} such polynomials in $\mathbb{F}_q[t]_k$. We know that by interpolating $k+1$ input points we get a unique polynomial of degree at most k. Let $h \in \mathbb{F}_q[t]_k$. Now interpolating all the possible evaluations for $k+1$ distinct input points of h, we get q^{k+1} choices for h. On fixing $h(i) = l$ and $h(j) = p$ in these evaluations we have q^{k-1} such polynomials. □

We know that each entry of B_{ij} is a sum of product of linear forms. Using an argument similar to that of Observation 4.2, one can observe that there are q^{k-1} products of linear forms in every entry of B_{ij}. We do not care about the actual number of monomials in an entry of B_{ij}.

Suppose A is not a product of a permutation and a diagonal matrix. Then there exists a column in A having at least two non zero entries (as A is invertible). It is easy to see that A^{-1} also has a column with more than one non zero entry. If A is a block diagonal matrix with A_i as the i-th block then A^{-1} is a block diagonal matrix with A_i^{-1} as the i-th block on the diagonal. There is some $j \in [q]$ for which the p-th column of matrix A_j^{-1} has more than one non zero entries. Fix such a j and consider Equation (4.7). For $l \in [q]$, let g_{lp} and f_{lp} be the (l,p)-th entries of the left and right sides of Equation (4.7) respectively. Then g_{lp} should be equal to f_{lp}.

Claim 4.2.1 *g_{lp} is an $\mathbb{F}$-linear combination of at least two entries of C_{ij}, for every $l \in [q]$.*

Proof: g_{lp} is the (l,p)-th of $(A_i^T)^{-1} \cdot C_{ij} \cdot A_j^{-1}$. We know the p-th column of A_j^{-1} has more than one non zero entries. Since all the entries of C_{ij} are non zero (Observation 4.2) and monomial disjoint (Observation 4.1), the (l',p)-th entry of $C_{ij} \cdot A_j^{-1}$ is an $\mathbb{F}$-linear combination of at least two entries from the l'-th row of C_{ij} for every $l' \in [q]$. Moreover, the polynomials in the (l',p)-th entries of $C_{ij} \cdot A_j^{-1}$ for $l' \in [q]$ are mutually monomial disjoint. Hence, the (l,p)-th entry of $(A_i^T)^{-1} \cdot C_{ij} \cdot A_j^{-1}$ i.e. g_{lp} is an $\mathbb{F}$-linear combination of at least two entries of C_{ij} for every $l \in [q]$. □

It immediately follows from the above claim that there are at least $2 \cdot q^{k-1}$ monomials in g_{lp} because the entries of C_{ij} are monomial disjoint. Since $g_{lp} = f_{lp}$, the evaluation dimensions of these polynomials must be the same with respect to every subset of variables.

We now show (in the next two claims) that $\text{evalDim}_{\boldsymbol{z}}(g_{lp}) > \text{evalDim}_{\boldsymbol{z}}(f_{lp})$ for every $l \in [q]$ and for a particular $\boldsymbol{z} \subseteq \boldsymbol{x}$, implying $g_{lp} \neq f_{lp}$ thereby proving Theorem 1.2 when A is block diagonal. Let $T \subseteq [q] \setminus \{i, j\}$ such that $|T| = k + 1$. Then set $\boldsymbol{z}$ is defined as

$$\boldsymbol{z} := \biguplus_{r \in T} \boldsymbol{x}_r \tag{4.8}$$

Claim 4.2.2 *$\text{evalDim}_{\boldsymbol{z}}(f_{lp}) \leq q^{k-1}$.*

Proof: Let ℓ_{iu} be the linear form corresponding to the variable x_{iu}, obtained from $A \cdot \boldsymbol{x}$ i.e. $\ell_{iu} = \sum_{j,v \in [q]} a_{iu,jv} \cdot x_{jv}$, where $(a_{iu,00} \ldots a_{iu,q-1\,q-1})$ is the (i,u)-th row of A. Since f_{lp} is the (l,p)-th entry of B_{ij},

$$f_{lp} = \sum_{\substack{h \in \mathbb{F}_q[t]_k,\\ h(i)=l,\\ h(j)=p}} \prod_{r \in [q] \setminus \{i,j\}} \ell_{r\,h(r)},$$

where $\ell_{r\,h(r)}$ is the linear form corresponding to $x_{r\,h(r)}$. Since A is a block diagonal matrix, the linear form $\ell_{r\,h(r)}$ contains the variables only from the set $\boldsymbol{x_r}$. Now if $r \in T$ then $\boldsymbol{x_r} \subseteq \boldsymbol{z}$ and $\ell_{r\,h(r)}$ is set to a constant after any evaluation of the $\boldsymbol{z}$ variables. Thus, f_{lp} (after any evaluation of the $\boldsymbol{z}$ variables) is an $\mathbb{F}$-linear combination of $\prod_{r \in [q] \setminus (\{i,j\} \uplus T)} \ell_{r,h(r)}$ for $h \in \mathbb{F}_q[t]_k$ satisfying $h(i) = l$ and $h(j) = p$ is q^{k+1} (as in Observation 4.2.2), we conclude that $\text{evalDim}_{\boldsymbol{z}}(f_{lp}) \leq q^{k-1}$. □

Claim 4.2.3 *$\text{evalDim}_{\boldsymbol{z}}(g_{lp}) \geq 2 \cdot q^{k-1}$ if $k < \frac{q}{2} - 2$.*

Proof: We know that g_{lp} is an $\mathbb{F}$-linear combination of at least two entries of C_{ij} and so contains at least $2 \cdot q^{k-1}$ monomials. It means there exists a set $P \subseteq \mathbb{F}_q[t]_k$ such that $|P| \geq 2 \cdot q^{k-1}$, $h \in P$ satisfies $h(i) = l$ and $h(j) = p$, and

$$g_{lp} = \sum_{h \in P} \prod_{r \in [q] \setminus \{i,j\}} \ell_{r,h(r)}.$$

Fix a summand, i.e. an $h \in P$, in the RHS of the above equation. For this $h \in P$ and every $r \in T$ we set the variables $x_{r,h(r)} = 1$ and the remaining variables of $\boldsymbol{z}$ to 0.This substitution reduces the above sum to a single monomial, namely $\prod_{r \in [q] \setminus (\{i,j\} \uplus T)} x_{r,h(r)}$. As $2 \cdot (k+1) < q - 2$ (by assumption), the monomial $\prod_{r \in [q] \setminus (\{i,j\} \uplus T)} x_{r,h(r)}$ is uniquely determined by $h \in P$. Hence, under various similar substitutions of the $\boldsymbol{z}$-variables, we can arrive at $|P| > 2 \cdot q^{k+1}$ distinct

monomials implying $\text{evalDim}_{\boldsymbol{z}}(g_{lp}) \geq 2 \cdot q^{k-1}$. □

Thus $\text{evalDim}_{\boldsymbol{z}}(f_{lp})$ is less than $\text{evalDim}_{\boldsymbol{z}}(g_{lp})$, which contradicts $f_{lp} = g_{lp}$. Thus f_{lp} and g_{lp} are different polynomials, which is a contradiction. This means every columns of A_j have exactly one non zero entry. This holds true for every $j \in [q]$, which implies A is a product of a block permuted permutation matrix and a diagonal matrix.

4.3 Proof of Theorem 1.2 for arbitrary block permuted matrix

We point out the adjustments in the above proof of Theorem 1.2 for an arbitrary block permuted matrix A, which may not be block diagonal. Let σ be a permutation on the set $[q]$ and A be a block permuted matrix such that other than the $(r, \sigma(r))$-th block of A, denoted $A_{r\,\sigma(r)}$, all other blocks are zero. Recall that $A_{r\,\sigma(r)}$ is the sub matrix defined by r-th block of rows and $\sigma(r)$-th block of columns of A. Let $A \in \mathscr{G}_{NW}$, then

$$H_{NW}(\boldsymbol{x}) = A^T \cdot H_{NW}(A \cdot \boldsymbol{x}) \cdot A.$$

These matrices are viewed as block matrices of size $q \times q$ and C_{ij} and B_{ij} are the (i, j)-th blocks of $H_{NW}(\boldsymbol{x})$ and $H_{NW}(A \cdot \boldsymbol{x})$, defined in Equations (4.5) and (4.6) respectively. The details are already given in Section 4.2. As stated earlier, the entries of C_{ij} and B_{ij} are the sum of monomials and sum of product of $\mathbb{F}$-linear forms respectively. Now we claim the following

Claim 4.3.1 *From Equation (4.4), we get the following*

$$C_{ij} = A^T_{r\,\sigma(r)} \cdot B_{rs} \cdot A_{s\,\sigma(s)}, \tag{4.9}$$

for some $r, s \in [q]$ such that $\sigma(r) = i$ and $\sigma(s) = j$.

Proof: Let there exists $r \in [q]$ such that $A_{r\sigma(r)}$ is the only non zero block in the block of columns indexed by $\boldsymbol{x_i}$ in A. Then $A^T_{r\,\sigma(r)}$ is the non zero block in the block of rows indexed by $\boldsymbol{x_i}$ in A^T. Then the i-th block of rows of $A^T \cdot H_{NW}(A \cdot \boldsymbol{x})$ is $(A^T_{r\,\sigma(r)} \cdot B_{r\,1}, \ldots, A^T_{r\,\sigma(r)} \cdot B_{r\,q-1})$. There is an $s \in [q]$ such that $A_{s\,\sigma(s)}$ is the only nonzero block in the block of columns indexed by $\boldsymbol{x_j}$ in A. Thus, from Equation (4.4), we get

$$C_{ij} = A^T_{r\,\sigma(r)} \cdot B_{rs} \cdot A_{s\,\sigma(s)},$$

□

From Equation(4.9), we have

$$(A^T_{r\,\sigma(r)})^{-1} \cdot C_{ij} \cdot A^{-1}_{s\,\sigma(s)} = B_{rs}. \tag{4.10}$$

We know from Observation 4.1 that any two entries of C_{ij} are monomial disjoint and every entry of C_{ij} contains exactly q^{k-1} monomials (Observation 4.2). Now we assume for contradiction that A is not a product of a permutation and a diagonal matrices i.e. A has a column with more than one non zero entry. Similarly, A^{-1} also has a column with at least two non zero entries. Let the p-th column of $A^{-1}_{s\,\sigma(s)}$ be such a column. Also for $l \in [q]$, let g_{lp} and f_{lp} be the (l,p)-th entries of the left and right sides of Equation (4.10). It is easy to verify that after replacing $(A_i^T)^{-1}$ and A_j^{-1} with $(A^T_{r\,\sigma(r)})^{-1}$ and $A^{-1}_{s\,\sigma(s)}$ in the proof of Claim 4.2.1, we get the result that g_{lp} is an $\mathbb{F}$-linear combination of at least two entries of C_{ij}. From Claim 4.2.2, we know that $\text{evalDim}_{\boldsymbol{z}}(f_{lp})$ for $\boldsymbol{z}$ mentioned in Equation (4.8) is at most q^{k-1}. Since g_{lp} is an $\mathbb{F}$-linear combination of at least two entries of C_{ij}, we know from Claim 4.2.3 that $\text{evalDim}_{\boldsymbol{z}}(g_{lp}) \geq 2 \cdot q^{k-1}$. This shows that f_{lp} and g_{lp} are different polynomials, which contradicts our assumption that A is not a product of a diagonal and a permutation matrices. This completes the proof.

Chapter 5

Continuous and discrete symmetries of Nisan-Wigderson polynomial family

In this chapter we show the richness of $\mathscr{G}_{NW}$ (especially the discrete symmetries of $\mathscr{G}_{NW}$) by giving explicitly some interesting discrete symmetries of $NW(\boldsymbol{x})$. Recall that the symmetries which are obtained from the Lie algebra of a polynomial f are called *continuous symmetries* of f and the other kinds of symmetries are called the *discrete symmetries* of f. In the first section we derive the continuous symmetries of $NW(\boldsymbol{x})$ using the Lie algebra $\mathfrak{g}_{NW}$ and show that these are diagonal matrices of a specific kind. In the second section we give non trivial discrete symmetries of $NW(\boldsymbol{x})$. We know from Chapter 4 that any symmetry of $NW(\boldsymbol{x})$ is a product of a diagonal matrix S and a permutation matrix P that is also block permuted [1], i.e. $A = S \cdot P$. It can also be easily derived that both S and P are in $\mathscr{G}_{NW}$. The block permuted permutation matrix P is in essence the source of the discrete part in a symmetry of $NW(\boldsymbol{x})$.

5.1 Continuous symmetries

In this section we assume that $\mathbb{F} = \mathbb{C}$ and then use the exponential map (Definition 2.21) to obtain the continuous symmetries. In particular, we prove the following lemma.

Lemma 5.1 *Let A be a continuous symmetry of $NW(\boldsymbol{x})$. Then A looks as follows*

$$A = diag(a_0, \ldots, a_0, \ldots, a_{q-1}, \ldots, a_{q-1}),$$

where $a_0, \ldots, a_{q-1} \in \mathbb{F}$ and each a_i for $i \in [q]$ appears exactly q times and $a_0 \cdot a_1 \cdots \cdot a_{q-1} = 1$.

We show the continuous symmetry A in Figure 5.1.

[1] We call these matrices as block permuted permutation matrices

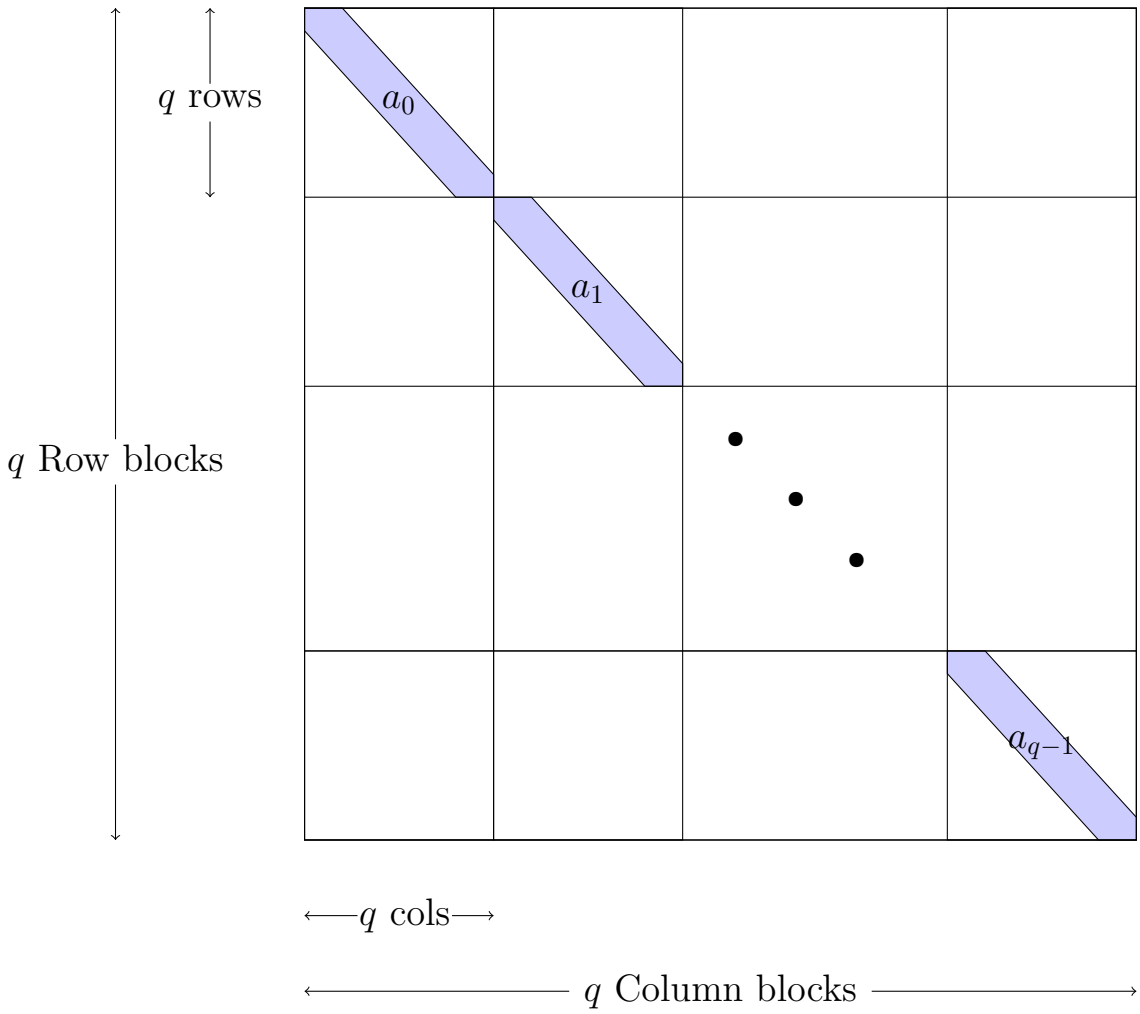

Figure 5.1: Continuous symmetry A

Proof: We know from Definition 2.21 that for any B in the Lie algebra, $e^{t\cdot B}$ is in the corresponding matrix Lie group for any real number t. As mentioned in Lemma 2.2, $\mathscr{G}_{NW}$ is a matrix Lie group and we have the following exponential map.

$$\begin{aligned} exp_t : \mathfrak{g}_{NW} &\to \mathscr{G}_{NW} \\ B &\mapsto e^{t\cdot B}. \end{aligned}$$

We know from Chapter 3 that any element $B \in \mathfrak{g}_{NW}$ looks as follows

$$B = \alpha_1 \cdot R_1 + \cdots + \alpha_{q-1} \cdot R_{q-1},$$

where $\alpha_i \in \mathbb{F}$ and R_i is an $\mathbb{F}$-basis of $\mathfrak{g}_{NW}$ for $i \in \{1, \ldots, q-1\}$ as mentioned in Section 3.6. Thus B can be written as

$$B = \text{diag}(\alpha_0, \ldots, \alpha_0, \ldots, \alpha_{q-1}, \ldots, \alpha_{q-1}),$$

where $\alpha_0 = -(\alpha_1 + \cdots + \alpha_{q-1})$. Since B is a diagonal matrix, we know from Claim 2.3.3 that

$$e^{t\cdot B} = \text{diag}(e^{t\cdot\alpha_0}, \ldots, e^{t\cdot\alpha_0}, \ldots, e^{t\cdot\alpha_{q-1}}, \ldots, e^{t\cdot\alpha_{q-1}}).$$

As $\alpha_i \in \mathbb{F}$, $e^{t\cdot\alpha_i}$ is also in $\mathbb{F}$ for $i \in [q]$. Thus the matrix A is $e^{t\cdot B}$ with $a_i = e^{t\cdot\alpha_i}$ for $i \in [q]$. □

5.2 Discrete symmetries

Recall that the block permuted permutation matrix P in Theorem 1.2 is the source of the discrete part in a symmetry of $NW(\boldsymbol{x})$. In this section, we will call such block permuted permutation matrices the discrete symmetries of $NW(\boldsymbol{x})$. Any such discrete symmetry P naturally defines a permutation μ on $\mathbb{F}_q$ (as P is block permuted) and a permutation ψ on $\mathbb{F}_q[t]_k$ (as P is a symmetry that permutes the monomials of $NW(\boldsymbol{x})$ and every monomial can be identified with an element of $\mathbb{F}_q[t]_k$). In the following claim, we make an attempt to understand the reverse direction i.e. what kinds of μ and ψ together can define a P in $\mathscr{G}_{NW}$.

Claim 5.2.1 *Let ψ be a permutation on $\mathbb{F}_q[t]_k$ and μ a permutation on $\mathbb{F}_q$. Then we can get a discrete symmetry of $NW(\boldsymbol{x})$ from ψ and μ if the following relation is satisfied for all $h_1, h_2 \in \mathbb{F}_q[t]_k$ and $l \in \mathbb{F}_q$.*

$$h_1(l) = h_2(l) \quad \textit{if and only if} \quad \psi(h_1)(\mu(l)) = \psi(h_2)(\mu(l)). \tag{5.1}$$

Proof: Let x_{lr} be a variable and S_{lr} be a set defined as $S_{lr} := \{h \in \mathbb{F}_q[t]_k \,|\, h(l) = r\}$. Then x_{lr} can be identified via any polynomial $h \in S_{lr}$ with $x_{l\,h(l)}$. Let $\sigma_{\psi,\mu}$ be a map defined on $\boldsymbol{x}$ as

$$\begin{aligned} \sigma_{\psi,\mu} : \boldsymbol{x} &\rightarrow \boldsymbol{x} \\ x_{l\,h(l)} &\mapsto x_{\mu(l)\,\psi(h)(\mu(l))}. \end{aligned}$$

Since x_{lr} can be identified with $x_{l\,h_1(l)}$ and $x_{l\,h_2(l)}$ for two polynomials h_1, h_2 in S_{lr}, we need to show that that $\sigma_{\psi,\mu}$ is well defined, i.e. $x_{l\,h_1(l)} = x_{l\,h_2(l)}$ implies $x_{\mu(l)\,h_1(\mu(l))} = x_{\mu(l)\,h_2(\mu(l))}$. This implication is clearly true form Equation (5.1). Now $\sigma_{\psi,\mu}$ would readily define a block permuted permutation matrix $P \in \mathscr{G}_{NW}$ if $\sigma_{\psi,\mu}$ is also an injective map, which from pigeonhole principle implies that $\sigma_{\psi,\mu}$ is a permutation on $\boldsymbol{x}$. Observe that Equation (5.1) implies that $\sigma_{\psi,\mu}$ is indeed an injective map. Since ψ is a permutation on $\mathbb{F}_q[t]_k$, a monomial m_h of $NW(\boldsymbol{x})$ obtained from the univariate polynomial $h \in \mathbb{F}_q[t]_k$ is mapped to the monomial $m_{\psi(h)}$ of $NW(\boldsymbol{x})$ obtained from $\psi(h) \in \mathbb{F}_q[t]_k$. This shows that on applying $\sigma_{\psi,\mu}$ to $\boldsymbol{x}$ the polynomial $NW(\boldsymbol{x})$ does not change and thus the corresponding block permuted permutation matrix $P_{\sigma_{\psi,\mu}} \in \mathscr{G}_{NW}$. □

Now we present some interesting discrete symmetries of Nisan-Wigderson polynomial family.

Lemma 5.2 *Let c, d be arbitrarily fixed non zero elements of $\mathbb{F}_q$ and g be any fixed polynomial in $\mathbb{F}_q[t]_k$ and ϕ be a Frobenius automorphism on $\mathbb{F}_q$. Let $h \in \mathbb{F}_q[t]_k$ be a polynomial defined as $h := a_k \cdot t^k + \cdots + a_0$, with $a_0, \ldots, a_k \in \mathbb{F}_q$ and ψ be the following map on $\mathbb{F}_q[t]_k$*

$$\begin{aligned} \psi : \mathbb{F}_q[t]_k &\rightarrow \mathbb{F}_q[t]_k \\ h &\mapsto \psi(h), \end{aligned}$$

where $\psi(h)$ is defined as

$$\psi(h) = d \cdot (\phi(\frac{a_k}{c^k}) \cdot t^k + \cdots + \phi(\frac{a_1}{c}) \cdot t + \phi(a_0)) + g.$$

Then ψ induces a permutation σ on $\boldsymbol{x}$ such that the corresponding permutation matrix P_σ is in $\mathscr{G}_{NW}$.

Proof: We will show that ψ is a permutation and there exists a permutation μ on $\mathbb{F}_q$ such that Equation (5.1) is satisfied for $h_1, h_2 \in \mathbb{F}_q[t]_k$ and $l \in \mathbb{F}_q$. Since $\mathbb{F}_q[t]_k$ is finite, ψ is injective or surjective would imply ψ is bijective. We show that the map is injective. Let $h = a_k \cdot t^k + \cdots + a_1 \cdot t + a_0$ and $f = b_k \cdot t^k + \cdots + b_1 \cdot t + b_0$ be two polynomials in $\mathbb{F}_q[t]_k$. We

want to show $\psi(f) = \psi(h)$ implies $f = h$. Let

$$\psi(f) = \psi(h),$$

which means

$$d \cdot (\phi(\frac{a_k}{c^k}) \cdot t^k + \cdots + \phi(\frac{a_1}{c}) \cdot t + \phi(a_0)) + g = d \cdot (\phi(\frac{b_k}{c^k}) \cdot t^k + \cdots + \phi(\frac{b_1}{c}) \cdot t + \phi(b_0)) + g,$$

which implies

$$\phi(\frac{a_k}{c^k}) \cdot t^k + \cdots + \phi(\frac{a_1}{c}) \cdot t + \phi(a_0) = \phi(\frac{b_k}{c^k}) \cdot t^k + \cdots + \phi(\frac{b_1}{c}) \cdot t + \phi(b_0).$$

Thus

$$\phi(\frac{a_r}{c^r}) = \phi(\frac{b_r}{c^r}), \quad r \in [k+1],$$

which means $a_r = b_r$ for $r \in [k+1]$ (as ϕ is a Frobenius automorphism), implying $f = h$. This shows that ψ is a permutation. Now we define $\mu(i) := \phi(c \cdot i)$ for $i \in \mathbb{F}_q$. Clearly μ is a permutation on $\mathbb{F}_q$ as ϕ is a Frobenius automorphism. Let $h_1 = \alpha_k \cdot t^k + \cdots + \alpha_1 \cdot t + \alpha_0$ and $h_2 = \beta_k \cdot t^k + \cdots + \beta_1 \cdot t + \beta_0$, where $\alpha_0, \ldots, \alpha_k, \beta_0, \ldots, \beta_k \in \mathbb{F}_q$ and $i \in \mathbb{F}_q$. We use the fact that ϕ is a field automorphism in the following derivation:

$$\begin{aligned}
& h_1(i) = h_2(i) \\
\iff & \alpha_k \cdot i^k + \cdots + \alpha_0 = \beta_k \cdot i^k + \cdots + \beta_0 \\
\iff & \phi(\alpha_k) \cdot \phi(i^k) + \cdots + \phi(\alpha_0) = \phi(\beta_k) \cdot \phi(i^k) + \cdots + \phi(\beta_0) \\
\iff & \phi(\frac{\alpha_k}{c^k}) \cdot \phi((c \cdot i)^k) + \cdots + \phi(\alpha_0) = \phi(\frac{\beta_k}{c^k}) \cdot \phi((c \cdot i)^k) + \cdots + \phi(\beta_0) \\
\iff & \phi(\frac{\alpha_k}{c^k}) \cdot (\phi(c \cdot i))^k + \cdots + \phi(\alpha_0) = \phi(\frac{\beta_k}{c^k}) \cdot (\phi(c \cdot i))^k + \cdots + \phi(\beta_0) \\
\iff & \phi(\frac{\alpha_k}{c^k}) \cdot (\mu(i))^k + \cdots + \phi(\alpha_0) = \phi(\frac{\beta_k}{c^k}) \cdot (\mu(i))^k + \cdots + \phi(\beta_0) \\
\iff & d \cdot (\phi(\frac{\alpha_k}{c^k}) \cdot (\mu(i))^k + \cdots + \phi(\alpha_0) + g = d \cdot (\phi(\frac{\beta_k}{c^k}) \cdot (\mu(i))^k + \cdots + \phi(\beta_0)) + g \\
\iff & \psi(h_1)(\mu(i)) = \psi(h_2)(\mu(i)).
\end{aligned}$$

This implies the desired result and thus we get a discrete symmetry of $NW(\boldsymbol{x})$ for every such ψ.

□

Chapter 6

Future Works

From here, we have some open questions to pursue on the Nisan-Wigderson polynomial family. At first we would like to figure out all the discrete symmetries of $NW(\boldsymbol{x})$, which will complete our investigation of the group of symmetries of the Nisan-Wigderson polynomial family. In other words, we want to know if there are discrete symmetries of $NW(\boldsymbol{x})$ other than those, which are mentioned in Chapter 5. After this we would like to understand the complexity the equivalence test for the Nisan-Wigderson polynomial family. Following the footsteps of the equivalence test of permanent ([Kay11]), we are interested to know if in this case also the Lie algebra $\mathfrak{g}_{NW}$ plays a crucial role in designing an efficient equivalence test. As mentioned in [Kay11], the last step of equivalence test is polynomial identity testing. This step can be accomplished for polynomials in VP using the randomized algorithm based on DeMillo-Lipton-Schwarz-Zippel lemma ([Zip79],[Sch80]). But we do not have a generalized procedure to do it for the polynomials outside VP. However, the last step can be carried out for the permanent by using the downwards self reducibility property of permanent given by Impagliazzo and Kabanets in [KI04]; see also [Kay11].

As mentioned in Chapter 1, the exact computational complexity of Nisan-Wigderson polynomial family is not known, we would like to know if Nisan-Wigderson polynomial family is in VP or is VNP intermediate or VNP complete. We hope that our work here on the symmetries of Nisan-Wigderson polynomial family would provide us with some insights on this problem (keeping in mind the area of geometric complexity theory).

Bibliography

[GKKS13] N. Kayal R. Saptharishi A. Gupta, P. Kamath. Arithmetic circuits: A chasm at depth three. In *Proceedings of the 54th Annual IEEE Symposium on Foundation of Computer Science (FOCS 2013)*, pages 578–587, 2013. 2

[Art91] M. Artin. *Algebra*. Prentice Hall, Unites States, 1991. 10

[AS06] M. Agrawal and N. Saxena. Equivalence of f-algebras and cubic forms. In *Proceedings of the 23rd Annual Symposium on Theoretical Aspects of Computer Science*, pages 115–126, 2006. 4

[AV08] M. Agrawal and V. Vinay. Arithmetic circuits: A chasm at depth four. In *Proceedings of the 49th Annual IEEE Symposium on Foundation of Computer Science (FOCS 2008)*, pages 67–75, 2008. 2

[B̈98] P. Bürgisser. *Completeness and reduction in algebraic complexity theory*. PhD thesis, 1998. Habilitation thesis. 2

[BS83] W. Baur and V. Strassen. The complexity of partial derivatives. *Theoretical Computer Science*, 22:317–330, 1983. 2

[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. 16

[Csa79] L. Csanky. Fast parallel matrix inversion algorithms. *SIAM Journal of Computing*, 5:618–623, 1979. 1

[CT65] J.W. Cooley and J.W. Tukey. An algorithm for the machine calculation of complex fourier series. *Mathematics of Computation*, 19(90):297–301, 1965. 1

[DS06] Z. Dvir and A. Shipilka. Locally decodable codes with 2 querries and polynomial identity testing for depth 3 circuits. *SIAM Journal of Computing*, 36(5):1404–1434, 2006. 3

[Hal03] B. Hall. *Lie Groups, Lie Algebras, and Representations: An Elementary Introduction*. Graduate Texts in Mathematics. Springer, 2003. 17, 19

[Her75] I.N. Herstein. *Topics in Algebra, second edition*. Wiley, 1975. 10

[Kal89] E. Kaltofen. Factorization of polynomials given by straight line programs. In S. Micali, editor, *Randomness in Computation*, volume 5, pages 375–412, 1989. 1

[Kay11] N. Kayal. Affine projection of polynomials. In *Symposium of Theory of Computer Science (STOC)*, 2011. iii, 3, 4, 5, 19, 20, 21, 49

[Bab16] László Babai. Graph isomorphism in quasipolynomial time [extended abstract]. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC*, pages 684–697, 2016. 1

[ASSS12] Manindra Agrawal, Chandan Saha, Ramprasad Saptharishi and Nitin Saxena. Jacobian hits circuits: hitting-sets, lower bounds for depth-D occur-k formulas & depth-3 transcendence degree-k circuits. In *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC*, pages 599–614, 2012. 3

[KI04] V. Kabanets and R. Impagliazzo. Derandomizing polynomial identity testing means proving circuit lower bounds. *Computational Complexity*, 13(1-2):1–46, 2004. 3, 5, 49

[KLSS14] Neeraj Kayal, Nutan Limaye, Chandan Saha, and Srikanth Srinivasan. An exponential lower bound for homogeneous depth four arithmetic formulas. In *55th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2014, Philadelphia, PA, USA, October 18-21, 2014*, pages 61–70, 2014. iii

[KNST17] N. Kayal, V. Nair, C. Saha, and S. Tavenas. Reconstruction of full rank algebraic branching programs. 32nd IEEE Conference on Computational Complexity (CCC), 2017. iii, 4, 5, 19

[KS07] N. Kayal and N. Saxena. Polynomial identity testing for depth 3 circuits. *Computational Complexity*, 16(2):115–138, 2007. 3

[KS08] Z.S. Karnin and A. Shipilka. Deterministic black box polynomial identity testing of depth-3 arithmetic circuits with bounded top fan-in. In *Proceedings of 24th Annual CCC*, pages 274–285, 2008. 3

[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. iii, 5, 6

[KST16] Neeraj Kayal, Chandan Saha, and Sébastien Tavenas. An almost cubic lower bound for depth three arithmetic circuits. 43rd International Colloquium on Automata, Languages, and Programming (ICALP), 2016. iii, 5

[MS01] K. Mulmuley and M. Sohoni. Geometric complexity theory 1: An approach to the p vs np and related problems. *SIAM Journal of Computing*, 31(2):496–526, 2001. 4

[NW94] Noam Nisan and Avi Wigderson. Hardness vs randomness. *J. Comput. Syst. Sci.*, 49(2):149–167, 1994. 5

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978. 1

[LLL82] A. K. Lenstra, H.W. Lenstra and L. Lovász Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982. 1

[MM62] Marvin Marcus and Francis May. The permanent function. *Canadian Journal of Math.*, 14:177-189, 1962. 5

[Fro97] Georg Frobenius. Ueber die darstellung der endlichen gruppen durch linearc substitutionen. *Sitzungber. der Berliner Akademie*, 7:994-1015, 1897. 5

[Ges16] Fulvio Gesmundo. Gemetric aspects of iterated matrix multiplication. *Journal of Algebra*, 461:4264, 2016. 5

[AGKS14] Manindra Agrawal, Rohit Gurjar, Arpita Korwar and Nitin Saxena Hitting-sets for ROABP and Sum of Set-Multilinear circuits. *CoRR*, 2014. 3

[AKS04] Manindra Agrawal, Neeraj Kayal and Nitin Saxena PRIMES is in P. *Ann. of Math*,160:781-793 , 2004. 1

[SS13] Nitin Saxena and C. Seshadhri From sylvester-gallai configurations to rank bounds: Improved blackbox identity test for depth-3 circuits. *J. ACM*, 60(5):1-33 , 2013. 3

[Sax08] N. Saxena. Diagonal circuit identity testing and lower bounds. In *ICALP (1)*, pages 60–71, 2008. 3

[Sch80] J.T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of ACM*, 27(4):701–717, 1980. 3, 49

[SKMV10] A. Shipilka, Z.S. Karnin,P. Mukhopadhyay and I. Volkovich. Determinstic identity testing of depth 4 multilinear circuits with bounded top fan-in. In *Proceedings of 42nd Annual STOC*, pages 649–658, 2010. 3

[Str69] V. Strassen. Gaussian elimination is not optional. *Numerische Mathematik*, 13:354–356, 1969. 1

[Val79a] L.G. Valiant. Completeness classes in algebra. In *11th Annual ACM Symposium on the Theory of Computing*, pages 249–261, 1979. 2

[Val79b] L.G. Valiant. The complexity of computing permanent. *Theoretical Computer Science*, 8(2):189–201, 1979. 2

[Val82] L.G. Valiant. Reductibility by algebraic projections. *L'Enseignment Mathematique*, 28:253–268, 1982.

[Wel16] Andre Thorsten Weltsch. Algorithmic testing of equivalence of polynomials to the determinant, 2016. Bachelor Thesis. 19

[Zip79] R. Zippel. Probabilistic algorithms for sparse polynomials. In *Symbolic and algebraic computation*, pages 216–226, 1979. 3, 49

[SKMV10] A. Shipilka, Z.S. Karnin,P. Mukhopadhyay and I. Volkovich. Determinstic identity testing of depth 4 multilinear circuits with bounded top fan-in. In *Proceedings of 42nd Annual STOC*, pages 649–658, 2010. 3